CYBER MEDIA

Обзор инструментов для SOC-центров

Обзор инструментов для SOC-центров

Введение

Тенденции отечественной кибербезопасности в последнее время - массовые кибератаки, импортозамещение, дефицит специалистов, законодательные нормы - диктуют российскому рынку ИБ-решений и услуг новые требования: SOC-центры, услуги MSS-провайдеров, решения классов SIEM и XDR, системы автоматизации реагирования на инциденты и управления данными о киберугрозах, решения для комплаенс-автоматизации сейчас буквально нарасхват. В связи с этим, редакция КиберМедиа решила провести сводный обзор отечественных продуктов классов SIEM, SOAR, XDR, TIP, SGRC – все эти решения активно используются SOC-центрами (ранее редакция проводила опрос инструментария SOC центров) и командами реагирования для эффективной обработки киберинцидентов, автоматизации своей деятельности, отправки отчетности по инцидентам регуляторам. Расскажем немного о каждом классе и о методике выбора решений для обзора.

Решения SIEM (Security Information and Event Management, системы управления информацией о безопасности и событиях ИБ) предназначены для сбора данных о событиях ИБ и изменениях в информационной инфраструктуре для выявления киберинцидентов на основе корреляционной логики с использованием методов обработки получаемой из разнородных источников информации (парсинг, нормализация, таксономия). Первые решения класса SIEM появились на международном рынке еще в конце 90-х, но особую популярность в России приобрели в конце 2010-х, когда у заказчиков появилось понимание целесообразности эксплуатации в целом недешевых решений, а на рынок вышли отечественные игроки, подхватив тренд на импортозамещение и необходимость выполнения заказчиками отечественных регуляторных норм в части мониторинга событий ИБ. В настоящий обзор мы включили ключевых участников отечественного SIEM-рынка: Kaspersky Unified Monitoring and Analysis Platform (KUMA) от Лаборатории Касперского и MaxPatrol SIEM от Positive Technologies. Кроме них, были включены и другие игроки: RuSIEM и R-Vision SIEM – к сожалению, R-Vision практически в последний момент отказалась от участия в обзоре по своему SIEM-решению (а найти референсные источники нам не удалось), но представила свои продукты в других категориях нашего обзора. Более того, в обзор включено западное решение IBM QRadar для сравнения возможностей этого продукта с более чем 20-летней историей с функционалом российских SIEM, появившихся в конце 2010-х.

Решения SOAR (Security Orchestration, Automation and Response, платформы для оркестровки (координации и управления) СЗИ, автоматизации действий аналитиков и реагирования на инциденты) предназначены для комплексной автоматизации управления киберинцидентами – от подготовки к реагированию и первичного анализа инцидента до локализации, устранения угрозы и восстановления после атаки. SOAR-решения используют разработанные сценарии реагирования на инциденты (плейбуки) и управление интегрированными СЗИ и инфраструктурными компонентами (сетевыми устройствами, конечными точками). Благодаря тому, что в SOAR агрегируется вся релевантная инциденту информация и все действия выполняются из единого интерфейса, значительно ускоряется проведение анализа и реагирования, а аналитик ИБ или работник SOC-центра эффективно распределяют свои ресурсы. Несколько лет назад на отечественном рынке появились решения класса IRP (Incident Response Platform, платформы реагирования на инциденты), которые у каких-то вендоров эволюционировали в SOAR, приобретя дополнительные функции, такие как централизованное управление парком СЗИ, интеграция с аналитикой киберугроз, механизмы расширенного анализа аномалий и инцидентов и т.д. В настоящее время на решения класса SOAR отмечается высокий спрос как со стороны SOC-центров, так и со стороны MSS-провайдеров, для которых скорость выявления и реагирования на инциденты критически важна, а дефицит кибераналитиков стал уже хроническим. Для обзора мы выбрали значительное количество продуктов: отечественные вендоры представлены такими решениями, как ePlat4m Orchestra, Makves IRP, Innostage (NextSTage) IRP, R-Vision SOAR, Security Vision [NG]SOAR, UserGate LogAnalyzer. Западные продукты, попавшие в обзор (опять же, для сравнения возможностей отечественных и импортных аналогов): Google Chronicle SOAR (ex-Siemplify), Microsoft Sentinel, Palo Alto Cortex XSOAR. К сожалению, по Makves IRP вендор отказался предоставлять данные, поэтому использовались только открытые источники. Кроме того, в обзор планировалось включить MaxPatrol O2 от Positive Technologies, но сам вендор сообщил, что не позиционирует это решение как SOAR, а как метапродукт, объединяющий продукты Positive Technologies под единым брендом для предотвращения кибератак.

Решения XDR (Extended Detection and Response, системы расширенного обнаружения и реагирования на кибератаки) предназначены для выявления инцидентов и активного реагирования (сдерживание, устранение угрозы). В основе XDR-решений лежат несколько продуктов от одного вендора, объединенные единой логикой и методами управления инцидентами. Как правило, выявление и реагирование происходит за счет моновендорной интеграции EDR-продукта (расширенная защита конечных точек), решений по защите email и корпоративной сети (NTA/NDR/SWG), решений по защите учетных записей и облачных инфраструктур, системы управления уязвимостями, "песочницы", данных киберразведки и SIEM-системы. XDR-решения в чем-то конкурируют с системами SOAR в части автоматизации выявления и реагирования на киберугрозы, однако SOAR-решения вендоронезависимы и предполагают интеграцию в уже сложившуюся инфраструктуру, без необходимости замещения имеющихся СЗИ. Однако, компоненты XDR-решения более глубоко интегрированы между собой (благодаря единому производителю), и подойдут тем, кто строит «с нуля» моновендорную ИБ. В обзор мы планировали включить отечественные решения F.A.C.C.T. Managed XDR (ex-Group-IB), Kaspersky Symphony XDR (Лаборатория Касперского) и PT XDR (Positive Technologies), а в качестве импортного аналога выбрали Microsoft 365 Defender, однако, ввиду массового обновления своих XDR-решений ведущими игроками, решили сделать сравнение продуктов данного класса чуть позже.

Решения TIP (Threat Intelligence Platform, платформы управления информацией о киберугрозах) применяются для сбора аналитических данных о киберугрозах, которые поступают от источников – фидов Threat Intelligence (антивирусные лаборатории, группы CERT, ИБ-компании, независимые исследователи). Аналитическими данными могут быть индикаторы компрометации (сокращенно IoC, Indicator of Compromise: вредоносные IP-адреса и URL, хэши файлов ВПО и т.д.), индикаторы атак (сокращенно IoA, Indicator of Attack: использующиеся атакующими тактики, техники и процедуры, сокращенно TTPs – Tactics, Techniques and Procedures, т.е. характерный "почерк" различных киберпреступных групп), а также иные структурированные и неструктурированные данные, касающиеся кибератак и ВПО, такие как бюллетени безопасности, описание уязвимостей и эксплойтов, содержание постов в мессенджерах, соцсетях и на Даркнет-форумах и т.д.. В TIP полученная информация классифицируется, проверяется, приоритизируется в зависимости от ее релевантности для конкретного заказчика и инфраструктуры. Вендоры TIP-решений могут использовать как собственные TI-фиды, так и сторонние (коммерческие и бесплатные) – разница в качестве получаемых данных и необходимости их дополнительного анализа. В отличие от других рассматриваемых решений, качество данных киберразведки существенно зависит от контекста, отрасли и географического расположения потенциальных жертв атаки – например, отечественные киберпреступники редко атакуют российские компании, а западные производители и TI-поставщики могут намеренно скрывать индикаторы киберкампаний, проводимых иностранными спецслужбами в отношении России. Поэтому для обзора мы выбрали исключительно российские решения: BI.ZONE ThreatVision, F.A.C.C.T. Threat Intelligence, Kaspersky CyberTrace, PT Cybersecurity Intelligence, R-Vision TIP, Security Vision TIP.

Решения SGRC (Security Governance, Risk and Compliance, системы управления кибербезопасностью, киберрисками и соответствием законодательству) применяются для автоматизации множества процессов, связанных с системой управления ИБ в компаниях: например, управление активами, уязвимостями, конфигурациями, проведение аудитов (внешних и внутренних), самооценка соответствия применимым нормам ИБ-законодательства, управление киберрисками. В контексте работы SOC-центров применение SGRC-систем может быть целесообразно в силу необходимости управления процессами самого SOC, а также ИБ-процессами защищаемой организации (если это входит в зону ответственности SOC). SGRC поможет проанализировать киберриски самого SOC и степень соответствия процессов SOC внутренним регламентам, оценить и визуализировать выполнение KPI, а также выполнить законодательные требования в части отправки отчетности по КИИ, ПДн, требованиям ЦБ РФ. Специализация SGRC-решений на выполнении норм законодательства позволяет производителям этих решений своевременно актуализировать необходимые шаблоны документов и отчетов, базу применимых нормативных актов и требований, поддерживать интеграции для автоматизированных способов обмена информацией с регуляторами. В обзор мы включили две "облачные" отечественные SGRC-системы (АльфаДок, SECURITM), три классические SGRC-платформы (ePlat4m SGRC, R-Vision SGRC, Security Vision SGRC), а также одного зарубежного вендора для сравнения подходов к реализации функционала продукта (Archer Suite (ex-RSA Archer)).

Методология оценки и сравнения функциональных возможностей продуктов включала в себя разработку перечня основных критериев, которые были сформированы авторами обзора на основе методологий компании "Гартнер" (Gartner Market Guide, Gartner Critical Capabilities), на основе анализа открытых источников с информацией о характеристиках продуктов, по результатам обратной связи от заказчиков указанных классов решений, а также руководствуясь экспертизой авторов. Вендорам рассылались опросники с перечнем основных критериев по их продуктам для заполнения, при этом формат некоторых вопросов предполагал развернутые ответы. Кроме ответов от вендоров, производился опрос выделенных вендорами экспертов по продуктам, проводилась оценка характеристик и функционала решений на live-демонстрациях решений, на основе предоставленных производителями доступов к демонстрационным стендам, на основе работы с референсными площадками (клиенты, интеграторы, эксперты-консультанты), которые предоставляли свои мнения и данные об используемых продуктах Производителям также предлагалось добавить свои расширенные критерии сравнения для включения их в обзор, с проведением второй итерации сравнения по уже расширенному перечню критериев. В перечень вопросов также был включен пункт о планах развития функционала продукта, куда вендоры могли включать пункты из своих "Дорожных карт развития продуктов", при этом в ответах на критерии не учитывался функционал, который на момент проведения опроса не был реализован, а был лишь запланирован.

Принцип выбора вендоров и решений для обзора был следующим: для каждого класса решений выбиралось не менее 3 различных продуктов от разных производителей, при этом обзор сфокусирован на отечественных решениях ввиду законодательных и санкционных ограничений на приобретение и использование зарубежных продуктов, поэтому российские производители доминируют в общем перечне продуктов, а зарубежные продукты представлены для сравнения текущих статусов и векторов развития

решений на различных рынках. Для высококонкурентных классов российских решений выбирались продукты от наиболее известных вендоров на основе анализа открытых данных о доле рынка, занимаемой различными компаниями, включая различные рейтинги и прогнозы. Для низкоконкурентных решений выбирались все известные авторам отечественные производители продуктов определенного класса. Для обзора и сравнения выбирались, по возможности, наиболее актуальные стабильные версии продуктов.

Также необходимо отметить, что в части терминологии не все вендоры придерживаются единого подхода, особенно в отношении недавно появившихся и еще не устоявшихся явлений в ИБ. Поэтому авторы обзора, по возможности, давали пояснения в отношении некоторых терминов, но зачастую под одним и тем же функционалом производители понимают несколько разную реализацию.

SIEM

Основные критерии	IBM QRadar	Kaspersky KUMA	PT MaxPatrol SIEM	RuSIEM
1. Общие технические характеристики:				
1.1. Технические требования к платформе и среде внедрения (системные требования к аппаратному и программному обеспечению, окружению);	ОС: Red Hat Enterprise Linux V7.9 64-bit Аппаратные требования (для инсталляций All-in-one, до 5000 EPS, минимум): 16 ЦПУ, 32Гб ОЗУ, 256 Гб дисковой подсистемы	Поддерживаемые ОС: Oracle Linux 8.6, 8.7, Astra Linux Special Edition РУСБ.10015-01 (2021-1126SE17 оперативное обновление 1.7.1), Astra Linux Special Edition РУСБ. 10015-01 (2022-1011SE17MD оперативное обновление 1.7.2.UU.1), Astra Linux Special Edition РУСБ.10015-01 (2022-1110SE17 оперативное обновление 1.7.3). СУБД: используется встроенная СУБД ClickHouse. Аппаратные требования (при условии обработки потока данных до 40000 EPS): Ядро KUMA: 4 ЦПУ, 16 Гб ОЗУ, от 500 Гб дискового пространства; Коллектор: 8 ЦПУ, 16 Гб ОЗУ, от 500 Гб дискового пространства; Коррелятор: 8 ЦПУ, 16 Гб ОЗУ, от 500 Гб дискового пространства; Хранилище: 24 ЦПУ, 48 Гб ОЗУ, от 500 Гб дискового пространства.	ОС: Astra Linux Special Edition 1.7, Debian 10.3 - 10.13. Для MaxPatrol 10 Collector: Microsoft Windows Server 2012, 2012 R2, 2016, 2019, 2022. Аппаратные требования: для различных компонент отличаются, минимальные требования: Для установки «всё в одном» (MaxPatrol 10 Core, PT Management and Configuration, Knowledge Base, MaxPatrol SIEM Server, MaxPatrol SIEM Events Storage и MaxPatrol 10 Collector): 24 ЦПУ 64Гб ОЗУ для актуальной версии 26.1 Для выделенного сервера с PT UCS и PT CP: 4 ЦПУ, 4 Гб ОЗУ	ОС: Ubuntu Server 18.04 LTS (x64) и 22.04 LTS (x64), Astra Linux Special Edition РУСБ.10015-01 (версия не ниже обновления 1.7) Аппаратные требования: 16 ЦПУ, 32 Гб ОЗУ, 200 Гб (система) + 500 Гб (хранение) дискового пространства
1.2. Варианты поставки и инсталляции (аппаратный апплайнс, образ, контейнер, установка на «голое железо», установка on-prem, установка в облаке, наличие графических инсталляторов, поддержка виртуализации);	Поставляется в виде аппаратных и программных апплайнсов, возможна установка на предустановленную ОС, возможна работа в режиме SaaS, поддержка установки в облаке Amazon Web Services. Поддержка систем виртуализации VMWare ESXi, KVM, Nutanix AHV, Hyper-V (на Windows Server 2016, с предварительной установкой RHEL в качестве гостевой ОС)	Поддержка сред виртуализации: VMware 6.5 и выше, Hyper-V для Windows Server 2012 R2 и выше, QEMU-KVM 4.2 и выше, ПК СВ "Брест" РДЦП.10001-02. Поддерживается установка в Kubernetes	Поддержка установки на «голое железо», в виртуальной среде (VMware vSphere версии 11, VMware ESXi версии 6) Образами не поставляется, но внутри есть контейнеризация	Поддерживаемые платформы виртуализации: VmWare Esxi, Hyper-V, ProxMox VE, установка On-Premise или в частном облаке. Установка осуществляется через скрипт
1.3. Архитектурные особенности решения (стек технологий, возможность прямого доступа к внутренним структурам, возможность доступа покупателя к ОС/СУБД решения с правами администратора);	Tomcat, Ariel DB, PostgreSQL, SQLite, Docker (для работы интегрируемых приложений самостоятельной разработки или скачанных из маркетплейса)	Используется микросервисная архитектура.	Возможность прямого доступа к базам данных и шине данных у пользователя есть, но официально такие манипуляции не рекомендуются и не поддерживаются	Микросервисная архитектура
1.4. Параметры масштабируемости, кластеризации, производительности;	Поддерживается многонодовая установка	Приведен расчет сайзинга для сервера-коллектора: при потоке событий 1000 EPS, выключенном обогащении и агрегации событий, при использовании 5000 аккаунтов и 5000 активов в тенанте, одному коллектору требуются 1 ЦПУ, 512 Мб ОЗУ, 1 Гб дискового пространства.	D × 3600 × 24 × скорость потока событий (в секунду), где D — коэффициент, который может принимать следующие значения: 1200 — при использовании хранилища Elasticsearch; 200 — при использовании хранилища LogSpace. Горизонтальное масштабирование достигается за счет установки компонента AEC (Asset and Event Collector) для учета архитектуры сети и каналов связи. Увеличение количества конвейеров обработки событий и иерархические схемы	Поддерживается кластеризация
1.5. Поддержка отказоустойчивости (реализация, требования вендора к инфраструктуре покупателя);	Поддержка создания отказоустойчивого кластера	Поддерживается развертывание в отказоустойчивой конфигурации. Поддерживается работа в режиме Active-Passive, Active-Active	Отказоустойчивость возможна на уровне компонентов, шины данных (RabbitMQ) и СУБД	Поддерживается. Требования к инфраструктуре зависят от общего потока событий
1.6. Обеспечение безопасной работы	Поддержка ролевой модели разграничения доступа (3 роли по умолчанию), создание пользовательских ролей, разграничение	Поддерживается ролевая модель (роли «Главный	Ролевая модель доступа, поддерживается SSO-аутентификация через решение	Обеспечиваются все указанные меры обеспечения безопасной

решения (ограничение доступа, ролевая модель, защита канала связи, защита обрабатываемых данных, журналирование, способы аутентификации пользователей, контроль действий пользователей решения);	доступа к определенным функциям и разделам на основе ролей, защита передаваемых между нодами данных с помощью OpenSSH, действия пользователей с компонентами решения логируются. Поддержка RADIUS, TACACS, LDAP-аутентификации. Возможность установки TLS-сертификата от доверенного центра сертификации для защищенного доступа к веб-интерфейсу	администратор», «Администратор», «Аналитик», «Аналитик первой линии», «Оператор»), поддерживается интеграция с Active Directory (вход по доменной учетной записи), поддерживается создание API-токена для каждой учетной записи в решении	PT Management and Configuration. Поддерживается гибкое разграничение доступа к событиям на основе ролей, с указанием условий фильтрации событий, к которым предоставляется доступ. Поддерживается резервное копирование средствами самого решения (с помощью сценариев). Журналирование гибко настраивается (с помощью конфигурационных файлов) Взаимодействие компонентов решения осуществляется с использованием сертификатов	работы решения. Используется TLS для обеспечения защищенной передачи данных между компонентами системы. Аутентификация с локальной УЗ либо через AD.
1.7. Локализация интерфейса, поддержка мультиязычности, возможность кастомизации интерфейса, возможность сквозного поиска по всем обрабатываемым данным.	Английский, китайский, немецкий, корейский, португальский, русский, испанский, итальянский, французский, японский	Поддерживается русский, английский языки в интерфейсе	Язык интерфейса: русский, английский	Поддерживаются русский, английский языки
2. Общие организационные характеристики:				
2.1. Дата первого релиза, текущая версия;	Текущая версия 7.5.0, дата первого релиза 2001 г. (Q1 Labs QRadar)	Дата первого релиза – 2020 год, текущая версия 2.1.	Текущая версия 7.3. первый релиз в 2015 г.	Первый релиз - 02 февраля 2015г. Текущая версия 3.10.0
2.2. Наличие документации, наличие API;	Документация на веб-портале, в виде PDF	Документация на онлайн-портале, API поддерживается	Онлайн-документация на сайте, поддерживается REST API по протоколу HTTPS	Есть
2.3. Наличие технической поддержки, режим работы, SLA-нормативы;	Техническая поддержка предоставляется в режиме 24/7	Режим работы 24x7, каналы связи: телефон, email, онлайн	Обращение в техническую поддержку круглосуточно через единый портал вендора, время реакции на критические запросы до 4 часов в режиме техподдержки и до 1 часа для тех. поддержки уровня premium	Есть
2.4. Наличие гарантии, срок предоставления гарантийного обслуживания, что включено в стандартное гарантийное обслуживание, возможность расширенной гарантии;	Предоставляется поддержка на 1 год при покупке апплайнсов	Нет данных	Сервисное обслуживание, консультационные услуги, услуги экспертного центра кибербезопасности PT Expert Security Center (PT ESC)	Гарантийные обязательства исполняются в течение всего периода приобретенной технической поддержки
2.5. Лицензионная политика: стоимость дополнительных интеграций (ИТ/ИБ-системы, СЗИ, внешние сервисы и т.д.), лицензирование API, правила расчета лицензии (по пользователям, потоку событий, инцидентам, интеграциям и т.д.), отличие в стоимости при разных вариантах инсталляции, специальные условия для MSS-провайдеров;	Нет данных	Работа по подписной модели, на стоимость влияет количество EPS, дополнительные модули системы (поддержка Netlow, работа с ГосСОПКА, модуль Threat Intelligence)	Продукт лицензируется по количеству активов и событий. Интеграции и API не лицензируются отдельно и доступны всем пользователям. Для MSSP существуют специальные условия	Лицензирование осуществляется по общему потоку событий. Дополнительно приобретаются модули расширения функционала системы: модуль поведенческого анализа RuSIEM Analytics, RuSIEM IoC, RuSIEM Monitoring. Имеется бесплатный продукт класса Log Management - RvSIEM
2.6. Опыт внедрений.	Нет данных	Нет данных	Более 600 инсталляций в России и за рубежом	Нет данных
2.7. Наличие сертификатов регуляторов, присутствие в реестре российского ПО;	Не применимо	Сертификат соответствия ФСТЭК №4455 (УД4). Присутствует в реестре российского ПО	Сертификат соответствия ФСТЭК России № 3734 от 16.03.2022 (УД4, ТУ). Решение присутствует в реестре российского ПО	Включено в реестр отечественного ПО (Реестровая запись №3808 от 16.08.2017), имеется сертификат ФСТЭК по 4 уровню доверия (Сертификат соответствия ФСТЭК России № 4402)
3. Обработка событий ИБ, создание инцидентов ИБ:				
3.1. Типы, количество поддерживаемых из коробки транспортов / протоколов взаимодействия с источниками событий ИБ;	Поддерживаются Syslog (Syslog-ng, TLS Syslog), HTTP, OPSEC LEA, SNMP, LEEF, JDBC, SMB, RPC, доступ к файлам, API-взаимодействие.	Поддерживаются протоколы Syslog, Syslog-ng, SNMPv2, HTTP(S), SQL, ODBC, WMI, FTP, SFTP, xFlow, SCP, OPsec, CEF, RPC, Windows Event Log, Windows File log, SNMP Traps	Syslog, Windows (Event log, WMI), NetFlow, ODBC, SSH, CheckPoint OPSEC, SNMP, файлы TXT, JSON и XML	Поддерживается более 20 транспортов / протоколов (полный список: rusiem.com)
3.2. Типы, количество поддерживаемых из коробки источников событий ИБ;	Более 300 источников	Поддерживается «из коробки» 179 типов источников, регулярно пополняются. Полный список: support.kaspersky.ru	Антивирусные средства, бизнес-приложения, сетевые устройства (межсетевые экраны, коммутаторы, маршрутизаторы, Wi-Fi-контроллеры), операционные системы, прокси-серверы, DHCP, VPN и шлюзы доступа, AAA-системы, системы виртуализации, системы защиты конечных точек, IDS/IPS, СУБД, службы каталогов, удостоверяющие центры	Поддерживается более 350 источников
3.3. Типы, количество поддерживаемых из коробки парсеров, правил нормализации;	Поставляются парсеры для всех поддерживаемых источников, поддерживается добавление собственных правил парсинга и нормализации	Поддержка методов парсинга json, cef, regexp, syslog, csv, kv (пара "ключ-значение", key-value), xml, netflow5, netflow9, sflow5, ipfix, sql	7889 правил нормализации	Поддерживается более 150 парсеров, правил нормализации
3.4. Возможность подключения нестандартных источников событий ИБ, функционал создания / изменения парсеров и правил нормализации, функционал настройки опций поддерживаемых транспортов / протоколов взаимодействия с источниками событий ИБ;	Поддерживается подключение кастомных источников через модули DSM (Device Support Module), ограниченная настройка используемых протоколов	Поддерживается	Поддерживается, возможна доработка вендором по запросу, при написании правил нормализации, корреляции и обогащения событий применяется внутренний язык eXtraction and Processing (XP)	Поддерживается
3.5. Поддержка API-интеграций для	Поддерживается	Поддерживается KUMA REST API (работа через HTTP(S))	Поддерживается REST API по протоколуHTTPS	Поддерживается

взаимодействия ИТ/ИБ-систем с SIEM;				
3.6. Поддержка способа получения данных от источников (push / pull);	Поддерживаются оба способа, в зависимости от типа источников	Поддержка обоих режимов	Поддерживаются оба варианта	Поддерживается
3.7. Количество поддерживаемых из коробки правил таксономии;	Поддерживаются «из коробки» более 20 правил высокоуровневого категорирования (для каждого правила высокого уровня поддерживаются несколько десятков низкоуровневых правил), расширяются за счет пакетов расширения содержимого (QRadar content extensions), доступных в маркетплейсе IBM Security App Exchange	Нет данных	300	Поддерживается более 670 правил таксономии
3.8. Количество поддерживаемых из коробки правил корреляции;	Поддерживаются «из коробки» более 1000 правил высокоуровневого категорирования, расширяются за счет пакетов расширения содержимого (QRadar content extensions), доступных в маркетплейсе IBM Security App Exchange	Поддерживается «из коробки» 343 правил корреляции	882	Поддерживается более 400 правил корреляции
3.9. Количество поддерживаемых из коробки правил установки (приоритизации) уровня критичности / опасности события / инцидента;	Правила приоритизация поставляются с правилами корреляции в пакетах расширения содержимого, настраиваются для каждого правила	Нет данных	У инцидента 3 уровня критичности, у скоррелированных событий 3 уровня критичности	Поддерживается 5 правил
3.10. Поддержка хранения событий в исходном формате (raw).	Поддерживается	Поддерживается	Поддерживается, с возможностью поиска по тексту и копирования текста «сырого» события	Сырые события всегда сохраняются
4. Интеграции:				
4.1. Интеграция с системами управления и учета активов (CMDB, ITAM);	Поддерживается	Нет данных	Поддерживается, ведется внутренний учет активов в решении	Поддерживается
4.2. Интеграция с системами управления и учета конфигураций (CMDB);	Поддерживается	Нет данных	Поддерживается, ведется внутренний учет конфигураций в решении	Поддерживается
4.3. Интеграция с системами класса ITSM, Case Management, тикетинг-системами;	Поддерживается отправка инцидентов во внешние системы по Syslog, по API	Нет данных	Поддерживается	Поддерживается
4.4. Интеграция с системами класса TIP;	Поддерживается за счет собственного решения IBM QRadar Threat Intelligence	ThreatConnect Threat Intelligence Platform, ThreatQuotient, Kaspersky CyberTrace, Kaspersky Threat Intelligence Portal	Поддерживается за счет интеграции с решением PT Cybersecurity Intelligence	Поддерживается
4.5. Интеграция с системами класса SOAR;	Поддерживается за счет собственного решения IBM QRadar SOAR (ex-Resilient)	Интеграция с R-Vision Incident Response Platform, Security Vision Incident Response Platform	Innostage IRP, R-Vision SOAR, Security Vision [NG]SOAR	Поддерживается
4.6. Интеграция с системами класса XDR;	Поддерживается за счет собственного решения IBM Security QRadar XDR	Интеграция в рамках экосистемы Kaspersky Symphony XDR	Интеграция с собственным решением PT XDR	Поддерживается
4.7. Построение внутреннего репозитория ИТ-активов;	Поддерживается функционал построения базы активов в решении (в том числе за счет интеграции с сканерами уязвимостей и самостоятельного сканирования на уязвимости с помощью IBM QRadar Vulnerability Manager)	Поддерживается импорт активов из Max Patrol 8, RedCheck, KSC, KICS for Networks, импорт из CSV-файла, создание активов через API или веб-интерфейс. Поддерживается структурированная модель данных для свойств (полей) активов	Поддерживается построение собственной модели активов за счет получения данных из интегрированных систем и путем импорта XML-отчетов из сканера MaxPatrol 8. Поддерживается работа встроенных модулей аудита (с аутентификацией на активе), поиска активов в инфраструктуре (методы ICMP ping, TCP ping), пентеста (без аутентификации на активе, поиск уязвимостей, тестирование на проникновение). Поддерживается ведение истории изменения свойств актива	Поддерживается
4.8. Построение внутреннего репозитория уязвимостей;	Поддерживается за счет собственного решения IBM QRadar Vulnerability Manager	Поддерживается хранение информации об уязвимостях в качестве свойств актива (не отдельные сущности), данные об уязвимостях импортируются из KSC, KICS for Networks	Поддерживается в интеграции с MaxPatrol VM (единый интерфейс)	Поддерживается
4.9. Построение внутреннего репозитория конфигураций.	Поддерживается за счет собственного решения IBM QRadar Risk Manager	Не поддерживается	Поддерживается в интеграции с MaxPatrol HCC (единый интерфейс)	Не поддерживается
5. Поддержка процессов управления киберинцидентами:				
5.1. Функционал поиска событий, инцидентов (удобство, гибкость, скорость, поддержка синтаксисов regex / wildcard);	Поддерживается с помощью внутреннего языка запросов AQL (Ariel Query Language)	Поддерживается создание поискового SQL-запроса (синтаксис ClickHouse) вручную и с помощью интерактивного конструктора запросов	Поддержка полнотекстового поиска, в том числе по «сырым» событиям, поддержка поиска и фильтрации данных с помощью запросов Positive Data Query Language (PDQL)	Поддержка гибкого, быстрого поиска, поддержка регулярных выражений
5.2. Единый интерфейс для совместной работы аналитиков над событиями, инцидентами (War room);	Не поддерживается	Поддерживается	Поддерживается	Нет данных
5.3. Поддержка методологий реагирования на инциденты (матрица MITRE ATT&CK, методология ФСТЭК);	Поддерживается методология MITRE ATT&CK в расширении QRadar Use Case Manager, доступном в маркетплейсе IBM Security App Exchange	Поддерживается указание названия тактики и техники из матрицы MITRE ATT&CK в свойствах события	Поддержка «тепловой карты» покрытия решением тактик и техник матрицы MITRE ATT&CK	Поддерживается
5.4. Поддержка процессов соответствия законодательству в части сохранения		Поддерживается экспорт инцидентов, отправка файлов, обработка ответов, обмен сообщениями с НКЦКИ	Поддержка с помощью решения «ПТ Ведомственный центр» вендора	

данных по инцидентам и реагированию (в том числе интеграция с ГосСОПКА, ФинЦЕРТ);	Не поддерживается для российского законодательства	(ГосСОПКА), в рамках отдельной лицензии на модуль «GosSOPKA»	(автоматическое получение событий, относящихся к КИИ, из решения MP SIEM)	Поддерживается
5.5. Поддержка построения timeline инцидентов;	Не поддерживается	Не поддерживается	Есть виджеты по инцидентам с распределением по дням. Более гранулярно можно построить на основе событий, лежащих в основе инцидентов	Поддерживается
5.6. Поддержка использования, загрузки, обновления пакетов экспертизы (парсеров, правил корреляции, use cases, рекомендаций по реагированию);	Поддерживается, доступно в маркетплейсе IBM Security App Exchange	Не поддерживается	Поддерживается, в том числе за счет экспертизы центра PT Expert Security Center и сообщества пользователей продукта. Экспертиза сфокусирована на киберугрозах, актуальных для российских компаний. В экспертных пакетах (выходят 1-2 раза в месяц) поставляются рекомендации по реагированию, правила корреляции, репутационные списки, рекомендации по защищенной настройке систем, настройки аудита, рекомендации по реагированию. Поддерживается SDK для написания и тестирования правил корреляции и обогащения, присутствует утилита-конструктор для тестирования и контроля версионности правил	Осуществляется при обновлении версии ПО
5.7. Поддержка формирования рекомендаций по реагированию в соответствии с законодательными требованиями и лучшими практиками (ГОСТ 59709-59712, NIST 800-61, ISO 27035);	Не поддерживается	Не поддерживается	Для правил корреляции есть описание контекста, что произошло и рекомендации, как на это реагировать	Не поддерживается
5.8. Формирование отчетности и визуализации данных по инцидентам, в том числе формирование отчетности по требованиям применимых норм законодательства.	Поддерживается визуализация данных на настраиваемых дашбордах с drilldown, поддерживается формирование отчетности вручную и по расписанию (PDF, MS Office)	Поддерживается создание отчетов, в том числе с применением шаблонов. Поддерживается отображение информации на панели мониторинга (набор виджетов, в том числе набор предустановленных макетов), поддержка отображения данных в «режиме ТВ» (показ макетов в режиме слайд-шоу). На виджетах поддерживается отображение графиков вида «Круговая диаграмма», «Счетчик», «Таблица», «Столбчатая диаграмма», «Календарная диаграмма», «Линейная диаграмма»	Поддержка виджетов, отображение статистической информации на дашбордах, отображение данных об активах, событиях, инцидентах, внутренних проверках (чек-листы состояния инсталляции решения). Поддерживается создание пользовательских виджетов	Поддерживается
6. Визуализация, отчетность, удобство использования:				
6.1. Наличие сообщества / маркетплейса для получения дополнительных правил корреляции, парсеров, интеграций и т.д.;	Поддерживается маркетплейс IBM Security App Exchange	Не поддерживается	Присутствует собственный маркетплейс, каталог расширений (порядка 30 шт.), сообщество пользователей с возможностью поделиться наработками	Телеграмм-канал t.me
6.2. Возможность экспорта / импорта контента (парсеры, интеграции), возможность «отката» на предыдущие версии (для парсеров, интеграций);	Поддерживается экспорт расширений (приложений) за счет встроенного инструмента «Extensions Management», путем выполнения Perl-скрипта «Content management script»	Нет данных	Поддерживается с помощью экспорта / импорта пакетов экспертизы (файлы формата KB), в которые можно включить правила корреляции и иные релевантные объекты системы	Поддерживается
6.3. Отчетность (разнообразные виды и форматы отчетов, включая создание стратегических, оперативных, тактических, аналитических отчетов для различных групп потребителей решения), отправка отчетов автоматически и по запросу (электронная почта, мессенджеры и т.д.);	Поддерживается формирование пользовательских отчетов, с кастомизацией расположения содержимого и брендированием, с отправкой отчетов по email	Поддерживается создание отчетов, в том числе с применением шаблонов, с поддержкой сохранения в файлы форматов HTML, PDF, CSV, XLSX, с поддержкой формирования по расписанию, с отправкой по email. Поддерживается отправка оповещений об инцидентах по email, SMS, через API, поддерживаются кастомизируемые способы оповещений	Поддерживается путем создания задачи на выпуск отчетов по активам, событиям, инцидентам вручную или по расписанию, с отправкой отчетов по email, поддерживается отправка уведомлений через POST-запросы	Гибко конфигурируемые отчеты с возможностью выгрузки вручную либо по расписанию с оправкой на email или в Telegram
6.4. Выгрузка данных по инцидентам в отчете (doc, pdf), экспорт данных в разных форматах (xml, json, csv);	Поддерживается выгрузка данных по событиям в CSV	Поддерживается экспорт событий (в TSV-файл), экспорт активных листов (в JSON-файл), экспорт данных об активах (в CSV-файл)	Поддерживается выгрузка отчетов в формате PDF. Поддерживается экспорт, импорт данных из табличных списков в формате CSV, экспорт отфильтрованных инцидентов в формате JSON. Поддерживается экспорт данных виджетов в форматах PNG, CSV	Поддержка выгрузки в форматах pdf, csv, docx, xlsx
6.5. Встроенная веб-помощь в интерфейсе системы.	Поддерживается	Поддерживается	Поддерживается	Только портал документации

Расширенные критерии	**IBM QRadar**	**Kaspersky KUMA**	**PT MaxPatrol SIEM**	**RuSIEM**
1. Общие технические характеристики:				
1.1. Возможность использования SIEM как услуги (SaaS-модель);	Поддерживается	Нет данных	Есть несколько крупных MSSP провайдеров, которые могут оказывать комплексный сервис на базе MaxPatrol SIEM. SaaS в чистом виде отсутствует	Да, предоставляется партнерами
1.2. Поддержка работы в сетях, изолированных от Интернет;	Поддерживается с помощью установки модуля Disconnected Log Collector	Поддерживается	MaxPatrol SIEM может работать в изолированных сегментах. Обновление экспертизы при этом ставится вручную	Поддерживается
1.3. Поддержка работы в режиме multitenancy.	Поддерживается	Поддерживается	Поддерживается несколько сценариев, основанных на архитектуре инсталляции	Поддерживается

2. Общие организационные характеристики:				
2.1. Наличие авторизованного обучения от вендора, стоимость обучения;	Поддерживается в собственных и авторизованных учебных центрах	Проводится обучение в авторизованных вендором учебных центрах	Обучение в учебных центрах на основе курсов от вендора	Обучение, проводимое вендором, является бесплатным без выдачи сертификата государственного образца. Обучение выдачей сертификата осуществляется партнером «Академия Информационных Систем»
2.2. Дорожная карта развития продукта (планируемый к внедрению функционал и ориентировочные сроки реализации, планируемые изменения в лицензионную политику).	Нет данных	Нет данных	Нет данных	Поддерживается
3. Обработка событий ИБ, создание инцидентов ИБ:				
3.1. Глубина хранения событий / инцидентов, поддержка исторической корреляции, кластеризация хранилищ информации, хранение данных в холодном хранилище с возможностью поиска в нем;	Поддерживается выполнение исторической корреляции, глубина хранения настраивается в политиках хранения, зависит от объема дисковой подсистемы	Поддерживается проведение ретроспективных проверок. Глубина хранения зависит от объема дискового пространства	Поддерживаются хранилища Elasticsearch и LogSpace, поддержка кластеризации и сжатия данных средствами Elasticsearch	Настраиваемые сроки хранения событий как в оперативном доступе, так и в архиве. Поддерживается историческая корреляция, кластеризация хранилищ информации, хранение данных в холодном хранилище с возможностью поиска в нем
3.2. Интеграция с решениями Big Data (например, Hadoop, Spark);	Поддерживается	Не поддерживается	Поддерживается интеграция с брокером сообщений Apache Kafka	Поддерживается
3.3. Поддержка создания и сохранения форензик-данных инцидентов;	Не поддерживается	Не поддерживается	Хранение копии событий и копии трафика при использовании компонента Network Sensor	Создается вручную
3.4. Поддержка получения событий из облачных инфраструктур;	Поддерживается (для Amazon Web Services, Microsoft Azure)	Не поддерживается	Поддерживается интеграция с Yandex Cloud и сервисом для сбора и выгрузки логов (Yandex Audit Trails)	Поддерживается
3.5. Поддержка получения событий из OT/ICS-инфраструктур.	Поддерживается через Nozomi Networks QRadar App	Поддерживается с помощью решения KICS for Networks	Напрямую за счет интеграции с решением PT Industrial Security Incident Manager (PT ISIM)	Поддерживается
4. Интеграции:				
4.1. Интеграция с внешними сервисами обогащения данных по событиям и инцидентам (например, Whois, Spamhaus, VirusTotal и т.д.);	Поддерживается: выполнение геопривязки IP-адресов, данные из WHOIS, интеграция с VirusTotal (приложение QVTI VirusTotal)	Поддерживаются запросы на внутренний DNS-сервер, запрос географической привязки IP-адресов, запрос обогащения в Kaspersky CyberTrace	Поддерживается начиная с версии 26.1 с Whois, VirusTotal. Со следующей версии пользователь сможет добавлять любые сервисы самостоятельно через конфигурационный файл	Не поддерживается
4.2. Интеграция с источниками данных аналитики киберугроз (TI-фидами);	Поддерживается путем установки QRadar Threat Intelligence app, поддержка STIX / TAXII, добавление произвольных фидов. Поддерживается интеграция с собственным TI-фидом BM X-Force Exchange	Поддерживается интеграция с Kaspersky CyberTrace, Kaspersky Threat Intelligence Portal	Поддерживается за счет интеграции с решением PT Cybersecurity Intelligence	Поддерживается
4.3. Наличие, функционал магазина приложений / расширений, перечень вендоров-партнеров;	Поддерживается работа с маркетплейсом IBM Security App Exchange, содержащим правила корреляции, парсеры, приложения	Не поддерживается	Поддерживается собственный маркетплейс, каталог расширений (порядка 30 шт.)	Не поддерживается
4.4. Поддержка собственного API для интеграции SIEM-системы с другими решениями в инфраструктуре.	Поддерживается	Поддерживается	Поддерживается REST API по протоколу HTTPS	Поддерживается
5. Поддержка процессов управления киберинцидентами:				
5.1. Поддержка работы MSS-провайдеров с решением, разграничение доступа тенантов;	Поддерживается, с разграничением доступа тенантов	Поддерживается, разграничение доступа тенантов поддерживается на уровне объектов и прав доступа пользователей	Ролевая модель доступа к данным	Поддерживается
5.2. Возможности по реагированию на инциденты силами SIEM (создание плейбуков реагирования, автоматизация задач и процессов реагирования);	Поддерживается в решении IBM QRadar SOAR (ex-Resilient)	Поддерживается выполнение задач в KSC, действия по реагированию для KEDR, KICS for Networks, действия в Active Directory (добавить / удалить учетную запись из группы, сбросить пароль, заблокировать учетную запись), поддерживается запуск пользовательского скрипта	Можно реагировать с помощью интеграции с PT XDR	Поддерживается при интеграции со сторонними решения, поддерживается возможность автоматического реагирования через использование скриптов
5.3. Функционал построения графов реализованных и возможных кибератак (с учетом обнаруженных событий, уязвимостей, критичности активов, прав пользователей на активах);	Поддерживается построение схемы атаки в инциденте в модуле IBM QRadar Risk Manager	Не поддерживается	Поддерживается с построением графа сетевой связности и достижимости, с отображением свойств активов. Поддерживается построение топологии сети	Не поддерживается

5.4. Выявление аномалий, выявление киберинцидентов на основе внутреннего аналитического движка (функции UEBA);	Поддерживается в приложении QRadar User Behavior Analytics	Не поддерживается	Поддерживается выявление аномалий в модуле BAD (Behavioral Anomaly Detection) с использованием статистических методов	Поддерживается в модуле RuSIEM Alalytics
5.5. Применение методов обработки Big Data;	Поддерживается	Не поддерживается	Нет данных	Не поддерживается
5.6. Наличие, функционал, кастомизация механизма статистического анализа свойств инцидентов;	Нет данных	Не поддерживается	Поддерживается	Поддерживается
5.7. Применение методов машинного обучения (наличие и количество предварительно настроенных и обученных моделей машинного обучения), возможность подстройки параметров моделей под конкретную инфраструктуру;	Поддерживается в приложении Machine Learning Analytics (расширение приложения QRadar User Behavior Analytics)	Не поддерживается	Поддерживается с прогнозированием возникновения инцидентов с помощью машинного обучения, с приоритизацией выявленных инцидентов	Поддерживается
5.8. Интеграция или встроенная поддержка систем Искусственного Интеллекта, возможность двусторонней связи с решением.	Поддерживается в отдельном модуле QRadar Advisor with Watson, использующем ИИ (IBM Cognitive Artificial Intelligence)	Не поддерживается	Нет данных	Не поддерживается
6. Визуализация, отчетность, удобство использования:				
6.1. Возможность создания персонального рабочего окружения исходя из процессов / бренда организации: кастомизация расположения элементов на странице, быстрых фильтров, карточек и жизненного цикла инцидентов ИБ / атак с применением подхода low-code / no-code;	Не поддерживается	Не поддерживается	Поддержка изменения формата отображения информации, отображение определенных столбцов, фильтрация, сортировка	Поддерживается
6.2. Визуализация (включая интерактивные графы для отображения связей между инцидентами и связанными объектами и для интерактивного управления инцидентами в рамках реагирования), дашборды, панели визуализации (виджеты), функционал drilldown;	Поддерживается построение схемы атаки, поддерживаются дашборды с drilldown	Поддерживается выводи информации на виджетах, панелях мониторинга, в отчетах. Поддерживается функционал drilldown в виджетах	Поддержка визуализации информации на графике, в таблице, с возможностью экспорта в отчет. Поддержка встроенного конструктора панелей визуализации, функционал Drilldown поддерживается	Поддерживается
6.3. Возможность кастомизации дашбордов, панелей визуализации с применением подхода low-code / no-code;	Поддерживается создание кастомизированных дашбордов	Поддерживается кастомизация виджетов, но без применения подхода low-code / no-code	Поддерживается	Поддерживается
6.4. Возможность создания кастомизированных отчетов с применением подхода low-code / no-code;	Не поддерживается	Поддерживается кастомизация отчетов, но без применения подхода low-code / no-code	Поддерживается	Поддерживается
6.5. Функционал тэгирования инцидентов (в ручном и автоматическом режиме);	Не поддерживается	Не поддерживается	Отдельного поля нет, можно хранить теги в поле «Комментарий»	Поддерживается
6.6. Интеграция с ФинЦЕРТ, ГосСОПКА (отправка отчетов по киберинцидентам, получение и обработка ответов);	Не применимо	Поддерживается экспорт инцидентов, отправка файлов, обработка ответов, обмен сообщениями с НКЦКИ (ГосСОПКА), в рамках отдельной лицензии на модуль «GosSOPKA»	Поддержка с помощью решения «ПТ Ведомственный центр» вендора (автоматическое получение событий, относящихся к КИИ, из решения MP SIEM)	Поддерживается, двухсторонняя интеграция
6.7. Формирование отчетности по требованиям действующего законодательства (указать выполняемые требования)	Не поддерживается для российского законодательства	Поддерживается отображение данных об активах, алертах и инцидентах, относящихся к КИИ, в виджетах и отчетах	Пересылка инцидентов в НКЦКИ в требуемом формате	Возможность построения кастомизированных отчетов под любые требования законодательства

SOAR

Основные критерии	ePlat4m Orchestra (UDV ePlat4m SOAR)	Google Chronicle SOAR	Makves IRP	Microsoft Sentinel	Innostage IRP	Palo Alto Cortex XSOAR	R-Vision SOAR	Security Vision [NG]SOAR	UserGate LogAnalyzer
1. Общие технические									

характеристики:									
1.1. Технические требования к платформе и среде внедрения (системные требования к аппаратному и программному обеспечению, окружению);	ОС: Windows 10 и выше, Ubuntu v.20 и выше, Debian v.11 и выше, CentOS v.7 и выше, Astra Linux v.1.7.1 и выше. СУБД: MSSQL/PostgreSQL/Jatoba. Аппаратные требования: 32 Гб RAM, 8 CPU, 1000 Гб дискового пространства	Для on-prem установки: ОС: CentOS 7.5, 7.8, 7.9, Red Hat 7.8. Аппаратные требования («All-in-one»): 12 ЦПУ, 32 Гб ОЗУ, 800 Гб дискового пространства	ОС: Windows 10, Windows 2016 - 2019, OS X 10.9 - 10.11, macOS 10.14 и старше, Ubuntu 16 LTS, Ubuntu 18 LTS СУБД: PostgreSQL 9.6. Аппаратные требования: 8 Гб RAM, 10 Гб дискового пространства. Дополнительно: Docker 18.* (для OS X, Linux), Docker Desktop 18 или Docker Enterprise (для Windows).	Поддерживается работа только в облаке Microsoft Azure	ОС: Линукс (Debian, Astra Linux). Аппаратные требования (компоненты системы разворачиваются на 4 ВМ): 15 ЦПУ, 40 Гб ОЗУ, 510 Гб дискового пространства	Не применимо (SaaS-решение)	ОС: CentOS 7.5 - 7.9, RHEL 7.7 - 9.2, Debian 10.x - 11.1, Astra SE 1.6, Astra SE 1.7, Astra CE 2.12, RED OS 7.3, RED OS 7.3c, ALT Server 10 (p 10.x), ALT 8 SP Server (c 8.2). СУБД: PostgreSQL 14, Jatoba J4. Аппаратные требования: в зависимости от количества активов, сценариев реагирования, пользователей, от 12 Гб RAM, 4 CPU, 100 Гб дискового пространства	ОС: Microsoft Windows Server 2012 R2 или выше, CentOS 7 или выше, Red Hat Ent. Linux 7 или выше, Ubuntu 18.04 или выше, Debian 10 и выше, Astra Linux CE (Common Edition) релиз "Орел", Astra Linux SE (Special Edition) релиз «Воронеж» и "Смоленск", Альт 8 СП, Альт Сервер 10 или выше, Oracle Linux 8 и выше, РЕД ОС актуальной версии, РОСА "КОБАЛЬТ", AlmaLinux, AlterOS. СУБД: Microsoft SQL Server версии 2016 или выше, PostgreSQL версии 11 или выше, Postgres Pro версии 11 или выше, Jatoba. Аппаратные требования: 8 ЦПУ, 12 Гб ОЗУ, 100 Гб дискового пространства	Аппаратные требования (для виртуальной машины, минимально): 2 ЦПУ, 8 Гб ОЗУ.
1.2. Варианты поставки и инсталляции (аппаратный апплайнс, образ, контейнер, установка на «голое железо», установка on-prem, установка в облаке, наличие графических инсталляторов, поддержка виртуализации);	Поставка в виде образа, дистрибутива	Возможна установка on-prem и использование в режиме SaaS (в облаке Google). Поддерживается установка из OVA-образа на VMware ESXi версии 5.0 и выше	Установка из Docker-контейнера либо установка из MSI-файла (для Windows) на физической или виртуальной машине	Поддерживается работа только в облаке Microsoft Azure	Варианты поставки и инсталляции: аппаратный апплайнс, образ, установка на «голое железо», установка on-prem, установка в облаке, поддержка виртуализации (пп 1.1)) Система разворачивается силами вендора/партнера или самостоятельно Заказчиком. Решение поддерживает среды виртуализации VMware vSphere, Microsoft Hyper-V, KVM	Поддерживается работа только в облаке (SaaS) для версий 8.x, on-prem инсталляция возможна для версий 6.x.	Поддерживается установка "на голое железо", on-prem. Поддерживается виртуализация, контейнеризация. Решение поставляется в виде виртуального апплайнса (виртуальная машина с предустановленным ПО для работы решения)	Поддержка установки в виде контейнера, на «голое железо», в виде ISO образа, RPM-пакетов, из графического инсталлятора и из командной строки. Поддержка систем виртуализации (VMware, VirtualBox, Hyper-V, Xen, Parallels, KVM). Поддерживается установка в облаке и on-prem.	Поддержка систем виртуализации VMware, Hyper-V, Xen, KVM, OpensStack, VirtualBox Поставка решения: в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде
1.3. Архитектурные особенности решения (стек технологий, возможность прямого доступа к внутренним структурам, возможность доступа покупателя к ОС/СУБД решения с правами администратора);	Amazon States Language, SQL с доступом с правами администратора без прямого доступа извне к внутренним структурам. Используемые технологии: PostgreSQL, MinIO		Нет данных	Поддерживается совместная работа всех облачных продуктов Microsoft (Log Analytics, Microsoft 365 Defender, Microsoft Defender for Cloud, Azure Resource Manager, Azure Monitor, Azure Application Gateway, Azure Firewall, VPN Gateway, Azure Load Balancer и т.д.)	Клиент-серверная архитектура, построенная на платформе .Net Core. Имеется поддержка ОС семейства Линукс (Debian, Astra Linux), свободно распространяемой СУБД PostgreSQL. Имеется поддержка отказоустойчивой архитектуры развертывания на уровнях приложения, ОС, СУБД. Для эксплуатации и администрирования используется «тонкий» клиент, без необходимости установки дополнительного ПО. Имеются веб-сервисы для взаимодействия с внешними сервисами и информационными системами. Администрирование и настройка продукта, осуществляется только с использованием учетной записи администратора	Docker, Python	Используется СУБД PostgreSQL и Jatoba, работа с решением ведется через веб-интерфейс, поддерживается возможность инсталляции с выделенными коллекторами для сканирования и реагирования в сегментированных сетях (филиалы, удаленные площадки)	Возможность отдельной установки выделенного сервера коннекторов (для взаимодействия с интегрируемыми системами), не требующего прямого соединения с основной базой данных решения. Взаимодействие всех компонент по защищенным протоколам сетевого доступа. Наличие административного доступа к компонентам решения. Используемые сторонние компоненты: Elasticsearch, RabbitMQ, IIS / NGINX, MSSQL / PostgreSQL / Postgres Pro / Jatoba	Используется собственная ОС UGOS LOGAN, поддерживается возможность подключения к ОС в терминальном режиме, поддерживается работа с решением через интерфейс командной строки (CLI)

1.4. Параметры масштабируемости, кластеризации, производительности;	Поддержка масштабирования, поддержка кластера горячего резервирования, кластера холодного резервирования, катастрофоустойчивого кластера	Поддерживается мультинодовая установка	Нет данных	Поддерживается масштабируемость за счет сети дата-центров по всему миру	Параметры масштабируемости - горизонтальное наращивание серверных мощностей, поддержка иерархической архитектуры. Параметры кластеризации - поддержка режимов отказоустойчивого кластера: Active/Active, Active/Passive, отказоустойчивость на уровнях приложения, ОС, СУБД. Параметры производительности - количество обрабатываемых ИТ-активов, количество внешних систем (коннекторов), количество одновременных подключений пользователей (операторов).	Поддерживается гибкое горизонтальное масштабирование	Поддержка кластеризации, поддерживается балансировка нагрузки	Поддерживается мультинодовая установка. Поддерживается балансировка нагрузки между компонентами, возможность установки неограниченного количества нод каждого компонента решения с целью горизонтального масштабирования, возможность установки каждого компонента решения на выделенный сервер	Производительность определяется выбранной виртуальной платформой. Например, для виртуальной платформы UserGate Log Analyzer VE6: · Объем хранилища: до 6 ТБ ·Количество записей в секунду: 160 000 ·Расчетное время хранения журналов: 1 000 дней Рекомендованное количество пользователей: до 1 000
1.5. Поддержка отказоустойчивости (реализация, требования вендора к инфраструктуре покупателя);	Поддерживаются все типы отказоустойчивости, в том числе с применением избыточного кодирования базы данных	Поддерживается режим «высокой доступности»	Нет данных	Поддерживается отказоустойчивость за счет сети дата-центров по всему миру	Для поддержки отказоустойчивости Заказчику необходимо расширять только аппаратную часть от рекомендованных требований (пп 1.1), а также приобрести балансировщик нагрузки (рекомендовано HAProxy). Дополнительных лицензий со стороны Системы не требуется	Отказоустойчивость обеспечивается вендором в сети своих дата-центров	Поддержка работы в режиме отказоустойчивого кластера, поддерживается реализация отказоустойчивости для кластера приложений и кластера базы данных	Поддерживается создание кластера высокой доступности, дублирование и резервирование всех элементов решения, возможность создания геокластера, поддержка отказоустойчивости для провайдеров MSS	Поддержка создания отказоустойчивого кластера в режиме «Актив-Пассив», «Актив-Актив»
1.6. Обеспечение безопасной работы решения (ограничение доступа, ролевая модель, защита канала связи, защита обрабатываемых данных, журналирование, способы аутентификации пользователей, контроль действий пользователей решения, шифрование критичных данных (например, паролей для интегрируемых систем));	Встроенная ролевая модель разграничения доступа в соответствии с ролями персонала SOC, включая встроенную роль Администратора. Шифрование "секретов" - аутентификационной информации для доступа к интегрированным системам с использованием HashiCorp Vault, шифрование с применением стандарта AES-256.	Поддержка SAML, поддержка LDAP (для версии on-prem), поддержка мультифакторной аутентификации, поддержка ролевой модели и групп пользователей (7 групп по умолчанию), разграничение доступа к операциям и определенным модулям, поддержка установки запретов на выполнение определенных действий	Нет данных	Поддерживается хранение данных в изолированных средах (Log Analytics Workspace), поддерживается разграничение доступа на основе ролей (5 предустановленных ролей), назначение ролей определенным ресурсным группам (resource group) для доступа к определенным данным, поддержка создания кастомизированных ролей,	Организованно обеспечение безопасной работы решения (ограничение доступа, ролевая модель, защита обрабатываемых данных, журналирование, аутентификации пользователей (логин/пароль), контроль действий пользователей решения (аутентификация пользователей, изменение полей карточек объектов, запуск сценариев реагирования, скриптов и т.д.), шифрование критичных данных (например, паролей для интегрируемых систем)	Централизованное управление доступом через облачную консоль Cortex Gateway. Поддерживается ролевая модель, гранулированная настройка ролей, поддержка создания групп пользователей. Не поддерживается LDAP-аутентификация. Поддержка цифровой подписи для пакетов одержимого (content packs). Поддержка SSO на базе SAML 2.0 с возможностью подключения любого провайдера аутентификации, поддерживается мультифакторная аутентификация. SaaS-сервис соответствует стандарту SOC 2.	Ролевая модель доступа, дискреционный доступ, доступ к инцидентам на основе атрибутов. Аутентификация: локальная, SSO. Поддерживается логирование изменений, вносимых пользователями. Применяется шифрование учетных данных, сохраненных в системе	Поддерживается ограничение доступа на основе IP-адресов, двухфакторная аутентификация (интеграция со сторонними решениями), аутентификация по сертификатам для пользователей и компонентов решения (использование самоподписанных сертификатов или сертификатов, выданных внутренним центром сертификации), наличие SSO, использование SSL/TLS для защиты доступа к веб-интерфейсу, аудит попыток входа в систему, аудит действий пользователей и администраторов (включая факт просмотра карточек), ролевая модель управления доступом ко всем элементам решения, поддержка multitenancy, шифрование парольной информации.	Поддерживается назначение профилей доступа, создания политики управления паролями, настройки доступа к веб-консоли на уровне разрешения сервиса в свойствах зоны сети. Поддерживается задание сложности пароля, правил блокировки учетной записи на определенное время при превышении количества неудачных попыток авторизации. Для доступа к веб-консоли используется HTTPS (поддерживаются сертификаты самоподписанные и выданные доверенным удостоверяющим центром организации). Поддерживаются серверы аутентификации: LDAP-коннектор (поддерживается интеграция с Active Directory, FreeIPA), RADIUS и TACACS+. Поддерживается ролевая модель доступа (работа с инцидентами, создание комментариев, добавление наблюдателей к инцидентам), управление свидетельствами (уликами) инцидентов, управление схемами инцидентов, правилами аналитики, действиями реагирования, сенсорами, оповещениями, обогащениями. Поддерживается ведение журнала событий, связанных с изменением настроек решения, например, добавление/удаление/изменение данных учетной записи, правила или любого другого элемента.
1.7. Локализация интерфейса, поддержка мультиязычности, возможность кастомизации интерфейса, возможность	Локализация на русском языке. Поддерживается кастомизация и брендирование интерфейса.	Поддержка мультиязычности, сквозного поиска, частичная	Локализация на русском языке, поиск присутствует	Поддерживается мультиязычность, сквозной поиск, ограниченно	Локализация интерфейса, поддержка русского языка, возможность кастомизации интерфейса (конструктор карточек объектов, конструктор дашбордов), возможность	Поддерживается мультиязычность, кастомизация интерфейса не	Поддерживается русская и английская локализации, настройка карточки интерфейса, поддержка тем (темная и светлая), поддержка кастомизации интерфейса	Локализация интерфейса и всех элементов на русском и английском, возможность добавления других языков, поддержка тем (темная и светлая), поддержка кастомизации	Поддерживается русский, английский язык

сквозного поиска по всем обрабатываемым данным.	Поддерживается семантический поиск по всем объектам	кастомизация интерфейса		поддерживается кастомизация	сквозного поиска по всем обрабатываемым данным	поддерживается	(брендирование, логотип), кастомизация вкладок и дашбордов, сквозной поиск по инцидентам	интерфейса (брендирование, логотип), возможность создания рабочих мест пользователей под пользовательский функционал	
2. Общие организационные характеристики:									
2.1. Дата первого релиза, текущая версия;	Дата первого релиза: 02.12.2020 Версия IRP 15.0 Версия Оркестратора 3.2.2	Текущая версия: 6.2.28 (облако), 6.2.7.9 (on-prem). Ранее решение называлось Siemplify, в начале 2022 года было куплено Google	Нет данных		Дата первого релиза - 2013 год. Текущая версия - 3.08	Текущая версия 8.3, дата выхода июль 2023	Дата первого релиза – 2017, текущая версия 5.2	Первый релиз – 2015, текущая версия - 5.0.1694417270	Текущая версия 7.0
2.2. Наличие документации, наличие API;	Документация представляется в виде веб-справки или pdf-документов. API присутствует, задокументирован, можно использовать для запуска и тестирования плейбуков.	Документация на веб-портале, API поддерживается	Документация представляется в виде веб-справки или pdf-документов	Документация на веб-портале, API поддерживается	Имеются руководство пользователя, руководство администратора, а также описание API	Документация на онлайн-портале, API поддерживается	Документация поставляется с системой, API документирован, в том числе поставляется с коллекцией в формате Postman	Документация в виде интерактивной справки в решении, в виде PDF-файлов, поддержка и документация на API.	Документация доступна на онлайн-портале, API поддерживается
2.3. Наличие технической поддержки, режим работы, SLA-нормативы;	Есть несколько уровней техподдержки в зависимости от договора. Стандартный базовый уровень: режим 8x5 (в рабочие дни с 9:00 до 17:00 по московскому времени)	Предлагается скидка на дальнейшее обслуживание в случае простоя сервиса SaaS (от 1% времени простоя)	Нет данных	SLA-нормативы: предлагается скидка 25% в случае недоступности сервиса более чем в 1% случаев	Есть. Режим технической поддержки 8x5, 24x7. SLA в зависимости от критичности обращения (обработка заявки - от 30 минут)	Возможность создания запросов на техническую поддержку через веб-портал, по телефону. Режим работы технической поддержки: 24/7, SLA менее 15 минут (для критичных запросов при приобретении «Платиновой поддержки»)	Поддержка в режиме 24/7, различные уровни поддержки	Техническая поддержка трёх уровней. Максимальная - 24/7. Показатели SLA для тарифа «Максимальный»: время реакции: 4 часа, время предоставления решения: 24 часа. Возможность согласования и подписания произвольных SLA-нормативов и условий предоставления услуг.	Нет данных
2.4. Наличие гарантии, срок предоставления гарантийного обслуживания, что включено в стандартное гарантийное обслуживание, возможность расширенной гарантии;	Оговаривается в договоре	Не применимо	Нет данных	Не применимо	Есть, стандартная гарантийная поддержка предоставляется на 1 год с последующем продлением. Стандартное гарантийное обслуживание включает в себя: - прием заявок по телефону и эл. почте (кол-во обращений не ограничено); -предоставление обновлений и исправлений ПО; - предоставление консультаций и инцидентной поддержке ПО по телефону и эл. почте; - консультации по: настройке и администрированию программных продуктов, диагностике и сбора информации для определения неисправностей в работе программных продуктов, применению решений по устранению неисправностей и восстановлению работы программных продуктов. При необходимости имеется возможность приобрести расширенную техническую поддержку (сжатый SLA, доработки под Заказчика)	В рамках срока использования сервиса	Предоставляется гарантия	Стандартное гарантийное обслуживание на 1 год: -личный кабинет с маркетплейсом дистрибутивов платформы, окружения, ОС, модулями и обновлениями - прием заявок через портал, телефон и эл. почта (кол-во обращений не ограничено); - предоставление консультаций по ВКС, телефону и email; - консультации по: настройке и администрированию программных продуктов, диагностике и сбора информации для определения неисправностей в работе программных продуктов, применению решений по устранению неисправностей и восстановлению работы программных продуктов. При необходимости имеется возможность	Нет данных

								приобрести расширенную техническую поддержку (сжатый SLA)	
2.5. Лицензионная политика: стоимость дополнительных интеграций (ИТ/ИБ-системы, СЗИ, внешние сервисы и т.д.), лицензирование API, правила расчета лицензии (по пользователям, потоку событий, инцидентам, интеграциям и т.д.), отличие в стоимости при разных вариантах инсталляции, специальные условия для MSS-провайдеров;	Расчет согласно прайсу, предоставляемому по запросу. В основе прайса лежит лицензирование модулей и отдельных функциональных элементов, например, коннекторов. Дифференциация по количественным техническим характеристикам (такие как скорость соединения, количество событий и т.д.) не производится. Коннекторы поставляются как в составе продукта, так и отдельно. Разработка новых уникальных коннекторов осуществляется по отдельному договору	Нет данных	Нет данных	Стоимость услуги зависит от объема данных, передаваемых в решение (от 296$ за 100 Гб в день, а также гибкая модель «Pay-as-you-go» с погигабайтной оплатой от 4.30$ за 1 Гб), стоимость зависит от географического местоположения используемого дата-центра	Выделяются следующие факторы, влияющие на стоимость ПО: 1. Количество инсталляций ПО; 2. Количество обрабатываемых ИТ-активов (под узлом понимаются: АРМ, сервер, сетевое оборудование, ПАК средств защиты информации); 3. Количество пользователей/операторов, работающих с ПО; 4. Состав внешних систем, инфраструктурных служб, с которыми ПО должно быть интегрировано/взаимодействовать; 5. Срок и уровень технической поддержки (стандартный уровень поддержки сроком на 1 год входит в стоимость базовой комплект поставки ПО). Стоимость дополнительных интеграций рассчитывается в соответствии с политикой лицензирования. Имеются специальные условия для MSS-провайдеров.	Присутствуют ограничения по количеству инцидентов в день (10000) и общему количеству хранящихся артефактов (3000000)	Решение поставляется бандлами с предустановленными опциями либо может быть сконфигурировано кастомно. Стоимость лицензии зависит от количества активов и интеграций, опция «multitenancy» лицензируется отдельно	Предусмотрены временные и бессрочные лицензии. Метрики лицензирования: 1)Перечень выбранных модулей 2)Количество конкурентных лицензий коннекторов для подключения к внешним системам 3)Режим функционирования (количество дополнительных нод) 4)Мультиарендность для MSSP провайдеров, холдингов, групп компаний. Других ограничительных метрик не предусмотрено. API не лицензируется и включен в любую поставку ПО.	Решение лицензируется по количеству настроенных сенсоров, с которых он собирает информацию. В качестве сенсора может выступать шлюз UserGate либо любое другое устройство, которое может отправлять информацию по протоколу SNMP на сервер LogAn
2.6. Опыт внедрений.	9 заказчиков	Нет данных		Нет данных	С 2013 года	Нет данных	Внедрения на ведущих предприятиях в крупнейших отраслях экономики. «Центр экспертизы R-Vision» сопровождает заказчика на каждом этапе проекта.	Опыт внедрения во многих отраслях экономики. Среди Заказчиков – Сбербанк России, Альфа-Банк, Тинькофф Банк, Норильский Никель, Северсталь, Евраз, X5 Group, Магнит, ФСО России, Совет Федерации, ФГУП Интеграл, Мегафон MSSP, Центр киберустойчивости Angara SOC, МТС, Первый Канал, Правительство Тюмени, Правительство Красноярска и другие.	
2.7. Наличие сертификатов регуляторов, присутствие в реестре российского ПО;	Сертификат соответствия ФСТЭК России № 4433 от 29.07.2021 (УД6, ТУ). Решение присутствует в реестре российского ПО	Не применимо	Не поддерживается	Не применимо	Присутствует в реестре российского ПО. Сертификат ФСТЭК России - в процессе получения, ориентировочный срок 2 кв. 2024 года.	Не применимо	Сертификат соответствия ФСТЭК России № 4346 от 22.12.2020 (УД4). Решение присутствует в реестре российского ПО	Сертификат соответствия ФСТЭК России № 4574 от 02.09.2022 (УД4). Сертификат соответствия ОАЦ при Президенте Республики Беларусь № BY/112 02.02. ТР027 036.01 00492 от 05 августа 2022 года (по требованиям технического регламента ТР	Сертификат ФСТЭК России № 3905. Решение присутствует в реестре российского ПО

								2013/027/BY). Решение присутствует в реестре российского ПО	
3. Управление киберинцидентами:									
3.1. Подготовка к реагированию на киберинциденты:									
3.1.1. Интеграции с СЗИ / источниками для получения данных о событиях / инцидентах ИБ: типы СЗИ / источников, количество интеграций, способы интеграции, импортируемые сущности, наличие двухсторонней связи;	MaxPatrol SIEM, RuSIEM, Ankey SIEM, Kuma, Symantec SIM, ArcSight, Alertix, FortiSIEM, MP SIEM, DATAPK, KSC, Efros CI, MaxPatrol 8, Ankey IDM, RedCheck, XSpider, Symantec DLP, Infowatch DLP, SearchInform DLP, UserGate, Zabbix, 10-strike, HPE Systems Insight Manager, VmWare vSphere, Checkpoint, Microsoft SCCM, HP Service Desk, AD, 1С. Общее количество готовых интеграций: более 50	Поддерживаются более 300 интеграций (внешние и внутренние решения и сервисы), возможность скачать интеграции из маркетплейса. Полный список cloud.google.com	С помощью PowerShell-скриптов, предоставляемых в решении, поддерживается сбор и анализ файлов (форматы docx, xlsx, pdf, evtx), событий в форматах json и evtx, мониторинг объектов Active Directory, мониторинг действий пользователя (снимки экрана, смена активного окна, журналирование клавиатурного ввода), сбор событий из журналов событий Windows с удаленных компьютеров с фильтрацией по типам событий (события входа, события MS SQL, удаленные подключения и т.д.), сбор данных с серверов MS Exchange (тема, тело email, служебные сообщения Exchange), сбор событий из БД СКУД RusGuard. Поддерживается полная интеграция с продуктом Makves DCAP (импорт инцидентов через API, реагирование через DCAP). Поддерживается встроенная обработка данных, собранных PowerShell-скриптами, с возможностью выявления риск-факторов пользователей (отсутствующий пароль, неизменный пароль и т.д.), риск-факторов компьютеров (версия ОС, неиспользуемый компьютер, данные о лицензиях и установленном ПО), риск-факторов почтовых ящиков Exchange (доступ других пользователей к почтовому ящику), нарушения правил обработки информации (путем анализа прав доступа к файлам)	Поддерживается за счет более 320 интеграций в маркетплейсе Azure	Основные интеграции: 1.Получение информации об инцидентах ИБ - интеграция с SIEM (MP SIEM, KUMA, ArcSight), интеграция с ГосСОПКА; 2. Обогащение инцидента ИБ по IoC - интеграция с TIP, AbuseIPDB, VirusTotal; 3. Автоматизированное реагирование: -прокси, МЭ (UserGate, VipNet, Check Point, FortiGate), - системы АВЗ (Kaspersky Security Center) -контролеры домена (MS Active Directory, FreeIPA, ALP Pro); - WAF (PT Application Firewall); - SandBox (PT SandBox); - SIEM (PT SIEM, KUMA); - системы электронной почты (Microsoft Exchange, ruPost) - TI-системы (Innostage TIP, MISP); - HTTP-запросы; -SSH- запросы (хосты Windows, Linux) - WinPsexec, WindowsRemote (хосты Linux) 4.Оповещение сотрудников/постановка задач - интеграция (коннектор) с Microsoft Exchange, Task Tracking (Atlassian Jira), Service Desk (HPSM, BPMSoft); 5. Инвентаризация: MS Active Directory, Kaspersky Security Center, MP SIEM, MP 8, MP VM, встроенный сканер, HPSM, интеграция с файлами: экспорт-импорт активов, Nmap. 6. Получение данных по уязвимостям: MP8, MP VM 7.Сбор данных по сотрудникам/аутентификация: Active Directory.	Интеграция с более чем 850 продуктами, включая SIEM-системы, система аутентификации, ведения заявок, базы данных, решения для защиты конечных точек и сетей, системы анализа ВПО, системы управления уязвимостями	Почтовые системы (протоколы IMAP, EWS), IBM QRadar, ArcSight ESM, Group-IB Bot-Trek Intelligence, Solar JSOC, Kaspersky Fraud Prevention, HP Service Manager, MP SIEM, McAfee ESM, FortiSIEM, Kaspersky Unified Monitoring and Analysis Platform (KUMA). Коннекторы активируются и настраиваются в решении в рамках реализации проекта. Есть режим двусторонней синхронизации статусов инцидента	200+ интеграций с системами различных классов Поддерживается интеграция с SIEM-системами MaxPatrol SIEM, Kaspersky KUMA, Pangeo RADAR, RuSIEM, NEURODAT SIEM, ArcSight SIEM, IBM QRadar, Splunk. Поддерживается интеграция со следующими СЗИ для получения событий ИБ - Kaspersky Security Center, InfoWatch, SearchInform, PaloALto Panorama, Positive Technologies Application Firewall, UserGate, VipNet IDS, ViPNet TIAS, COB Континент, Microsoft Security Essentials, Secret Net Studio. Поддерживается интеграция со следующими системами для получения информации об инцидентах и событиях– электронная почта, OTRS, Naumen, Creatio BPM. Поддерживается интеграция с MSSP провайдерами – Solar JSOC, Angara SOC, Megafon MSSP, Infosecurity SOC и др. Возможна интеграция как по инцидентам, так и по событиям с систем первоисточников, по которым зарегистрирован инцидент. Поддерживается двусторонняя интеграция с синхронизацией статуса.	Поддерживается интеграция с МЭ UserGate, конечными устройствами UserGate Client (ОС Windows), сенсорами WMI, сторонними сетевыми устройствами, поддерживающими передачу данных по протоколу SNMP
								Поддержка протоколов и механизмов REST API, HTTP / HTTPS, RPC, SNMP, SSH, LDAP, WMI, DNS, EWS (Exchange Web Services), SMTP, POP3, IMAP, Syslog.	

3.1.2. Поддержка и кастомизация механизмов интеграции с СЗИ (поддерживаемые протоколы, методы);	Адаптеры для интеграции с внешними системами: XML, MS Excel, CSV, SOAP, Oracle Data Provider, Npgsql, ODBC, OLEDB, LDAP, HTTP REST, REST API, SSH, SNMP. Коннекторы для доступа к СУБД MS SQL, MySQL, PostgreSQL. Поддержка интерпретаторов Python, PowerShell, cmd		WinRM, syslog, HTTP, LDAP, SMB	Поддержка syslog, CEF, API, DB2, FTP, HTTP, MQ, SFTP, SMTP, SQL, XML, файлы, интеграция с агентом Log Analytics agent	Встроенный конструктор коннекторов (подсистема Оркестрации), возможность кастомной настройки коннекторов к целевым системам	API, SSH, подключение к СУБД (MSSQL, MySQL, Oracle, PostgreSQL), IMAP, syslog	Кастомизация поддерживается, механизмы PowerShell/CMD, LDAP, MSSQL, MySQL, OracleDB, PostreSQL, REST API, SNMP, SOAP, SSH, Python, возможность использования регулярных выражений, переменных	Поддерживается возможность парсинга машиночитаемых файлов любого объема (в том числе в ZIP-архивах), размещенных локально, на SMB или SFTP ресурсах. Поддерживается удаленное подключение к Windows Event Log, получение и отправка сообщений в очередь Apache Kafka, подключение к СУБД (MSSQL, MySQL, Oracle, PostgreSQL). Поддерживается выполнение команд через интерпретаторы CMD, Bash, Shell, Java, JavaScript, PowerShell, Python. Поддержка регулярных выражений, переменных, формул и обработки данных в нескольких шагов	Поддерживается интеграция по SNPM, WMI, SSH, HTTP, HTTPS, syslog, API
3.1.3. Наличие агентного / безагентного метода сбора данных о событиях / инцидентах ИБ;	Поддерживается безагентный, агентный способ с шифрованием конфиденциальных данных	Поддержка агента Remote Agent для работы с удаленными площадками	Поддерживается использование агентов сбора данных для инспекции файлов, evtx-файлов, событий журнала Windows, данных Active Directory, LDAP (события служб с контроллера домена), Exchange-серверов.	Использование Log Analytics agent для сбора событий с Windows, Linux устройств. Интеграция с MS Defender для сбора событий с Windows, Linux, MacOS устройств	Безагенсткий метод сбора данных через API	Используется безагентный метод, но есть агент TS Agent для учета пользователей терминальных серверов Windows	Да, безагентный метод сбора данных либо сбор с помощью агента в рамках экосистемы продуктов R-Vision EVO	Поддерживается. Безагентный способ, удаленное подключение к Linux, Windows, сетевым устройствам с помощью протоколов и механизмов REST API, HTTP / HTTPS, WinRM, RPC, SNMP, SSH, LDAP, WMI, подключения к СУБД (MSSQL, MySQL, Oracle, PostgreSQL). Возможность установки агента для сбора и получения данных	Поддерживается работа с агентом для конечных устройств UserGate Client (ОС Windows) и безагентный метод сбора данных
3.1.4. Источники обогащения инцидентов: типы СЗИ / источников, количество интеграций;	Доступны 45+ интеграций. Поддерживаются все типы систем, в том числе CMDB, SIEM	Поддерживаются более 300 интеграций (внешние и внутренние решения и сервисы), возможность скачать интеграции из маркетплейса	Active Directory, MS Exchange, Makves DCAP	Поддерживается за счет более 320 интеграций в маркетплейсе Azure	Источники обогащения инцидентов ИБ: CMDB, TIP, AbuseIPDB, Virus Total, сканер уязвимостей, Sandbox, встроенный сканер для обогашения инвентаризационной информации	Поддерживается обогащение данных по артефактам и индикаторам с помощью встроенного модуля DBot (используются внешние TI-источники, данные MITRE ATT&CK, внешние	Данные об активах: AD, Forcepoint TRITON AP-DATA, Kaspersky Security Center, MS SCCM, SecretNet, Symantec EPM, MaxPatrol, XSpider, Nessus, Tenable.sc, Qualys, Rapid7 Nexpose, RedCheck, InfoWatch Device Monitor, McAfee ePolicy Orchestrator, MP SIEM, Zabbix, сервис «Антифишинг», HP Service Manager, Naumen Service Desk, Micro Focus UCMDB, VMware, Skybox, интеграции с базами данных MS SQL/MySQL/Oracle/PostgeSQL, R-Vision Endpoint, универсальный коннектор Python.	Аналитические сервисы: · ChatGPT · MITRE ATT&CK · AbuseIPDB · cleantalk.org · ipgeolocation.io · IPInfo.io · Kali tools · KasperskyOpenTip · Kaspersky Threats · MaxMind Geo-IP · MXToolBox · WhoISIQ (IP) · Shodan (API) · urlscan.io · VirusTotal · IP-Geolocation (HTTP) · IP-Netblocks (HTTP) ·WhoIsHistory (WhoIsXMLAPI, HTTP) · WhoIs (WhoIsXMLAPI, HTTP) · AttackerKB · NVD · OpenCVE · VulDB · Vulners CMDB-системы: · iTop · HP uCMDB Инфраструктура: ·Конечные узлы под	Поддерживаются МЭ UserGate, конечные устройства UserGate Client (ОС Windows)

						песочницы и т.д.)	Данные о задачах: HP Service Manager, Naumen Service Desk. Данные об уязвимостях: MaxPatrol, XSpider, OpenVAS, Nessus, Vulners.com. Коннекторы активируются и настраиваются в решении в рамках реализации проекта	ОС Microsoft Windows ·Конечные узлы под управлением *nix подобных ОС · Сетевые устройства · Active Directory · Open LDAP · Zabbix · Microsoft Exchange СЗИ: · Group-IB DRP · MISP ·Kaspersky Security Center · Symantec Endpoint Protection Manager · Efros Config Inspector · Palo Alto · PT NAD · Elasticsearch · TrendMicro IMSVA Описанные коннекторы поставляются в составе модуля	
3.1.5. Отображение исходных событий/инцидента ИБ в формате источника;	Через обращение к источнику инцидента (например, SIEM-системе) из интерфейса решения (кнопка "Ссылка на источник")	Поддерживается	Только для продукта Makves DCAP	Поддерживается	Есть, отображение в карточке корреляционного события SIEM и его параметров	Поддерживается	Поддерживается, зависит от источника и настроенного маппинга свойств	Поддерживается, с возможностью просмотра и поиска информации	Не поддерживается
3.1.6. Приоритизация инцидентов ИБ, наличие и кастомизация формулы расчета критичности инцидента ИБ;	Приоритизация в ручном режиме	Поддерживается ручная и автоматическая приоритизация (один из 5 уровней приоритета) для предупреждений (alert), кейсов (сгруппированные предупреждения) и инцидентов (подтвержденные кейсы).	Приоритизация выполняется вручную либо по данным от Makves DCAP	Поддерживается установка одного из 3 уровней критичности инцидента (вручную или в соответствии с правилами выявления угроз)	Имеется приоритезация инцидентов ИБ	Поддерживается автоматическая приоритизация (в зависимости от критичности, установленной интегрированной СЗИ, наличием индикаторов и артефактов вредоносной активности, свойств затронутых инцидентом сущностей), поддерживается установка приоритета вручную	Кастомизируемая приоритизация на основе значений свойств карточки инцидента	Поддерживается ручная и автоматическая приоритизация, с поддержкой пользовательских алгоритмов расчета приоритета (учет свойств затронутых активов и пользователей, параметров инцидента, наличия обнаруженных индикаторов компрометации, уязвимостей и т.д.)	Поддерживается настройка уровня угрозы, приоритета, категории с помощью правил аналитики
3.1.7. Реализация автоматизированного триажа инцидентов, правила автоматической аналитики для ложноположительных инцидентов ИБ;	Автоматическая обработка предусмотрена для подозрений на инциденты, загруженных с помощью импорта из подключенных внешних систем мониторинга. В результате данной обработки подозрение на инцидент может быть переведено в статус "ложное срабатывание".	Поддерживается аналитика ложноположительных срабатываний за счет интеграции с платформой Google Cloud Vertex AI	Не поддерживается	Поддерживается создание временных исключений (24 часа) для ложноположительных срабатываний, поддерживается настройка исключений в правилах выявлений угроз	Аналитики для ложноположительных инцидентов ИБ на текущий момент нет	Поддерживается автоматическая проверка ложноположительных событий с помощью встроенных сценариев	Поддерживается	Поддержка триажа на основе белых списков активов и email, а также классификация инцидентов, в том числе с автоматическим определением тактик, техник, субтехник по матрице MITRE ATT&CK, поддержка классификации более 250 типов инцидентов и событий ИБ «из коробки». Настройка признаков отнесения инцидентов к ложноположительным срабатываниям	Не поддерживается
3.1.8. Наличие механизма «белых списков» для упрощения триажа инцидентов и автоматического определения ложноположительных инцидентов ИБ;	Поддерживается	Поддерживается снижение уровня ложноположительных срабатываний за счет интеграции с платформой Google Cloud Vertex AI	Не поддерживается	Поддерживается через функционал создания «watchlists»	Не поддерживается	Поддерживается, с автоматическим и ручным пополнением списков	Поддерживается работа с произвольными «белыми списками» в сценариях и конструкторе коннекторов	Поддерживается создание «белых списков» для настройки исключений, с использованием составляемых списков в переобучении моделей машинного обучения	Поддерживается внесение URL в «белый список», в том числе по запросу пользователя
								Поддерживается «из коробки» 80+ динамических	

3.1.9. Наличие и количество сценариев реагирования (плейбуков) «из коробки»;	Поддерживается	Нет данных	Нет данных	Поддерживается с помощью функционала Azure Logic Apps с возможностью использования более 2100 действий и коннекторов к различным приложениям из маркетплейса (полный объем доступных коннекторов определяется уровнем подписки на сервисы)	Есть, более 20 сценариев реагирования (плейбуков) «из коробки»	Более 1200 сценариев в маркетплейсе вендора, могут быть установлены без ограничений	Плейбуки разрабатываются под инфраструктуру заказчика, они могут быть собраны из предзаданных скриптов реагирования на этапе внедрения (70 встроенных скриптов). Скрипты можно запускать через агент или с помощью удаленного подключения к целевой системе, скрипты можно запускать по расписанию, автоматически и вручную	сценариев, автоматически выстраиваемыми системой с учетом инфраструктуры, типов событий и атрибутов, тактик и техник атак, встроенной экспертизы (экспертные рекомендации вендора по классификации, обогащению, сдерживанию и реагированию). Встроенных скриптов реагирования – 130+, встроенных плейбуков обогащения и классификации – 60+	Правила аналитики поставляются по подписке
3.1.10. Поддержка настройки сценариев реагирования в графическом редакторе;	Да, включая разработку и настройку скриптов реагирования в интерфейсе решения	Поддерживается	Не поддерживается	Поддерживается	Есть графический редактор создания сценариев реагирования	Поддерживается	Да, включая разработку и настройку скриптов реагирования в интерфейсе решения	Поддерживается разработка сценариев реагирования в графическом редакторе в виде интерактивных блок-схем с применением подхода low-code / no-code, с отображением прохождения этапов реагирования на графической блок-схеме сценария, с возможностью интерактивного управления работой сценариев, контроля их состояния	Поддерживается создание правил аналитики, действий реагирования, схем инцидентов в веб-интерфейсе
3.1.11. Поддержка настройки выполняемых действий с применением подхода low-code / no-code;	Графический конструктор выполнения логических действий и скриптов реагирования с условиями выполнения	Поддерживается	Не поддерживается	Поддерживается	Есть конструктор сценариев реагирования	Поддерживается	Поддерживается возможность создавать собственные действия с помощью low-code на базе конструктора коннекторов.	Поддерживается настройка выполнения сценариев реагирования и действий по реагированию в графическом редакторе блок-схем с применением подхода low-code / no-code, с ветвлениями и настройкой сложных условий выполнения активных действий по реагированию, с выполнением математических, логических, текстовых, операций, а также операций с массивами	Не поддерживается
3.1.12. Интеграции с СЗИ/источниками для выполнения реагирования на инцидент: типы СЗИ/источников, количество	Доступны 45+ интеграций	Поддерживаются более 300 интеграций (внешние и внутренние решения и сервисы),	Выполнение действий в инфраструктуре с помощью предустановленных и	Поддерживается за счет более 320 интеграций в	Есть, кол-во интеграций - более 20. Кол-во действий - более 45	Поддерживается интеграция с несколькими сотнями источников для	Поддерживается интеграция для реагирования с произвольными источниками, в том числе с использованием универсального коннектора Python. Коннекторы	100+ СЗИ, 100+ действий, инструментов реагирования ITSM-системы: · Jira · Naumen SD · OTRS · BPM Online (Creatio) Инфраструктура: ·Конечные узлы под управлением семейства ОС Microsoft Windows · Конечные узлы под управлением *nix подобных ОС · Сетевые устройства · Active Directory · Open LDAP · Zabbix · Microsoft Exchange · Veeam Backup	Поддерживаются действия по реагированию: отправка email (по протоколу SMTP, поддерживается создание шаблонов оповещений с переменными), отправка уведомления в мессенджеры (по

интеграций, количество действий по реагированию;		возможность скачать интеграции из маркетплейса	кастомизируемых PowerShell-скриптов	маркетплейсе Azure		выполнения действий по реагированию	активируются и настраиваются в решении в рамках реализации проекта	СЗИ: · Check Point · Cisco ASA · Cisco Firepower · Cisco Switch · Juniper · Fortigate ·Kaspersky Security Center · Microsoft Defender · TrendMicro DDA · KATA · Kaspersky OpenTIP · PT Sandbox · FireEye ·Symantec Endpoint Protection Manager · Palo Alto · TrendMicro IMSVA Коннекторы поставляются в составе коробки	протоколу SMPP), создание webhook (получение уведомления о срабатывании правила на веб-странице)
3.1.13. Ведение журнала аудита, отображение истории выполненных действий по сдерживанию/реагированию;	История запусков сценариев из раздела мониторинга выполнения (административный режим) с отображением лога работы с датой и временем, сообщений об ошибках, входных и выходных параметров. Карточка инцидента содержит вкладку "История изменений", в которой сохраняется информация о назначении ответственного, смене статуса инцидента и формировании отчета.	Поддерживается	Ведение истории по инциденту (вкладка «Активность») с указанием выполненных действий, внесенных изменений и их авторов	Поддерживается	Есть, в журнале и в карточке инцидента ИБ отображается вся информация по выполненным действиям оператора в рамках сдерживания/реагирования, а именно информацию по запущенным скриптам реагирования и результатам данного реагирования, информация от внешних пользователей (в случае постановки задач внешнему пользователю), выполненные действия оператора в соответствии со сценарием реагирования на инцидент ИБ. Вся информация сохраняется в карточке инцидента ИБ в том числе после закрытия данного инцидента ИБ.	Поддерживается просмотр истории инцидента и действий по реагированию в интерфейсе War room	Журналирование работы с инцидентами, активами, документами, защитными мерами, аудитами, проверками, киберрисками, задачами. Журналируются действия пользователей (аутентификация, изменение прав доступа), изменения настроек решения. Просмотр в интерфейсе системы, в БД, поддержка ротации журналов, отправка журналов по syslog	Поддерживается ведение журнала аудита с возможностью экспорта записей аудита, с контролем отсутствия сохранения конфиденциальной информации в журнале (например, паролей). Для всех выполняемых в рамках сценария действий ведется запись в журнал аудита с указанием времени, наименования события, объекта действия, имени пользователя.	Поддерживается ведение истории внесения изменений в инцидент (добавление наблюдателей, изменение статуса рабочего процесса, комментарии и т.д.) в разделе «Активность» в карточке инцидента
3.1.14. Возможность отмены действия по сдерживанию/реагированию независимо от того, как действие было выполнено (вручную, автоматизировано, автоматически);	Возможна реализация через плейбуки	Поддерживается выполнение отмены действий вручную	Не поддерживается	Не поддерживается	Есть возможность отмены действия по сдерживанию/реагированию через подсистему Оркестрации (блокировка/разблокировка учетной записи, IP и т.д.)	Поддерживается выполнение отмены действий вручную	Поддерживается возможность настройки пары «действие для реагирования / действие для отката» в случаях, когда это возможно	Поддерживается отмена выполнения действия (применения обратного действия) с возвратом объекта воздействия в исходное состояние	Не поддерживается
3.1.15. Типы инфраструктурных элементов (объектов), с которыми реализовано реагирование (хост, учетная запись и т.д.);	Хост (рабочая станция, АРМ), объект AD (Учетная запись), межсетевой экран, шлюз, IDS/IPS, NTA, антивирусное ПО, почтовый сервер, техническое средство (физический сервер, виртуальный сервер)	Все поддерживаемые в интеграциях элементы: устройства, учетные записи, данные, файлы, конфигурации	Пользователь (доменная / локальная учетная запись Windows), устройство (компьютер на базе Windows)	Поддерживаются устройства, учетные записи, приложения (облачные), IP-адреса, файлы, процессы, ресурсы Azure, email	Типы инфраструктурных элементов (объектов), с которыми реализовано реагирование: хост с ОС семейства Windows и Linux, учетные записи, активное сетевое оборудование, межсетевые экраны, иные средства защиты информации	Все поддерживаемые в интеграциях элементы: устройства, учетные записи, файлы, IP-адреса	Поддерживаются произвольные объекты, включая хост, учетную запись, файл, процесс и т.п. Поддерживается безагентное выполнение команд либо с использованием агента в рамках экосистемы R-Vision EVO	Поддерживается взаимодействие с ресурсно-сервисной моделью (в том числе кастомными типами объектов, которые предоставляются инфраструктурой и интегрированными системами): продукты, бизнес-процессы, информационные системы, приложения, ПО, СЗИ, технологическое оборудование, ИТ-активы, учетные записи, устройства, процессы, почтовые адреса, уязвимости, внешний хост, вредоносное ПО и т.д.	Устройство, учетная запись
3.1.16. Наличие массовых операций над инцидентами / отфильтрованным наборам			Поддерживаются	Поддерживается выполнение массовых	Имеется возможность работы с группой инцидентов ИБ одновременно (назначение на группу инцидентов ИБ статус "дочерние" и выбор из данных инцидентов ИБ "родительский"	Поддерживается выполнение массовых		Поддерживается фильтрация и сортировка инцидентов, выполнение автоматических и ручных массовых операций над	

инцидентов ручным или автоматическим способом, по расписанию;	Поддерживается	Поддерживается	ручные массовые операции	операций вручную и в соответствии с правилами	инцидент ИБ. Дальнейшие действия можно проводить с одним "родительским" инцидентом ИБ, все действия будет транслироваться на "дочерние" инциденты ИБ.	операций вручную, по расписанию, автоматически	Поддерживается	сформированным списком или выбранными инцидентами. Возможность создания пользовательского действия для массовой операции	Поддерживается
3.1.17. Возможность работы с объектами инцидента (в том числе выполнения действий по анализу и реагированию) в табличном представлении;	Полноценная работа с инцидентами ведется при открытии полной карточки инцидента. В табличном представлении осуществляется поиск и отбор инцидентов (по статусу)	Поддерживается	Поддерживается	Поддерживается	Поддерживается	Поддерживается	Поддерживается	Поддерживается работа с записями об инцидентах в табличном виде, с выполнением действий из табличного представления без необходимости перехода в карточку инцидента	Поддерживается просмотр инцидентов в табличном представлении
3.1.18. Экспертные рекомендации по первичному и расширенному анализу, сдерживанию, реагированию, восстановлению и пост-инцидентному анализу в соответствии с техникой атаки / инцидента ИБ;	Пакеты экспертизы поставляются в обновлениях решения	Поддерживается за счет интеграции с сервисом анализ киберугроз Mandiant, за счет использования технологии «Duet AI» (на базе машинного обучения и искусственного интеллекта) с рекомендациями аналитикам на основе обработанной информации	Предустановленные рекомендации (инструкции) по реагированию на типовые инциденты с возможностью добавления пользовательских инструкций	Поддерживается с использованием Azure OpenAI Service	Имеется возможность получать аналитику и рекомендации от Innostage SOC CyberART	Поддерживается за счет информации в пакетах содержимого и рекомендаций от Unit42 (центр киберэкспертизы Palo Alto)	Поддерживается в рамках предоставления лучших практик от команды «Центра экспертизы» вендора	Поддерживается с помощью пакета внутренней экспертизы, встроенного в решение, с учётом реализованных техник по матрице MITRE ATT&CK по каждому инциденту. Есть возможность включить экспертные рекомендации от ChatGPT	Не поддерживается
3.1.19. Типы сущностей, с которыми реализована связь инцидента ИБ/атаки (хост, учетная запись, уязвимость и т.д.);	Технические средства (с различными подтипами), программное обеспечение (с различными подтипами), средства защиты информации (как ПО, так и техническое средство), информационные системы (как совокупность ПО и/или технических средств)	Связь инцидентов с активами (устройства, учетные записи), индикаторами, артефактами, уязвимостями	Учетная запись (пользователь Windows), устройство (компьютер или сервер Windows), файл, почтовый ящик MS Exchange	Поддерживаются устройства, учетные записи, приложения (облачные), данные, IP-адреса, DNS-имена, файлы, процессы, ресурсы Azure, хэш, ключ и ветка реестра, email	Структурное подразделение, рабочая группа, хост, учетная запись, сотрудник, уязвимость, информационные/автоматизированные системы, IoC	Связь инцидентов с активами (устройства, учетные записи), артефактами, IoC / IoA	Хост, учетная запись, бизнес-процесс, категория информации, кастомные объекты, настраиваемые пользователем.	Поддерживается формирование (с отображением на графе, табличном представлении и дриллдауном) связей между всеми внутренними объектами, использующимися в решении (внешний хост, почтовые адреса, ИТ-актив, учетная запись, инцидент, уязвимость, вредоносное ПО, СЗИ, процесс, URL и т.д.)	Устройство, учетная запись
3.1.20. Настройка сценариев реагирования в соответствии с процессами управления киберинцидентами (ролевая модель разграничения полномочий в соответствии с организационной структурой команды реагирования, настройка метрик SLA / SLO / KPI, выполнение автоматических	Ролевая модель разграничения полномочий предустановлена в решении без возможности кастомизации. Предустановлены роли: Руководитель SOC, Руководитель направления (Клиент), Аналитик 1 / 2 / 3 линии, Администратор решения. Настройка норм	Поддерживается адаптация сценариев реагирования под конкретную инфраструктуру и процессы, ролевая модель адаптирована под SOC-центры и использование MSS-провайдерами,	Установка ролей пользователей для каждого инцидента (автор, исполнитель,	Поддерживается гибкая настройка сценариев, ведение статистики по количеству инцидентов, времени анализа и закрытия,	Возможности в рамках настройки сценариев реагирования: -ролевая модель разграничения полномочий в соответствии с организационной структурой команды реагирования (гибко настраиваемая ролевая модель позволяет разграничивать полномочия сотрудников в зависимости от юр. лица, структурного подразделения и функциональных обязанностей конкретного сотрудника (оператора), - настройка метрик SLA / SLO / KPI (настройка времени реагирования и выполнения задач в соответствии с критичностью инцидента ИБ), -выполнение автоматических действий в зависимости от наступления организационно определенных условий (настройка автоматизированного реагирования в	Поддерживается создание гибкой ролевой модели с разграничением доступа к данным, сценариям, скриптам, конфигурации, определенным разделам, определенным потенциально опасным действиям по реагированию. Поддерживается ведение графика дежурных смен, возможность установить статус	Поддерживается возможность настройки и кастомизации процессов реагирования для соответствия внутренним процессам. Поддерживается задание SLA, возможность построения графиков по критериям соблюдения SLA. Возможность настройки ролей пользователей для разграничения доступа к различным разделам и операциям в системе, включая	Поддерживается «из коробки» ролевая модель SOC-центра, типового департамента ИБ, отдела ИБ (аналитик L1 / L2 / L3, аудитор, администратор SOAR, аналитик, руководитель группы и т.д.), поддерживается создание пользовательских ролей. Каждая роль содержит настройки доступа к представлениям разделов, объектам, меню, справочникам, отчетам, содержит разрешения на работу со свойствами объектов, шаблонами сценариев, коннекторами и т.д. Поддерживается учет рабочего графика (календаря) сотрудников и членов дежурных смен. Поддерживается	Поддерживается создание схем инцидентов с описанием типов инцидентов, способов решения инцидентов, состояний инцидентов (открыто, в работе,

действий в зависимости от наступления организационно определенных условий, выполнение ручных действий в зависимости от функциональных обязанностей члена команды реагирования, выполнение организационно определенных действий по коммуникации и эскалации);	SLA, контроль выполнения SLA (в том числе на виджетах). Возможность дополнительной настройки и кастомизации процессов реагирования ограничена предустановленными и неизменяемыми ролями пользователей решения	контроль выполнения метрик SOC-центра (SLA, время на выполнение определенных действий, загруженность аналитиков, статистика работы SOC-центра)	наблюдатель), установка срока расследования для каждого инцидента	разбивка инцидентов по создателю, критичности, тактике. Поддерживается настройка процессов эскалации и коммуникации.	зависимости от выполненных проверок, например IoC), -выполнение ручных действий в зависимости от функциональных обязанностей члена команды реагирования (возможность настройки сквозных сценариев реагирования между сотрудниками разных рабочих групп, постановка задач внешним сотрудникам, не являющимися операторами Системы и т.д.), - выполнение организационно определенных действий по коммуникации и эскалации (возможность постановки задач и переназначение инцидента ИБ целиком в рамках одного сценария реагирования, эскалация задач путем формирования тикета в системе Task Tracking\ Service Desk)	«Отошел» для аналитика SOC, автоматическое назначение инцидента на аналитика (в зависимости от графика дежурств, загруженности, с возможностью использовать скрипты автоназначения). Поддерживается выполнение действий по управлению инцидентами в соответствии с матрицами эскалации, коммуникации	механизм разграничения доступа для настройки видимости инцидентов на разных стадиях воркфлоу для разных исполнителей. Возможность кастомизировать отображения карточки инцидента в зависимости от его содержимого и роли пользователя, который с ним работает, включая размещение в карточке кнопок для запуска тех или иных плейбуков	задание SLA-метрик для выполнения каждого действия в рамках сценария реагирования, в зависимости от свойств инцидента, связанного актива, иного объекта (например, критичность инцидента, категория актива, уровень доступа атакованного пользователя). Поддерживается формирование матриц коммуникации и эскалации в сценариях реагирования (рабочих процессах), с указанием условий перехода по разным уровням коммуникации и эскалации. Выполнение координации действий, коммуникация и эскалация происходит в специально отведенном пространстве war room	закрыто). Поддерживается создание нескольких схем расследования инцидентов, но активной может быть только одна
3.1.21. Отображение последовательности обнаружения инцидентов, связанных в контексте одной атаки;	Не поддерживается	Поддерживается отображение графа атаки (в виде кейса как совокупности связанных предупреждений) с возможностью просмотра всех связанных сущностей	Не поддерживается	Поддерживается, с отображением на графе связей	Не поддерживается	Поддерживается возможность дедупликации инцидентов, возможность связывания инцидентов вручную и автоматически с помощью правил предобработки инцидентов (pre-process rule) и методов машинного обучения	Поддерживается возможность связывания инцидентов, настраиваемые типы связей	Поддерживается выстраивание инцидентов в цепочку и формирование объекта атаки. Инциденты связываются автоматически по ключевым атрибутам и объектам: IP адреса / имена атакующих и скомпрометированных узлов, скомпрометированные учетные записи, уязвимости на хостах, хакерский инструментарий, ВПО. За счет дополнительного сбора сырых данных с источника: сетевой связности, сессий, аутентификации и т.д. Автоматическое построение kill chain атаки. Визуализация на временной шкале (timeline) инцидентов, связанных в атаку в автоматическом или ручном режиме	Не поддерживается
3.1.22. Поддержка способов оценки и визуализации состояния процесса управления	Виджеты (столбчатые диаграммы, графики, отображение текстовой информации), отображение статистической информации в табличном виде. Отображение статистики в разрезе объектов и субъектов	Поддерживаются дашборды с виджетами (диаграммы, таблицы), на дашборде может быть до 12 виджетов. Поддерживается формирование отчетности по работе и метрикам SOC-центра (SLA, время на выполнение определенных действий, загруженность аналитиков, статистика работы	Дашборд с отображением линейных, столбчатых, круговых диаграмм, графиков, таблиц с отображением информации по пользователям и устройствам, с	Поддерживаются дашборды, отчеты, метрики работы с	Есть, поддерживаются метрики, отчетность, дашборды	Поддержка визуализации информации на настраиваемых пользователем дашбордах, отображение информации по SLA, инцидентам, статистика реагирования, данные по TI-фидам, тепловая карта используемых атакующими TTPs по матрице MITRE ATT&CK. Поддерживается возможность создавать пользовательские виджеты для добавления на	Реализуется средствами конструктора графиков, конструктора отчетов, настройкой кастомизируемых дашбордов. Так же	Поддерживается визуализация информации об инцидентах как на большом количестве преднастроенных из коробки отчетах и дашбордах, так и с помощью конструктора (типы виджетов для настройки: линейный график, столбчатая диаграмма, круговая	Поддерживается визуализация на дашборде, с отображением нескольких виджетов. Поддержка создания и кастомизации виджетов с настройкой количества записей, группировки, формата отображения – число, диаграмма, гистограмма, таблица, график, карта мира. Поддерживается SQL-запросы для выборки данных для отображения, поддерживается

отчетность, дашборды).	отчетов автоматически и вручную (отчеты по инцидентам, квартальные отчеты по деятельности мониторинга и реагирования)	финансовым показателям (показатель ROI использования решения). Поддерживается формирование отчетов в PDF, DOCX. Поддерживается формирование отчетов вручную и по расписанию, отправка по email.	статистики в разрезе типов инцидентов, их состояния, назначенных ответственных			виды диаграмм и графиков, выполнение скриптов и запросов для визуализации данных). Поддерживается создание отчетов вручную, из виджетов, из перечня предустановленных шаблонов. Поддерживается формирование отчетов по расписанию, отправка по email, выгрузка в форматах PDF, CSV	преднастроенных дашбордов, виджетов, отчетов)	таблица, радар, географическая карта, глобус, графы связей, временные шкалы (timeline), цепочки (killchain). Поддерживаются форматы docx, cvs, pdf, xlsx, ods, odt, txt	которого будут визуализированы. Поддерживается формирование отчетов в форматах PDF, HTML, CSV, создание пользовательских шаблонов отчетов, формирование отчетов вручную и по расписанию, отправка отчетов по email
3.2. Выявление, анализ киберинцидентов:									
3.2.1. Поддержка и кастомизация совместной работы аналитиков в интерфейсе решения (чаты по инцидентам, обмен информацией по инцидентам, передача инцидентов между аналитиками), поддержка ChatOps-взаимодействия;	Чат с клиентом (отправка сообщения по email)	Поддерживается интеграция с мессенджерами (Slack, MS Teams, Google Chat за счет интеграций), поддерживается отправка уведомлений пользователям в самом решении (например, при работе с кейсом заказчика в случае MSSP)	Поддерживается совместная работа в карточке инцидента (создание комментариев, изменение данных инцидента)	Поддерживается работа аналитиков по инциденту в карточке инцидента, в мессенджере MS Teams с отправкой уведомлений, обсуждением, действиями по инциденту	Имеется поддержка совместной работы аналитиков в интерфейсе Системы: чаты, лента сообщений в карточках объектов, возможность подписаться на изменения карточек объектов, возможность эскалации/переназначения инцидента	Поддерживаются чаты в «War room» (пространство для совместной работы аналитиков над инцидентом), поддерживается работа над инцидентами в мессенджере Slack с помощью встроенного модуля DBot	Встроенный чат по инциденту с возможностью упоминания пользователей системы и быстрого подключения к работе над инцидентом новых аналитиков, возможность передачи инцидентов между аналитиками как посредством назначения ответственного, так и распределения инцидентов между аналитиками заданной линии на основании показателя нагрузки.	Поддерживается совместная работа аналитиков SOC над инцидентом во внутреннем чате по инциденту с возможностью приложить файл (артефакт) , цифровые свидетельства по инциденту. Поддерживается возможность отправки оповещений по изменению инцидента в Telegram, в корпоративные мессенджеры (Synapse, MatterMost и т.д.) с возможностью работы с инцидентом напрямую из мессенджера (смена статуса, внесение комментариев, передача между аналитиками и т.д.). Передача инцидента между аналитиками может быть реализована в автоматическом режиме (при выполнении заранее заданных условий при настройке сценария реагирования) или вручную, с поддержкой разграничения прав доступа и ограничения видимости определенных полей и их значений в карточке инцидента. Возможность автоматического назначения аналитика на основании атрибутов в карточке инцидента и с учетом балансировки нагрузки. Возможность взаимодействия с нейронными сетями (ChatGPT и аналоги) в процессе расследования	Поддерживается возможность ручного назначения и переназначения ответственного за инцидент, добавление наблюдателей за инцидентом (с отправкой им оповещений об изменении инцидента), возможность устанавливать приоритет инцидента, комментировать инцидент, прикреплять вложения (файлы), добавлять дополнительную обогащающую информацию по инциденту (на вкладке «Улики», с указанием типа улики, типа атаки, TLP-маркера, признака принадлежности объекта к потенциальному индикатору компрометации)
								Поддерживается в виде внутреннего чата по инциденту с отображением событий решения (выполнение действий	

3.2.2. Наличие «war room» или пространства для коммуникаций по инциденту между всеми участниками расследования;	Совместное обсуждение в карточке инцидента, задачи	Поддерживается	Совместное обсуждение в карточке инцидента	Поддерживается	Есть, чат для коммуникаций по инциденту ИБ между всеми участниками расследования	Поддерживается, с возможностью планирования работ, ведением перечня задач по расследованию, прикреплением файлов со свидетельствами	Поддерживается в виде внутреннего чата по инциденту с отображением событий решений и передачи артефактов друг другу	коннекторами, изменение свойств инцидента) и отображением комментариев аналитиков SOC, с возможностью создания задач по инциденту напрямую в решении (с контролем исполнения) и заявок во внешних ServiceDesk-системах. Поддерживается возможность отправки оповещений по изменению инцидента в Telegram, в корпоративные мессенджеры (Synapse, MatterMost и т.д.) с возможностью работы с инцидентом напрямую из мессенджера (смена статуса, внесение комментариев, передача между аналитиками и т.д.). В war room можно взаимодействовать с ChatGPT	Не поддерживается
3.2.3. Возможность совместной многопользовательской работы над атакой или выстроенной цепочкой инцидентов;	Поддерживается совместная работа над подозрением на инцидент и с инцидентом, в соответствии с ролевой моделью	Поддерживается	Не поддерживается, частично реализовано для единичных инцидентов	Поддерживается	Есть, совместная работа над инцидентом ИБ разными линиями SOC в рамках единого сценария реагирования	Поддерживается	Поддерживается	Поддерживается ведение совместной многопользовательской работы из карточек по инциденту, в чатах по инцидентам, поддерживается работа разных пользователей над разными инцидентами в контексте одной атаки	Не поддерживается
3.2.4. Наличие, функционал, кастомизация средств отправки оповещений об инцидентах (электронная почта, мессенджеры и т.д.);	Телеграм-бот, email	Поддерживается отправка email, отправка уведомлений в мессенджеры Slack, MS Teams, Google Chat за счет интеграций, отправка СМС через сервис Twilio	Отправка уведомлений по email, в мессенджеры Telegram, Slack, внутренние оповещения в веб-интерфейсе	Поддерживается отправка оповещений по email, MS Teams, Slack, Discord, Telegram, отправка SMS оповещений	Имеется интеграция с Microsoft Exchange, системами Task Tracking\ Service Desk для отправки оповещений об инцидентах ИБ, постановки задач. Наличие встроенного в систему функционала: чаты, лента сообщений в карточках объектов, возможность подписаться на изменения карточек объектов.	Поддерживается отправка уведомлений через email, в мессенджерах Slack, MS Teams, Discord, Telegram	Поддерживается интеграция с Service Desk (Naumen, Jira), почтовыми системами на базе MS Exchange и другими продуктами, использующими протоколы IMAP, SMTP	Поддерживается возможность отправки оповещений по изменению инцидента в Telegram, в корпоративные мессенджеры (Synapse, MatterMost и т.д.), в ServiceDesk-системы (Jira, Naumen Service Desk, MicroFocus Service Manager (HP Service Manager), BPM Online (Creatio)), в почтовые системы (на базе MS Exchange или любых других с использованием протоколов IMAP, SMTP) с возможностью работы с инцидентом напрямую из мессенджера (смена статуса, внесение комментариев, передача между аналитиками и т.д.). Поддерживается работа с инцидентами из почтового сообщения: ответ на email-сообщение парсится в решении с дальнейшим изменением свойств инцидента (статус, комментарии и т.д.)	Поддерживается отправка email (по протоколу SMTP, поддерживается создание шаблонов оповещений с переменными), отправка уведомления в мессенджеры (по протоколу SMPP)
							Поддерживается создание	В коробке поставляется набор шаблонов оповещений «из коробки», так же	

3.2.5. Наличие базы шаблонов оповещений;	В рамках настройки сценариев реагирования	Поддерживается	Поддерживается с кастомизацией	Поддерживается	Имеется база шаблонов оповещения, а также возможность создания новых и кастомизация существующих шаблонов оповещения	Поддерживается	пользовательских оповещений за счет кастомизации и настройки текста сообщения на уровне действия в сценарии в процессе внедрения решения у заказчика (настройки свойств, форматирование текста и т.д.)	возможно создание пользовательских оповещений с кастомизацией как внешнего вида, так и содержания (логотип, форматирование, набор отправляемых свойств инцидента и т.д.)	Поддерживается
3.2.6. Поддержка и кастомизация обогащения данных инцидентов (внешние, внутренние аналитические сервисы, включая общедоступные и коммерческие);	Поддерживается	Поддерживается за счет интеграций (IPinfo, URLscan, whois и т.д.), в том числе с входящим в экосистему Google сервисом VirusTotal	Не поддерживается	Поддерживается за счет более 320 интеграций в маркетплейсе Azure	Имеется поддержка обогащения данных инцидентов ИБ при интеграции со следующими системами: TIP (общедоступные и коммерческие), AbuseIPDB, Virus Total, Sandbox	Поддерживается использования внешних источников: VirusTotal, IPinfo, abuse.ch, Feodo Tracker, Spamhaus, AlienVault, Recorded Future, Proofpoint, данные MITRE ATT&CK, внешние песочницы и т.д.	Возможность обогащения из произвольных сервисов с использованием механизма конструктора коннекторов, в рамках экосистемы R-Vision EVO реализовано обогащение данными из решения R-Vision TIP (данные агрегированы из множества источников, используется собственный рейтинг IoC)	Поддержка и кастомизация набора коннекторов из коробки внешних аналитических сервисов: · ChatGPT · MITRE ATT&CK · AbuseIPDB · cleantalk.org · ipgeolocation.io · IPInfo.io · Kali tools · KasperskyOpenTip · Kaspersky Threats · MaxMind Geo-IP · MXToolBox · WhoISIQ(IP) · Shodan (API) · urlscan.io · VirusTotal · IP-Geolocation (HTTP) · IP-Netblocks (HTTP) ·WhoIsHistory (WhoIsXMLAPI, HTTP) ·WhoIs (WhoIsXMLAPI, HTTP) · AttackerKB · NVD · OpenCVE · VulDB · Vulners Поддержка и кастомизация набора коннекторов из коробки внутренних	Поддерживаются внешние сервисы обогащения: dnsgoogle, urlhaus, dshield, cybercrime, cyberprotect, unshorten, ipwhois, ipinfo, hashdd, urlscan, emailrep, greynoise, abuseip, hybridanalysis

								NGFW, Exchange, «песочницы», IDS/IPS, получение данных с устройств, IRP, TIP, системы управления уязвимостями, системы asset management, базы данных, AD, сетевые сканеры и утилиты (Nmap, nslookup), системы мониторинга (Zabbix)	
3.2.7. Поддержка проведения анализа инцидента с помощью настроенных интеграций (сбор артефактов, дополнительных обогащающих данных и форензик-информации с конечных точек, СЗИ, ИТ/ИБ-систем).	Поддерживается	Поддерживаются более 300 интеграций (внешние и внутренние решения и сервисы), возможность скачать интеграции из маркетплейса	Частично: с помощью настраиваемых PowerShell-скриптов, через интеграцию с Makves DCAP	Поддерживается за счет более 320 интеграций в маркетплейсе Azure, включая глубокую интеграцию с MS Defender	Имеется возможность сбора данных по индикаторам компрометации (IoC) при интеграции со следующими системами: TIP (общедоступные и коммерческие), AbuseIPDB, Virus Total, Sandbox	Поддерживается сбор форензик-информации с помощью пакета Cyber Triage	Поддерживается Kaspersky KATA, TIP, AbuseIPDB, Virus Total, Sandbox, AlienVaultOTX, FortiSIEM, VMWare, Zabbix, AD, MP SIEM, Qradar, MCAfee, ArchSight, Redcheck, RVision EndPoint, Qalis, SecretNet, ForcePoint Triton, InfoWatch,	Поддерживается интеграция с «песочницей» Any.Run, Kaspersky KATA, Kaspersky EDR, MS Defender EDR, PT Sandbox, PT NAD, Trend Micro Deep Discovery Analyzer (DDA), Cisco StealthWatch SIEM, NGFW Exchange, «песочницы», IDS/IPS, получение данных с устройств, IRP, TIP, системы управления уязвимостями, системы asset management, базы данных, AD. сетевые сканеры и утилиты (Nmap, nslookup), системы мониторинга (Zabbix). Поддерживаются аналитические сервисы: · ChatGPT · MITRE ATT&CK · AbuseIPDB · cleantalk.org · ipgeolocation.io · IPInfo.io · Kali tools · KasperskyOpenTip · Kaspersky Threats · MaxMind Geo-IP · MXToolBox · WhoISIQ(IP) · Shodan (API) · urlscan.io · VirusTotal · IP-Geolocation (HTTP)	Поддерживаются МЭ UserGate, конечные устройства UserGate Client (ОС Windows)

								·WhoIsHistory (WhoIsXMLAPI, HTTP) ·WhoIs (WhoIsXMLAPI, HTTP) · AttackerKB · NVD · OpenCVE · VulDB · Vulners	
3.3. Сдерживание распространения киберинцидентов, устранение последствий:									
3.3.1. Поддержка и кастомизация настройки действий по сдерживанию и устранению, выполняемых вручную и автоматически из интерфейса решения (через отправку управляющих команд на интегрированные СЗИ, ИТ/ИБ-системы);	Да, в рамках сценариев реагирования, с помощью скриптов (автоматически для автономного реагирования, работа с интегрированными системами через API) и задач (ручные действия)	Поддерживается	Частично: с помощью настраиваемых PowerShell-скриптов, через интеграцию с Makves DCAP	Поддерживается за счет более 320 интеграций в маркетплейсе Azure	Поддержка следующих основных операций: - проверка IP-адреса, - проверка доменного имени, - блокировка учетной записи, - разблокировка учетной записи, -исключение учетной записи из группы, - требование смены пароля учетной записи, -получение информации о пользователе, - получение информации о группе пользователей, -получение информации о хосте пользователя, - изменение расположения хоста или пользователя, - блокировка доступа к веб-ресурсу по IP-адресу, -блокировка доступа к веб-ресурсу по доменному имени, - получение списка последних IP-адресов, добавленных в список блокируемых, - блокировка писем от определенного отправителя, -поиск и удаление всех писем от определенного отправителя с определенной темой, - полная блокировка определенного пользователя, -блокировка запуска файла по хеш-сумме, - запуск антивирусного сканирования устройства - проверка доменного имени, - проверка email, - проверка имени файла, - проверка файла по хеш-сумме, - проверка IP-адреса, - проверка URL-адреса, - запуск команды через PsExec, - запуск команды через WinRM-подключение	Поддерживается интеграция с несколькими сотнями источников для выполнения автоматических и ручных действий по сдерживанию и устранению угроз	Поддерживается кастомизация действия над инцидентом в процессе внедрения с помощью добавления и изменения скриптов (более 70 встроенных скриптов по реагированию)	Поддерживается выполнение активных действий по локализации инцидента и устранению угрозы: блокирование сетевых коммуникаций, сетевая изоляция, отключение учетных записей, завершение процессов, остановка служб, перезагрузка устройства и т.д. Выполнение действий возможно вручную (по команде от аналитика SOC с соответствующими правами доступа, с ограничением на выполнение критичных операций) и автоматически (при наступлении условий, задаваемых в сценариях реагирования, и при выявлении аномалий методами машинного обучения), в том числе по расписанию. «Из коробки» поддерживается интеграция с системами, указанными в п. 3.1.12 Поддерживается «из коробки» 80+ динамических сценариев. Встроенных скриптов реагирования – 130+, встроенных плейбуков обогащения и классификации – 60+	Не поддерживается, действия по реагированию в решении предполагают только оповещение ответственных по различным каналам (email, мессенджеры)
3.3.2. Наличие и количество действий по активному автоматическому / ручному реагированию «из коробки»;	Из коробки предустановлены типовые задачи для ручного выполнения (локализация, расследование,	Поддерживаются активные действия по реагированию за счет интеграций с различными	Преднастроенные процедуры реагирования из коробки (на основе PowerShell-скриптов): отключение / включение / разблокирование / удаление учетной записи, смена пароля, запрос обоснования,	Поддерживается с помощью функционала Azure Logic Apps с возможностью использования более 2100 действий и коннекторов к различным приложениям из	Есть, более 20 сценариев реагирования (плейбуков) «из коробки»	Более 1200 сценариев в маркетплейсе вендора, могут быть установлены без	Решение поставляется с набором скриптов реагирования, дополнительно сценарии под конкретную инфраструктуру могут быть	Поддерживается выполнение действий по реагированию «из коробки» с системами, указанными в п. 3.1.12 130+ встроенных скриптов реагирования,	Не поддерживается

	ликвидация последствий), 51 скрипт из коробки	решениями	отключение срока действия пароля, установка срока действия учетной записи, выключение / перезагрузка компьютера	маркетплейса (полный объем доступных коннекторов определяется уровнем подписки на сервисы)		ограничений	разработаны инженерами вендора на этапе внедрения	100+ СЗИ, 100+ источников по проведению реагирования	
3.3.3. Поддержка и кастомизация настройки действий по активному автоматическому / ручному реагированию (работа с интегрированными системами через скрипты, интеграции, API-команды и т.д.);	Поддержка выполнения скриптов на Python, PowerShell, cmd. Работа с интегрированными системами через API для передачи команд для выполнения.	Поддерживается выполнение ручных и автоматических действий, работа через API, выполнение python-скриптов	Поддержка выполнения скриптов автоматизации (JavaScript, Python, Bash, PowerShell) с параметрами, отправка HTTP-запроса, syslog-сообщения в рамках выполнения настраиваемых процедур реагирования	Поддерживается работа через API, интеграции	Поддерживается	Поддерживается выполнение ручных и автоматических действий. Поддерживается работа с интегрированными системами через API, Python-скрипты	Поддерживается с использованием скриптов реагирования, универсального Python-коннектора, API-взаимодействия с интегрируемыми системами через механизмы PowerShell/CMD, LDAP, MSSQL, MySQL, OracleDB, PostreSQL, REST API, SNMP, SOAP, SSH, возможность использования регулярных выражений, переменных	Поддержка и кастомизация выполнение команд через интерпретаторы CMD, Bash, Shell, Java, JavaScript, PowerShell, Python. Поддерживается выполнение действий с интегрированными системами через API, файловые интеграции, доступ к БД, удаленный доступ (SSH, WinRM, WMI, LDAP, RPC). Поддерживается выполнение автоматических (при выполнении заданных условий в сценарии реагирования) и ручных (по команде аналитика SOC) действий по активному реагированию	Не поддерживается
3.3.4. Поддержка и кастомизация настройки действий по активному автоматическому / ручному реагированию (встроенный в решение функционал).	Настраивается через конструктор сценариев реагирования и написание скриптов во встроенном редакторе в интерфейсе решения	Поддерживается	Частично: с помощью настраиваемых PowerShell-скриптов, исполняемых на сервере инсталляции решения	Поддерживается за счет конфигурирования действий и работы коннекторов Azure Logic Apps	Поддерживается	Поддерживается создание вручную и кастомизация плейбуков, загружаемых в «пакетах содержимого» из маркетплейса	Поддерживается выполнение реагирования с помощью агента в рамках экосистемы R-Vision EVO	Поддерживается выполнение ручных и автоматических действий средствами самого решения с использованием удаленного доступа к объектам инфраструктуры, с поддержкой настройки условий выполнения действий и выявления аномалий методами машинного обучения, передачей свойств инцидентов в качестве параметров для реагирования (например, IP-адрес, имя устройства или учетной записи), обработкой ответов на отправленные команды с внесением изменений в карточку инцидента или актива. Решение предлагает аналитикам SOC экспертные рекомендации и действия по активному реагированию на основе матрицы MITRE ATT&CK, с возможностью ручной корректировки автоматически определенной тактики / техники атаки	Не поддерживается
3.4. Восстановление после киберинцидентов, пост-инцидентные действия:									
								Поддерживается выполнение действий по восстановлению инфраструктуры (путем создания и постановки дочерних задач из карточки инцидента с	

3.4.1. Наличие процесса поддержки выполнения задач по восстановлению и/или пост-инцидентным действиям по результату расследования атак/инцидентов ИБ;	В задачах для ручного выполнения заложен этап выполнения действий по ликвидации последствий с рекомендуемыми задачами в зависимости от типа инцидента	Поддерживается за счет интеграций с внешними и внутренними решениями и сервисами	Частично, в виде возможности создания пользовательских дополнительных процедур (сценариев реагирования) по восстановлению	Поддерживается	Поддерживается (пп 3.4.3, 3.4.4., 3.4.5.)	Поддерживается	Поддерживается, настраивается с использованием механизма сценариев в процессе внедрения: рассылка уведомлений и постановка задач по восстановлению инфраструктуры, установка SLA по выполнению задач, интеграция с ServiceDesk системами	установкой SLA, назначением ответственных, контролем результата), интеграцией с Service Desk системами, приведению объектов инфраструктуры в известное безопасное состояние (путем установки / удаления ПО и СЗИ, настройки рекомендуемых параметров ОС, ПО, СЗИ), фиксации артефактов и свидетельств инцидентов (за счет сбора и сохранения информации об инциденте в карточке инцидента)	Поддерживается возможность создания рекомендаций по восстановлению при формировании схемы инцидента (ручное создание записи «Решение инцидента» с рекомендациями)
3.4.2. База знаний с экспертными рекомендациями по плану восстановлению после киберинцидентов и пост-инцидентным действиям в соответствии с техникой атаки/инцидента ИБ;	Встроенная база знаний с рекомендациями по реагированию от Центра Кибербезопасности UDV Group, ТТУ ФСТЭК, MITRE ATT&CK	Поддерживается за счет работы с Google Cloud Community, за счет использования технологии «Duet AI» (на базе машинного обучения и искусственного интеллекта) с рекомендациями аналитикам на основе обработанной информации	Предустановленные рекомендации (инструкции) по реагированию на типовые инциденты с возможностью добавления пользовательских инструкций. Поддерживается возможность создавать и пополнять статьи встроенной базы знаний, добавлять файлы, поддерживается экспорт и импорт статей базы знаний	Поддерживается с использованием Azure OpenAI Service	Имеется возможность получать аналитику и рекомендации от Innostage SOC CyberART	Поддерживается за счет информации в пакетах содержимого и рекомендаций от Unit42 (центр киберэкспертизы Palo Alto)	Поддерживается в рамках предоставления лучших практик от команды «Центра экспертизы» вендора	Поддерживается с помощью пакета внутренней экспертизы, встроенного в решение, с учётом реализованных техник по матрице MITRE ATT&CK по каждому инциденту. Возможность формирования внутренней базы знаний на основе решенных инцидентов вручную (аналитиками SOC) и автоматически (на основе обучения ML-моделей с учетом особенностей инфраструктуры и допустимых автоматических действий по реагированию).	Предоставляется по запросу силами Центра мониторинга и реагирования UserGate
3.4.3. Поддержка и кастомизация настройки действий по восстановлению, выполняемых вручную и автоматически из интерфейса решения (через отправку управляющих команд на интегрированные СЗИ, ИТ/ИБ-системы);	Да, в рамках сценариев реагирования, с помощью скриптов (автоматически для автономного реагирования, работа с интегрированными системами через API) и задач (ручные действия)	Поддерживается за счет интеграций, работу через API, выполнение python-скриптов	Частично: с помощью настраиваемых PowerShell-скриптов	Поддерживается за счет более 320 интеграций в маркетплейсе Azure	Реализована возможность отмены выполненных действий по реагированию на инцидент ИБ (автоматизировано/вручную) - разблокирование пользователей/УЗ, удаление IoC из черных списков/политик блокировок	Поддерживается работа с интегрированными системами через API, Python-скрипты. Более 1200 сценариев в маркетплейсе вендора, могут быть установлены без ограничений	Поддерживается, настраивается с использованием механизма сценариев в процессе внедрения	Поддерживается выполнение активных действий по восстановлению инфраструктуры (путем создания и постановки задач в ServiceDesk-системах из карточки инцидента с синхронизацией статуса задачи в карточке инцидента), приведению объектов инфраструктуры в известное безопасное состояние (путем установки / удаления ПО и СЗИ, настройки рекомендуемых параметров ОС, ПО, СЗИ).	Не поддерживается
3.4.4. Поддержка и кастомизация настройки действий по активному автоматическому / ручному выполнению действий по восстановлению (работа с интегрированными	Поддержка выполнения скриптов на Python, PowerShell, cmd. Работа с интегрированными системами через API для	Поддерживается за счет интеграций, работу через API, выполнение	Поддержка выполнения скриптов автоматизации (JavaScript, Python, Bash, PowerShell) с параметрами, отправка HTTP-запроса,	Поддерживается работа через API, интеграции	Реализована возможность отмены выполненных действий по реагированию на инцидент ИБ (автоматизировано/вручную) - разблокирование пользователей/УЗ,	Поддерживается работа с интегрированными системами через API, Python-скрипты. Более 1200 сценариев в маркетплейсе вендора,	Поддерживается через механизмы PowerShell/CMD, LDAP, MSSQL, MySQL, OracleDB, PostreSQL, REST API, SNMP, SOAP, SSH, возможность использования	Поддерживается выполнение команд через интерпретаторы CMD, Bash, Shell, Java, JavaScript, PowerShell, Python. Поддерживается выполнение действий с интегрированными системами через API, файловые интеграции, доступ к БД, удаленный доступ (SSH, WinRM, WMI,	Не поддерживается

системами через скрипты, интеграции, API-команды и т.д.);	передачи команд для выполнения.	python-скриптов	syslog-сообщения в рамках выполнения настраиваемых процедур реагирования		удаление IoC из черных списков/политик блокировок	могут быть установлены без ограничений	регулярных выражений, переменных	LDAP, RPC). Поддерживается выполнение автоматических (при выполнении заданных условий в сценарии реагирования) и ручных (по команде аналитика SOC) действий по восстановлению	
3.4.5. Поддержка и кастомизация проведения ретроспективного анализа киберинцидентов (в рамках пост-инцидентного анализа);	В задачах для ручного выполнения заложен этап выполнения действий по ликвидации последствий, есть возможность создания дополнительных задач и действий для выполнения пост-инцидентного анализа с использованием сохраненных данных по инциденту	Поддерживается ретропоиск (RetroHunt) событий с применением правила к историческим данным (через Chronicle SIEM)	Частично, в виде возможности создания пользовательских дополнительных процедур (сценариев реагирования) по ретроспективному анализу	Поддерживается за счет выполнения KQL-запросов на хранящихся данных (глубина хранения определяется подпиской)	Имеется возможность постановки задач по ретроспективному анализу киберинцидентов, работы с Базой знаний, обогащение информации из SIEM системы, задачи повторного сканирования хоста для сбора дополнительных данных, необходимых в рамках ретроспективного анализа	Поддерживается с помощью функции исторической кросс-корреляции с выявлением схожих артефактов и IoC в разнородных инцидентах	Поддерживается, включая возможность поиска похожих инцидентов по заданному набору критериев	Решение автоматизирует проведение ретроспективного анализа с целью сбора дополнительных объектов и артефактов по всем событиям в окрестностях инцидента. В рамках ретроспективного анализа производится поиск событий запуска подозрительных процессов, антивирусных сработок, алертов IDS/IPS и аутентификаций на основе Sigma-правил и пакетов экспертиз.	Поддерживается работа правил аналитики в «историческом режиме» (производится анализ событий за выбранный период) с заданием временного диапазона, в пределах которого будет выполняться ретроспективный анализ
3.4.6. Поддержка выполнения действий по автоматическому восстановлению конфигураций конечных точек, СЗИ, ИТ/ИБ-систем в известное хорошее состояние («эталонная конфигурация»).	Не поддерживается из коробки, только при создании кастомных скриптов, реализация через плейбуки	Не поддерживается	Частично: реализовано для некоторых свойств учетных записей, файлов, почтовых ящиков MS Exchange	Поддерживается контроль конфигураций с помощью MS Defender на ОС Windows, Linux, MacOS	Не поддерживается	Не поддерживается	Поддерживается с помощью отправки управляющей команды на внешнюю систему	Поддерживается за счет установки / удаления ПО и СЗИ, настройки рекомендуемых параметров ОС, ПО, СЗИ.	Не поддерживается
4. Общий функционал управления киберинцидентами, визуализация, отчетность:									
4.1. Запуск сценариев реагирования автоматически (при наступлении организационно определенного события, условия), вручную, по расписанию;	Поддерживается выполнение сценариев по наступлению события или по расписанию, с опциями: выполнение по условию (с использованием операторов сравнения значений переменных с заранее заданными значениями), параллельное выполнение, цикличное выполнение, передача, ожидание, завершение, завершение с фиксацией ошибки. Возможно выполнение следующих действий: создание задания, отправка email, отправка сообщения, создание подозрения / инцидента, выполнение скрипта. Входные данные могут быть статическими (заранее заданными) или динамическими (формируются по результату выполнения предыдущих шагов плейбука).	Поддерживается создание сценариев с условиями запуска	Поддерживается запуск скриптов (задач) вручную, запуск по расписанию (с помощью функционала «Планировщика Windows»), запуск автоматически при выявлении изменений в контролируемых объектах	Поддерживает запуск вручную, автоматически по правилам, по расписанию	Имеется возможность автоматического и ручного запуска сценария реагирования, при этом условия автоматического запуска сценария реагирования гибко настраиваются в системе и могут зависеть от наименования инцидента ИБ, его источника, даты регистрации, приоритета, типа инцидента ИБ и других условий (доступен конструктор логических выражений). Также имеется возможность запуска сценарием по расписанию (подсистема Оркестрации)	Поддерживается создание гибких сценариев реагирования с разнообразными условиями	Поддерживается запуск сценариев автоматически по триггеру (при выполнении критериев запуска), вручную	Поддерживается автоматическое выполнение сценариев реагирования при выполнении заранее заданных условий и при выявлении аномалий (с помощью методов машинного обучения путем анализа отклонений в нормальном поведении пользователей, учетных записей, устройств, процессов и т.д.), с поддержкой выполнения автоматических действий по расписанию, с учетом политик допустимых действий по реагированию. Поддерживается выполнение ручных действий аналитиками SOC с учетом ролевой модели разграничения доступа и политик допустимых действий по реагированию	Поддерживается формирование правил аналитики с настройкой поисковых запросов и условий срабатывания правил, с автоматическим формированием инцидентов и запуском работы по схеме реагирования. Поддерживается ручное создание инцидентов.
4.2. Встроенный функционал (среда разработки) для	Встроенный редактор и				Да, имеется возможность создания и редактирования сценариев реагирования (Playbook) и настройки выполняемых действий по	Поддерживается	Поддерживается в виде	Поддерживается с помощью встроенной в решение среды разработки с подсветкой синтаксиса,	

создания интеграций, сценариев реагирования, настройки выполняемых действий по реагированию;	отладчик для плейбуков, встроенный редактор для скриптов	Поддерживается встроенная IDE	Не поддерживается	Поддерживается с помощью Azure Developer Tools	реагированию в рамках данных сценариев, а также функционал (среда разработки в подсистеме Оркестрации) создания интеграций (коннекторов) и выполняемых действий для автоматизированного реагирования на ИТ-инфраструктуру	Demisto SDK (на базе Python), Cortex XSOAR IDE	графического редактора сценариев, конструктора коннекторов	подсказками, проверкой синтаксиса, тестированием разработанных сценариев, встроенной справкой, тестового режима прогона сценария	Не поддерживается
4.3. Наличие сообщества / маркетплейса для получения дополнительных сценариев реагирования, интеграций, скриптов и т.д.;	Не поддерживается	Поддерживается (маркетплейс, сообщество, GitHub (github.com)	Не поддерживается	Поддерживается маркетплейс, GitHub (github.com), сообщество Tech Community	Сообщества / маркетплэйса нет. Имеется возможность получать аналитику и готовые сценарии реагирования от Innostage SOC CyberART. Новые интеграции и скрипты предоставляет разработчик.	Поддерживается маркетплейс (более 900 пакетов содержимого, включающие в себя интеграции, скрипты, плейбуки, виджеты), есть сообщество пользователей и разработчиков сценариев и интеграций, есть Community-версия, есть GitHub-репозиторий (github.com)	Информация предоставляется командой «Центра экспертизы» вендора	Поддерживается веб-портал с ЛК для клиентов с возможностью обмена информацией (экспертизой по реагированию, настройками интеграций, скриптами и сценариями реагирования) и маркетплейсом коннекторов, модулей, обновлений	Сообщество профессионалов на базе «Академии UserGate»
4.4. Возможность экспорта / импорта контента (сценарии, интеграции), возможность «отката» на предыдущие версии (для сценариев, интеграций);	Возможность импорта (загрузки) файла с описанием сценария. Поддержка импорта сценариев, разработанных в нотации Amazon States Language. Возможность экспорта полного плейбука или только алгоритма действий. Возможность импорта справочников (формат xls). Поддерживается версионное хранение кода плейбуков, коннекторов и скриптов в централизованном хранилище.	Поддерживается с помощью Data Export API	Нет данных	Поддерживается экспорт с помощью Log Analytics API	Реализована возможность экспорта / импорта контента (сценарии, интеграции)	Поддерживается возможность экспорта и импорта всего пользовательского контента, поддерживается версионность контента, возможность восстановить предыдущие версии	Экспорт и импорт сценариев не поддерживается, перенос возможен только вручную. Поддерживается создание копий сценариев внутри решения	Поддерживается экспорт и импорт в формате JSON всех основных объектов решения (рабочие процессы, объекты, модули, роли, справочники, коннекторы, виджеты, дашборды, отчеты, изображения с зависимостями и связанными справочниками). Поддерживается версионность, возможность восстановления объектов решения до предыдущей известной версии («откат изменений» при случайном или намеренном изменении объектов). Поддерживается выгрузка данных в форматах: xlsx, csv, txt	Поддерживается экспорт и импорт всех настроек решения в BIN-файл, с указанием расписания выгрузки и поддержкой отправки файла на SSH или FTP сервер
4.5. Возможность проверки («прогона») сценариев и интеграций перед вводом в эксплуатацию без реального взаимодействия с инфраструктурой;	С помощью встроенного отладчика для плейбуков	Поддерживается с функционалом симулятора выполнения сценариев (Playbook Simulator)	Не поддерживается	Поддерживается тестирование плейбуков на синтетических данных	Отдельного режима тестирования сценариев не предусмотрено, возможен "прогон" существующего сценария на тестовом инциденте с возможностью получить коды возникающих ошибок (при их наличии).	Поддерживается в выделенной тестовой инфраструктуре	Поддерживается в виде тестирования в конструкторе коннекторов	Поддерживается на подготовленном наборе тестовых данных с обработкой ошибок	Не поддерживается
4.6. Отчетность (разнообразные виды и форматы отчетов, включая создание стратегических, оперативных, тактических, аналитических отчетов для различных групп потребителей решения), отправка отчетов автоматически и по запросу	Общий отчет по инциденту с подробностями, кастомизируемая форма отчета. Формирование отчета при закрытии инцидента автоматически или вручную, возможность скачивания отчета (в формате Word). Формирование отчетов по инцидентам, квартальных	Поддерживается формирование отчетности по работе и метрикам SOC-центра (SLA, время на выполнение определенных действий, загруженность аналитиков, статистика работы SOC-центра) и по финансовым показателям (показатель ROI использования решения).	Нет данных	Поддерживается с помощью функционала Power BI	Имеется конструктор отчетов в соответствии с которым у оператора имеется возможность формировать разнообразные виды и форматы отчетов по инцидентам ИБ и ИТ-активам для различных групп пользователей продукта. Есть возможность выгрузить отчет в следующих форматах: *.docx, *.pdf	Поддерживается создание отчетов вручную, из виджетов, из перечня предустановленных шаблонов. Поддерживается формирование отчетов по расписанию, отправка по email,	Поддерживаются разные виды отчетов, генерация по расписанию, отправка по электронной почте. В коробке заложен набор преднастроенных отчетов	База преднастроенных отчетов с возможностью редактирования, а также создания через конструктор отчетов. Поддерживается создание отчетов из визуального отображения объектов (виджетов, текста, таблиц) с возможностью передачи значений параметров из объектов решения в текст отчета и настройкой локализации отчета. Поддерживается формирование отчетов вручную и автоматически (из	Поддерживается формирование отчетов в форматах PDF, HTML, CSV, создание пользовательских шаблонов отчетов, формирование отчетов вручную и по расписанию, отправка отчетов по email

(электронная почта, мессенджеры и т.д.);	отчетов по деятельности мониторинга и реагирования, отчетов в НКЦКИ	Поддерживается формирование отчетов в PDF, DOCX. Поддерживается формирование отчетов вручную и по расписанию, отправка по email.				выгрузка в форматах PDF, CSV		сценария реагирования) и по расписанию. Поддерживается отправка отчетов в решении (через оповещения), по email, через интегрированные мессенджеры. Поддерживается экспорт и отправка отчетов в форматах DOCX, PDF, XLSX, ODS, ODT, TXT, CSV.	
4.7. Выгрузка данных по инцидентам в отчете (doc, pdf), экспорт данных в разных форматах (xml, json, csv);	Экспорт отчетов в формате doc. Возможность экспорта полного плейбука или только алгоритма действий. Экспорт плейбука/алгоритма в формате JSON (нотация Amazon States Language)	Поддерживается экспорт данных в JSON, формирование отчетов в PDF, DOCX, гибкая настройка экспорта через Data Export API	Экспорт графических представлений в формате png, экспорт данных об объектах в форматах pdf, csv	Поддерживается экспорт данных в CSV, PDF, DOCX, иные варианты с помощью функционала Power BI	Выгрузка отчетов по инцидентам и ИТ-активам в форматах: *.docx, *.pdf. Экспорт и импорт данных в формате: *.xlsx	Поддерживается выгрузка данных по инциденту в CSV, создание отчетов в форматах CSV, PDF	Поддерживается формирование отчетов в формате Microsoft Office (doc, xls, ppt), odt и PDF, экспорт данных инцидентов в JSON	Поддерживается экспорт и импорт как отчетов по инцидентам, так и настроек отчетов для импорта в другие системы. форматах PDF, DOCX, ODT, XLSX, ODS, TXT. Поддерживается экспорт в формате XLSX, CSV, JSON данных по инцидентам	Поддерживается экспорт событий, инцидентов в CSV-файл, поддерживается отправка журналов решения на серверы SSH (SFTP), FTP, по Syslog с использованием синтаксиса CEF, JSON
4.8. Встроенная веб-помощь в интерфейсе системы.	Поддерживается встроенное в веб-портале "руководство пользователя"	Поддерживается	Поддерживается	Поддерживается	Есть всплывающие подсказки в карточках объектов в Системе	Поддерживается	Поддерживается: присутствует как admin guide, так и пользовательская инструкция	Поддерживается встроенная веб-помощь с поиском и кросс-ссылками (помощь администратору по решению, помощь пользователю по модулю SOAR)	Поддерживается
Расширенные критерии	**ePlat4m Orchestra (UDV ePlat4m SOAR)**	**Google Chronicle SOAR**	**Makves IRP**	**Microsoft Sentinel**	**Innostage IRP**	**Palo Alto Cortex XSOAR**	**R-Vision SOAR**	**Security Vision [NG]SOAR**	**UserGate LogAnalyzer**
1. Общие технические характеристики:									
1.1. Возможность использования SOAR как услуги (SaaS-модель);	Поддерживается	Поддерживается	Нет данных	Поддерживается	Поддерживается	Поддерживается (только SaaS для версии 8.x)	По запросу	Поддерживается	Поддерживается предоставление сервисов на базе решений UserGate (UGaaS)
1.2. Поддержка работы в сетях, изолированных от Интернет;	Поддерживается	Не поддерживается	Нет данных	Не поддерживается	Поддерживается	Не поддерживается (возможно в версии 6.x)	Поддерживается	Поддерживается с установкой выделенного сервиса коннекторов в изолированном сегменте сети	Нет данных
1.3. Поддержка работы в режиме multitenancy.	Поддерживается	Поддерживается	Нет данных	Поддерживается	Поддерживается	Поддерживается	Поддерживается, с разграничением прав доступа на основе ролевой модели	Поддерживается, с разграничением доступа пользователей к объектам и справочникам на основе организационной структуры (разграничение доступа к объектам дочерних и головных организаций)	Нет данных
2. Общие организационные характеристики:									
2.1. Наличие авторизованного обучения от вендора, стоимость обучения;	Поддерживается (по запросу)	Поддерживается обучение на самой платформе (обучающие курсы), обучение через сервис Google Cloud Skills Boost	Нет данных	Поддерживается в авторизованных учебных центрах, на онлайн-курсах от вендора (платформа Microsoft Learn)	Обучение проводится на базе учебного центра вендора	Проводится обучение в Palo Alto Networks Cybersecurity Academy	Обучение по курсам администрирования и использования решения, выдается сертификат вендора	Проводится бесплатное обучение в собственном учебном центре вендора с выдачей сертификата	Авторизованные курсы в «Академии UserGate» (образовательное подразделение компании UserGate)
								Развитие корреляционного	

2.2. Дорожная карта развития продукта (планируемый к внедрению функционал и ориентировочные сроки реализации, планируемые изменения в лицензионную политику).	Поддерживается (по запросу)	Нет данных	Нет данных	Нет данных	Функционал Системы разрабатывается/дорабатывается в соответствии с дорожной картой развития продукта. Предусмотрено в Roadmap: формула расчёта критичности инцидента, автоматизированный триаж инцидентов ИБ, интеграция с мессенджерами (4 кв. 2023 года), отправка отчетов по эл. почте и через мессенджеры	Нет данных	По запросу	движка в модуле NG-SOAR. Расширение функционала ML в движках принятия решений. Развитие базы экспертизы и рекомендаций по различным типам инцидентов. Дальнейшее развитие концепции динамического плейбука с учетом новых типов инцидентов. Развитие функционала ретроспективного анализа, поиска артефактов и цифровых свидетельств инцидента. Разработка агента с целью более эффективного сдерживания инцидента и сбора данных.	Нет данных
3. Управление киберинцидентами:									
3.1. Подготовка к реагированию на киберинциденты:									
3.1.1. Поддержка и кастомизация правил группировки, дедупликации импортированной информации о событиях / инцидентах ИБ;	Дедупликация отсутствует, возможна группировка инцидентов по категориям	Поддерживается, выполняется автоматически	Не поддерживается	Поддерживается, с помощью автоматической агрегации предупреждений в единый инцидент	Имеются правила группировки/фильтрации инцидентов ИБ с гибкими возможностями кастомизации, дедупликации импортированной информации о инцидентах ИБ	Поддерживается возможность дедупликации инцидентов, возможность связывания инцидентов вручную и автоматически с помощью правил предобработки инцидентов (pre-process rule)	Поддерживается настройка правил группировки как автоматически, так и вручную с помощью создания связей инцидентов (вручную или с помощью ручного запуска создаваемых правил создания связей). Поддерживается простое (одноранговое) связывание инцидентов и группировка инцидентов (в иерархические группы).	Поддерживается настройка правил автоматической группировки с учетом свойств инцидента, так и других объектов, по которым определяется уникальность для избежания дублирования. Возможность создания нескольких правил группировки, каждое из которых включает от 1 до всех свойств инцидента. Поддерживается создание сложных фильтров для задания условий срабатывания правил группировки	Поддерживается группировка срабатываний правил аналитики (за определенный период времени, по количеству срабатываний).
3.1.2. Автоматизированное выстраивание цепочки атак из инцидентов;	Не поддерживается	Поддерживается выстраивание кейса как совокупности связанных предупреждений	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается частично с помощью автоматического связывания инцидентов	Не поддерживается, поддерживается только поиск похожих инцидентов на настраиваемым пользователем правилам	Поддерживается автоматическая агрегация инцидентов в атаку и выстраивание цепочки атаки («kill chain») по ключевым атрибутам и тактикам / техникам атак инцидентов (по матрице MITRE ATT&CK). Поддерживается автоматический сбор и ретроспективный анализ релевантных событий, произошедших в тот же временной промежуток, с поддержкой получения обогащающих данных с объектов инфраструктуры с дальнейшим автоматическим формированием комплексного сценария	Не поддерживается

								реагирования	
3.1.3. Критерии агрегации инцидентов в объекты типа «Атака» или «Маршрут атакующего»;	Не поддерживается	Поддерживается на основе правил	Не поддерживается	Поддерживается на основе правил и ML-движка «Fusion»	Не поддерживается	Поддерживается частично с помощью правил предобработки инцидентов (pre-process rule)	Не поддерживается, поддерживается только поиск похожих инцидентов на настраиваемым пользователем правилам	Поддерживается объединение инцидентов в атаки и построение поверхности распространения атаки на основе ретроспективного анализа окрестностей инцидента и релевантных событий посредством связывания задействованных в атаке инцидентов ИБ по ключевым атрибутам: IP адреса / имена атакующих и скомпрометированных узлов, скомпрометированные учетные записи, уязвимости на хостах, хакерский инструментарий, ВПО. За счет дополнительного сбора сырых данных с источника: сетевой связности, сессий, аутентификации	Не поддерживается
3.1.4. Наличие собственного корреляционного ядра, возможности гибкой настройки правил корреляции;	Поддерживается возможность настройки правил корреляции	Поддерживается через Chronicle SIEM	Поддерживается частично с помощью встроенной обработки данных, собранных PowerShell-скриптами	Поддерживается	Не поддерживается	Поддерживается частично, для проведения исторической корреляции	Поддерживается возможность настройки правил корреляции для связывания инцидентов (по заданным общим признакам, с созданием пользовательских правил группировки)	Поддерживается механизм корреляции и группировки данных с помощью встроенного в решение конструктора и средствами с поддержкой настройки правил корреляции с помощью логических выражений и математических операций, а также применением переменных и свойств, справочников системы	Поддерживается создание корреляционных правил аналитики
3.1.5. Автоматическое определение техник и тактик атаки в соответствии с фреймворком MITRE ATT&CK, возможность ручной корректировки определенной техники/тактики;	TTPs передаются SIEM-системой	Поддерживается за счет интеграции «Mitre ATT&CK»	Не поддерживается	Поддерживается автоматическое определение техник и тактик, ручное переопределение не поддерживается	Не поддерживается	Поддерживается с помощью пакета содержимого «MITRE ATT&CK Courses of Action»	Не поддерживается	Поддерживается. Поддержка классификации инцидентов по тактикам и техникам (а так же релевантным ВПО и злоумышленникам) матрицы MITRE ATT&CK и ФСТЭК, расширенными экспертизой вендора в виде как кратких, так и расширенных рекомендаций, а так же дополнительных подсказок – помощью в виде взаимодействия с ChatGPT , с поддержкой классификации 250+ типов инцидентов и событий ИБ с присвоением 110+ техник и тактик по MITRE ATT&CK	Не поддерживается
								Поддерживается. Матрица MITRE ATT&CK решения представляет собой полноценную информационную справочную систему со всеми уровнями	

3.1.6. Просмотр и детализация базы MITRE ATT&CK и всех ее элементов (в виде иерархии тактик, техник и т.д., в виде таблицы в инциденте, в виде общего списка элементов, другое (указать));	Да, в виде редактируемого справочника с поддержкой иерархии	Поддерживается за счет интеграции «Mitre ATT&CK»	Не поддерживается	Поддерживается просмотр в табличном виде с деталями	Не поддерживается	Поддерживается просмотр структуры матрицы	Не поддерживается	декомпозиции, связями и drilldown между подчиненными элементами, а также тесно интегрирована в инцидент и атаку. На базе модуля MITRE ATT&CK выстраиваться kill chain (атаки с учетом задействованных техник), экспертные рекомендации. В системе присутвует маппинг MITRE ATT&CK на модель угроз ФСТЭК	Не поддерживается
3.1.7. Автоматическое обновление базы MITRE ATT&CK;	В рамках обновления решения	Поддерживается за счет интеграции «Mitre ATT&CK»	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается автоматическое обновление содержимого матрицы MITRE ATT&CK	Не поддерживается
3.1.8. Поддержка и кастомизация правил классификации (в том числе по методологиям MITRE ATT&CK), поддержка ручной и автоматической классификации / переклассификации на всем времени жизни инцидента в зависимости от изменений контекста;	Поддерживается классификация по методологии MITRE ATT&CK и ТТУ ФСТЭК (тактики и техники угроз), ручная классификация / переклассификация в рамках реагирования. Автоматически TTPs проставляются в момент поступления событий от SIEM-системы	Поддерживается ручная и автоматическая переклассификация	Поддерживается возможность ручной классификации, переклассификации инцидентов	Поддерживается, с возможностью создания правил выявления угроз на основе выявленных техник и тактик по матрице MITRE ATT&CK	Поддерживается ручная классификация и переклассификация	Поддерживается классификация по методологии MITRE ATT&CK с помощью пакета содержимого «MITRE ATT&CK Courses of Action»	Поддерживается вручную, с использованием механизма сценариев реагирования	Поддерживается автоматическая классификация инцидентов и атак на основе матрицы MITRE ATT&CK вне зависимости от наличия классификации от источника. Поддерживается как ручная переклассификация выявленных тактик, техник, субтехник аналитиком SOC, так и автоматическая переклассификация тактик, техник, субтехник с учетом получаемой дополнительной информации об инциденте по результатам получения новых событий объектов инцидента	Поддерживается ручная переклассификация инцидента
3.1.9. Поддержка выполнения изолированных (независимых от конкретного сценария) действий реагирования, запуск изолированных действий в ручном / автоматическом режимах, возможность комбинирования изолированных действий в различных сценариях реагирования;	Создание сценариев реагирования и включение их в более комплексные сценарии	Поддерживается с функционалом «Playbook Blocks»	Не поддерживается	Не поддерживается	Поддерживается выполнение изолированных действий реагирования и их запуск в ручном режиме. Имеется возможность комбинирования изолированных действий в различных сценариях реагирования	Поддерживается с помощью выполнения отдельных скриптов	Создание сценариев реагирования и включение их в более комплексные сценарии (более 70 встроенных скриптов по реагированию)	Поддерживается запуск отдельных независимых (атомарных) действий по реагированию с возможностью их комбинирования в различных сценариях. Поддерживается выполнение атомарных действий в ручном и автоматическом режимах. «Из коробки» поставляются 130+ различных преднастроенных действий и атомарных сценариев реагирования на различные типы киберинцидентов. Возможность выполнения действий из карточки инцидента: с помощью инструмента расследования представленным как в виде графа, так и в табличном представлении	Не поддерживается
								Поддерживается создание правил	

3.1.10. Возможность создания политики/правил разрешенных действий по реагированию в отношении инфраструктурных объектов;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается частично (для конечных точек)	Имеется, в рамках модуля оркестрации	Частично поддерживается с помощью ограничения доступа к потенциально опасным действиям по реагированию на основе ролевой модели	Поддерживается путем привязки сценария реагирования по критериям к определенным группам активов	разрешения/запрета выполнения действий по активному реагированию на основе критериев инцидента и параметров объекта инцидента (например, триады КЦД актива или критичности). Формирование списка устройств и разрешенных правил блокирования на них, списка недоступных для блокирования учетных записей и критичных устройств чувствительных к выполнению активных действий. Поддерживается разграничение доступа пользователей решения на доступ к тем или иным действиям по активному реагированию	Не поддерживается
3.1.11. Поддержка технологии выстраивания сценариев реагирования «на лету» в зависимости от этапа атаки и ранее выполненных действий;	Реализовано в виде динамических входных параметров (формируются по результату выполнения предыдущих шагов плейбука)	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается через настройку динамического запуска сценариев по триггеру изменения инцидента и критериям, заданным в отношении полей инцидента	Поддерживается автоматическое формирование динамических сценариев реагирования на основе данных об объектах инцидента, их свойствам и разрешенным политикам реагирования, также в динамике выстраивания сценария реагирования участвует определенная техника атакующего и сведения об инфраструктуре	Не поддерживается
3.1.12. Поддержка кастомизации карточки инцидента, отображаемых свойств инцидентов, компоновки информации на карточке, возможность добавления файла в карточку инцидента, разграничение доступа к значениям свойств инцидентов;	Поддерживается возможность кастомизации карточки инцидента, расположения полей и свойств, компоновка информации, добавление файла в карточку. Гранулированное разграничение доступа к определенным свойствам инцидента не поддерживается, разграничение реализовано на уровне ролевой модели с полномочиями для выполнения более высокоуровневых действий (редактирование инцидента, редактирование справочников и т.д.)	Поддерживается	Поддержка создания кастомных полей в карточке инцидента, поддержка добавления файлов к карточке инцидента	Поддерживается	Поддерживается с помощью графического конструктора	Поддерживается	Поддерживается возможность кастомизации карточки инцидента, расположения полей и свойств, компоновка информации, добавление файла («файл свидетельства») в карточку инцидента. Гранулированное разграничение доступа к определенным свойствам инцидента реализовано с помощью настройки представлений для ролей пользователей	Поддерживается формирование содержимого и форматирование карточки инцидента в зависимости от потребностей пользователя, с использованием преднастроенных шаблонов, с использованием low-code / no-code подхода и с поддержкой настройки внешнего вида карточки инцидента в графическом редакторе. Поддерживается добавление артефактов инцидента, различные правила автозаполнения полей и правила видимости: гранулированное разграничение доступа (на основании ролевой модели и для конкретного пользователя) на просмотр, изменение, удаление значений свойств в карточке инцидента	Поддерживается настройка отображения определенных столбцов в общем списке срабатываний правил аналитики
								Поддерживается автоматическое выстраивание связей, с	

3.1.13. Поддержка установки и визуализации связей между объектами инцидента ИБ / инцидентами ИБ в контексте атаки (интерактивные графы для отображения и управления связями между объектами), выполнение действий над объектами / инцидентами ИБ из интерактивного отображения, отображение направления взаимодействия объектов ИБ, отображение метрик критичности связанных сущностей;	Не поддерживается	Поддерживают графы связей	Не поддерживается	Поддерживается отображение информации об инциденте на графе инцидента с выводом на граф затронутых сущностей (учетные записи, хосты, приложения, данные) с связей между сущностями	Не поддерживается, отображается только информация о пройденных этапах реагирования на схеме сценария	Поддерживается визуализация возможных взаимосвязанных инцидентов на схеме	Поддерживается с помощью схемы взаимосвязей инцидентов с отображением свойств и связей инцидента с объектами защиты, поддерживается возможность удаления элемента схемы и просмотра аналогичных инцидентов непосредственно их схемы инцидента. Действия по реагированию из схемы не поддерживаются. Поддерживается вывод информации об инцидентах на географической карте	возможностью ручного редактирования и отображения в табличном и графовом представлении связей объектов инцидентов (ИТ-актив, учетные записи, процессы, ВПО, уязвимости и т.д., включая цветовое отображение критичности объектов) поддерживается выполнение действий из графа связей (переход на карточки инцидента, реагирование, обогащение, построение дополнительных связей), с поддержкой добавления пользовательских действий на графе. На графе отображается взаимосвязь объектов и направление их взаимодействия. В карточке инцидента отображаются все связанные с инцидентом события в виде временной шкалы (хронология событий) возникновения событий с соблюдением их хронологии	Не поддерживается
3.1.14. Поддержка выполнения нормативных требований по управлению киберинцидентами (законодательные нормативы для субъектов КИИ, операторов ПДн, финансовой отрасли и т.д.), отправка отчетности по киберинцидентам в ГосСОПКА, ФинЦЕРТ.	Поддерживается интеграция с ГосСОПКА, ФинЦЕРТ. Отправка отчетности по инцидентам в ГосСОПКА (автоматически и вручную), получение комментариев и ответов от представителей НКЦКИ в интерфейсе решения. Получение бюллетеней по уязвимостям и угрозам из ГосСОПКА. Отправка отчетности по инцидентам в ФинЦЕРТ	Не применимо	Поддержка нормативных требований по защите ПДн (152-ФЗ), GDPR, HIPAA, PHIPA, PCI DSS, GLBA	Не применимо	Поддерживается работа с ГосСОПКА (получение бюллетеней с автоматическим созданием инцидентов в решении, отправка отчетности, получение и обработка ответа от НКЦКИ)	Не применимо	Поддерживается интеграция с ГосСОПКА, ФинЦЕРТ. Поддерживается отправка отчетности по инцидентам в ГосСОПКА (автоматически и вручную), получение сообщений от НКЦКИ в интерфейсе решения. Поддерживается отправка отчетности по инцидентам через АСОИ ФинЦЕРТ, формирование отчетности по форме 0403203 ЦБ РФ. Поддержка в каталоге угроз типов киберугроз, определенных ПП-1119 (защита ПДн). Поддерживается внесение в карточки активов информации по объектам КИИ и субъекту КИИ, внесение данных о кредитной организации и участнике НПС. Поддержка учета систем ИСПДн, ГИС, АСУТП	Поддерживается интеграция с ГосСОПКА (НКЦКИ) и АСОИ ФинЦЕРТ (ЦБ РФ) для получения сообщений и бюллетеней, отправки отчетности по инцидентам с получением ответов. Поддерживается формирование комплекта документов для соответствия 187-ФЗ (безопасность КИИ). Поддерживается формирование отчетности по нормам ЦБ РФ (0403202, 0403203). Поддерживается установка временных норм (SLA) по реагированию на инциденты по нормам законодательства о безопасности КИИ и о защите ПДн	Поддерживается передача информации об инцидентах ИБ в ГосСОПКА, в решении создан шаблон отправки уведомления в ГосСОПКА, отправка выполняется через встроенный коннектор «Gossopka»
3.2. Выявление, анализ киберинцидентов:									
						Поддерживается ведение графика		Поддерживается создание правил автоматического назначения ответственных за инцидент в зависимости от типа и свойств инцидента, с учетом квалификации и специализации аналитика, с	

3.2.1. Поддержка и кастомизация правил назначения ответственных за инцидент аналитиков, автоматической установки временных нормативов выполнения действий, поддержка работы дежурных смен (расписание сотрудников, график дежурств), поддержка механизма автоматического назначения ответственного (по настраиваемым правилам), учет рабочего времени (в том числе в режиме Multitenancy);	Только в рамках преднастроенной ролевой модели с ролями: Руководитель SOC, Руководитель направления (Клиент), Аналитик 1 / 2 / 3 линии. SLA устанавливаются автоматически. Механизм дежурных смен и автоматическое назначение ответственных не реализовано.	Поддерживается ручное назначение ответственных, установка нормативов реагирования, учет затраченного времени (в том числе в режиме Multitenancy)	Назначение ответственных и установка временных нормативов осуществляется вручную	Поддержка функционала учета дежурных смен через интеграцию с MS Teams, поддержка назначения ответственных в правилах выявления угроз, поддерживается учет затраченного времени на инциденты в разрезе каждого аналитика	Поддерживается с созданием групп и подразделений ответственных, установкой приоритета, плановой даты закрытия, учетом затраченного времени. Поддерживается настраиваемое автоматическое назначения ответственных в зависимости от типов инцидентов, подразделения, к которому относится сотрудник.	дежурных смен, возможность установить статус «Отошел» для аналитика SOC, автоматическое назначение инцидента на аналитика (в зависимости от графика дежурств, загруженности, с возможностью использовать скрипты автоназначения). С помощью функционала DBotc использованием машинного обучения анализируется загруженность аналитиков и ранее закрытые ими инциденты, в результате DBot дает подсказки по привлечению участников и назначению ответственных на инцидент (список из 3 наиболее подходящих сотрудников).	Поддержка ручного и автоматического назначения ответственного за инцидент, создание рабочих групп по инциденту с различными правами доступа участников в соответствии с ролевой моделью. Поддержка временных нормативов и динамическое управление ими, механизм автоназначения инцидентов по показателю нагрузки на исполнителя. Встроенная ролевая соответствует типовым ролям ИБ-подразделения, но не специализирована для SOC-центра	сохранением возможности ручного переназначения ответственного. Поддерживается функционал формирования расписания дежурств и рабочего календаря сотрудников и членов дежурных смен. Поддерживается задание SLA-метрик для выполнения каждого действия в рамках сценария реагирования, в зависимости от свойств инцидента, связанного актива, иного объекта (например, критичность инцидента, категория актива, уровень доступа атакованного пользователя). Поддерживается ведение учета рабочего времени для различных сотрудников, организаций и структурных подразделений, с учётом часового пояса географически распределенных подразделений, с поддержкой учета для работы решения в режиме Multitenancy	Поддерживается автоматическое и ручное назначение и переназначение ответственного за инцидент
3.2.2. Поддерживаемые методологии анализа и прогнозирования развития инцидентов в виде встроенных модулей (например, методология MITRE ATT&CK);	Прогнозирование развития инцидента отсутствует. Аналитика инцидента поддерживается с использованием методологий MITRE ATT&CK и ТТУ ФСТЭК	Поддерживается методология MITRE ATT&CK	Не поддерживается	Поддерживается с использованием методологии MITRE ATT&CK	Не поддерживается	Поддерживается методология MITRE ATT&CK	Не поддерживается	Поддерживается. Поддерживается анализ вектора атаки и дальнейшего развития инцидента на основе корреляции скрытых взаимосвязей между событиями идентифицированные пакетом экспертиз и правил детектирования угроз с применением анализа тактик, техник, субтехник в соответствии с матрицей MITRE ATT&CK.	Не поддерживается
3.2.3. Анализ инцидентов с использованием ретроспективного поиска релевантных событий, применение SIGMA-правил;	Не поддерживается	Поддерживается через Chronicle SIEM	Не поддерживается	Поддерживается с помощью импорта SIGMA-правил в Log Analytics	Не поддерживается	Поддерживается с помощью функции исторической кросс-корреляции с выявлением схожих артефактов и IoC в разнородных инцидентах. Использование SIGMA-правил поддерживается в некоторых плейбуках из пакетов содержимого	Поддерживается возможность поиска похожих инцидентов по настраиваемым правилам, применение SIGMA-правил не поддерживается	Поддержка в решении пакета экспертизы на основе как SIGMA-правил, так и других пакетов детектирования угроз для ретроспективного анализа событий инцидента и проактивного поиска угроз	Поддерживается работа правил аналитики в «историческом режиме» для выполнения ретроспективного поиска
3.2.4. Запрос (обогащение) дополнительных релевантных событий от источника по задействованным объектам инцидента;	Не поддерживается	Поддерживается в рамках построения кейса, запрос событий за последние 12 часов	Не поддерживается	Поддерживается вручную	Поддерживается возможность получения корреляционного события из SIEM и обогащения данных по затронутому активу	Поддерживается выполнение поисковых запросов по инциденту вручную из «War room»	Поддерживается обогащение из произвольных источников с использованием конструктора коннекторов	Поддерживается получение релевантных инциденту дополнительных событий и алертов с объектов инфраструктуры и средств защиты	Не поддерживается
								Поддерживается визуализация	

3.2.5. Поддержка анализа инцидента с помощью визуализации связей между объектами инцидента ИБ / инцидентами ИБ в контексте атаки (интерактивные графы для отображения и управления связями между объектами, возможность выполнения действий по обогащению инцидентов дополнительной значимой информацией), построение интерактивного графика хронологии инцидента.	Не поддерживается	Поддерживается отображение информации на графах связей с выполнением действий по реагированию	Не поддерживается	Поддерживается отображение информации об инциденте на графе инцидента с выводом на граф затронутых сущностей (учетные записи, хосты, приложения, данные) с связей между сущностями. Поддерживается возможность выполнения поисковых запросов, просмотра timeline, выполнения действий по реагированию на графе	Визуализация на графе не поддерживается, только в рамках отображения пройденных этапов реагирования на схеме сценария. Результаты реагирования отображаются также в отчетах	Поддерживается визуализация возможных взаимосвязанных инцидентов на схеме	Частично поддерживается с помощью схемы взаимосвязей инцидентов, без выполнения обогащения, с поддержкой расчета влияния инцидента на бизнес-процесс. Отображение timeline-графика доступно при создании сценария реагирования, если в инцидент добавляется больше одного действия или сценария	аналитической информации на полной и краткой карточках инцидентах в виде виджетов, таймлайнов, интерактивных графов и хронологий и на дашбордах (линейный график, столбчатая диаграмма, круговая диаграмма, спидометр, таблица, радар, географическая карта, глобус), на графах связей, в виде временной шкалы (timeline), в отчетах. Поддерживается выполнение действий по обогащению, установлению связей, активному реагированию из графическому представлению инцидента (графа связей, табличного представления, географической карты)	Не поддерживается
3.3. Сдерживание распространения киберинцидентов, устранение последствий:									
3.3.1. Возможность непрерывного обогащения данных по инциденту, выявление дополнительных артефактов киберинцидентов, динамический выбор дальнейших действий по реагированию;	Не поддерживается	Поддерживается обогащение в соответствии с настроенным сценарием реагирования	Не поддерживается	Поддерживается	Поддерживается динамический выбор дальнейших действий по реагированию в рамках плэйбука, а также из карточки инциденты. Поддерживается настраиваемая логика непрерывного обогащения данных по инциденту, работа с индикаторами компрометации.	Поддерживается обогащение в рамках реагирования, выбор действий по реагированию задается в плейбуке	Не поддерживается. Возможность выстраивания плейбука по регулярному обогащению объектов инцидента в процессе внедрения системы	Поддерживается выполнение обогащения и получения артефактов атаки на всех этапах реагирования и развития инцидента, с поддержкой динамического изменения перечня выполняемых далее действий в зависимости от актуализированной информации по инциденту и затронутым объектам	Не поддерживается
3.3.2. Поддержка выполнения действий по реагированию в изолированных сегментах сети.	Поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается в агентном / безагентном режиме	Поддерживается путем установки распределенных компонент (выделенного сервиса коннекторов в изолированном сегменте сети).	Не поддерживается
3.4. Восстановление после киберинцидентов, пост-инцидентные действия:									
3.4.1. Трекинг задач по восстановлению и/или пост-инцидентным действиям (по результату расследования атак/инцидентов ИБ);	В рамках создания и назначения задач по ликвидации последствий. Трекинг задач во внешних системах отсутствует	Поддерживается создание задач в такс-трекерах с помощью интеграций (Service Now, Jira, ServiceDesk Plus и т.д.)	Не поддерживается	Поддерживается создание задач в решении, интеграция с тикетинг-системами	Поддерживается в рамках интеграции с системами таск-трекинга	Поддерживается ведение перечня задач в карточке инцидента	Поддерживается в рамках создания списка задач, связанных с инцидентом, с отображением наименования, сроков исполнения, статуса. Service Desk: Naumen, Jira	Поддерживается формирование задач на восстановление и выполнение действий поле инцидента в самом решении и в сторонних ServiceDesk-системах (Jira, Naumen Service Desk, MicroFocus Service Manager (HP Service Manager), BPM Online (Creatio)). Поддерживается назначение ответственных, установка сроков, контроль выполнения, синхронизация статусов (для	Не поддерживается

								сторонних систем)	
3.4.2. Поддержка выполнения действий по восстановлению в изолированных сегментах сети;	Поддерживается	Не поддерживается	Нет данных	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается в агентном / безагентном режиме	Поддерживается с помощью использования выделенного сервиса коннекторов в изолированном сегменте сети	Не поддерживается
3.4.3. Наличие, функционал, кастомизация базы знаний обработанных инцидентов (первичное наполнение, обогащение, применение для выдачи рекомендаций по обработке новых аналогичных инцидентов), наполнение базы знаний перечнем нормативных активов и лучших практик и рекомендаций «из коробки».	Встроенная база знаний с рекомендациями по реагированию от Центра Кибербезопасности UDV Group, ТТУ ФСТЭК, MITRE ATT&CK. Пакеты экспертизы поставляются в обновлениях решения	Поддерживается использование базы знаний за счет работы с Google Cloud Community	Поддерживается возможность создавать и пополнять статьи встроенной базы знаний, добавлять файлы, поддерживается экспорт и импорт статей базы знаний	Поддерживается выдача рекомендаций по обработке инцидентов с использованием Azure OpenAI Service	База знаний присутствует	Поддерживается за счет информации в пакетах содержимого и рекомендаций от Unit42 (центр киберэкспертизы Palo Alto)	Поддерживается путем интеграции с продуктом R-Vision SGRC в рамках экосистемы R-Vision EVO. Поддерживается также в рамках предоставления лучших практик от команды «Центра экспертизы» вендора.	Поддерживается формирование внутренней базы знаний новых sigma-правил, угроз, детектирования, рекомендаций на основе решенных инцидентов вручную (аналитиками SOC) и автоматически. Поддерживается использование рекомендаций по реагированию на основе ISO 27035, NIST SP 800-61, данных проекта MITRE	Предоставляется по запросу силами Центра мониторинга и реагирования UserGate
4. Общий функционал управления киберинцидентами, визуализация, отчетность:									
4.1. Возможность кастомизации и создания персонального рабочего окружения исходя из бизнес-процессов и бренда организации: кастомизация размещения элементов на страницах, быстрых фильтров, карточек и жизненного цикла инцидентов ИБ / атак с применением подхода low-code / no-code;	Присутствуют возможности кастомизации внешнего вида рабочего окружения и отображаемых объектов с помощью графического конструктора	Частично поддерживается (кастомизация гридов, фильтров, карточек инцидентов)	Поддерживается ручная настройка изменения порядка отображения столбцов, фильтрация, сортировка инцидентов в табличном виде	Поддерживается частично (некоторые функции не поддерживаются с low-code / no-code подходом)	Поддерживается с помощью графического редактора	Поддерживается частичная кастомизация с применением подхода low-code / no-code	Присутствуют возможности кастомизации внешнего вида рабочего окружения и отображаемых объектов с помощь графического конструктора	Поддерживается кастомизация внешнего вида и внутренних процессов под бренд и процессы организации, с настройкой визуальных элементов, сценариев реагирования, карточек инцидентов в графическом редакторе с применением подхода low-code / no-code. Возможность реализации рабочего места сотрудника для каждой конкретной роли	Не поддерживается
4.2. Визуализация (интерактивные графы для отображения связей между инцидентами и связанными объектами и для интерактивного управления инцидентами в рамках реагирования), дашборды, панели визуализации (виджеты), функционал drilldown;	Интерактивные графы не поддерживаются. Присутствует функционал настраиваемых панелей визуализации (виджетов). Drill Down в виджетах - поддерживается	Поддерживается отображение информации об атаках на графах, функционал «Drilldown» поддерживается	Поддерживается формирование линейных, столбчатых, круговых диаграмм, графиков, таблиц с отображением информации по пользователям и устройствам, сводок в виде набора виджетов	Поддерживается отображение атак и связей между сущностями на графе с возможностью выполнения реагирования, поддерживаются дашборды с drilldown	Графы не поддерживаются, дашборды и панели визуализации с функционалом drilldownподдерживаются	Поддерживаются дашборды с набором виджетов и функцией «drill down». Интерактивные графы не поддерживаются.	Частично поддерживается. С помощью схемы взаимосвязей инцидентов, без полнофункционального управления инцидентами из схемы. Функционал «drilldown» поддерживается	Поддерживается. Отображение информации по инцидентам и возможность выполнения действий по реагированию из интерактивных графов связей между объектами инцидента. Поддерживается визуализация информации об инцидентах на виджетах (линейный график, столбчатая диаграмма, круговая диаграмма, спидометр, таблица, радар, географическая карта), на графах связей, в виде временной шкалы (timeline), на дашбордах, в отчетах. Во всех графических элементах поддерживается функционал «drill down» для непосредственного перехода от визуальных элементов к данным, на	Поддерживается создание виджетов, без функционала «drill down»

								основании которых было построено графическое отображение	
4.3. Возможность кастомизации визуализации дашбордов, панелей визуализации с применением подхода low-code / no-code;	Поддерживается	Поддерживается	Не поддерживается	Поддерживается	Частично поддерживается с помощью графического редактора	Не поддерживается	Частично поддерживается с помощью конструктора графиков	Поддерживается настройка внешнего вида визуальных элементов с применением подхода low-code / no-code	Не поддерживается
4.4. Возможность создания кастомизированных отчетов с применением подхода low-code / no-code;	Поддерживается, кастомизация отчетов возможна с помощью изменения шаблона документа	Поддерживается	Не поддерживается	Поддерживается с помощью функционала Power BI	Поддерживается с помощью изменения шаблонов отчетов в графическом редакторе	Не поддерживается	Поддерживается, кастомизация отчетов возможна с помощью формирования шаблонов отчетов через конструктор отчетов с помощью языка разметки HTML и шаблонизатора Handlebars, при этом для формирования запросов используется язык GraphQL. В шаблонах отчетов «из коробки» кастомизация невозможна, выводятся только свойства по умолчанию, дашборды не выводятся. Подход low-code / no-code не поддерживается, требуется формировать запросы вручную с помощью выражений GraphQL	Поддерживается возможность создания кастомизированных отчетов (на основе преднастроенных шаблонов или полностью «с нуля») с применением подхода low-code / no-code	Не поддерживается
4.5. Функционал тэгирования инцидентов (в ручном и автоматическом режиме);	Поддерживается	Поддерживается вручную и автоматически (на основании правил)	Поддерживается функционал создания и присвоения меток инцидентов	Поддерживается	Поддерживается	Поддерживается с помощью присвоения меток инцидентов	Поддерживается, через заполнение поля «Тег для распознавания»	Поддерживается ручная и автоматическая (по заданным правилам) установка меток (тэгов) для инцидентов для обеспечения удобного поиска и классификации инцидентов	Не поддерживается
4.6. Наличие базы знаний вредоносного ПО;	Не поддерживается	Поддерживается за счет интеграции с VirusTotal	Не поддерживается	Поддерживается через интеграцию с данными проекта MITRE ATT&CK	Частично поддерживается	Не поддерживается	Не поддерживается.	Поддерживается на основе сведений о ВПО из базы проекта MITRE ATT&CK, Kaspersky Threats, open source аналитических сервисов ВПО, SV TIP, а также собственной экспертизы	Не поддерживается
4.7. Возможности экосистемы: наличие опции совместной установки на одной платформе (в рамках одного решения) с модулями управления активами, уязвимостями, киберрисками, аналитикой киберугроз (TIP) и т.д.;	Не поддерживается	Поддерживается экосистема Google Cloud Platform	Поддержка совместной установки с Makves DCAP на одной платформе (одном сервере)	Не применимо	Не поддерживается	Поддерживается работа с TI-данными через модуль XSOAR Threat Intelligence Management. Поддерживается интеграция с коммерческими и Open Source TI-источниками, поддержка получения данных по TAXII, из CSV, JSON файлов	В SOAR Rvision включены продукты управления активами и управления уязвимостями. Поддерживается в рамках экосистемы продуктов R-Vision EVO. Экосистема R-Vision EVO включает продукты SOAR, SGRC, TIP, UEBA, SIEM, TDP (Deception), модуль управления активами и уязвимостями	Используется совместная работа SOAR и модулей управления активами и уязвимостей с расширением на корреляционный движок, покрывающий потребности детектирования инцидентов, возможна совместная работа с модулем SGRC (управление задачами, знаниями, документами, киберрисками, аудитами и соответствием требованиям, КИИ, операционными рисками)	Работа в рамках экосистемы UserGate SUMMA: NGFW, UserGate Management Center, UserGate Log Analyzer, UserGate Client
4.8. Интеграция с ФинЦЕРТ, ГосСОПКА (отправка отчетов по киберинцидентам, получение и обработка ответов).	Поддерживается интеграция с ГосСОПКА, ФинЦЕРТ. Отправка отчетности по инцидентам в ГосСОПКА (автоматически и вручную), получение комментариев и ответов от представителей НКЦКИ в интерфейсе решения.	Не применимо	Не поддерживается	Не применимо	Частично поддерживается. Работа с ГосСОПКА (получение бюллетеней с автоматическим созданием инцидентов в решении, отправка отчетности, получение и обработка ответа от НКЦКИ)	Не применимо	Поддерживается интеграция с ГосСОПКА, ФинЦЕРТ. Поддерживается отправка отчетности по инцидентам в ГосСОПКА (автоматически и вручную), получение сообщений от НКЦКИ в интерфейсе решения.	Поддерживается. Поддержка взаимодействия через API с ГосСОПКА и АСОИ ФинЦЕРТ с двухсторонним обменом информацией об инцидентах, получением	Частично поддерживается. Поддерживается передача информации об инцидентах ИБ в ГосСОПКА, в решении создан шаблон отправки уведомления в ГосСОПКА, отправка выполняется через встроенный

	Получение бюллетеней по уязвимостям и угрозам из ГосСОПКА. Отправка отчетности по инцидентам в ФинЦЕРТ						Поддерживается отправка отчетности по инцидентам через АСОИ ФинЦЕРТ	информации об уязвимостях и угрозах безопасности	коннектор «Gossopka»
5. Расширенный функционал управления киберинцидентами:									
5.1. Поддержка работы MSS-провайдеров с решением, разграничение доступа тенантов;	Поддерживается, с разграничением доступа по "Организациям" в ролевой модели	Поддерживается	Не поддерживается	Поддерживается	Поддерживается	Поддерживается	Поддерживается, с разграничением прав доступа по «Организациям» в ролевой модели	Поддерживается гранулярное разграничение доступа для MSS-провайдеров, включая возможность физического разделения данных для тенантов	Поддерживается
5.2. Выявление аномалий, выявление киберинцидентов на основе внутреннего аналитического движка;	Не поддерживается	Поддерживается	Частично поддерживается с помощью выявления аномалий в количестве событий, зафиксированных за определенный временной промежуток, выявления риск-факторов контролируемых объектов	Поддерживается в «коробочных» группах правил выявления «Machine Learning Behavioral Analytics» и «Fusion»	Не поддерживается	Поддерживается выявление схожих инцидентов, визуализация их возможных взаимосвязей на графической схеме	Не поддерживается непосредственно в решении. Реализовано в дополнительном модуле UEBA	Поддерживается выявление аномалий с использованием методик машинного обучения, обученных на различных датасетах моделей, моделей «без учителя», которые автоматически аппроксимируют действия сущностей и выявляют отклонения по различным комбинациям параметров, а также с применением нейросетей, учитывающих последовательность событий и их взаимосвязи	Не поддерживается
5.3. Наличие, функционал, кастомизация механизма статистического анализа свойств инцидентов;	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается выявление схожих инцидентов на основе их свойств	Поддерживает механизм статистического анализа в сопряжнном модуле UEBA, при этом поддерживается возможность ручной работы со статистикой свойств инцидентов в дашбордах с применением функционала «drilldown» в отфильтрованные списки инцидентов	Поддерживается в модуле UEBA, который является частью экосистемы, реализует несколько десятков встроенных правил для статистического анализа различных параметров активностей пользователей, учетных записей, хостов, процессов. Поддерживается гибкое расширение и настройка новых правил анализа, включая активность, оценку и порог влияния на создание итогового инцидента	Не поддерживается
5.4. Применение методов машинного обучения (наличие и количество предварительно настроенных и обученных моделей машинного обучения), возможность подстройки параметров моделей под конкретную инфраструктуру;	Не поддерживается	Поддерживается, используется технология «Duet AI» с рекомендациями аналитикам на основе обработанной информации	Не поддерживается	Поддерживается технологии машинного обучения (выявление аномалий, инцидентов, построения цепочек атак)	Не поддерживается	Поддерживается использование методов машинного обучения для назначения наиболее подходящих ответственных и участников расследования (на основе их загруженности и работы с предыдущими инцидентами), для выдачи подсказок по выполнению команд, ранее исполняемых в аналогичных инцидентах, для выдачи подсказок при создании сценариев, для автоматической дедупликации инцидентов, для выявления	Реализовано в дополнительном модуле UEBA, входящем в экосистему R-Vision EVO	Поддерживает в модуле UEBA, который является частью экосистемы, использует преднастроенные и обученные модели машинного обучения, с возможностью переобучения, ручного и автоматического подбора параметров моделей	Не поддерживается

						фишинговых email			
5.5. Применение методов обработки Big Data.	Не поддерживается	Поддерживается за счет интеграции с Google Cloud Platform	Не поддерживается	Поддерживается через интеграцию с Azure Synapse Analytics	Не поддерживается	Нет данных	Не поддерживается непосредственно в решении. Реализовано в дополнительном модуле UEBA	Поддерживается за счет интеграции с «озерами данных» на основе Kafka, Hadoop, Elasticsearch и др.	Не поддерживается

TIP

Основные критерии	BI.ZONE ThreatVision	F.A.C.C.T. Threat Intelligence	Kaspersky CyberTrace	PT Cybersecurity Intelligence	R-Vision TIP	Security Vision TIP
1. Общие технические характеристики:						
1.1. Технические требования к платформе и среде внедрения (системные требования к аппаратному и программному обеспечению, окружению);	Только облачная инсталляция на мощностях вендора	Только облачная инсталляция на мощностях вендора	ОС: Linux (предпочтительно) или Windows Server Аппаратные требования: Типовые начальные требования для Kaspersky CyberTrace с коммерческими фидами ЛК: 8 ЦПУ, 24 Гб ОЗУ, 500 Гб дискового пространства, сетевое соединение 1GB Ethernet.	Нет данных	ОС: CentOS, Astra Linux, Ред ОС, Red Hat Enterprise Linux СУБД: PostgreSQL, Redis, RocksDB, ClickHouse Аппаратные требования: 8 ЦПУ (2 ГГц и выше), 16 Гб ОЗУ, 150 Гб дисковой подсистемы	ОС: Microsoft Windows Server 2012 R2 или выше, CentOS 7 или выше, Red Hat Ent. Linux 7 или выше, Ubuntu 18.04 или выше, Debian 10 и выше, Astra Linux CE (Common Edition) релиз "Орел", Astra Linux SE (Special Edition) релиз «Воронеж» и "Смоленск", Альт 8 СП, Альт Сервер 10 или выше, Oracle Linux 8 и выше, РЕД ОС актуальной версии, РОСА "КОБАЛЬТ", AlmaLinux, AlterOS. СУБД: Microsoft SQL Server версии 2016 или выше, PostgreSQL версии 11 или выше, Postgres Pro версии 11 или выше, Jatoba. Аппаратные требования: 16 ЦПУ, 24 Гб ОЗУ, 350 Гб дисковой подсистемы
1.2. Варианты поставки и инсталляции (аппаратный апплайнс, образ, контейнер, установка на «голое железо», установка on-prem, установка в облаке, наличие графических инсталляторов, поддержка виртуализации);	Только облачная инсталляция на мощностях вендора	Только облачная инсталляция на мощностях вендора	Для Kaspersky CyberTrace - дистрибутивы для ОС Linux или Windows. На текущий момент CyberTrace - On-prem решение. Установка в виртуальной среде или на bare metal. Установка выполняется с помощью интерактивного скрипта или инсталлятора. Kaspersky Threat Intelligence Portal - облачный портал. Заказчикам предоставляется доступ к порталу, который размещен в ЦОД вендора. Создаются группы с настройками доступа к сервисам. В группе создаются учетные записи индивидуальных пользователей. Интеграция CyberTrace как on-prem модуля гибридной TIP платформы, включающей облачный TIP портал и on-prem решение (собственно CyberTrace) для работы с чувствительными данными, планируется в будущих релизах.	Поддерживается установка on-prem	Поддерживается установка на физической (bare metal) и виртуальной машине. Поддерживается среда виртуализации VMWare. Для установки платформы предоставляется файл-образ	Поддержка установки в виде контейнера, на «голое железо», в виде ISO образа, RPM-пакетов, из графического инсталлятора и из командной строки. Поддержка систем виртуализации (VMware, VirtualBox, Hyper-V, Xen, Parallels, KVM). Поддерживается установка в облаке и on-prem.
1.3. Архитектурные особенности решения			БД Kaspersky CyberTrace основана на ElasticSearch. Доступ заказчика в базу данных в обход веб-интерфейса и API не предполагается.			Возможность установки отдельного компонента модуля TIP во внешнем контуре для передачи данных во внутренний сегмент сети в целях исключения прямого соединения решения с интернет.

(стек технологий, возможность прямого доступа к внутренним структурам, возможность доступа покупателя к ОС/СУБД решения с правами администратора);	Только облачная инсталляция на мощностях вендора	Только облачная инсталляция на мощностях вендора	Поддерживается установка с выносом компонента загрузки фидов в сегмент DMZ, при этом основной сервер размещается в сегменте без доступа к сети Интернет. Взаимодействие с Kaspersky Threat Intelligence Portal предполагается через веб-интерфейс или REST API.	Нет данных	Используемые СУБД: PostgreSQL, Redis, RocksDB, ClickHouse. Сервисы работают внутри контейнеров Docker	Взаимодействие всех компонент по защищенным протоколам сетевого доступа. Наличие административного доступа к компонентам решения. Используемые сторонние компоненты: Elasticsearch, RabbitMQ, IIS / NGINX, MSSQL / PostgreSQL / Postgres Pro / Jatoba
1.4. Параметры масштабируемости, кластеризации, производительности;	Только облачная инсталляция на мощностях вендора	Только облачная инсталляция на мощностях вендора	Один сервер Kaspersky CyberTrace позволяет обработать поток событий от SIEM до 25000 EPS. Поддерживается балансировка запросов и отправки событий от SIEM. Поддерживается работа в режиме Multitenancy для крупных Enterprise клиентов и MSS-провайдеров. Один сервер CyberTrace может взаимодействовать с несколькими SIEM и проверять индикаторы по разным наборам поставщиков	Нет данных	Поддерживается вертикальная масштабируемость через выделение дополнительных аппаратных ресурсов для платформы и горизонтальное масштабирование с помощью географически распределенных сенсоров SIEM.	Поддерживается балансировка нагрузки между компонентами, возможность установки неограниченного количества нод каждого компонента решения с целью горизонтального масштабирования, возможность установки каждого компонента решения на выделенный сервер
1.5. Поддержка отказоустойчивости (реализация, требования вендора к инфраструктуре покупателя);	Только облачная инсталляция на мощностях вендора	Только облачная инсталляция на мощностях вендора	Поддерживается схема высокой доступности для Kaspersky CyberTrace	Нет данных	Поддерживается	Поддерживается создание кластера высокой доступности, дублирование и резервирование всех элементов решения, возможность создания геокластера, поддержка отказоустойчивости для провайдеров MSS
1.6. Обеспечение безопасной работы решения (ограничение доступа, ролевая модель, защита канала связи, защита обрабатываемых данных, журналирование, способы аутентификации пользователей, контроль действий пользователей решения);	Поддерживается двухфакторная аутентификация, функционал рассылки оповещений о сроке истечения пароля. Действия пользователей отражаются на вкладке истории по объектам. Ролевая модель не поддерживается	Поддержка двухфакторной аутентификации, разграничение доступа по списку IP-адресов, разграничение доступа на уровне компаний и иерархии компаний с предоставлением доступа только к определенным разделам и к некоторым данным (домены, IP-адреса, BIN-номера, бренды), разграничение доступа на уровне пользователей (к определенным разделам, проектам, компаниям)	Доступ в веб-интерфейс CyberTrace осуществляется с помощью логина и пароля учетной записи. Доступна интеграция с LDAP. Ролевая модель предусматривает две роли - Администратор и Аналитик. Аналитик не имеет доступа к секции с настройками продукта в веб-интерфейсе. Веб-сервер CyberTrace входит в состав дистрибутива, перед релизом проходит тщательные проверки на наличие уязвимостей. Для защиты подключения используются защищенные протоколы. Допускается применение доверенных сертификатов TLS для веб-сервера. Аудит действий пользователя не поддерживается. Kaspersky Threat Intelligence Portal поддерживает двухфакторную аутентификацию либо с помощью клиентского сертификата, либо с помощью одноразовых временных паролей. В Kaspersky Threat Intelligence Portal поддерживается 3 уровня доступа: полный, Web (доступ только к веб-консоли), API (доступ только к API).	Поддержка использования пользовательских SSL-сертификатов, шифрование конфигурационных файлов. Поддерживается локальная аутентификация в PT CybSI или SSO-аутентификация через решение PT MC (Management and Configuration). Назначение ролей пользователей происходит в PT MC или в PT CybSI, роль определяет доступные пользователю разделы интерфейса и операции. Для заведенных через PT MC пользователей доступно включение их в группы (администратор, оператор, аналитик, гость). Поддерживается гранулированное разграничение доступа с помощью функционала установки уровня доступа к объектам для пользователей решения	Обеспечивается журналирование событий с возможностью фильтрации событий по временному интервалу и уровню важности события. Поддерживается ролевая модель, аутентификация по учетной записи Active Directory, технология SSO	Поддерживается ограничение доступа на основе IP-адресов, двухфакторная аутентификация, аутентификация по сертификатам для пользователей и компонентов решения (использование самоподписанных сертификатов или сертификатов, выданных внутренним центром сертификации), наличие SSO, использование SSL/TLS для защиты доступа к веб-интерфейсу, аудит попыток входа в систему, аудит действий пользователей и администраторов, ролевая модель управления доступом ко всем элементам решения, поддержка multitenancy, шифрование парольной информации. Наличие специализированного вендорского документа с лучшими практиками по безопасной настройке ПО и окружения.
1.7. Локализация интерфейса, поддержка мультиязычности, возможность кастомизации интерфейса, возможность сквозного поиска по всем обрабатываемым данным.	Локализация интерфейса на русском и английском, интерфейс не кастомизируется, сквозной поиск присутствует	Локализация на русском и английском языках, возможность редактировать панель управления (набор виджетов, отображаемая информация), сквозной поиск только по IP-адресам и доменам	Веб-интерфейс Kaspersky CyberTrace представлен на английском языке. Планируется локализация с русским языком в следующих релизах. Документация доступна на английском, японском и русском языках. В веб-интерфейсе CyberTrace есть возможности поиска по базе данных с индикаторами и отдельно с детектами. Сквозной поиск частично реализован в рамках функции визуализации данных на графах. Кастомизация интерфейса представлена возможностью выбора темной или светлой темы. Веб-интерфейс Threat Intelligence Portal доступен заказчикам на английском языке. Документация доступна на английском или японском языках. Также доступна темная или светлая тема.	Локализация интерфейса на русском и английском, интерфейс не кастомизируется, сквозной поиск присутствует	Поддерживаются языки русский, английский, поддерживается индивидуальная локализация для каждого пользователя. Поддерживается индивидуальный поиск по каждой сущности с возможностью применения обширного фильтра, без возможности сквозного поиска по всем данным. Поддерживается возможность настройки отображения полей, их порядка	Локализация интерфейса и всех элементов на русском и английском, возможность добавления других языков, поддержка тем (темная и светлая), поддержка кастомизации интерфейса (брендирование, логотип), возможность создания рабочих мест пользователей под пользовательский функционал, поддерживается сквозной поиск
2. Общие организационные характеристики:						
			Дата первого релиза Kaspersky CyberTrace: 04.02.2019. В этот день была анонсирована версия 3.0. До этого у продукта не было веб-интерфейса, он назывался Kaspersky Threat Feed Service, поэтому			

2.1. Дата первого релиза, текущая версия;	Нет данных		версионирование продолжилось. Kaspersky Threat Feed Service появился в 2016 году. Текущая версия 4.3 выпущена 11.08.2023. Дата первого релиза Kaspersky Threat Intelligence portal: 10.2016. Текущая версия 1.4 выпущена в мае 2023.	Текущая версия 2.10.1	Дата первого релиза 2019 год. Текущая версия 4.0	Дата первого релиза – 2022 год. Текущая версия – 5.0.1694417270
2.2. Наличие документации, наличие API;	Документация поставляется в онлайн-формате и в виде pdf-документов. API поддерживается, документация на API предоставляется в формате PDF-файла и в формате Swagger	Документация в виде онлайн-справки или отдельного документа. API присутствует и задокументирован	Документация Kaspersky CyberTrace доступна онлайн (русский, японский, английский языки). REST API поддерживается. Kaspersky Threat Intelligence Portal поддерживает взаимодействие через REST API	Документация в формате PDF, API поддерживается	Предоставляется руководство пользователя, API поддерживается, описание API доступно внутри платформы	Документация в виде интерактивной справки в решении, в виде PDF-файлов, поддержка и документация на API
2.3. Наличие технической поддержки, режим работы, SLA-нормативы;	Нет данных	SLA-нормативы определены в зависимости от типа запроса, рабочие часы от 24*7 до 8*5, срок первоначального реагирования от 30 минут, время решения проблемы от 4 рабочих часов	Техническая поддержка сервисов Kaspersky TI оказывается заказчикам в рамках стандартных SLA B2B продуктов. Есть возможность покупки расширенной технической поддержки.	Обращение в техническую поддержку круглосуточно через единый портал вендора, время реакции на критические запросы до 4 часов	Обеспечивается в режиме 24/7	Техническая поддержка трёх уровней. Максимальная - 24/7. Показатели SLA для тарифа «Максимальный»: время реакции: 4 часа, время предоставления решения: 24 часа. Возможность согласования и подписания произвольных SLA-нормативов и условий предоставления услуг.
2.4. Наличие гарантии, срок предоставления гарантийного обслуживания, что включено в стандартное гарантийное обслуживание, возможность расширенной гарантии;	Нет данных	В гарантийную поддержку входит восстановление работоспособности веб-портала, аналитическая поддержка пользователей (включая проведение целевых исследований киберугроз по запросу пользователей),	Условия предоставления продукта, включая условия поддержки, прописаны в пользовательском соглашении.	Нет данных	Предоставляется	Стандартное гарантийное обслуживание на 1 год: -личный кабинет с маркетплейсом дистрибутивов платформы, окружения, ОС, модулями и обновлениями - прием заявок через портал, телефон и эл. почта (кол-во обращений не ограничено); -предоставление консультаций по ВКС, телефону и email; - консультации по: настройке и администрированию программных продуктов, диагностике и сбора информации для определения неисправностей в работе программных продуктов, применению решений по устранению неисправностей и восстановлению работы программных продуктов. При необходимости имеется возможность приобрести расширенную техническую поддержку (сжатый SLA)
2.5. Лицензионная политика: стоимость дополнительных интеграций (ИТ/ИБ-системы, СЗИ, внешние сервисы и т.д.), лицензирование API, правила расчета лицензии (по пользователям, активам, интеграциям и т.д.), отличие в стоимости при разных вариантах инсталляции, специальные условия для MSS-провайдеров;	Нет данных	Предоставление API-доступа входит в стандартную поставку сервиса, стоимость лицензии не зависит от количества пользователей одной компании-клиента.	Kaspersky CyberTrace: бесплатная версия Community Edition доступна после установки продукта. Лицензия Matching engine с ограничениями доступна коммерческим заказчикам сервиса Kaspersky Threat Intelligence Data Feeds. Доступна платная лицензия CyberTrace TIP Enterprise, которая снимает ограничения на использование любых функций продукта. Есть специальные лицензии для MSS-провайдеров. Стоимость лицензии не зависит от инсталляции. Методы API доступны для использования в соответствии с ограничениями текущей лицензии. Например, если лицензия не предоставляет возможность поиска индикаторов в базе с вкладки Search, соответствующий метод не будет возвращать результат и через API. При покупке подписки на фиды ЛК есть возможность приобретения полной лицензии Kaspersky CyberTrace со скидкой. Лицензия Kaspersky CyberTrace TIP Enterprise также входит в состав некоторых комплексных предложений. Threat	Нет данных	Нет данных	Предусмотрены временные и бессрочные лицензии. Метрики лицензирования TIP: 1) Наличие дополнительных модулей 2)Количество обрабатываемых событий в секунду 3)Режим функционирования (количество дополнительных нод) 4)Мультиарендность для MSSP провайдеров, холдингов, групп компаний. Других ограничительных метрик не предусмотрено.

			Intelligence Portal лицензируется по сервисам и по количеству запросов к выбранным сервисам.			API – не лицензируется и включен в любую поставку ПО.
2.6. Опыт внедрений.	Нет данных	Нет данных	Есть большой опыт внедрений Kaspersky CyberTrace на глобальном рынке присутствия Лаборатории Касперского. Заказчику оказывается консультативная поддержка выделенного инженера на этапах пилотирования и внедрения решения.	Нет данных	Опыт внедрений в разных областях	Опыт внедрения во многих отраслях экономики. Среди Заказчиков – Сбербанк России, Альфа-Банк, Тинькофф Банк, Норильский Никель, Северсталь, Евраз, X5 Group, Магнит, ФСО России, Совет Федерации, ФГУП Интеграл, Мегафон MSSP, Центр киберустойчивости Angara SOC, МТС, Первый Канал, Правительство Тюмени, Правительство Красноярска и другие.
2.7. Наличие сертификатов регуляторов, присутствие в реестре российского ПО;	Присутствует в реестре отечественного ПО	Присутствует в реестре российского ПО	Присутствует в реестре российского ПО	Присутствует в реестре российского ПО	Сертификат соответствия ФСТЭК России № 4614 от 02.11.2022 (УД4). Решение присутствует в реестре российского ПО	Сертификат соответствия ФСТЭК России № 4574 от 02.09.2022 (УД4). Сертификат соответствия ОАЦ при Президенте Республики Беларусь № BY/112 02.02. ТР027 036.01 00492 от 05 августа 2022 года (по требованиям технического регламента ТР 2013/027/BY). Решение присутствует в реестре российского ПО
3. Внутренняя обработка сущностей:						
3.1. Типы индикаторов компрометации (IoC) (хэши, домены, IP-адреса и т.д.);	Хэши, адреса IPv4 / IPv6, домены, URL, имена учетных записей (UPN), номера банковских карт, SSL-сертификаты, IMEI, email, JA3-хэши, имена процессов, ключи реестра, номера телефонов	Домен, IP, URL, хэш, имя файла, email-адрес, отпечаток SSH, отпечаток SSL, номер телефона, никнейм атакующего	Kaspersky CyberTrace и Kaspersky Threat Intelligence Portal поддерживают в качестве индикаторов компрометации: Hash (MD5, SHA1, SHA256), IP, URL, Domain.	Файлы (метаданные, хэши), домен, IP-адрес, URL, email, номер телефона, контактные данные и сфера деятельности организации или физического лица,	Поддерживаются следующие типы IoC: хэши (sha256, sha1, md5), домены, IP-адреса (IPv4, IPv6), URL-адреса, e-mail адреса, файлы, маски, банковские карты, учетные записи, хэш паспорта, СНИЛС, номер счета, номер телефона	Поддерживаются следующие типы индикаторов: IP, домен, ключ реестра, строка запуска процесса, URL, хэш (SHA1, SHA256, MD5), JA3S, JARM, Угроза, Злоумышленник, Вредоносное ПО, и др. Поддерживается использование масок (записей, содержащих выражения «*» и «?», для охвата заранее неизвестных имен доменов).
3.2. Возможность создавать свои типы IoC;	Не поддерживается	Не поддерживается	В Kaspersky CyberTrace доступно добавление индикаторов в базу данных вручную или через REST API. Добавление новый типов индикаторов не поддерживается.	Создание пользовательских типов IoC не поддерживается	Не поддерживается	Поддерживается, с применением подхода low-code / no-code
3.3. Внутренняя корреляция IoC, полученных из различных TI-фидов (источников данных киберразведки): например, хэши по ssdeep, IP по CIDR, связь по вредоносным кампаниям и т.д. для сопоставления различных IoC между собой в решении;	Нет данных	Поддерживается, в рамках обработки информации, полученной из различных источниковплатформой F.A.C.C.T. Unified Risk Platform	В Kaspersky CyberTrace если информация об индикаторе поступила в базу данных сразу из нескольких источников, это будет отображаться в карточке с описанием индикатора. В Kaspersky Threat Intelligence Portal реализована связность для сопоставления различных IOC между собой.	Нет данных	Поддерживается	Поддерживается. Строится взаимосвязь между различными IOC и индикаторами атак (IOA) и стратегической атрибуцией на основании данных от поставщиков и обогащения из аналитических источников. Выстроенные взаимосвязи представлены как на карточках индикаторов, так и на графах связей IOC
3.4. Уровни покрытия типов IoC по «пирамиде боли»: технические, поведенческие, операционные, стратегические;	Полное покрытие: от технических индикаторов (хэши, адреса, домены) до ВПО, киберпреступных групп, конкретных кибератак	Полное покрытие, от хэшей и IP-адресов до TTPs и их атрибуции конкретным кибергруппировкам	Kaspersky CyberTrace в сочетании с Threat Intelligence Portal покрывают индикаторы всех уровней. Информация предоставляется на Threat Intelligence Portal в рамках сервиса Reporting с разделением на Crimeware Threat Intelligence Reporting, APT Threat Intelligence Reporting, Industrial Threat Intelligence Reporting, а также в CyberTrace.	Поддерживаются стратегические IoC (злоумышленники, вредоносные кампании), технические (хэши, домены, IP-адреса и т.д.). Не поддерживается информация о TTPs атакующих,	Поддерживается, используемые в решении виды сущностей: индикаторы, уязвимости, вредоносное ПО, отчеты (документы с описанием киберугроз), вредоносные кампании, жертвы кибератак (атакуемые люди, организации), личности (киберпреступники), субъекты угроз (атакующие люди, организации), техники и тактики атак.	Поддерживаются следующие уровни охвата «пирамиды боли»: технические (IP, домен, хэш, URL), поведенческие (ключ реестра, строка запуска процесса), операционные (описание TTPs атакующих, уязвимости), стратегические (угрозы, злоумышленники, ВПО)
3.5. Поддержка обработки индикаторов атак (IoA), поддерживаемые типы;	TTPs по матрице MITRE ATT&CK, связанные с атаками объекты (файлы, домены, URL), инструменты, исполняемые на атакованном устройстве команды	TTPs по матрице MITRE ATT&CK, индикаторы (IP, порты, домены, URL, сертификаты, хэши), используемые инструменты (ВПО, эксплуатируемые уязвимости, используемые легальные инструменты), контакты членов кибергрупп (email, аккаунты на хакерских форумах, партнеры по киберкриминальному бизнесу)	В Kaspersky CyberTrace IoA доступны в контекстных полях индикаторов, в TIP портале - в отчетах.	Поддерживается информация об используемых инструментах (ВПО, эксплуатируемые уязвимости)	Не поддерживается	Поддерживаются IoA следующих типов: ключи реестра, строка запуска процесса, JARM, описание TTPs атакующих из базы MITRE ATT&CK, описание APT-групп
3.6. Поддержка атрибутирования TTPs, APT-групп, конкретных злоумышленников, атакованных организаций, вредоносных кампаний, киберугроз, используемых	Для киберпреступных групп отображаются используемые TTPs по матрице MITRE ATT&CK, связанные с атаками объекты (файлы, домены, URL), используемые атакующими инструменты, страна	Полная поддержка атрибутирования, с разбивкой на прогосударственных хакеров, киберпреступные группы, утечки в результате атак шифровальщиков. Поддержка указания TTPs атакующих, связей атакующих между собой, описания кибератак с указанием атакованных компаний и информации о	В Kaspersky CyberTrace поддерживается в качестве контекста, поступающего в полях фидов. Подробная информация о группировках APT доступна в рамках сервиса APT Threat Intelligence Reporting на Kaspersky Threat Intelligence Portal. Аналогичные сервисы доступны для других типов угроз: Crimeware Threat Intelligence, Industrial Threat Intelligence reporting. Атрибутирование доступно в разделе Threat Analysis	Поддерживается атрибутирование киберрупп, вредоносных кампаний	Поддерживается	Поддерживается атрибуция злоумышленников (APT-группы), ВПО, угроз и уязвимостей для получения полной картины киберугроз, их критичности, уровня развития и распространения

уязвимостей, выявление этапа «kill chain»;	происхождения, мотивация (тип кибергруппы)	конкретном вредоносном воздействии	TIP портала, в будущих релизах планируется добавить атрибуцию APT групп в фиды, на текущий момент уже доступна атрибуция TTPs в фидах ЛК, используемых в CyberTrace.			
3.7. Возможность помечать определенные IoC (например, выбранные по определенным критериям фильтрации) для ведения внутреннего перечня отслеживаемых IoC для контроля их изменений;	Поддерживается, с возможностью указания тэгов, комментариев, голосования «за» или «против» («лайки» характеризуют обратную связь от пользователя о полезности или нерелевантности информации)	Поддерживается возможность добавить результаты обнаружения в «избранное». Возможно также реализовать с помощью функционала получения отчетов по определенным сетевым и файловым индикаторам компрометации за определенный период	В Kaspersky CyberTrace такая возможность есть, выполняется из карточки с описанием индикатора. Для этой цели в системе предусмотрен поставщик InternalTI. Также есть возможность указывать тэги для классификации индикаторов.	Поддерживается с помощью функционала добавления справочных меток, добавления наблюдений для объектов, создания поисковых фильтров. Поддерживается создание репутационных списков релевантных объектов, которые можно экспортировать по API в сторонние системы	Поддерживается с помощью функционала тэгирования	Поддерживается установка признака отслеживания изменений с отправкой оповещений (Telegram, email) при внесении изменений в IoC. Поддерживается фильтрация IoC и выполнение групповой операции «Отслеживать изменения»
3.8. Поддержка стандартов передачи данных об IoC (STIX, OpenIOC, MISP);	Возможность подключаться к Платформе и загружать данные в формате STIX/TAXII (например, реализовано в интеграции с Cisco FMC)	Поддерживается через API с поддержкой STIX/TAXII	Поддерживаются указанные стандарты	Поддерживается STIX	Поддерживается STIX, MISP, OpenIOC	Поддерживается загрузка данных об IoC в форматах CSV, STIX, MISP
3.9. Фильтрация ложных IoC (автоматически, вручную, по расписанию);	Автоматически по внутренней логике, поддерживается возможность ручного удаления или понижения рейтинга некорректных результатов обнаружения в интерфейсе решения	Автоматически по внутренней логике, возможность скрытия некорректных результатов обнаружения в интерфейсе решения для всех пользователей компании	В Kaspersky CyberTrace индикаторы, по которым не было сработок, в случае признания их ЛК ложноположительными, автоматически удаляются из CyberTrace при следующем обновлении фидов. Есть возможность задать явный список индикаторов, по которым не должно быть сработок и сообщений в SIEM: это могут быть как доверенные IP-адреса (например, внутренние адреса локальной сети) и домены (популярные поисковые системы и т.п.), так и индикаторы, которые уже вызвали ложные срабатывания в CyberTrace - в этом случае события сработок автоматически вычищаются.	Поддерживается вручную, с помощью редактирования объектов в решении. Поддерживается возможность вручную присвоить объектам статус «Доверенный», в настройках фида указать «Исключить доверенные»	Поддерживается автоматическое ранжирование угроз (путем интеграции со списками MISP Warninglists) с пользовательской настройкой расчета рейтинга для ранжирования угроз, ручная фильтрация (с помощью создания фильтра исключений – достоверно не вредоносных IoC)	Поддерживается возможность пометки IOC как ложных в автоматическом и ручном режиме. Поддерживается фильтрация IoC и выполнение групповой операции «Пометить как ложный». Возможность ведения белого списка исключений IOC. Поддерживается возможность дополнительной ручной проверки IOC на ложноположительность через внешние сервисы
3.10. Дедупликация IoC;	Автоматически по внутренней логике	Автоматически по внутренней логике	В Kaspersky CyberTrace если информация об индикаторе поступила в базу данных сразу из нескольких источников, это будет отображаться в карточке с описанием индикатора	Автоматически по внутренней логике	Поддерживается	Автоматически поддерживается с помощью объединения одних и тех же индикаторов, полученных от разных поставщиков, в один индикатор, который аккумулирует в себе всю уникальную информацию из разных источников. При возникновении пересечений (от разных источников поступила разная информация по одному и тому же свойству IoC) выполняется дополнение или перезапись информации по настраиваемому пользователем алгоритму
3.11. Поддержка TLP-признаков для IoC и отчетов;	Поддерживается для IoC и групп (атакующие, атака, инцидент, ВПО, сигнатура, правило, отчет, инструмент, уязвимость)	Поддерживается	В Kaspersky CyberTrace можно ввести уровни TLP с помощью тэгов. В Threat Intelligence Portal TLP признаки помечены в сервисе Threat Intelligence Reporting (APT, Crimeware, ICS).	Нет данных	Поддерживается для бюллетеней	Поддерживаются стандартные TLP-уровни (red, amber, green, white)
3.12. Поддержка агрегации обнаружений IoC по ключевым критериям (например, идентичный IP источника / назначения, URL, хэш, домен).	Поддерживается с помощью функционала ручного связывания индикаторов и групп	Нет данных	Не поддерживается.	Нет данных	Поддерживается	Агрегация обнаружении осуществляется по ключевым параметрам обнаружения: IP источника, IP назначения, URL, домен, хэш, email с учетом направления обнаружения.
4. Интеграции:						
4.1. Перечень включенных по умолчанию TI-фидов – источников TI-данных (коммерческие, общедоступные);	Более 30 источников данных (открытые источники, коммерческие базы, информация от операторов связи): собственные источники вендора, данные ФинЦЕРТ, данные от ИБ-вендоров (ESET), данные от защищаемых компаний (ПАО «Сбербанк»), CERT (Итальянский CERT, BI.ZONE CERT)	Собственные фиды компании, собранные платформой F.A.C.C.T. Unified Risk Platform. При этом поддерживается интеграция с TIP других вендоров: Anomali, EclecticIQ, ThreatConnect, ThreatQuotient, MineMeld Threat Intelligence Sharing, MISP (Malware Information Sharing Platform)	В конфигурации Kaspersky CyberTrace поддерживаются потоки данных от Лаборатории Касперского. Если у ЛК появляется новый фид, его можно добавить в конфигурацию Kaspersky CyberTrace в список с другими фидами ЛК. Предустановлен базовый набор популярных источников OSINT. Допускается добавление других источников, используя индустриальные стандарты и протоколы. Данная функция доступа с лицензиями Community Edition и TIP Enterprise.	ФинЦЕРТ, AlienVault Open Threat Exchange, MISP (BOTVRIJ, CIRCL), антивирусы (Avast, Avira, BitDefender, ClamAV, DrWeb, ESET, F-Secure, GData, Kaspersky, McAfee, Microsoft Defender, NANO, Symantec, Trend Micro), базы DNS и Whois записей, данные Россвязь и ЦНИИС (телефонные номера), данные из «песочниц» PT MultiScanner, Trend Micro Deep Discovery Analyzer, Pyshok (RU-CERT), VirusLocal (RU-CERT)	Поддерживается работа с источниками R-Vision Threat feed, Kaspersky Threat Intelligence, Group-IB, AT&T Cybersecurity, IBM X-Force Exchange, RST Cloud, MISP, BI.ZONE, ФинЦЕРТ АСОИ, Mitre CWE List, MITRE ATT&CK, ESET Threat Intelligence, Shadowserver Network Reporting, National Vulnerability Database, Open source фиды. Поддерживается возможность добавления произвольных поставщиков (поддерживается доступ по HTTP(S), API, разбор текстовых, CSV, PDF файлов)	Поддерживаются «из коробки» следующие поставщики TI-данных: RST Cloud, BI.ZONE, FACCT (ex-Group-IB), Kaspersky, AlienVault, MISP, URLhaus, DigitalSide, Feodo Tracker, Shodan, ФинЦЕРТ, NVD, БДУ ФСТЭК, НКЦКИ, MITRE ATT&CK. Поддерживается возможность подключения новых источников с применением подхода low-code / no-code без привлечения вендора
4.2. Возможность управления			В Kaspersky CyberTrace расписание загрузки			Поддерживается настройка расписания загрузки данных для каждого поставщика, расписание «из

расписанием загрузки TI-данных от различных вендоров;	Не поддерживается	Не поддерживается	устанавливается глобально для всех источников данных.	Поддерживается для каждого фида в отдельности	Поддерживается	коробки» настроено на оптимальную периодичность загрузки (в зависимости от объема данных от каждого поставщика)
4.3. Наличие собственных TI-фидов от вендора решения;	Поддерживается: BiZone C&C (перечень C&C-серверов ВПО), BiZone CERT (данные от CERT компании BiZone), BiZone CESP (данные от решения Cloud Email Security & Protection), BiZone DGA (DGA-домены, используемые ВПО), BiZone Infected Hosts (зараженные устройства по данным специалистов BiZone), BiZone SOC (данные от SOC компании BiZone)	Собственные фиды компании, собранные платформой F.A.C.C.T. Unified Risk Platform	Поддерживаются следующие собственные TI-фиды: ·Коммерческие потоки данных об угрозах (Botnet C&C URL Data Feed, IP Reputation Data Feed, Malicious Hash Data Feed, Malicious URL Data Feed, Mobile Botnet C&C URL Data Feed, Mobile Malicious Hash Data Feed, Phishing URL Data Feed, Ransomware URL Data Feed, IoT URL Data Feed, ICS Hash Data Feed); ·Потоки данных об угрозах «APT feeds» (APT Hash Data Feed, APT IP Data Feed, APT URL Data Feed); ·Демонстрационные потоки данных об угрозах (Demo Botnet C&C URL Data Feed, Demo IP Reputation Data Feed, Demo Malicious Hash Data Feed); Инкрементные потоки данных об угрозах (Botnet C&C URL Data Feed, Phishing URL Data Feed, Malicious URL Data Feed).	Данные от центра экспертизы PT ESC (Expert Security Center), результаты анализа в PT Sandbox и PT MultiScanner	Не поддерживается	Не поддерживается
4.4. Наличие встроенной базы уязвимостей;	Поддерживается, с указанием CVSS-вектора, связанных объектов (кампании, ВПО, IP, домены), комментариев	Поддерживается, с информацией об уязвимостях: CVSS, временная шкала изменения статусов уязвимости, использование в эксплойтах, использование кибергруппами, упоминание уязвимости в DarkWeb, ссылки на Twitter и GitHub с описанием эксплуатации уязвимости. Доступно в виде отдельного фида с данными по новым/актуальным уязвимостям	Доступно в виде отдельных фидов. Часть данных можно загрузить и использовать в CyberTrace.	Не поддерживается, при этом для вредоносных объектов используется свойство «Эксплуатирует уязвимости»	Поддерживается база уязвимостей National Vulnerability Database	Поддерживается ведение списка уязвимостей в виде отдельных объектов с установкой связей между IoC / IoA / стратегической атрибуцией и уязвимостями. Поддерживаемые «из коробки» источники данных об уязвимостях: Group IB, Kaspersky, NVD, БДУ ФСТЭК, НКЦКИ
4.5. Поддержка протоколов получения событий для поиска в них IoC (TCP / UDP, API, получение событий из очереди, выполнение запросов к БД, Syslog, CEF, LEEF и т.д.);	Поддерживается через API-взаимодействие с помощью модуля для поиска информации в решении	Поддержка интеграции с SIEM-системами: IBM QRadar, ArcSight, MaxPatrol SIEM, Splunk.	В Kaspersky CyberTrace основной способ получения событий и IoC для поиска - TCP. Поддерживается выполнение запросов через REST API. Формат входящих событий по протоколу TCP значения не имеет, так как используются регулярные выражения для извлечения индикаторов из любых входящих событий. Форматы CEF, LEEF поддерживаются по умолчанию при выборе интеграций с соответствующими SIEM (ArcSight, IBM QRadar), регулярные выражения и формат событий о детектах уже преднастроен для соответствия этим форматам.	Поддерживается API-интеграция с внешними системами для экспорта IoC, хранящихся в решении. Получение событий для поиска в них IoC возможно только при совместной работе решения с MP SIEM, PT NAD	Частично поддерживается с помощью механизма сенсоров (специальных программных модулей), которые осуществляют поиск IoC в ArcSight ESM, ArcSight Logger, IBM QRadar, MaxPatrol SIEM, Apache Kafka, SmartMonitor. Сенсоры настраиваются на нодах, ноды устанавливаются отдельно. Сенсоры предназначены для обнаружения IoC в интегрированных SIEM/LM-системах. Оповещения о найденных IoC отправляются в само решение (TIP), без возможности создать инцидент / алерт в SIEM/LM-системе	Поддержка событий в формате CEF, LEEF, Syslog, EMBLEM (Cisco Syslog), ELFF (Blue Coat), JSON, Windows Event Log, REST API-взаимодействие, Kafka, запросы к БД (MS SQL, Postrges, MySQL, Oracle).
4.6. Возможность интеграции с СЗИ в режимах Push (инициатор – решение) и Pull (инициатор – СЗИ);	Поддерживается через API-взаимодействие (инициатор – СЗИ) и через Syslog-отправку информации в формате CEF (инициатор – решение, используется для интеграции с ArcSight)	Нет данных	В Kaspersky CyberTrace передача индикаторов в СЗИ в режиме Push может быть реализована с помощью функции Indicators Export. Режим Pull может быть реализован с использованием REST API Kaspersky CyberTrace или Threat Intelligence Portal.	Поддержка только режима Pull	Поддерживается API-интеграция с решением R-Vision SOAR версии 4.2.1 и выше, поддерживается интеграция (с инициализацией запроса со стороны СЗИ, режим Pull) с межсетевыми экранами Cisco ASA v9 и выше, PaloAlto v9 и выше, Checkpoint R80.10 и выше, UserGate 6.X и выше	Поддерживаются оба варианта
4.7. Интеграция с внешними сервисами обогащения данных об IoC (например, Whois, Spamhaus, VirusTotal и т.д.);	Базы Passive DNS, WHOIS	Базы Passive DNS	В Kaspersky CyberTrace в качестве источников для обогащения данных на графах доступны Kaspersky Threat Intelligence Portal и VirusTotal. Из карточки описания индикатора возможен переход к описанию IoC в Kaspersky Threat Intelligence Portal, если у заказчика есть лицензия на сервис Threat Lookup.	Whois, DNS сервисы	Поддерживается работа с Whois, VirusTotal, Cisco Umbrella, IBM xForce, DomCop, Hybrid Analysis, Majestic Million, OPSWAT Metadefender	Поддерживается обогащение IoC данными из источников: IPgeolocation.io, KasperskyOpenTip, IPInfo.io, MaxMind Geo-IP, Whoisxmlapi, VirusTotal, Shodan, HaveiBeenPwned, SecurityTrails, Urlscan.io, Censys, MXToolBox, Scamalytics, PassiveDNS, RiskIQ, WhoIsXMLAPI, RSTCloud, any.run, censys, DomainTools, FOFA, Intezer, MXTools, Netlas.io, Scamalytics, SourceForge, Lolbas
						Поддерживается большой набор функций реагирования на хосте, на котором произошло обнаружение: снятие телеметрии, блок процесса, помещение в карантин, дроп сессий и многие другие.

4.8. Возможность выполнения реагирования с устройствами, находящимися в защищаемой инфраструктуре;	Частично поддерживается с помощью интеграций (например, выгрузка списков IoC в СЗИ)	Не поддерживается	Событие матчинга IOC можно отправить в SIEM решение для формирования алерта. Также в CyberTrace интеграция осуществляется путем автоматизации экспорта индикаторов из базы по преднастроенным фильтрам. В результате формируется ссылка на CSV файл, который сторонние устройства могут использовать в качестве источника данных, также доступно API для более сложных вариантов интеграции.	Не поддерживается	Поддерживается интеграция с Cisco ASA через API CLI по протоколу ssh в список безусловной блокировки командой shun	Поддерживается реагирование по внешнем хосту, задействованному в обнаружении с помощью: ·Отправки инцидента в SIEM-систему или добавление в списки значений: MaxPatrol SIEM, IBM QRadar SIEM, KUMA, Microfocus ArcSight, Splunk; ·Блокирования IoC на межсетевом экране: поддерживается создание правил на NGFW CheckPoint, Cisco ASA, Cisco Firepower, Fortigate, Juniper; Возможна отправка инцидента в SOAR-систему: поддерживается интеграция с решением Security Vision SOAR; Отправки IoC в «песочницу»: поддерживается интеграция с Kaspersky KATA (внутренняя песочница), PT Sandbox (внутренняя песочница), TrendMicro DDA (внутренняя песочница), VirusTotal (внешняя песочница), Kaspersky TIP (внешняя песочница). Дополнительно предусмотрены действия над почтовым адресом и учетными записями, связанными с обнаружением (поиск, блокировка, разблокировка).
4.9. Интеграция с тикетинг-системами, возможность двусторонней связи с решением;	В перечне интеграций отсутствуют тикетинг-системы	Не поддерживается	Могут быть разработаны с использованием REST API Kaspersky CyberTrace и Threat Intelligence Portral, нативные интеграции с тикетинговыми системами отсутствуют.	Не поддерживается	Поддерживается с помощью решения R-Vision SOAR	Поддерживается двусторонняя интеграция с Security Vision различных комплектаций (возможность создания задач в платформе и трекинг, сбор статусов, атрибутов), возможность создания задач и заявок во внешних ServiceDesk-системах Jira, Naumen Service Desk, MicroFocus Service Manager (HP Service Manager), BPM Online (Creatio), OTRS) и обратный сбор статусов, атрибутов заявок/задач.
4.10. Поддержка географической ассоциации IoC / IoA (страны, территории).	Поддерживается ассоциация по отраслям, атакуемым странам	Поддерживается (страны и регионы)	Да, в CyberTrace и TIP портале на карточке с подробным описанием индикатора доступна предоставленная информация, включая поля geo. Также эта информация доступна при работе с графами.	Поддерживается ассоциация по странам для IoC	Поддерживается для IoC	Поддерживается обработка географических признаков IoC. Дополнительная возможность отображения IoC на географической карте (дашборд).
5. Поддержка процессов:						
5.1. Контроль, создание и управление жизненным циклом IoC (включая автоматическую обработку IoC в соответствии с настраиваемыми правилами получения, обогащения, обнаружения, экспорта);	Автоматический контроль жизненного цикла: удаление IOC спустя заданное время в силу потери актуальности	Автоматический контроль жизненного цикла: удаление IOC спустя заданное время в силу потери актуальности	В Kaspersky CyberTrace есть возможность настройки автоматического получения индикаторов из заданных источников, автоматического обнаружения индикаторов в событиях для поиска (по заданному типу регулярных выражений), автоматического экспорта индикаторов (по заданному набору фильтров). Автоматическое обогащение индикаторов не поддерживается. Жизненный цикл настраивается для источника данных. Возможно задать срок хранения индикаторов из фида в базе данных Kaspersky CyberTrace. Контроль за жизненным циклом IOC осуществляется в рамках работы сервиса «saved search» в Kaspersky Threat Intelligence Portal	Поддерживается настройка правил обогащения (анализ артефакта в «песочнице», поиск во внешних источниках), правил экспорта (для отправки данных во внешние системы расписание настраивается как частота формирования среза данных по определенному фильтру)	Поддерживается с помощью правил обнаружения, обогащения, экспорта, работы с интеграциями, оповещения. Система управляет активностью IOC на основе TTL критерия	Поддерживается автоматическое и ручное управление жизненным циклом IoC с возможностью настройки правил получения, обогащения, обнаружения, экспорта IoC. Есть возможность настройки TTL, определяющего актуальность IOC конкретного типа. Неактуальные IOC удаляются из системы по прошествии заданного времени
5.2. Поддержка создания «белого списка» IoC, установка признака «ложноположительный» для IoC;	Возможность удалить IoC, отметить как нерелевантный	Не поддерживается	В Kaspersky CyberTrace белый список поддерживается с ранних версий продукта. В более поздних версиях он переименован в список ложноположительных индикаторов, однако функциональность добавления в данный список доверенных индикаторов - наряду с ложноположительными - по-прежнему доступна.	Поддерживается возможность вручную присвоить объектам статус «Доверенный», в настройках фида указать «Исключить доверенные»	Поддерживается с помощью ручной фильтрации (с помощью создания фильтра исключений – достоверно не вредоносных IoC)	Поддержка создания исключений («белый список») для IoC, с контролем отсутствия загрузки отмеченных IoC в решение (ранее загруженные IoC, подпадающие под критерии исключения, будут исключены из обнаружений). Поддерживается внесение подсетей IP-адресов (в CIDR-формате) в исключения. Для обнаруженных IoC можно установить признак «False-Positive»
5.3. Актуализация IoC, установка срока жизни IoC, настройка пользовательских параметров срока жизни IoC, отображение дат создания, изменения и	Отображаются даты первого и последнего обнаружения IoC, создания и обновления записи об IoC. Для IoC вендором устанавливается TTL, по истечению которого	Не поддерживается возможность пользовательской настройки, все действия выполняются вендором. Отображается информация о дате первого и последнего обнаружения	В Kaspersky CyberTrace актуализация IoC производится автоматически при обновлении фидов. Даты обнаружения и последнего детекта отображаются для индикаторов, полученных из Kaspersky Threat Data Feeds. Сроки жизни индикаторов зависят от источника данных. Индикаторы, полученные ранее из Kaspersky Threat Data Feeds, сразу же удаляются из базы индикаторов CyberTrace, если они отсутствуют в последней	Для объектов поддерживается указание даты регистрации в решении, создания, публикации, обновления в решении. Настройка хранения информации об атрибутах и связях объектов выполняется путем редактирования	Поддерживается установка времени и скорости устаревания IoC с помощью настройки ранжирования угроз. Поддерживается указание даты первого и последнего появления, даты получения и создания IoC. Поддерживается установка срок	Поддерживается автоматическое и ручное управление жизненным циклом IoC с возможностью настройки времени активности (IoC получает статус «Неактивный» по истечении заданного времени от его последнего обнаружения) и времени жизни (IoC удаляется по истечении заданного времени от его

обнаружения (первое, промежуточные, последнее) IoC;	объекты перемещаются в архив с пользовательской возможностью восстановления из архива	объекта	версии фида, и по ним не происходило детектов. Индикаторы, полученные из сторонних источников, автоматически удаляются из базы через 90 дней в случае отсутствия детектов. При наличии детектов индикаторы сохраняются, пока пользователь не удалит их.	конфигурационного файла	действия данных обогащения данных по IoC (дни, часы, минуты) с повторным запросом устаревших данных.	последнего обнаружения). Возможность настройки индивидуальных значений периодов активности и времени жизни для каждого типа IOC.
5.4. Поддержка в модели данных IoC / IoA с «пирамидой боли».	Все IoC / IoA в соответствии с «пирамидой боли» присутствуют	Все IoC / IoA в соответствии с «пирамидой боли» присутствуют	Да, в Kaspersky CyberTrace и Threat Intelligence Portal поддерживаются все уровни IoC и IoA.	Частично, не все IoC / IoA в соответствии с «пирамидой боли» присутствуют	Поддерживается для IoC	Поддерживается
6. Взаимодействие с пользователем, удобство использования, оптимизация работы:						
6.1. Поддержка вариантов поиска по IoC (полнотекстовый, regex, маски, быстрый поиск);	Поддерживается гибкий поиск и поиск по полному соответствию	Поддерживается поиск по всем индексированным данным с помощью синтаксиса Lucene (построение сложных запросов с использованием регулярных выражений, подстановочных знаков и логических выражений). Поддержка регулярных выражений присутствует также в настройке создания правил Threat Hunting	Для поиска по IoC в CyberTrace есть несколько вариантов: 1. Поиск индикаторов; 2.Формирование сложных поисковых запросов к базе данных на вкладке Indicators, доступно сохранение поисковых запросов для переиспользования. В Kaspersky Threat Intelligence Portal можно осуществлять поиск по хэшам (MD5, SHA-1, SHA-256), IP-адресам, доменам. Доступен полнотекстовый поиск. Для поиска в Darkweb доступен синтаксис ElasticSearch.	Поддержка быстрого поиска объектов по ключевым атрибутам, поддержка расширенного поиска с указанием параметров объектов, поддержка задания масок при поиске	Поддерживается полнотекстовый поиск и поиск с заданием маски.	Поддерживается полнотекстовый поиск (по всем колонкам) и фильтрация записей в таблице (с созданием дерева условий по комбинации любых атрибутов IOC / IOA / стратегической атрибуции и возможностью сохранения фильтра). Поддерживается выполнение быстрого поиска и сортировка.
6.2. Выгрузка IoC в отчете (doc, pdf), экспорт и импорт в разных форматах (xml, json, csv, STIX, OpenIOC), в том числе через API-взаимодействие;	Поддержка экспорта данных через универсальный модуль экспорта в форматах CSV, JSON. Поддерживается экспорт IoC в формате STIX/TAXII (например, реализовано в интеграции с Cisco FMC). Поддерживается импорт IoC в решение из файлов формата DOCX, из тела email, с веб-страницы	Поддерживается экспорт данных в CSV-формате, выгрузка через API в интегрируемые системы, экспорт TTPs атакующих по матрице MITRE ATT&CK в JSON-формате	В Kaspersky CyberTrace доступен экспорт индикаторов в CSV-формате по фильтрам, автоматически и настраиваемые поля. Также доступен экспорт дашбордов в формате HTML. Экспорт отчетов в формате PDF не поддерживается. Импорт допускается через Custom feed в различных форматах или REST API. В Kaspersky Threat Intelligence Portal можно экспортировать результаты поиска в форматы CSV, OpenIOC, STIX. Результаты исполнения файла в облачной песочнице можно экспортировать в формате CSV, JSON, PCAP, STIX. Результаты анализа Cloud Attribution могут быть экспортированы в формате JSON, STIX, YARA.	Экспорт в JSON-формате вручную или через API, поддержка формата STIX	Поддерживается формирование аналитических отчетов в формате PDFc отправкой по email. Поддерживается экспорт IoC в файлы JSON, CSV, XLSX, STIX	Поддерживается функционал выгрузки IoC в форматах XLSX, CSV и STIX2 с сохранением в локальном или сетевом каталоге. Поддерживается экспорт данных (включая IoC) из решения в формате JSON через API. Поддерживается формирование отчетов (общий отчет, по индикаторам, по обнаружениям, по уязвимостям, по фидам и поставщикам) в форматах DOCX, PDF, XLSX, ODS, ODT, TXT. Поддерживается формирование отчетов вручную, автоматически, по расписанию, с отправкой отчетов на email, в Telegram, на файловый сервер, через API-интеграцию во внешние системы
6.3. Методы оптимизации вычислительной нагрузки на решение (например, конвейерная обработка данных, пакетная обработка данных, оптимизация кода и т.д.);	Нет данных	Нет данных	В Kaspersky CyberTrace поддерживается многопоточность с возможностью конфигурации решения в зависимости от профиля нагрузки.	Нет данных	Нет данных	Используются алгоритмы многопотоковой обработки индикаторов компрометации, нормализация, хранение и работа с нормализованными данными; группировки однотипных данных, дедупликации, агрегации и индексации данных
6.4. Каналы оповещений об обнаружении совпадения, выявления IoC (например, почта, СМС, мессенджеры);	Оповещение выполняется с помощью подписки на уведомления (события, связанные с объектами решения), которые приходят на email	Email	В Kaspersky CyberTrace событие об обнаружении индикатора отправляется по протоколу TCP в приемник SIEM системы в кастомизируемом формате. Предполагается, что другие способы уведомления об инцидентах реализованы на стороне SIEM в результате сработки правил корреляции. Это позволит отфильтровать низкоприоритетные сработки и рассматривать их в связке с другими событиями от источников в SIEM. Отправка уведомлений о сработках и отправка статистических отчетов не поддерживается.	Email	Поддерживается отправка по email, отправка по API в решение R-Vision SOAR	Поддерживается «из коробки» отправка оповещений по email и Telegram, с поддержкой настройки произвольного канала оповещений (HTTP-POST, запись в БД и т.д.)

			Kaspersky Threat Intelligence Portal поддерживает оповещения по электронной почте.			
6.5. Ролевая модель для пользователей, поддержка ролевой модели SOC из коробки;	Не поддерживается	Ролевая модель пользователей функционирует на основе принадлежности пользователя к компании, для которой задаются права доступа. Доступ пользователя может быть предоставлен к определенным разделам, проектам, компаниям. Полноценная ролевая модель SOC не поддерживается	В Kaspersky CyberTrace поддерживается ролевая модель доступа - Аналитик и Администратор. Аналитик не имеет доступа к секции с настройками в веб-интерфейсе Kaspersky CyberTrace. В Kaspersky Threat Intelligence Portal пользователи группы имеют равные права доступа к сервисам. Возможно назначение учетной записи администратора, которая имеет права на создание других учетных записей в рамках текущей группы.	Ролевая модель поддерживается, но не соответствует типовой ролевой модели SOC	Поддерживаются роли «Пользователи», «Администраторы», «Аналитики»	В решении настроены роли «Администратор TIP», «Аналитик угроз», «Оператор», «Руководитель отдела» с возможностью полной перестройки ролевой модели под требования внутренних процессов конкретного Заказчика
6.6. Настройка отображения данных (карточки IoC, вывод определенных столбцов в общем списке), темы интерфейса;	Выводимые поля для IoC и группы настраиваются	Поддерживается возможность редактировать панель управления (набор виджетов, отображаемая информация)	В Kaspersky CyberTrace и Threat Intelligence Portal поддерживаются светлая и темная темы интерфейса. Карточки индикаторов в Kaspersky CyberTrace доступны с вкладки Indicators. При просмотре вкладки Indicators доступна фильтрация по типам индикаторов, поставщикам, тэгам.	Не поддерживается, отображение выводимых данных не кастомизируется	Поддерживается кастомизация списка отображаемых столбцов в табличном представлении, фильтрация и сортировка данных в табличном представлении	Поддерживается настройка внешнего вида карточки объекта (IoC, IoA, уязвимость и т.д.) в графическом редакторе с применением подхода low-code / no-code, поддерживается настройка вывода любых столбцов в списке. Возможность настройки состава столбцов в общем списке индивидуально для каждого пользователя. Поддерживаются темная и светлая темы интерфейса
6.7. Сохранение фильтров;	Поддерживается	Поддерживается использование только предустановленных фильтров	В Kaspersky CyberTrace доступно сохранение поисковых запросов на вкладке Indicators.	Поддерживается создание и сохранение поисковых фильтров	Поддерживается	Возможность создания предустановленных фильтров для ролей и быстрый переход между данными по разным фильтрам. Возможность создания и сохранения индивидуального фильтра для каждого пользователя
6.8. Возможность создавать свои представления;	Поддерживается создание собственных виджетов	Поддерживается для панели управления	В Kaspersky CyberTrace есть возможность сохранения поисковых запросов с целью работы с определенной выборкой индикаторов. Кастомные дашборды не поддерживаются.	Не поддерживается	Не поддерживается	Поддерживается в графическом редакторе с применением подхода low-code / no-code
6.9. Возможность обмена (выгрузки) IoC сторонним компаниям/вендору (если да, то какие применяются способы защиты и анонимизации передаваемых данных);	Поддерживается, ограничение доступа с помощью TLP-признаков	Выгрузка в csv-файл, интеграция с другими TIP-решениями Anomali, EclecticIQ, ThreatConnect, ThreatQuotient, MineMeld Threat Intelligence Sharing, MISP (Malware Information Sharing Platform)	В CyberTrace доступен экспорт индикаторов в CSV формате по фильтрам, автоматически и настраиваемые поля. Возможно использование basic authentication для доступа к URL с экспортируемым множеством индикаторов.	Поддерживается выгрузка JSON-файлов через API, разграничение доступа и анонимизация выполняется на этапе создания выгрузки	Поддерживается через выгрузку и экспорт IoC	Поддерживается автоматизация экспорта данных в JSON-формате через API или файловой выгрузки
6.10. Наличие истории изменений по IoC / IoA / уязвимостям и т.д.;	Поддерживается ведение истории изменения для IoC	Поддерживается для IoA (временная шкала атак для кибергрупп) и для уязвимостей (временная шкала изменения статусов уязвимости)	В Kaspersky CyberTrace есть возможность вести историю изменений индикатора с помощью комментариев в карточке индикатора. В Kaspersky Threat Intelligence Portal предоставляется информация об истории изменений статуса IP-адреса / домена.	Не поддерживается	Поддерживается хранение истории IoC в блоке «Жизненный цикл» карточки индикатора компрометации	Поддерживается ведение и сохранение истории изменений всех атрибутов IoC, обнаружения IoC, TI-фида, угрозы, уязвимости (с отображением даты и времени, инициатора изменений)
6.11. Наличие массовых операций (например, проставление тэгов в IoC, добавление в СЗИ и т.д.), включая создание пользовательских массовых действий;	Предустановленные массовые операции поддерживаются (удаление, комментарии, добавление тэгов, голосование), создание пользовательских массовых операций не поддерживается	Не поддерживается	В Kaspersky CyberTrace возможна пометка индикаторов как False Positive в массовом режиме, также доступен массовый экспорт для автоматического импорта в сторонние СЗИ.	Поддерживается	Поддерживается выполнение групповых операций над IoC, без возможности создания пользовательских массовых действий	Наличие различных предустановленных действий – добавление тэгов, добавление в списки различных СЗИ, отметка как ложных, отметка как неактивные, возврат в активные. Поддерживается добавление произвольных массовых операций над объектами в решении
6.12. Встроенная веб-помощь в интерфейсе системы.	Поддерживается, скачивается в виде PDF-файлов	Поддерживается	На каждой странице веб-интерфейса Kaspersky CyberTrace доступна ссылка на соответствующую страницу онлайн-справки. В Kaspersky Threat Intelligence Portal есть отдельное меню с онлайн-документацией по всему функционалу портала.	Поддерживается	Поддерживается	Присутствует встроенная веб-помощь с поиском и кросс-ссылками
Расширенные критерии	**BI.ZONE ThreatVision**	**F.A.C.C.T. Threat Intelligence**	**Kaspersky CyberTrace**	**PT Cybersecurity Intelligence**	**R-Vision TIP**	**Security Vision TIP**
1. Общие технические характеристики:						
1.1. Поддержка работы во внутреннем сегменте без доступа Интернет;	Не поддерживается	Не поддерживается, поддержка работы только через интернет-сервис	Поддерживается	Поддерживается установка в отдельных сетевых сегментах	Поддерживается	Поддерживается, работа решения не требует доступа в сеть Интернет
1.2. Возможность загрузки IoC из внешних источников через	Не поддерживается	Не поддерживается	Поддерживается	Нет данных	Поддерживается	Поддерживается с установкой опционального

отдельный компонент, расположенный в DMZ;						сервера коннекторов для изолированных сетей
1.3. Возможность использования TIP как услуги (SaaS-модель);	Поддерживается	Поддерживается, функционирует как интернет-сервис	Поддерживается	Нет данных	Не поддерживается	Поддерживается
1.4. Поддержка работы в режиме multitenancy.	Поддерживается	Поддерживается, с разграничением доступа на уровне компаний или иерархии компаний	Поддерживается	Нет данных	Поддерживается через подключение нод с различных площадок заказчиков	Поддерживается
2. Общие организационные характеристики:						
2.1. Наличие авторизованного обучения от вендора, стоимость обучения;	Нет данных	Официальное обучение в образовательном центре F.A.C.C.T.	Проводится обучение в авторизованных вендором учебных центрах	В рамках обучающих курсов от вендора	Обучение по курсам администрирования и использования решения, выдается сертификат вендора	Проводится бесплатное обучение в собственном учебном центре вендора с выдачей сертификата
2.2. Дорожная карта развития продукта (планируемый к внедрению функционал и ориентировочные сроки реализации, планируемые изменения в лицензионную политику).	Нет данных	Нет данных	Планируется реализовать: аудит действий пользователя, локализация с русским языком, кастомные дашборды, добавление новых типов индикаторов, более тесная интеграция IoA в on-prem часть решения, атрибуция APT групп в фиды, агрегация обнаружений IoC по ключевым критериям, расширение источников обогащения, интеграции с тикетинговыми системами, интеграция с системами управления уязвимостями для приоритизации уязвимостей, автоматическое обогащение индикаторов, экспорт отчетов в формате PDF, отправка уведомлений о сработках и статистических отчетов	Нет данных	Нет данных	Расширение коробочных типов IoC/IoA, с акцентом на финансовые организации. Расширение модели данных и добавление новых типов индикаторов компрометации. Расширение типов индикаторов возможных для обнаружения в инфраструктуре, имплементация методологии автоматизированного ThreatHunting. Выстраивание KillChain атаки на основе обнаружений индикаторов компрометаци. Расширение перечня коробочных интеграций с СЗИ и ИТ-системами, в том числе с акцентом на российское ПО.
3. Внутренняя обработка сущностей:						
3.1. Поддержка обработки неструктурированных отчетов (html, pdf, email, отчеты исследователей в произвольной форме, соцсети, сайты, блоги, мессенджеры) в случае использования собственных TI-фидов от вендора решения;	Поддержка обработки данных от сервисов BiZone (CERT, SOC), анализ утечек (учетные записи, данные с Pastebin, GitHub, Trello), анализ подозрительных мобильных приложений, фишинговых и мошеннических ресурсов, ресурсов в даркнет, закрытых групп, сообщений в СМИ (инфополе)	Поддержка обработки отчетов исследователей, данных paste-сайтов, соцсетей, мессенджеров, форумов, GitHub, собственная экспертиза (реверс-инжиниринг, данные собственной «песочницы» Malware Detonation Platform (MDP), результаты форензик-исследований, результаты оперативной работы в сообществах кибератакующих), собственная сеть сенсоров, honeypot, веб-краулеров, сканеров, результаты работы собственного CERT. Все данные агрегируются в платформе F.A.C.C.T. Unified Risk Platform	Поддерживается обработка данных в форматах JSON, STIX, XML, CSV, MISP, email, PDF	Не поддерживается	Поддержка обработки текстовых, CSV, PDF файлов	Поддерживается возможность анализа индикаторов компрометации, загруженных на платформу с последующей генерацией кастомизированных отчетов в форматах docx, pdf, xlsx, ods, odt, txt, csv
3.2. Внутренняя приоритизация IoC, встроенная модель оценки (скоринг) для управления уровнем критичности получаемых IoC в зависимости от уровня доверия к TI-фиду и получаемых от него данных аналитики киберугроз;	Поддерживается с простановкой уровня доверия источнику и уровня опасности угрозы	Информации присваивается степень доверия к данным, процент надежности и достоверности	Поддерживается	Поддерживается оценка достоверности предоставленной информации и точности источника. Автоматически проставляется агрегированное значение достоверности атрибута на основании фактов, полученных от разных источников	Поддерживается через расчет рейтинга для ранжирования угроз	Поддерживается обработка уровней критичности и доверия IoC по данным от TI-поставщика, а также автоматический расчет уровней критичности и доверия в решении на основе данных о достоверности, значимости категории и актуальности IoC. Логика и формула для расчета критичности может быть настроена пользователем.
3.3. Возможность кастомизации вышеуказанной модели оценки;	Поддерживается с помощью настройки уровня доверия источнику и уровня опасности угрозы	Не поддерживается	Нет данных	Не поддерживается	Поддерживается	Поддерживается с помощью настройки логики и формулы для расчета критичности
3.4. Поддержка поиска IoC в получаемых данных от СЗИ и элементов ИТ-инфраструктуры, отображение «сырого» события при обнаружении, поддерживаемые типы	Не поддерживается	Не поддерживается	Поддерживается в решении Kaspersky Cyber Trace.	Выполняется только при совместной работе с MP SIEM, PT NAD	Поддерживается	Поддерживается обработка данных от SIEM-систем (MaxPatrol SIEM, Kaspersky KUMA, Splunk, ArcSight (ESM, Logger, SmartConnector), IBM QRadar, Fortinet FortiSIEM, RuSIEM, Splunk, Pangeo Radar), межсетевых экранов (Cisco, Check Point, FortiGate, IdecoUTM, Juniper, UserGate, VipNet, Континент), прокси-серверов (Squid, Blue Coat SG), от Elasticsearch и Kafka, от SOAR-решения Security Vision SOAR, события от иных источников в форматах CEF и LEEF.

IoC, пропускная способность (EPS);						Поддерживается отображение данных «сырого» события.
3.5. Поддержка ретроспективного поиска, поддерживаемая глубина поиска, объем / ограничение внутреннего хранилища исторической информации по IoC;	Не поддерживается	Не поддерживается	Поддерживается в решении Kaspersky Cyber Trace.	Не поддерживается	Не реализовано внутри решения	Поддерживается ретроспективный поиск (ретроспективный анализ – проверка совпадения новых IoC с событиями, полученными в прошлом). В решении хранится оптимизированная информация: идентификатор соответствующего события из системы источника, адрес источника, адрес назначения, ссылка, хэш, домен. Данные проверки запускаются автоматически по расписанию. Срок хранения событий не ограничен (определяется свободным местом в дисковой подсистеме), может быть настроен пользователем
3.6. Поддержка выявления DGA-доменов;	Поддерживается, специальный источник BiZone DGA	Не поддерживается	Поддерживается	Только с помощью механизма ручного проставления признака DGA для объекта типа домен	Не поддерживается	Поддерживается с применением нейросетей LSTM, за Возможность настройки точности работы DGA-модели для увеличения/уменьшения количества сработок
3.7. Поддержка выявления фишинговых доменов.	Поддерживается путем выявления фишинговых ресурсов	По результатам работы собственного CERT	Поддерживается	Не поддерживается	Поддерживается	Поддерживается путем поиска доменов с подстроками, схожими с известными «оригинальными» доменами (пользователю доступна настройка списка доменов, для определения сходства используется расстояние Левенштейна)
4. Интеграции:						
4.1. Оптимизация и релевантность TI-фидов для конкретной отрасли, сектора экономики, географического местоположения;	По отрасли (сектору экономики)	Поддерживается, по странам, регионам, секторам экономики, партнерам и клиентам	Поддерживается для целевых отраслей, географических регионов	Поддерживается для стран, сфер деятельности	Поддерживается	Поддерживается настройка TI-фидов для сектора экономики, страны, территории
4.2. Поддержка возможности просмотра TI-данных в «сыром» виде, исходно полученном из TI-фида;	Поддерживается, с возможностью скачать в формате JSON	Не поддерживается, данные поступают из внутренних источников вендора решения	Поддерживается	Не поддерживается	Поддерживается	Поддерживается просмотр необработанного JSON от TI-поставщика
4.3. Поддержка обработки бюллетеней безопасности с указанными в них IoC;	Поддерживается обработка бюллетеней от ФинЦЕРТ	Вендор создает бюллетени самостоятельно силами своего аналитического центра, IoC к бюллетеням не привязываются	Вендор создает бюллетени самостоятельно силами своего аналитического центра, IoC к бюллетеням не привязываются	Не поддерживается	Поддерживается получение и обработка бюллетеней в форматах JSON, PDF, EML по API	Поддерживается «из коробки» загрузка бюллетеней безопасности и выстраивание взаимосвязи с индикаторами компрометации от RSTCloud, НКЦКИИ, FACCT (ex-Group-IB) и ФинЦЕРТ
4.4. Интеграция с системами управления уязвимостями для приоритизации уязвимостей, возможность двусторонней связи с решением;	Не поддерживается	Поддерживается интеграция с решением F.A.C.C.T. Attack Surface Management	Не поддерживается. В собственных фидах передаются данные об уязвимостях	MP VM	Не поддерживается «из коробки», возможно реализовать через интеграцию с R-Vision SOAR	Поддерживается с помощью Security Vision SGRC / SOAR
4.5. Интеграция с системами борьбы с ВПО (антивирусные средства, EDR / XDR) для установления связей между IoC и образцами ВПО, возможность двусторонней связи с решением;	Интеграция с BiZone EDR	Поддерживается интеграция с решением F.A.C.C.T. Managed XDR	Поддерживается в рамках экосистемы Kaspersky Symphony XDR	PT XDR	Не поддерживается «из коробки», возможно реализовать через API	Поддерживается с помощью Security Vision SGRC / SOAR
4.6. Интеграция с «песочницами» (внутренними, внешними);	Не поддерживается	Поддерживается интеграция с собственной «песочницей» Malware Detonation Platform (MDP) с возможностью отправить файлы и ссылки на анализ непосредственно из интерфейса решения	Информация предоставляется в рамках сервиса Threat Analysis в Threat Intelligence Portal.	Интеграция с «песочницами» PT MultiScanner, Trend Micro Deep Discovery Analyzer, Pyshok (RU-CERT), VirusLocal (RU-CERT). Для решения PT MultiScanner поддерживается возможность отправить объект (PCAP-дамп, контейнер, файл) на проверку непосредственно из интерфейса решения, получить отчет.	Не поддерживается «из коробки», возможно реализовать через API	Поддерживается интеграция с Kaspersky KATA (внутренняя песочница), PT Sandbox (внутренняя песочница), TrendMicro DDA (внутренняя песочница), VirusTotal (внешняя песочница), Kaspersky TIP (внешняя песочница), any.run (внешняя песочница).
4.7. Интеграция с SIEM-системами для загрузки «сырых» событий, управления табличными списками,	Интеграция с ArcSight,	Поддержка интеграции с IBM QRadar,	Поддержка 13 SIEM-решений (в частности, KUMA, Splunk, ArcSight, QRadar, RSA NetWitness,		Поддерживается интеграция с ArcSight ESM, ArcSight Logger, IBM	Поддерживается интеграция с SIEM-системами MaxPatrol SIEM, Kaspersky KUMA, ArcSight

создания и приоритизации инцидентов, возможность двусторонней связи с решением;	IBM QRadar, Splunk	ArcSight, MaxPatrol SIEM, Splunk	LogRhythm), возможность интеграции с другими SIEM.	Поддерживается интеграция с MP SIEM	QRadar, MaxPatrol SIEM в части получения событий / инцидентов ИБ для поиска IoC	(ESM, Logger, SmartConnector), IBM QRadar, Fortinet FortiSIEM, Splunk. RuSIEM, Pangeo Radar
4.8. Интеграция с IRP / SOAR-системами для создания инцидентов, приоритизации, локализации, устранения инцидентов (активные действия), обогащение инцидентов данными из TIP, возможность двусторонней связи с решением;	Интеграция с TheHive	Поддерживается	Частично поддерживается в рамках экосистемы Kaspersky Symphony XDR	Не поддерживается	Поддерживается интеграция с решением R-Vision SOAR	Поддерживается интеграция с Security Vision SOAR и другими SOAR системами
4.9. Интеграция с IDS / IPS-системами, возможность двусторонней связи с решением;	Интеграция с Cisco FMC (FirePower), Suricata	Поддерживается	Поддерживается в рамках экосистемы Kaspersky Symphony XDR	Не поддерживается	Не поддерживается «из коробки», возможно реализовать через API	Поддерживается
4.10. Интеграция с системами FW, NGFW;	Интеграция с FortiGate	Поддерживается	CyberTrace позволяет экспортировать индикаторы в формате внешних списков индикаторов Palo Alto, Cisco, Fortigate. Экспортированный список индикаторов автоматически размещается на веб-сервере с возможностью указать URL на обновляемый список непосредственно в консоли администрирования NGFW, после чего данный список будет подключен к NGFW	Не поддерживается	Поддерживается интеграция с Cisco ASA v9 и выше, PaloAlto v9 и выше, Checkpoint R80.10 и выше, UserGate 6.X и выше	Поддерживается интеграция с межсетевыми экранами CheckPoint, Cisco ASA, Cisco Firepower, Fortigate, Juniper. Поддерживается интеграция с прокси-серверами Squid, Blue Coat SG IdecoUTM, UserGate, VipNet, Континент,
4.11. Интеграция с системами защиты бренда в Интернет;	Интеграция с BiZone Brand Protection	Интеграция с решением F.A.C.C.T. Digital Risk Protection	Не поддерживается	Не поддерживается	Не поддерживается «из коробки», возможно реализовать через API	Поддерживается
4.12. Интеграция с матрицей MITRE ATT&CK;	Поддерживается, с разбивкой угроз по матрице	Поддерживается	Техники и тактики MITRE ATT&CK присутствуют в фидах и отображаются в CyberTrace в поле контекста индикатора	Не поддерживается	Поддерживается	Матрица MITRE ATT&CK реализована в виде отдельного модуля, включенного в коробку TIP. Модуль представляет собой полноценную информационную справочную систему со всеми уровнями декомпозиции, связями и дриллдауном между подчиненными элементами, а также тесно интегрирована в IOC. Матрица MITRE автоматически обновляется по расписанию. В системе присутствует маппинг MITRE ATT&CK на модель угроз ФСТЭК. Поддерживается отображением базы знаний MITRE ATT&CK, контекстуализацией данных об IoC / IoA на основе данных матрицы, отображением связей между IoC / IoA и TTPs матрицы
4.13. Просмотр и детализация базы MITRE ATT&CK и всех ее элементов (в виде иерархии тактик, техник и т.д., в виде таблицы в инциденте, в виде общего списка элементов, другое (указать));	Не поддерживается	Поддерживается в виде отображения TTPs для кибератак, киберпреступных групп, образцов ВПО	Поддерживается	Не поддерживается	Поддерживается просмотр раскрывающегося списка с тактиками из базы MITRE ATT&CK, отображение техник и субтехник в списке угроз при подключении источника данных MITRE ATT&CK	Модуль представляет собой полноценную информационную справочную систему со всеми уровнями декомпозиции, связями и дриллдауном между подчиненными элементами в карточке обнаружения IoC
4.14. Автоматическое обновление базы MITRE ATT&CK;	Не поддерживается	Поддерживается	Поддерживается	Не поддерживается	Поддерживается	Поддерживается
4.15. Интеграция с матрицей БДУ ФСТЭК;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается
4.16. Интеграция с данными проекта OWASP;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается
4.17. Поддержка API (для экспорта / импорта данных, управления внутренними сущностями в решении, подключения новых	Поддерживается с помощью модуля для экспорта и поиска информации через API-взаимодействие, с выгрузкой данных в форматах CSV, JSON и поиском данных в	API поддерживается, задокументировано, может	Поддерживается работа через REST API через HTTPS, поддерживается выполнение действий по поиску IoC, управление источниками данных об угрозах, управление IoC для источников InternalTI и	API поддерживается для экспорта информации, доступна API-интеграция с коннекторами решения	Частично поддерживается. API с возможностью управления (создание, изменение, удаление) IoC, получения бюллетеней об угрозах, получения аналитических отчетов,	Поддерживается API для работы с объектами в решении, настройки, выгрузки данных, запуска скриптов (поддерживается CMD, Bash, Shell, Java, JavaScript, PowerShell, Python), получения информации по выявленным обнаружениям для

фидов, обращения к внешним сущностям, включая запуск скриптов Python, Java, Bash, Batch, PowerShell), документация на API;	платформе через API-запрос с выводом результатов на экран и в JSON-файл. Документация на API предоставляется в формате PDF-файла и в формате Swagger	использоваться только для получения контента из решения	FalsePositive, управление тэгами в базе данных Kaspersky CyberTrace (назначение, снятие тэгов для IoC)	для взаимодействия с внешними системами	получение информации о сенсорах. Поддерживается API-взаимодействие с решением R-Vision SOAR. Запуск скриптов не поддерживается	IOC. API документирован.
4.18. Интеграция с ФинЦЕРТ, ГосСОПКА (получение и обработка отчетов, содержащих IoC).	Интеграция с ФинЦЕРТ	Не поддерживается	Поддерживается обработка отчетов, выпускаемых НКЦКИ, с извлечением из них IoC	Поддерживается получение данных из ФинЦЕРТ	Поддерживается интеграция с АСОИ ФинЦЕРТ. Поддерживается получение бюллетеней из НКЦКИ (ГосСОПКА)	Поддерживается. Загрузка бюллетеней безопасности и получение IoC из ЛК ФинЦЕРТ, ГосСОПКА посредством API
5. Поддержка процессов:						
5.1. Поддержка ручного редактирования IoC, ручная установка уровня критичности IoC, ручная установка связей между IoC, указание комментариев к IoC;	Поддерживается	Поддерживается возможность скрыть и добавить результаты обнаружения в «избранное». Возможность редактирования IoC вручную отсутствует	Поддерживается установка тэгов для IoC вручную или через API	Поддерживается	Поддерживается редактирование IoC (по отдельности или в группе) с возможностью добавления измененной информации или перезаписью имеющейся информации. Поддерживается создание IoC вручную, с указанием типа, значения, описания, тэга, типа вредоносной активности, тактик по матрице MITRE ATT&CK, атакуемые отрасли и страны, даты первого и последнего появления, срока жизни.	Поддерживается выполнение ручных действий с IoC / IoA / стратегической атрибуцией (изменение, добавление, удаление значений свойств и записей). Поддерживает изменение как отдельного IoC / IoA, так и выбранного списка IoC / IoA
5.2. Поддержка оптимизации и точной настройки частоты обновления TI-данных от каждого TI-фида в отдельности;	Не поддерживается	Не поддерживается, всё функционирует в автоматическом режиме на стороне вендора	Нет данных	Поддерживается	Поддерживается	Поддерживается
5.3. Поддержка выявления и контроля трендов кибератак и TTPs атакующих.	Поддерживается с отображением на дашборде	Поддерживается, с выводом релевантных для компании трендов и угроз на панели управления	Поддерживается	Не поддерживается	Не поддерживается	Поддерживается
6. Взаимодействие с пользователем, удобство использования, оптимизация работы:						
6.1. Интерактивные графы для отображения связей между объектами в рамках реагирования на киберинциденты, возможность выполнения действий на графах при анализе IoC и реагировании на киберинциденты;	Поддержка отображения графов для связей объектов и групп, фильтрации объектов на графах	Поддерживается отображение связей в виде графов, но недоступна возможность выполнения действий по реагированию непосредственно из графа	Поддерживается визуализация (на графах) информации об индикаторах угроз и их взаимосвязях, обнаруженных киберугрозах, отчетах и т.д, поддерживается обогащение информацией из внешних источников (Kaspersky Threat Intelligence Portal, VirusTotal)	Поддерживается с помощью схемы связей, с просмотром свойств объектов и связей между ними	Поддерживается граф связей для IoC, объектов наблюдения, уязвимостей, отчетов, ВПО. Поддерживается экспорт отображения графа в формате JPEG	Поддерживается вывод информации на графе со связями IoC с обнаруженными хостами, IoA, угрозами, злоумышленниками, ВПО, уязвимостями, техниками и тактиками из базы знаний MITTRE ATT&CK, с возможностью перехода из элемента графа к полной карточке с детальной информацией. На графе поддерживается выполнение действий по отображению связей, по обогащению IoC, блокировке IOC на FW, отправке IoC в Active List (справочник) в SIEM-системе, добавлению нового тэга, выгрузке отчета по IoC, выгрузке IoC в формате STIX2, отслеживанию изменений IoC, редактированию IoC, изменению статуса IoC
6.2. Дашборды (количество преднастроенных дашбордов и виджетов, возможность ручной кастомизации пользователями, возможность drilldown);	Преднастроено 10 дашбордов (тренды, отчеты, динамика изменения объектов, разбивка объектов по характеристикам и т.д.). Drilldown в дашбордах не поддерживается	Выводятся графики, таблицы, столбчатые диаграммы, с помощью фильтров настраивается отображаемая информация	Поддерживается отображение данных на информационной панели (дашборде) с информацией об общей статистике, данных по поставщикам TI (статистика обнаруженных киберугроз, сгруппированная по источникам данных об угрозах), данных по IoC (статистика проверенных индикаторов), данных о пересечении TI-источников (процент пересечения источников данных об угрозах, используемых в Kaspersky CyberTrace). Поддерживается возможность скчать отчеты (в формате HTML). Функционал drilldown не поддерживается	Поддерживается, с отображением графиков и круговых диаграмм. Drilldown не поддерживается	Поддерживаются добавление на дашборд виджетов с отображением показателей работы решения (количество индикаторов по типам, список новых индикаторов, скорость обработки индикаторов и т.д.), поддерживается отображение графиков (на отдельных виджетах) с автоматическим обновлением информации. Поддерживается разграничение доступа пользователей к дашбордам. Функция drilldown не поддерживается	Поддерживается, «из коробки» настроены несколько дашбордов (аналитический, операционный, стратегический, показатели платформы, географическая карта). Доступно добавление любого числа дополнительных дашбордов в графическом редакторе с применением подхода low-code / no-code. Во всех дашбордах поддерживается drilldown.
6.3. Отчетность (виды и форматы отчетов, включая создание стратегических, оперативных, тактических, аналитических отчетов	Возможность скачать PDF-файл с отчетом по некоторым объектам (например, вредоносным	Вендор выпускает ежемесячные, ежеквартальные, годовые аналитические отчеты. Пользователь может вручную создать отчет по релевантным для индустрии, региона,	Информация предоставляется на Threat Intelligence Portal в рамках сервиса Reporting с разделением на Crimeware Threat Intelligence Reporting, APT Threat Intelligence Reporting, Industrial Threat Intelligence	Формирование отчетов не поддерживается, но в решении хранятся отчеты, содержащие сгруппированные данные об объектах, поступившие из внешних источников (песочниц и	Поддерживается создание аналитических отчетов с представлением срезов количественных и качественных данных по поставщикам индикаторов компрометации и событиям	Поддерживается формирование отчетов (общий отчет, по индикаторам, по обнаружениям, по уязвимостям, по фидам и поставщикам) в форматах DOCX, PDF, XLSX, ODS, ODT, TXT. Поддерживается формирование отчетов вручную, автоматически, по расписанию, с отправкой отчетов на email, в Telegram, на

для различных групп потребителей решения, возможность создания новых форм отчетов пользователями);	кампаниям, кибергруппировкам)	страны киберугрозам, утечкам, уязвимостям за определенную дату с отправкой отчета на email.	Reporting, а также в CyberTrace.	анализаторов кода)	обнаружений. В решении поддерживается фиксированный набор типов отчетов	файловый сервер, через API-интеграцию во внешние системы. Поддерживается создание новых форм отчетов в графическом редакторе с применением подхода low-code / no-code
6.4. Аудит и управление изменениями, внесенными пользователем в TIP-решении (например, установка неверной связи между IoC, неверная пометка «ложноположительный IoC»);	Выполненные пользователями операции отображаются в истории изменений объектов	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается хранение истории изменений IoC	Поддерживается ведение и сохранение истории изменений IoC, обнаружения IoC, TI-фида, угрозы, уязвимости (с отображением даты и времени, инициатора изменений)
6.5. Поддержка совместной, одновременной работы аналитиков с TI-данными в едином интерфейсе расследования с возможностью drilldownпо инцидентам, обнаружениям;	Поддерживается частично с помощью функционала голосования и комментариев к объектам	Поддерживается	Поддерживается	Совместная работа поддерживается, но без учета типовой ролевой модели SOC	Поддерживается	Поддерживается
6.6. Функционал тэгирования индикаторов (в ручном и автоматическом режиме);	Поддерживается указание тэгов пользователем вручную, тэги проставляются для объектов вендором	Не поддерживается, инциденты не создаются	Поддерживается	Поддерживается, с помощью функционала справочных меток	Поддерживается ручное задание пользовательских тэгов для индикаторов, отчетов, вредоносного ПО, уязвимостей	Поддерживается ручное и автоматическое проставление тэгов из преднастроенного справочника, с возможностью изменения и добавления новых тэгов
6.7. Поддержка MSSP модели.	Поддерживается одновременный совместный доступ к решению, без поддержки ролевой модели и без гранулярного разграничения доступа пользователей к отдельным объектам	Поддерживается	Поддерживается	Нет данных	Не поддерживается	Поддерживается
7. Расширенный функционал:						
7.1. Выявление аномалий работы ИТ-инфраструктуры на базе анализа IoC;	В ручном режиме с помощью анализа динамики и изменения количества обнаруживаемых в инфраструктуре IoC	В ручном режиме на основе анализа предоставляемых данных в решении	Частично поддерживается с помощью ручного анализа	Вручную, путем анализа IoC	Поддерживается через функцию обнаружения	Поддерживается с помощью механизма Security Vision Anomaly Detection с использованием обученных и перенастраиваемых моделей машинного обучения
7.2. Поддержка использования механизмов выявления фишинговой активности;	Поддерживается через соответствующий источник TI-данных	Поддерживается, выявляется по результатам работы собственного CERT	Поддерживается	Не поддерживается	Поддерживается через функцию обнаружения и экспорта	Поддерживается путем поиска доменов с подстроками, схожими с известными «оригинальными» доменами (пользователю доступна настройка списка доменов, для определения сходства используется расстояние Левенштейна)
7.3. Интеграция с модулем UEBA, комбинирование подходов Machine Learning (ML) на сетевом и хостовом уровнях для выявления аномалий;	Не поддерживается	Не поддерживается	С помощью решения Kaspersky Machine Learning for Anomaly Detection	Не поддерживается	Не поддерживается	Поддерживается выявление аномалий с использованием методик машинного обучения, обученных на различных датасетах моделей, моделей «без учителя», которые автоматически аппроксимируют действия сущностей и выявляют отклонения по различным комбинациям параметров, а также с применением нейросетей, учитывающих последовательность событий и их взаимосвязи
7.4. Применяемые методики ML (обучение с учителем, обучение без учителя, нейросети);	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается использование нейросети LSTM для выявления DGA-доменов с использованием случайных доменов или случайного набора слов в имени доменов
7.5. Наличие, количество преднастроенных и обученных ML-моделей для выявления аномалий;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживаются преднастроенные и обученные модели машинного обучения, с возможностью переобучения
7.6. Наличие ручной / автоматической						

настройки параметров ML-моделей для повышения качества выявления аномалий;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается ручной и автоматический подбор параметров ML-моделей
7.7. Интеграция или встроенная поддержка систем Big Data, возможность двусторонней связи с решением;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается интеграция с Apache Kafka и SmartMonitor, возможно реализовать дополнительные интеграции через API	Поддерживается за счет интеграции с «озерами данных» на основе Kafka, Hadoop, Elasticsearch и др.

SGRC

Основные критерии	АльфаДок	Archer Suite	ePlat4m SGRC (UDV ePlat4m SGRC)	R-Vision SGRC	SECURITM	Security Vision SGRC
1. Общие технические характеристики:						
1.1. Технические требования к платформе и среде внедрения (системные требования к аппаратному и программному обеспечению, окружению);	ОС: Debian 11, Rocky 9, Альт 8, Redos-MUROM-7.3.2. Необходимые предустановленные пакеты: docker, docker-compose, xz, tz-data. Аппаратные требования (при количестве пользователей до 10): 4 ЦПУ, 8 Гб ОЗУ, 250 Гб дискового пространства	ОС: Windows Server 2022, 2019, 2016. СУБД: Microsoft SQL Server 2022, 2019, 2017. (поддерживаются версии Standard и Enterprise, в том числе установленные на Ubuntu). Аппаратные требования: от 2 ЦПУ, 8 Гб ОЗУ, от 40 Гб дискового пространства (при работе до 10 пользователей одновременно, работа с максимум 75000 записей)	ОС: Windows Server 2012R2 и выше, Linux с поддержкой NetCore 3.1 (РЕД ОС, Astra Linux, Ubuntu). СУБД: MSSQL/PostgreSQL/Jatoba. Аппаратные требования: 16-32 Гб RAM, 4 CPU, 200-300 Гб дискового пространства	ОС: CentOS, RHEL, Debian, Astra SE, Astra CE, RED OS, ALT Server, ALT 8, SP Server. СУБД: PostgreSQL 14, Jatoba J4. Аппаратные требования: 12 Гб RAM, 4 CPU, 100 Гб дискового пространства	ОС: Астра Линукс, RedOS, CentOS, Ubuntu, Debian. Аппаратные требования (на 1 сервер, минимально): 2 ЦПУ, 6 Гб ОЗУ, 100 Гб дискового пространства. Для распределенных и комплексных инсталляций требуется установка на несколько серверов	ОС: Microsoft Windows Server 2012 R2 или выше, CentOS 7 или выше, Red Hat Ent. Linux 7 или выше, Ubuntu 18.04 или выше, Debian 10 и выше, Astra Linux CE (Common Edition) релиз "Орел", Astra Linux SE (Special Edition) релиз «Воронеж» и "Смоленск", Альт 8 СП, Альт Сервер 10 или выше, Oracle Linux 8 и выше, РЕД ОС актуальной версии, РОСА "КОБАЛЬТ", AlmaLinux, AlterOS. СУБД: Microsoft SQL Server версии 2016 или выше, PostgreSQL версии 11 или выше, Postgres Pro версии 11 или выше, Jatoba. Аппаратные требования: 8 ЦПУ, 12 Гб ОЗУ, 100 Гб дисковой подсистемы
1.2. Варианты поставки и инсталляции (аппаратный аплайнс, образ, контейнер, установка на «голое железо», установка on-prem, установка в облаке, наличие графических инсталляторов, поддержка виртуализации);	Поддерживается работа из «облачной» веб-консоли и локальная (on-prem) установка. Поддерживается установка дистрибутива из командной строки.	Поддержка установки on-prem и в облаках Amazon Web Services, Microsoft Azure	Варианты поставки конечному пользователю: Аппаратный аплайнс: да (в этом случае ПАК собирает и поддерживает партнер-интегратор) Контейнер: нет Установка на ""голое железо"": нет (требуется предустановленная ОС из списка совместимых) Установка on-prem: да Установка в облаке: да (облачный сервис предоставляет либо партнер-интегратор, либо Заказчик) Наличие графических инсталляторов: да Поддержка виртуализации: да	Поддерживаемые варианты установки: on-prem, виртуализация, контейнер. Поддержка систем виртуализации: VMware, MS Hyper-V, Xen, Parallels, VirtualBox. Решение поставляется в виде виртуального аплайнса (виртуальная машина с предустановленным ПО для работы решения)	Варианты поставки: 1) подписка на SaaS или 2) покупка лицензии на on-prem. Локальная версия устанавливается на Linux сервер заказчика (физический или виртуальный) как набор Docker-контейнеров.	Поддержка установки в виде контейнера, на «голое железо», в виде ISO образа, RPM-пакетов, из графического инсталлятора и из командной строки. Поддержка систем виртуализации (VMware, VirtualBox, Hyper-V, Xen, Parallels, KVM). Поддерживается установка в облаке и on-prem.
			Решение UDV ePlat4m SGRC разработано на основе Low-code платформы ePlat4m от UDV Group. Система имеет модульную архитектуру. Для функционирования различных прикладных модулей, необходимо предварительно развернуть low-code платформу UDV ePlat4m.			

1.3. Архитектурные особенности решения (стек технологий, возможность прямого доступа к внутренним структурам, возможность доступа покупателя к ОС/СУБД решения с правами администратора);		Используются Microsoft IIS 10, MS SQL, Redis, ASP.NET Core	Применяемый стек технологий: Frontend: React, TypeScript Backend: C#, NET CORE Используемые СУБД: PostgreSQL, Jatoba, MS SQL Используемые ОС: Linux, Windows Инструменты CI/CD: Gitlab, Jenkins Возможность прямого доступа к внутренним структурам: да (в рамках функционала Low-code платформы) Возможность доступа покупателя к ОС/СУБД решения с правами администратора: нет	Используется СУБД PostgreSQL и Jatoba, работа с решением ведется через веб-интерфейс решения с поддержкой JavaScript	Стек JavaScript, PHP, Node.js, Python, HTML/CSS, Redis, NGINX, PostreSQL, MySQL, Docker. Поддерживается возможность прямого доступа к внутренним структурам, контейнерам, к ОС/СУБД с правами администратора.	Возможность отдельной установки выделенного сервера коннекторов (для взаимодействия с интегрируемыми системами), не требующего прямого соединения с основной базой данных решения. Взаимодействие всех компонент по защищенным протоколам сетевого доступа. Наличие административного доступа к компонентам решения. Используемые сторонние компоненты: Elasticsearch, RabbitMQ, IIS / NGINX, MSSQL / PostgreSQL / Postgres Pro / Jatoba
1.4. Параметры масштабируемости, кластеризации, производительности;			Поддерживается кластеризация на уровне low-code платформы, а также средствами ОС, среды виртуализации и аппаратными средствами	Поддерживается возможность кластеризации	Базовая инсталляция на 1 сервер, при сложной архитектуре (например, вынос части функций в DMZ) настраиваются несколько взаимосвязанных серверов.	Поддерживается балансировка нагрузки между компонентами, возможность установки неограниченного количества нод каждого компонента решения с целью горизонтального масштабирования, возможность установки каждого компонента решения на выделенный сервер
1.5. Поддержка отказоустойчивости (реализация, требования вендора к инфраструктуре покупателя);		Поддержка режима высокой доступности	Поддерживается кластеризация на уровне low-code платформы, а также средствами ОС, среды виртуализации и аппаратными средствами	Поддерживается реализация отказоустойчивости для кластера приложений и кластера базы данных	Резервирование сервера инструментами заказчика. Есть встроенный механизм резервных копий (снапшотов) для базы данных приложения (запускаемый из интерфейса приложения). Есть механизм переустановки приложения (запуск из командной строки).	Поддерживается создание кластера высокой доступности, дублирование и резервирование всех элементов решения, возможность создания геокластера, поддержка отказоустойчивости для провайдеров MSS
1.6. Обеспечение безопасной работы решения (ограничение доступа, ролевая модель, защита канала связи, защита обрабатываемых данных, журналирование, способы аутентификации пользователей, контроль действий пользователей решения);	Поддержка ролевой модели доступа с разграничением доступа на уровне организаций и назначением прав доступа к определенным разделам и выполнению шагов в них. Поддерживается ведение истории действий с учетными записями пользователей.	Шифрование данных при передаче (SSL/TLS), при хранении (шифрование определенных полей, шифрование всей БД), доступ к веб-интерфейсу по HTTPS, работа в режиме соответствия стандарту FIPS 140-2, поддержка SSO с аутентификаций через LDAP, поддержка Kerberos-аутентификации, поддержка хранения ключевой информации в HSM-модуле. Поддерживается ролевая модель доступа, гранулированное предоставление доступа к определенным объектам внутри решения	Ограничение доступа: да Ролевая модель: да Защита канала связи: поддерживается сторонними решениями. Способы аутентификации пользователей: есть возможность интеграции средствами Low-code платформы с AD/KeyCloak. Контроль действий пользователей: есть журналирование	Ролевая модель доступа, дискреционный доступ, доступ к инцидентам на основе атрибутов. Аутентификация: локальная, SSO. Поддерживается логирование изменений, вносимых пользователями. Применяется шифрование учетных данных, сохраненных в системе	Поддерживается ограничение доступа на сетевом уровне (настройка из командной строки), ролевая модель для пользователей приложения, доступ к приложению только через HTTPS с использованием сертификата заказчика или генерируемый приложением. Поддерживается шифрование критичных данных в БД, журналирование всех изменений объектов в приложении (включая предыдущие и новые значения), двухфакторная аутентификация, доменная аутентификация, парольные политики (включая запрет использования словарных паролей), уведомление пользователя о подозрительном входе из-под его учетной записи по email и в Telegram, журналирование успешных и неуспешных попыток входа, с фиксацией IP и браузера подключавшегося	Поддерживается ограничение доступа на основе IP-адресов, двухфакторная аутентификация, аутентификация по сертификатам для пользователей и компонентов решения (использование самоподписанных сертификатов или сертификатов, выданных внутренним центром сертификации), наличие SSO, использование SSL/TLS для защиты доступа к веб-интерфейсу, аудит попыток входа в систему, аудит действий пользователей и администраторов (включая факт просмотра карточек), ролевая модель управления доступом ко всем элементам решения, поддержка multitenancy
1.7. Локализация интерфейса, поддержка мультиязычности, возможность кастомизации интерфейса, возможность сквозного поиска по всем обрабатываемым данным.	Поддерживается локализация на русском языке	Локализация на английском, немецком, португальском, испанском, японском, итальянском, французском, китайском языках с возможностью добавления новых языков. Поддерживается брендирование интерфейса (логотипы, цвета)	Поддержка русского языка, поддержки мультиязычности нет, сквозного поиска нет	Поддерживается русская и английская локализации, настройка карточки интерфейса, поддержка тем (темная и светлая), кастомизация вкладок и дашбордов, сквозной поиск по объектам	Интерфейс только на русском языке, можно изменять стиль (цвета) приложения и рассылаемых писем, можно менять логотип и название приложения. Поддерживается глобальный поиск по всем объектам в приложении (команде)	Локализация интерфейса и всех элементов на русском и английском, возможность добавления других языков, поддержка тем (темная и светлая), поддержка кастомизации интерфейса (брендирование, логотип), возможность создания рабочих мест пользователей под пользовательский функционал, поддерживается сквозной поиск
2. Общие организационные характеристики:						

2.1. Дата первого релиза, текущая версия;	Нет данных	Текущая версия платформы 6.14	Дата появления продукта и регистрации прав: 06.08.2021 Текущая версия Low-code платформы ePlat4m 2.0 Для различных модулей (>20 шт), как самостоятельных систем, текущие версии разные	Дата первого релиза – 2011, текущая версия 5.2	Первый релиз 06.2021. Текущая версия 1.3.572	Первый релиз - 2010, текущая версия - 5.0.1694417270
2.2. Наличие документации, наличие API;	Документация в виде PDF, взаимодействие с решением по API не поддерживается	Документация представлена на сайте, API поддерживается	Разработаны руководства пользователя, документирован API, разработаны руководства разработки на ePlat4m, также есть учебный курс в авторизированном учебном центре	Документация поставляется с системой, API документирован, в том числе поставляется с коллекцией в формате Postman	Есть документация, есть API	Документация в виде интерактивной справки в решении, в виде PDF-файлов, поддержка и документация на API
2.3. Наличие технической поддержки, режим работы, SLA-нормативы;	Нет данных		Техническая поддержка: да Режим работы: 5x8, может быть расширена до 24/7 SLA: прописаны в соответствии с регламентом техподдержки	Поддержка в режиме 24/7, различные уровни поддержки	Тех.поддержка для платных клиентов - в рабочие часы, SLA на ответ 1 рабочий день, каналы - телефон, telegram, почта. Тех.поддержка для пользователей бесплатной Community версии - через общую форму в приложении.	Техническая поддержка трёх уровней. Максимальная - 24/7. Показатели SLA для тарифа «Максимальный»: время реакции: 4 часа, время предоставления решения: 24 часа. Возможность согласования и подписания произвольных SLA-нормативов и условий предоставления услуг.
2.4. Наличие гарантии, срок предоставления гарантийного обслуживания, что включено в стандартное гарантийное обслуживание, возможность расширенной гарантии;	Нет данных		Наличие гарантии: да Срок предоставления гарантийного обслуживания: от 1 года и более В стандартное гарантийное обслуживание включена возможность открывать сервисные заявки, получать консультации по решению, бесплатно получать новые версии продуктов	Предоставляется гарантия	Гарантия (тех.поддержка) на SaaS действует весь срок подписки. Гарантия для on-prem включена в стоимость и действует 1 год. Включает в т.ч. удаленное подключение и восстановление работоспособности приложения	Стандартное гарантийное обслуживание на 1 год: -личный кабинет с маркетплейсом дистрибутивов платформы, окружения, ОС, модулями и обновлениями -прием заявок через портал, телефон и эл. почта (кол-во обращений не ограничено); - предоставление консультаций по ВКС, телефону и email; -консультации по: настройке и администрированию программных продуктов, диагностике и сбора информации для определения неисправностей в работе программных продуктов, применению решений по устранению неисправностей и восстановлению работы программных продуктов. При необходимости имеется возможность приобрести расширенную техническую поддержку (сжатый SLA)
2.5. Лицензионная политика: стоимость дополнительных интеграций (ИТ/ИБ-системы, СЗИ, внешние сервисы и т.д.), лицензирование API, правила расчета лицензии (по пользователям, активам, интеграциям и т.д.), отличие в стоимости при разных вариантах инсталляции, специальные условия для MSS-провайдеров.	Различные лицензионные опции в зависимости от типа организации, возможность заказа дополнительной услуги от вендора (аудит ИБ, обучение, аттестация информационных систем, проектирование, создание, сопровождение системы защиты информации)	Решение имеет модульную структуру, все модули («Solutions») и включенные в них приложения («Applications») и опросники («Questionnaires») лицензируются отдельно	Все лицензии можно получить либо по бессрочной, либо по срочной схеме лицензирования. В зависимости от того, требуется или нет отказоустойчивая (кластерная) схема инсталляции ПО, лицензии берутся либо только на активный узел (не отказоустойчивая схема), либо на активный и пассивный узлы (отказоустойчивая схема). Состав лицензий может быть обязательным и опциональным. Программное обеспечение «Базовая платформа Eplat4m» - обязательная лицензия на платформу, остальные лицензии для каждого модуля могут быть приобретены опционально по мере надобности. Для интеграции с внешними системами, требуется покупка лицензии на коннектор. Лицензионная политика не зависит от числа пользователей системы, активов и т.д. В случае внедрения решения для коммерческих SOC, когда программное обеспечение используется для коммерческого использования и извлечения прибыли, то помимо вышеуказанных лицензий, требуется купить	Предоставляется по запросу	Есть публичная оферта (прайс) и калькулятор цен на сайте производителя. Использование API или количество интеграций не лицензируются. Стоимость зависит от варианта поставки (SaaS, on-prem), модулей, количества активов. Есть бесплатная Community версия веб-портала.	Предусмотрены временные и бессрочные лицензии. Метрики лицензирования SGRC: 1) Перечень выбранных модулей 2)Количество конкурентных лицензий коннекторов для подключения к внешним системам 3)Режим функционирования (количество дополнительных нод) 4)Мультиарендность для MSSP провайдеров, холдингов, групп компаний. Других ограничительных метрик не предусмотрено. API – не лицензируется и включен в любую поставку ПО.

			специализированные лицензии на подключение каждого клиента SOC (юридического лица) к модулям eplat4m. Этот тип лицензий только срочные – на 1 год.			
2.6. Опыт внедрений.	Нет данных		Опыт внедрения достаточно обширный - в первую очередь это внедрения на газодобывающих и газотранспортных предприятиях, предприятиях газопереработки, профильных научных институтах, энергетических компаниях, промышленных предприятиях	Опыт внедрений во многих отраслях. «Центр экспертизы R-Vision» сопровождает заказчика на каждом этапе проекта	Среди внедрений компании из группы Сбербанка, финансовые организации, строительные компании, фармацевтические производители и дистрибьютеры, ИТ компании, ритейл, госорганизации.	Опыт внедрения во многих отраслях экономики. Среди Заказчиков – Сбербанк России, Альфа-Банк, Тинькофф Банк, Норильский Никель, Северсталь, Евраз, X5 Group, Магнит, ФСО России, Совет Федерации, ФГУП Интеграл, Мегафон MSSP, Центр киберустойчивости Angara SOC, МТС, Первый Канал, Правительство Тюмени, Правительство Красноярска и другие.
2.7. Наличие сертификатов регуляторов, присутствие в реестре российского ПО;	Присутствует в реестре российского ПО	Не применимо	Сертификат соответствия ФСТЭК России № 4433 от 29.07.2021 (УД6, ТУ). Решение присутствует в реестре российского ПО	Сертификат соответствия ФСТЭК России № 4346 от 22.12.2020 (УД4). Решение присутствует в реестре российского ПО	Присутствует в реестре российского ПО	Сертификат соответствия ФСТЭК России № 4574 от 02.09.2022 (УД4). Сертификат соответствия ОАЦ при Президенте Республики Беларусь № BY/112 02.02. ТР027 036.01 00492 от 05 августа 2022 года (по требованиям технического регламента ТР 2013/027/BY). Решение присутствует в реестре российского ПО
3. Управление информационной безопасностью:						
3.1. Управление активами:						
3.1.1. Поддерживаемые типы активов (аппаратное, программное обеспечение, сетевое оборудование, техника и т.д.);	Поддерживаются типы: СКЗИ, ключи ЭП, помещения, организации, сотрудники, документы, заявки, хранилища, АРМ, серверы, сетевое оборудование, иные технические средства	Поддерживается импорт данных о произвольных типах объектов, поддерживаются определенные типы свойств (текстовое, числовое, дата, IP-адрес), поддерживается возможность приложить файл, указать ссылку, форму, пользователя, группу	Бизнес-процессы, бизнес-функции, информационные системы, информационные ресурсы, подразделения, объекты защиты, программное обеспечение, технические средства, средства защиты информации, информационные активы (файл, база данных, каталог, персональные данные, коммерческая тайна и т.д. с возможностью создания пользовательских типов активов). Импорт из интегрируемых систем, создание вручную.	Поддерживаемые типы активов: информационные системы, оборудование, ПО, подразделения, помещения, бизнес-процессы, информация, персонал, группы ИТ-активов, сети	Поддерживаются любые типы активов, более 200 типов из коробки.	Поддерживается создание активов любого типа с произвольными свойствами, типы активов «из коробки»: бизнес-процесс, информационная система, оборудование, помещение, поставщик, продукт, сервер / АРМ, приложение, обновление ПО, сетевое устройство, система хранения данных, принтер / МФУ, телефон / VoIP, интерфейс удаленного управления, СЗИ, другое устройство, подсети, программное обеспечение, учетные записи.
3.1.2. Возможность создания пользовательских типов активов;	Не поддерживается	Поддерживается	Поддерживается создание в интерфейсе решения, с использованием Low-code платформы ePlat4m	Да, поддерживаются создание пользовательских типов материальных и нематериальных активов, с рядом ограничений (невозможность выстроить иерархию, невозможность проводить аудиты, невозможность связать с инцидентами для пользовательских типов активов)	Поддерживается	Поддерживается создание активов любого типа с применением подхода low-code / no-code. Созданные пользовательские типы активы могут использовать во всех процессах, ролевой модели, дашбордах и т.д. на равне с типами активов «из коробки»
3.1.3. Поддержка создания и настройки различных свойств активов, типы данных свойств активов;	Не поддерживается	Поддерживается	Поддерживается создание с использованием Low-code платформы ePlat4m	Поддерживается создание дополнительных свойств (полей) активов. Типы полей: текстовое поле, числовое поле, несколько текстовых строк, числовое поле с денежным символом, список, IP-адрес/адрес сети, пользователь, дата.	Поддерживается создание полей различного типа, включая горизонтальные и вертикальные связи активов.	Поддерживается создание произвольных свойств с применением подхода low-code / no-code Поддерживаемые типы данных: строка, дата, время, число (целое, большое целое, дробное), булево значение, ссылка на справочник, ссылка на объект системы, таблица, временной интервал, пароль, файл, IP-адрес
3.1.4. Работа с активами типа ПО, СЗИ, контроль обновлений ПО, ведение списков разрешенного / запрещенного ПО, управление ПО (удаление, обновление, установка ПО на активах через консоль решения в ручном и автоматическом режимах);	Поддерживается ведение списков ПО	Поддерживается ведение перечня ПО, не поддерживается управление ПО	Поддерживается работа с активами типа ПО и СЗИ с указанием версии, типа ПО и СЗИ (например, СУБД или антивирус), статуса, уровня критичности, владельца, ответственного, наименования производителя, данных о лицензии, технических характеристик (каталог установки, версия, контрольная сумма), свойств СЗИ (номер сертификата, орган сертификации, срок действия). Указан перечень технических средств, на которых установлены ПО и СЗИ, связанные объекты защиты, связанные организационные подразделения, обнаруженные уязвимости (по результатам обработки отчетов сканеров защищенности), история изменения актива, учет движения актива. Управление ПО из решения не поддерживается. Контроль обновления ПО	Поддерживается, с внесением данных об обнаруженном во время сканирования и установленном на устройстве ПО, с возможностью ручного добавления ПО. Поддерживается внесение информации о названии, версии, группе ПО, тег, администратор безопасности, комментарии, лицензии.	Поддерживается ведение реестров ПО/СЗИ как отдельных активов или как списки установленного ПО в составе основных активов (хостов). Управление ПО на хостах не поддерживается.	Поддерживается работа с активами типа ПО (учет лицензий, каталоги установки, граф связей ПО и устройства с установленным ПО, контроль установки обновлений), СЗИ (с контролем функционирования), обновление ПО (связанное с обновлением ПО, файлы обновлений и скрипт для их запуска для установки обновлений на устройства). Поддерживается ведение списков разрешенного / неразрешенного ПО / «белого списка» ПО (по производителю) с контролем установки, обновлением, автоматическим и ручным удалением (с помощью скриптов)

			реализуется через интеграции			
3.1.5. Связь активов с инцидентами, уязвимостями, требованиями, киберрисками;	Поддерживается установка связей между активами и применимыми нормативными требованиями, между активами и уязвимостями, между активами и инцидентами	Поддерживается связь между объектами («записями») произвольного типа, включая инциденты, меры защиты, политики, активы	Поддерживается указание связей с уязвимостями (интеграция со сканерами уязвимостей)	Поддержка создания связей между инцидентами и активами (за исключением пользовательских типов), между активами внутри группы ИТ-активов, между уязвимостями и активами, между рисками и активами, между активами и документами, поддерживается создание задачи и инцидента из уязвимости	Поддерживается установка связей активов с любыми объектами в системе.	Поддерживается возможность установки связей любых объектов решения друг с другом как в автоматическом, так и в ручном режиме. Поддерживается учет и отображение (в списке, на графе связей) активов и инцидентов, уязвимостей, требований, аудитов, рисков с возможностью выполнения действий со связанными сущностями
3.1.6. Поддержка и кастомизация правил группировки, дедупликации импортированной информации об активах;	Не поддерживается	Поддерживается с помощью встроенной утилиты Data Feed Manager и создания сложных рабочих процессов («Advanced Workflows»)	Поддерживается, при настройке коннектора	Поддерживается создание групп ИТ-активов, группирование активов типа ПО, группирование инцидентов (иерархическая связь с родительским и дочерними инцидентами до 50 инцидентов, одноранговая связь инцидентов друг с другом, создание групп инцидентов). Поддерживается устранение дубликатов при импорте данных из внешних систем, при сканировании сети (путем сверки статусов сетевых портов по итогам сканирования). Используется алгоритм создания идентификаторов просканированных узлов по ключам (UUID, SID, серийный номер), а также с помощью уникальных маркеров-файлов R-Vision key, создаваемых после первичного сканирования устройства, для исключения создания дубликатов узлов	Поддерживается корректировка полей активов, их типов и взаимосвязей через модуль RPA. Поддерживается группировка активов по различным свойствам через модуль «Метрики». Поддерживается функция объединения дублей по различным критериям.	Поддерживается настройка правил группировки с учетом свойств активов, по которым определяется уникальность объектов при импорте для избежания дублирования. Возможность создания нескольких правил группировки для каждого типа актива, каждое из которых включает от 1 до всех свойств актива. Поддерживается создание фильтров для задания условий срабатывания правил группировки. Правила группировки применяются при импорте информации из любого источника.
3.1.7. Поддержка и кастомизация правил классификации активов, поддержка ручной и автоматической классификации, автоматическое и ручное определение типа актива;	Поддержка ручной классификации бизнес-процессов в соответствии с методическим документом «Методика оценки угроз безопасности информации» ФСТЭК России, поддержка ручной классификации ИСПДн, ГИС и категорирования объектов КИИ.	Поддерживается с помощью встроенной утилиты Data Feed Manager и создания рабочих процессов («Advanced Workflows»)	Поддерживается ручная классификация объектов защиты (присвоение уровня критичности, заполняется пользователями в соответствии с их ролевой моделью), ручная классификация информационных систем с учетом их состава, поддержка формирования паспортов информационных систем и назначения ответственных, ведение реестра информационных систем, оповещение ответственных о необходимости проведения классификации. Настройка правил (как при интеграции, так и при создании) возможна с использованием Low-code платформы ePlat4m	Поддерживается ручная категоризация и классификация типов активов в соответствии с нормативными требованиями	Поддерживается вручную или через автоматически через шаблоны импорта или через модуль RPA. Поддерживается косвенная классификация через вхождение актива в области, через вертикальную связь с другими активами.	Поддерживается категорирование активов по IP-адресу с автоматическим присвоением свойств (по признакам конфиденциальность, целостность, доступность, критичность), поддерживается ручное категорирование (для пользователя с определенной ролью). Поддерживается указание уровней MTPD, RTO и RPO, функции технического актива, связей с бизнес-приложением, проектом, задание регуляторных требований для актива. Поддерживается ручное и автоматическое определение типа актива (на основании свойств актива, таких как тип и версия ОС, IP-адрес, FQDN-имя, залогиненный пользователь и т.д.) в рамках процесса идентификации обнаруженного сканированием актива
3.1.8. Поддержка и кастомизация настройки жизненного цикла активов в решении;	Поддерживается ручной контроль этапов жизненного цикла для экземпляров СКЗИ, поддерживается учет статуса документов и заявок	Не поддерживается специализированный функционал для управления активами, но доступна настройка логики по созданию жизненного цикла активов с помощью рабочих процессов («Advanced Workflows»)	Поддерживается, настраивается с использованием Low-code платформы ePlat4m	Частично поддерживается. Для настройки доступны только параметры устаревания активов, для оценки угроз по методике ФСТЭК России доступно ручное указание этапа жизненного цикла информационной системы (разработка или эксплуатация). Кастомизация жизненного цикла активов не поддерживается	Поддерживается через автоматизации RPA	Поддерживается настройка жизненного цикла устройства в соответствии с гибко кастомизируемым жизненным циклом, с указанием произвольных этапов и состояния жизненного цикла актива с применением подхода low-code / no-code. «Из коробки» жизненный цикл актива состоит из этапов «Новый», «На категорировании», «В эксплуатации», «Сломан», «В ремонте», «В резерве», «Выведен из эксплуатации». Поддерживается создание отдельного жизненного цикла для каждого типа актива.
3.1.9. Интеграции с системами управления активами (CMDB, ITAM, службы каталогов, иные источники), способ интеграции, импортируемые сущности, наличие двухсторонней связи;	Импорт данных об активах из файлов XLS, XLSX, CSV. Поддерживается импорт данных из XML-отчетов ПО AIDA.	Поддерживается импорт из файлов с разделителями (CSV, TXT), из XSLT, JSON, XML через API, через подключение к источникам (базы данных, FTP, HTTP, email, RSS) с помощью встроенной утилиты Data Feed Manager	Адаптеры для интеграции с внешними системами: XML, MS Excel, CSV, SOAP, Oracle Data Provider, Npgsql, ODBC, OLEDB, LDAP, HTTP REST, REST API. Поддерживается интеграция со следующими источникам данных, содержащих информацию об активах: MaxPatrol SIEM, RuSIEM, Ankey SIEM, Kuma, Symantec SIM, ArcSight, Alertix, FortiSIEM, MP SIEM, DATAPK, KSC, Efros CI, MaxPatrol 8, Ankey IDM, RedCheck, XSpider, Symantec DLP, Infowatch DLP, SearchInform DLP, UserGate, Zabbix, 10-strike, HPE Systems Insight Manager, VmWare vSphere, Checkpoint, Microsoft SCCM, HP Service Desk, AD, 1C	Поддерживаются следующие источники данных об активах: AD, Forcepoint TRITON AP-DATA, Kaspersky Security Center, MS SCCM, SecretNet, Symantec EPM, MaxPatrol, XSpider, Nessus, Tenable.sc, Qualys, Rapid7 Nexpose, RedCheck, InfoWatch Device Monitor, McAfee ePolicy Orchestrator, MP SIEM, Zabbix, сервис «Антифишинг», HP SM, Naumen Service Desk, Micro Focus UCMDB, VMware, Skybox, интеграции с базами данных MS SQL/MySQL/Oracle/PostgeSQL, R-Vision Endpoint, универсальный коннектор Python. Доступна настройка произвольных интеграций через API	Поддерживаются прямые интеграции с Active Directory, Kaspersky KSC, Zabbix, Sloar Dozor. Поддерживается универсальный импорт данных из любых систем через файлы или API. Поддерживается двухсторонняя связь с Jira. Поддерживается импорт любых сведений об активах.	Поддерживается интеграция с MicroFocus Service Manager (HP Service Manager), CMDB iTop, MS SCCM, MS WSUS, Kaspersky Security Center (подключение к БД и OpenAPI), Kaspersky Unified Monitoring and Analysis Platform (KUMA), Active Directory, Infoblox (IPAM), Skybox, SearchInform, Lansweeper, MaxPatrol 8, MaxPatrol SIEM, IBM QRadar, Symantec CSP, VmWare vCenter, VmWare vRops, HP OneView, Cisco UCS, Symantec Endpoint Protection Manager, Creatio BPM, Efros Config Inspector, Microsoft Endpoint Configuration Manager, Zabbix, Ovirt, NetBox. Поддерживается импорт данных об активах из CSV-файла. Поддерживается вычитка и нормализация данных по активам из различных СУБД: MS SQL, PostgreSQL, MySQL, Oracle. Подключение к произвольной системе посредством API.

3.1.10. Наличие агентного / безагентного метода сбора данных об активах;	Не поддерживается	Не поддерживается, сбор данных осуществляется только за счет импорта данных	Поддерживается через интегрируемые системы	Поддерживаются оба способа	Поддерживается: в модуле RPA есть функционал запуска скриптов PowerShell, Python, Bash и отправки API запросов. Агентный сбор данных не поддерживается	Безагентный способ, удаленное подключение к Linux, Windows, сетевым устройствам с помощью протоколов и механизмов REST API, HTTP / HTTPS, PowerShell, RPC, SNMP, SSH, LDAP, WMI, подключения к СУБД (MSSQL, MySQL, Oracle, PostgreSQL)/ Возможность установки агента для сбора и получения данных
3.1.11. Возможность обнаружения активов в сети;	Не поддерживается	Не поддерживается	Возможность обнаружения активов самим решением не предусмотрена, обнаружение возможно только по результатам работы интегрируемых систем	Поддерживается ручная и автоматическая (с настройкой политики сканирования) инвентаризация, осуществляемая при помощи сканера nmapc дальнейшим аутентифицированным удаленным подключением к сканируемому ресурсу (WMI, удаленный реестр, SNMP)	Поддерживается через запуск скриптов или из отчетов сканеров безопасности, в т.ч. nmap	Поддерживаются встроенные механизмы активного сканирования, идентификации, инвентаризации, запускаемые автоматически, по расписанию, вручную, с настройкой типа сканирования и сканируемых портов (SSH, WinRM, HTTP, UDP, TCP) Сканирование включает в себя автоматическое определение типа оборудования, версии ОС по баннерам, портам и другим параметрам
3.1.12. Возможность настройки алгоритма определения типа актива;	Не поддерживается	Не поддерживается специализированный функционал для управления активами, но доступна настройка логики по созданию жизненного цикла активов с помощью рабочих процессов («Advanced Workflows»)	Поддерживается с использованием Low-code платформы ePlat4m	Поддерживается с помощью настройки политик назначения атрибутов, выполняющихся по результатам инвентаризации или по расписанию. Поддерживается использование regex-выражений, SQL-оператора ilike, исключений для создания правил соотнесения обнаруженного актива с какой-либо группой активов. Политики не редактируемые, для их изменения требуется удаление и создание политики заново	Поддерживается через создание шаблонов импорта.	Поддерживается настройка механизмов активного сканирования и идентификации активов в сети, для идентификации и определения типа используется встроенный, кастомизируемый процесс проверок (с применением подхода low-code / no-code) по баннерам, портам и другим параметрам и настраиваемый служебный справочник, содержащий записи названий ОС, производителей оборудования и т.д.
3.1.13. Поддержка способов оценки и визуализации состояния процесса управления активами (метрики, отчетность, дашборды).	Поддерживается формирование и отображение графической схемы взаимодействия информационных систем (формирование автоматически по заполненным данным, с возможностью ручной правки элементов схемы), с поддержкой экспорта изображения в формате SVG	Поддерживается визуализация информации в «Рабочих пространствах» (набор дашбордов), виджетах, представлениях, таблицах, отчетах. Поддерживается публикация запросов, опросников, приложений на внешнем портале с помощью функционала модуля «Engage»	Виджеты с круговыми, столбчатыми диаграммами, табличным отображением информации по активам.	Поддерживается отображение данных об активах и их свойствах на графиках, географической карте, в виде графа с отображением связей с другими активами	Поддерживается конструктор метрик и дашбордов, визуализация на дашбордах и в таблицах, экспорт в xlsx.	Поддерживается отображение состояния активов на дашбордах, в гридах и карточках активов в виде виджетов (линейный график, столбчатая диаграмма, круговая диаграмма, радар («паутинка»), спидометр, таблица, географическая карта, глобус), на графах связей, на дашбордах, в отчетах
3.2. Управление уязвимостями:						
3.2.1. Поддерживаемые интеграции со сканерами уязвимостей и системами управления уязвимостями;	Поддерживается интеграция со средствами анализа защищенности	Поддерживаются интеграции с базой NIST NVD, сканерами уязвимостей Qualys и Tenable.sc, системой мониторинга рисков RiskRecon с помощью модуля Archer IT Security Vulnerabilities Program	Maxpatrol VM, MaxPatrol 8, RedCheck, XSpider. Возможна настройка интеграции с другими сканерами	Поддерживается интеграция с MaxPatrol, XSpider, OpenVAS, Nessus, Vulners.com	Поддерживаются инфраструктурные сканеры Qualys, Nessus, RedCheck, Nmap, OpenVas, Kaspersky, XSpider, сканеры веб приложений (например, OWASP ZAP) и сканеры кода (например, AppScreener, SNYK), поддерживающие формат Sarif	Поддерживается интеграция с Qualys (API-интеграция, XML-файлы), Nessus (XML-файлы), Tenable.io, Tenable.sc, RedCheck (подключение к БД, XML-файлы, API), MaxPatrol 8, MaxPatrol VM, OpenVAS, Kaspersky Security Center, сервисом Vulners.com
3.2.2. Поддерживаемые поставщики бюллетеней с информацией об уязвимостях;	Поддерживается интеграция с БДУ ФСТЭК России	Поддерживаются интеграции с базой NIST NVD с помощью модуля Archer IT Security Vulnerabilities Program	Не поддерживается	Поддерживается за счет интеграции с базой Vulners.com	Контент берется из отчетов сканеров	Поддерживается работа с бюллетенями НКЦКИ, ФинЦЕРТ, БДУ ФСТЭК России, базой NVD, базой Vulners.com, бюллетенями Microsoft, поддерживается импорт бюллетеней в формате CVRF и OVAL
3.2.3. Ведение списка исключений или белых списков уязвимостей;	Не поддерживается	Не поддерживается «из коробки», но может быть настроено с помощью рабочих процессов	Не поддерживается	Частично поддерживается. С помощью настройки политики управления уязвимостями с возможностью удаления уязвимости при выполнении заданных критериев	Поддерживается механизм принятия уязвимостей, в т.ч. временного	Поддерживается ручная и автоматическая (по задаваемым пользователем условиям) установка исключений для создаваемых в решении заявок на устранение уязвимостей
3.2.4. Поддержка и кастомизация правил группировки, дедупликации импортированной информации об уязвимостях;	Не поддерживается	Не поддерживается «из коробки», но может быть настроено с помощью рабочих процессов	Поддерживается при настройке коннекторов	Не поддерживается	Поддерживается группировка по затронутым бизнес-системам, типам уязвимостей, уязвимом ПО.	«Из коробки» применяется подход группирования уязвимостей по признаку «PluginID» сканера, по CVE-идентификатору. Группируются уязвимости, найденные разными сканерами на одном активе. Поддерживается настройка правил группировки с учетом свойств активов и уязвимостей, по которым определяется уникальность объектов при импорте для избежания дублирования. Возможность создания нескольких правил группировки, каждое из которых включает от 1 до всех свойств активов и уязвимостей. Поддерживается создание фильтров для задания условий срабатывания правил

						группировки
3.2.5. Поддержка и кастомизация настройки создания задач на устранение уязвимостей;	Поддерживается создание заявок вручную	Поддерживается создание заявок («tickets») в решении, кастомизация поддерживается	Поддерживается возможность редактирования формы заявки	Поддерживается с помощью настройки политики управления уязвимостями	Решение готовит шаблон задачи на устранение уязвимости (название, описание, приоритет, SLA, определяет ответственного), но запускает задачу в работу оператор вручную.	Поддерживается создание в решении заявок на устранение уязвимостей с назначением ответственных, установкой сроков, постановкой подзадач. Поддерживается создание заявок вручную и автоматически на основании настраиваемой политики устранения уязвимостей (с учетом CVSS-рейтинга и характеристик уязвимости и свойств актива)
3.2.6. Возможность автоматического создания задач на исправление уязвимостей во внешние тикет системы, количество интеграций;	Не поддерживается	Не поддерживается	Поддерживается при настройке соответствующего коннектора и наличия механизмов во внешней системе	Поддерживается передача задач на устранение уязвимостей, созданных в решении, во внешние системы Naumen Service Desk, HP Service Manager	После создания оператором задачи она может быть автоматически направлена в Jira (двухсторонняя связь) или другую систему заявок (по API, односторонняя связь).	Поддерживается интеграция с Jira, Naumen Service Desk, MicroFocus Service Manager (HP Service Manager), BPM Online (Creatio), OTRS.
3.2.7. Поддержка и кастомизация механизмов приоритизации уязвимостей в зависимости от свойств уязвимостей и активов;	Не поддерживается	Не поддерживается «из коробки», но может быть настроено с помощью рабочих процессов	Поддерживается средствами Low-code платформы ePlat4m	Поддерживается с помощью настройки формулы расчета рейтинга уязвимостей и настройки политики управления уязвимостями	Поддерживается выбор из набора формул для приоритизации, в том числе формулы по методике ФСТЭК России	Поддерживается с помощью настройки политики устранения уязвимостей, с установкой критичности и SLA вручную и автоматически (с учетом CVSS-рейтинга и характеристик уязвимости и свойств актива, с помощью «Дерева решений» с учетом характеристик актива, уязвимости, связанных объектов)
3.2.8. Поддержка и кастомизация настройки жизненного цикла уязвимостей;	Не поддерживается	Не поддерживается «из коробки», но может быть настроено с помощью рабочих процессов	Поддерживается, при этом учитываются заявки на устранение (планы по устранению), а также описание, CVSS-рейтинг, уровень опасности, рекомендации по устранению уязвимостей. Кастомизация возможна средствами Low-code платформы ePlat4m	Поддерживается фиксированный набор статусов уязвимостей с изменением статусов вручную или через политики управления уязвимостями. Кастомизация жизненного цикла уязвимостей не поддерживается	Срок жизни уязвимостей и поведение задается в настройках модуля	Поддерживается с помощью настройки политики устранения уязвимостей, перечень возможных статусов уязвимостей настраивается. Возможность редактирования и создания собственного жизненного цикла с использованием функционала конструктора рабочих процессов в режиме no code.
3.2.9. Контроль соблюдения SLA устранения уязвимостей;	Фиксируется дата устранения уязвимости (вносится вручную после выполнения действий по устранению)	Поддерживается	Поддерживается, выполняется вручную в рамках создаваемых планов по устранению уязвимостей (указание дат начала и завершения, ответственного)	Поддерживается с помощью создания задач на устранение уязвимостей и указания срока исполнения	Поддерживается через модуль задач, с контролем сроков и отправкой уведомлений о просрочке исполнителю и инициатору задачи.	Поддерживается с помощью настройки политики устранения уязвимостей, поддерживается установка различных ответственных и временных нормативов (дни / часы / минуты) в зависимости от свойств уязвимости и актива с учетом системы эскалаций и визуализации процесса устранения через таймлайн и систему виджетов
3.2.10. Контроль устранения уязвимостей и автоматическое закрытие уязвимостей по результатам отчетов от сканеров уязвимостей;	Не поддерживается	Не поддерживается	Поддерживается при настройке коннекторов	Частично поддерживается. С помощью анализа статусов уязвимостей от сканеров уязвимостей и сравнения статусов в решении с возможностью повторного открытия	Поддерживается автоматическое закрытие уязвимостей по результатам отчетов от сканеров уязвимостей.	Поддерживается через автоматическую проверку наличия уязвимостей после закрытия заявок на устранение уязвимостей по результатам обработки свежих отчетов от сканеров с учетом различных условий (например, применялся аналогичный профиль сканирования, актив был успешно просканирован, ПО было обнаружено и т.д.)
3.2.11. Связь уязвимостей с активами;	Поддерживается указание связи между уязвимостями, ПО, ОС и информационными системами	Поддерживается	Поддерживается, информация об активах и обнаруженных на них уязвимостях поступает из интегрируемых систем	Поддерживается	Поддерживается автоматическая связь, в том числе с бизнес-системами.	Поддерживается, с визуализацией связей на графе и географической карте
3.2.12. Поддержка способов оценки и визуализации состояния процесса управления уязвимостями (метрики, отчетность, дашборды).	Поддерживается формирование отчетности по документам, ответственным, доступам пользователей, по готовности к проверкам РосКомНадзора / ФСТЭК России / ФСБ РФ, по эксплуатируемым ПО, информационным системами и системам защиты информации, по категорированию объектов КИИ, выполнению применимых требований законодательства. Поддерживается отображение информации на «Рабочем столе» в виде изменяемых дашбордов (статистика, список задач, диаграммы, календари, структура подведомственных организаций). Поддерживается быстрый переход	Поддерживается визуализация информации в «Рабочих пространствах» (набор дашбордов), виджетах, представлениях, таблицах, отчетах. Поддерживается публикация запросов, опросников, приложений на внешнем портале с помощью функционала модуля «Engage»	Виджеты с круговыми, столбчатыми диаграммами, табличным отображением информации по уязвимостям	Поддерживается с отображением уязвимостей на графике (история изменения уязвимостей), на диаграммах (отображение групп активов с уязвимостями), на географической карте, на графе связей активов	Поддерживаются метрики, дашборды, отчетность (с выгрузкой в XLS)	Поддерживается отображение состояния на дашбордах, в гридах и карточках уязвимостей в виде виджетов (линейный график, столбчатая диаграмма, круговая диаграмма, радар («паутинка»), спидометр, таблица, географическая карта, глобус), на графах связей, на дашбордах, в отчетах

	от дашборда к отчету. Поддерживается учет метрики по заявкам (время обработки), метрики загруженности пользователей организации					
3.3. Управление задачами, знаниями, документами:						
3.3.1. Поддержка и кастомизация настройки жизненного цикла задач в решении;	Поддерживается создание задач с указанием даты исполнения и ответственных (исполнителей), установка статуса (состояния: создано, закрыто, переоткрыто, в работе, решено) и даты создания задачи	Поддерживается создание и управление задачами («tasks»), кастомизация поддерживается	Поддерживается, жизненный цикл задач настраивается и кастомизируется средствами Low-code платформы ePlat4m	Частично поддерживается: перечень статусов задач фиксирован (запланировано, выполняется, на проверке, завершено), возможно перемещение задачи в архив (действие необратимо)	Поддерживается в «Модуле задач». У задач есть приоритеты, отметки (тэги), ответственные, сроки, комментарии, присоединение файлов, связь с любыми объектами в системе (защитными мерами, активами), история изменений задачи, возможность отложить задачу. Задачи могут создаваться вручную или автоматически. Задачи могут назначаться в т.ч. не на пользователей системы (через модуль «Опросы»). Уведомления о задачах на почту, Telegram, MS Teams	Поддерживается создание и управление задачами, формируемыми по результату проведения аудитов, оценки рисков, обработки уязвимостей и т.д.. Настройка жизненного цикла выполняется с помощью рабочего процесса управления задачами в решении, с поддержкой условий ветвлений и выполнения действий, установкой статусов в зависимости от заданных условий, назначением ответственных и сроков, ролевой модели доступа.
3.3.2. Интеграция с системами управления заявками / задачами, тикетинг-системами, способ интеграции, импортируемые / экспортируемые сущности, наличие двухсторонней связи;	Не поддерживается	Не поддерживается	Есть возможность интеграции с внешними тикетинг-системами, системами электронного документооборота в т.ч. по API, поддерживается интеграция с СУБД, импорт файлов csv, xml, xls	Поддерживается экспорт и импорт задач из Naumen Service Desk, HP Service Manager	Поддерживается двухсторонняя связь с Jira, с другими системами – односторонняя, через отправку API-запросов.	Поддерживается интеграция с Jira, Naumen Service Desk, MicroFocus Service Manager (HP Service Manager), BPM Online (Creatio), OTRS. Поддерживается экспорт и импорт сущностей (заявки, связанные объекты, ответственные), синхронизация статусов и атрибутов.
3.3.3. Наличие, функционал, кастомизация встроенной базы управления документами (внутренние политики, регламенты, положения, инструкции, руководства) в решении;	Поддерживается автоматизированное создание организационно-распорядительной документации по ИБ, с возможностью выгрузки документов в форматах PDF, DOCX, ODS, с возможностью импорта (вложения) файлов в различных форматах (документы, таблицы, схемы, изображения, архивы). Поддерживается создание пользовательских документов и использование предварительно загруженных вендором шаблонов документов.	Поддерживается в модуле Archer Document Governance	Поддерживается возможность загрузки и учета пользовательских документов, требований, рекомендаций, включая соглашения о неразглашении конфиденциальной информации, договоры и соглашения о конфиденциальности. Поддерживается отслеживание взаимосвязей и версионности документов, оповещение о необходимости актуализации документов, согласование документов. Поддерживается автоматическое создание необходимых документов на базе заведенных шаблонов и данных из решения. Кастомизация выполняется средствами Low-code платформы ePlat4m	Поддерживается создание вручную и автоматически из сформированного отчета, поддерживается добавление файлов к документу, добавление связанных с документов активов и задач, ограничение доступа к документу (по пользователям, с назначением каждому уровня доступа к документу). Поддерживается создание дополнительных полей (свойств) документа с параметрами полей	Поддерживается ведение реестров документов по ИБ, с кастомными метриками, автоматическим контролем сроков, связями с другими активами, чеклистами по каждому документу.	Поддерживается создание пользовательских типов документов. Поддерживается формирование собственного набора мер (требований), их связь с документами и подпадающих под них информационных систем, поддерживается импорт требований (из файлов формата CSV)
3.3.4. Наличие, функционал, кастомизация встроенной базы управления договорами (взаимоотношения с поставщиками и подрядчиками, обязательства перед заказчиками и клиентами, требования NDA, SLA и т.д.) в решении.	Поддерживается управление данными о поставщиках услуг (ИТ/ИБ)	Поддерживается в модуле Archer Third Party Governance	Поддерживается в рамках управления пользовательскими документами. Кастомизация выполняется средствами Low-code платформы ePlat4m	Поддерживается в рамках управления документами, отсутствует специализированный функционал (например, для управления рисками цепочки поставок и доверенными отношениями с третьими лицами)	Поддерживается ведение реестров договоров и любых других типов документов, с кастомными полями, метриками, автоматизациями контроля. Поддерживается проведение оценки контрагентов (Vendor Risk Assessment) по собственным наборам требований, в том числе интерактивно направляя и собирая данные с контрагентов (через модуль «Опросы»)	Поддерживается функционал загрузки пользовательских договоров (документов) в решение, формирование опросных листов, требований для аудитов, задач на основе положений загруженных договоров. Поддерживается управление взаимоотношениями с третьими лицами (учет NDA, предоставление доступа и данных, учет зависимостей и т.д.)
4. Управление киберрисками:						
4.1. Возможность автоматизированного сбора оценок при помощи опросных листов с учетом ролевой политики	Поддерживается формирование задач и документов для контроля выполнения требований подведомственными организациями, а назначением задач исполнителям из	Поддерживается в модуле Archer IT Risk Management	Не поддерживается	Поддерживается, с функционалом создания области оценки рисков, назначения менеджера оценки рисков и рабочей группы по оценке рисков, задания ролей пользователей («Наблюдатель», «Участник»). В решении предусмотрены выделенные роли «Риск-менеджер», «Менеджер по управлению рисками» и «Аналитик по управлению рисками». Поддерживается возможность проведения оценки рисков автоматически без	Поддерживается через модуль «Опросы», в котором можно автоматически проводить оценку рисков у владельцев рисков и иных работников, в том числе не имеющих доступ в систему.	Поддерживается с помощью функционала создания процесса оценки рисков с указанием сроков и экспертов - ответственных (с учетом ролевой модели организации) за заполнение опросного листа, перечня информационных систем и оцениваемых угроз. На основании заполненных опросников автоматически рассчитывается величина уровня киберрисков для информационной системы, создаются задачи по обработке рисков. Возможность исключения оценок заданных опросных листов из расчёта.

компании;	подведомственных учреждений			участия экспертов и автоматизированно с участием экспертов (с проставлением экспертами количественных и качественных значений оценки рисков)		Настройка жизненного цикла опросных листов с возможностями утверждения и цикла доработок. Наличие рабочего места респондента для заполнения опросного листа. Возможность рассылки опросных листов по электронной почте и импорта результатов заполнения.
4.2. Наличие встроенных механизмов оценки киберрисков (качественная / количественная) с учетом свойств активов, уязвимостей, инцидентов и т.д.;	Поддерживается в рамках моделирования нарушителей и угроз безопасности информации в соответствии с методическим документом «Методика оценки угроз безопасности информации» ФСТЭК России	Поддерживается в модулях Archer IT Risk Management и Archer Insight	Управление киберрисками реализовано в соответствии с частной методологией одного из заказчиков: использование предустановленного реестра рисков и справочников, ручное заполнение карточек риска, формирование реестра мероприятий	Поддерживается, из коробки доступны следующие методики оценки рисков: ·Базовая 3-уровневая схема (простая схема оценки рисков с использованием качественных шкал из трёх уровней); ·Базовая числовая 3-уровневая схема (простая схема оценки рисков с использованием числовых качественных шкал из трёх уровней); ·Базовая количественная оценка (простая схема оценки рисков с использованием только количественных параметров и простых расчетов); · Типовая схема оценки рисков R-Vision (схема, разработанная специалистами R-Vision); · РС БР ИББС-2.2-2009 (методика ЦБ РФ); ·FAIR (Factor Analysis of Information Risk Methodology); · ALE (Quantitative Risk Assessment Method); Схема оценки угроз ФСТЭК (по методическому документу ФСТЭК России «Методика определения угроз безопасности информации в информационных системах»)	Поддерживается: риски рассчитываются автоматически исходя из свойств угроз, уязвимостей и активов. Поддерживаются несколько формул для оценки, несколько вариантов отображения величин рисков (баллы, проценты).	Поддерживается проведение качественной и количественной оценки, с учетом финансового эффекта реализации киберриска (ущерба), вероятности реализации угрозы, свойств уязвимостей, свойств активов (информационных систем). Возможность применения модели Монте Карло и других аналогичных моделей для расчёта количественной оценки. Возможность моделирования применения плана мер защиты и корректирующих мероприятий, оценка остаточного риска. Возможность использования коробочной методики (наиболее распространенные общеизвестные) и создания пользовательской методики оценки рисков.
4.3. Наличие встроенных механизмов анализа киберрисков, моделирования угроз и нарушителей, применяемые и поддерживаемые методологии, возможность кастомизации методологии.	Поддерживается, выполняется в соответствии с методическим документом «Методика оценки угроз безопасности информации» ФСТЭК России	Поддерживается в модуле Archer IT Risk Management, поддерживаемые методологии: COSO ERM, ISO 31000, NIST 800-30, ISO 27005	Перечень угроз ИБ из реестра УБИ БДУ ФСТЭК из коробки, формирование модели угроз по методике ФСТЭК ("Методика оценки угроз безопасности информации"), формирование планов устранения угроз ИБ.	Поддерживается моделирование угроз по методике ФСТЭК ("Методика оценки угроз безопасности информации") с поддержкой настройки параметров методики (поддержка простых сценариев атак и цепочек атак, настройка параметров источников атак с учетом возможности сговора нарушителей, настройка предпосылок и атрибутов безопасности)	Формируются реестры рисков, планы обработки рисков, реестры актуальных угроз. Проводится оценка первичного, текущего и проектного (остаточного) уровня риска. Поддерживается задание своих критериев оценки для ущерба, вероятности, приоритета активов, изменять уровень риск-аппетита.	Поддерживается моделирование угроз и нарушителей в соответствии с методологией ФСТЭК России. Возможность создания пользовательской методики моделирования угроз и нарушителей
5. Управление аудитами и соответствием требованиям:						
5.1. Наличие встроенных механизмов проведения аудитов кибербезопасности (на соответствие внутренним нормативным требованиям), применяемые и поддерживаемые методологии, возможность кастомизации методологии;	Поддерживается ведение плана внутренних проверок и их организация, с установкой плановой и фактической даты проведения мероприятий, исполнителя, вводом результатов проверки. Поддерживается формирование отчетов по проверкам с выгрузкой в форматах PDF, DOCX, ODT	Поддерживается в модуле Archer Audit Management	Методологии, заложенные из коробки: Законодательство по защите ПДн, по безопасности КИИ, ГОСТ Р ИСО/МЭК 27001, Методика оценки СОИБ (Газпром). Возможность автоматизации проведения проверок при интеграции с системами заказчика (например, регулярная проверка наличия определенного ПО или СЗИ, формирование задачи на устранение в случае отсутствия). Наличие встроенного таск-трекера, возможность двухсторонней интеграции со сторонними таск-трекерами	Поддерживается проведение аудитов простых (ручная оценка выполнения требований экспертом) и сводных (проведение оценки выполнения требований, обработка замечаний, формирование плана устранения недостатков). Поддерживается настройка параметров аудита, включая шкалу оценок. Поддерживаются преднастроенные типы аудитов: стандартный (по методологии R-Vision), СТО БР ИББС-1.0-2014 (ЦБ РФ), 382-П (ЦБ РФ), СТБ 34.101.41-2013 (для банков Республики Беларусь), SWIFT CSP, ГОСТ Р 57580.2-2018, ISO/IEC 27001:2022	Поддерживается создание собственных наборов внутренних требований и проведение по ним аудитов (контроль соответствия). Поддерживаются 3 типа (методологии) для оценки соответствия требованиям, которые могут применяться одновременно в рамках одного аудита - через явное задание уровня соответствия, через связь с защитными мерами, через кастомные метрики, собираемые системой. Поддерживается отдельный компонент аудита по методологии ГОСТ 57580.2	Поддерживается создание пользовательских процедур аудита с указанием сроков проведения, перечня аудируемых информационных систем, состава участников (с учетом ролевой модели организации), перечня применимых мер (требований), с формированием опросных листов (в них ответственные указывают оценку реализации мер, прикладывают свидетельства в виде файлов, оставляют комментарии) и отправкой заполненных опросных листов организатору аудита. Наличие рабочего места респондента для заполнения опросного листа.
5.2. Наличие, функционал, кастомизация процесса проведения аудитов кибербезопасности;	Поддерживается проведение аудитов	Не поддерживается «из коробки», но может быть настроено с помощью рабочих процессов	Проведение проверок в ручном режиме, с установкой задач ответственным, назначением роли аудитора, формированием плана устранения несоответствий. Общие требования разбиваются на атомарные требования, каждому назначается определенный вес. Кастомизация	Поддерживается с помощью создания полностью настраиваемого типа аудита (создание пользовательских форм аудита, показателей соответствия, использования пользовательских формул, кастомных статусов), с поддержкой импорта типа аудита, созданного	Поддерживается	Поддерживается, процедуры аудита полностью кастомизируются под требования организации. Возможна автоматизация оценки выполнения требования на основании данных из

			выполняется средствами Low-code платформы ePlat4m	ранее		интегрируемых ИТ и ИБ систем.
5.3. Наличие встроенных механизмов проведения оценки выполнения внешних нормативных требований кибербезопасности, поддерживаемые нормативные требования;	Поддерживается оценка соответствия требованиям регуляторов в части защиты ПДн, безопасности КИИ, защите информации в ГИС	Поддерживается в модуле Archer Corporate Obligations Management	Оценка выполнения проводится путем заполнения опросников в рамках назначенных задач с учетом ролевой модели. Поддерживаемые нормативные требования: Законодательство по защите ПДн (152-ФЗ), законодательство по безопасности КИИ (Приказ №239 ФСТЭК России), стандарт ГОСТ Р ИСО/МЭК 27001	Поддерживается, нормативные требования: Приказ ФСТЭК № 17, Приказ ФСТЭК № 239, Приказ ФСТЭК № 21, Приказ ФСТЭК № 31, 152-ФЗ, ПП РФ № 211, Приказ ФСБ № 378, ГОСТ 27001-2006, ГОСТ 27001-2021, ISO 27001:2013, ISO/IEC 27001:2013/DAM 1:2022, ISO/IEC 27002:2022, ТКЗИ КВОИ, ГОСТ Р 57580.1-2017, 49-Т, 382-П, 552-П, СТО БР (2014), Форма 0409071, 716-П, PCI DSS, PCI DSS 3.2, PCI DSS 3.2.1, SWIFT CSP, СТБ 34.101.41-2013, ТТП ИБ 5.1-2020	В системе загружены более 50 российских и международных стандартов и документов с требованиями по информационной безопасности. Требования стандартов скоррелированы друг с другом. Проведенный аудит по одному стандарту через механизмы рекомендательной модели позволяет пройди аудит по другим стандартам.	Поддерживается, нормативные требования: · Положение Банка России от 4 июня 2020 г. № 719-П · Положение Банка России от 20 апреля 2021 г. № 757-П · Положение Банка России от 25 июля 2022 г. № 802-П ·Положение Банка России от 17 апреля 2019 г. N 683-П ·Приказ ФСТЭК России от 21 декабря 2017 г. N 235 · CIS Critical Security Controls® Version 8 ·Приказ ФСТЭК России от 14 марта 2014 г. N 31 ·Приказ ФСТЭК России от 11 февраля 2013 г. N 17 ·Приказ ФСТЭК России от 18 февраля 2013 г. N 21 ·Приказ ФСТЭК России от 25 декабря 2017 г. N 239 · ГОСТ Р 57580.1-2017 · PCI DSS
5.4. Наличие, функционал, кастомизация процесса проведения оценки выполнения внешних нормативных требований кибербезопасности;	Поддерживается проведение оценки	Не поддерживается «из коробки», но может быть настроено с помощью рабочих процессов	В рамках изменения механизма назначения и выполнения задач, заполнения опросных листов с процентными соотношениями выполнения пунктов в отношении показателя. Также возможна интеграция со сторонними системами, автоматически обновляющими состояние безопасности (сканеры уязвимостей, системы контроля безопасности, системы антивирусной защиты и т.д.). Кастомизация выполняется средствами Low-code платформы ePlat4m	Поддерживается в рамках кастомизации аудитов	Поддерживается	Поддерживается в рамках кастомизации процедуры аудита
5.5. Возможность создания пользовательских нормативных документов и требований;	Поддерживается	Поддерживается в модуле Archer Corporate Obligations Management	Поддерживается возможность импорта / экспорта требований, рекомендаций по оценке требований, шаблонов проверок, справочников из xls-файла	Поддерживается в рамках кастомизации аудитов, создания пользовательских требований для аудита	Поддерживается	Поддерживается, с формированием произвольного набора документов и требований
5.6. Возможность проведения аудита по произвольному перечню требований из нормативных документов и стандартов ИБ.	Поддерживается	Поддерживается в модуле Archer Audit Management	Поддерживается, возможно создавать пользовательские наборы требований	Поддерживается	Поддерживается, если их вынести в отдельный набор требований и провести корреляцию (доступно в интерфейсе пользователя)	Поддерживается, с проведением аудитов по пользовательскому набору требований. Возможность выбора как единичных требований, так и с применением различных фильтров, включая тэги.
6. Управление КИИ:						
6.1. Возможность ведения критических бизнес-процессов организации;	Поддерживается	Не поддерживается	Поддерживается	Поддерживается возможность формирования перечня критических процессов в рамках процесса категорирования объекта КИИ. Поддерживается импорт перечня процессов из XLS-файла и из внешней базы данных	Поддерживается создание и ведение реестра критических бизнес-процессов организации	Поддерживается, с автоматическим соотнесением информационных систем и бизнес-процессов
6.2. Возможность определения объектов КИИ;	Поддерживается	Не поддерживается	Поддерживается возможность ведения реестра объектов КИИ	Поддерживается ручное и автоматическое (с помощью политики назначения атрибутов или на основе наследования связи объекта КИИ с процессом) формирование перечня объектов КИИ	Поддерживается создание и ведение реестра объектов КИИ	Поддерживается, с возможностью автоматического проставления признаков отнесения активов к объекту КИИ

6.3. Возможность формирования комиссии по категорированию;	Поддерживается	Не поддерживается	Поддерживается		Поддерживается создание карточки комиссии (комиссий) и определить состав через связь с активами типа работник	Поддерживается
6.4. Возможность выполнения процедуры категорирования ОКИИ с автоматизированным расчётом категории;	Поддерживается	Не поддерживается	Поддерживается	Поддерживается: категорирование производится для всех информационных систем в рамках объектов КИИ, поддерживается автоматическое присвоение категории значимости на основании оценки 14 показателей критериев значимости	Не поддерживается	Поддерживается, с автоматическим заполнением сведений о статусе объекта КИИ, статусе акта категорирования, внесении в реестр объектов КИИ, категории объекта КИИ, дате внесения в реестр, дате расчета критериев; при этом критерии значимости объекта КИИ заполняются вручную. Поддерживается возможность сбора информации по критериям значимости посредством опросных листов и автоматический расчёт критерия значимости на основании пользовательских данных.
6.5. Возможность выполнения оценки соответствии системы защиты ОКИИ на соответствие приказам ФСТЭК России;	Поддерживается	Не поддерживается	Поддерживается	Поддерживается с помощью проведения аудитов на соответствие выполнению требований Приказа ФСТЭК России №239	Поддерживается, все приказы уже загружены и декомпозированы на отдельные требования.	Поддерживается процесс оценки соответствия безопасности автоматизированной системы объекта КИИ требованиям приказов ФСТЭК России №239, 235, 236. При этом по каждой нереализованной или реализованной частично мере защиты или группе мер может быть сформирована задача по устранению замечаний, которая передается на исполнение ответственным специалистам
6.6. Возможность привлечения экспертов от структурных подразделений для выполнения оценки соответствии системы защиты ОКИИ на соответствие приказам ФСТЭК России;	Поддерживается	Не поддерживается	Поддерживается	Поддерживается	Поддерживается через модуль «Опросы»: в оценке могут участвовать работники, в т.ч. не имеющие доступа в систему, которые могут также присоединять свидетельства аудита (файлы) к каждому требованию.	Поддерживается привлечение дополнительных сотрудников с использованием функционала опросных листов для оценки соответствии системы защиты ОКИИ требованиям приказов ФСТЭК России №239, 235, 236. Наличие рабочего места респондента для заполнения опросного листа.
6.7. Возможность разработки планов по реализации мероприятий по обеспечению безопасности объектов КИИ;	Поддерживается	Не поддерживается	Поддерживается ручное проведение оценки соответствия выполнения требований приказов ФСТЭК, ручное создание задач	Поддерживается	Поддерживается через модуль «Защитные меры»: можно сформировать план мероприятий, контролировать его исполнение, формировать отчетность.	Поддерживается, путем формирования плана контрольных мероприятий по каждой нереализованной или частично реализованной мере защиты или группе мер, с дальнейшим созданием и контролем задач по устранению замечаний
6.8. Возможность формирования содержательной части сведений по результатам категорирования по установленной регулятором форме;	Поддерживается	Не поддерживается	Поддерживается автоматическая подготовка необходимых документов (сведения об объекте КИИ, акт категорирования объекта КИИ, перечень объектов, подлежащих категорированию) в соответствии с шаблонами, утвержденными ФСТЭК	Поддерживается	Не поддерживается, система не создает типовые документы	Поддерживается
6.9. Возможность формирования содержательной части акта (актов категорирования);	Поддерживается	Не поддерживается	Поддерживается	Поддерживается при условии заполнения данных в карточке объекта КИИ	Не поддерживается, система не создает типовые документы	Поддерживается
6.10. Возможность учёта и обработки запросов от регуляторов, поддержка взаимодействия с НКЦКИ (ГосСОПКА).	Поддерживается формирование отчетов и отправка уведомлений по инцидентами в НКЦКИ (ГосСОПКА).	Не поддерживается	Поддерживается взаимодействие с НКЦКИ из интерфейса решения для передачи информации об инцидентах ИБ, статусе их расследования, а также для получения информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения	Поддерживается, с автоматическим заполнением карточки инцидента для отправки в ГосСОПКА, с поддержкой автоматической или ручной отправки данных в ГосСОПКА, поддерживается отправка файлов и свидетельств по инциденту, обмена информацией с оператором ГосСОПКА, получением статуса уведомления в ГосСОПКА. Поддерживается получение сообщений (инцидентов) от НКЦКИ	Поддерживается: учет писем с требованиями/рекомендациями от регуляторов ведется в модуле «Контроль соответствия». Учет запросов / заявок ведется в реестрах в модуле активов	Поддерживается автоматическое заполнение карточки инцидента для отправки в ГосСОПКА, автоматическая или ручная отправка данных в ГосСОПКА, отправка файлов и свидетельств по инциденту, получением информации от НКЦКИ (статус уведомления в ГосСОПКА, ответ от сотрудников НКЦКИ по инциденту)
7. Управление операционными рисками:						
7.1. Возможность сбора и регистрации событий ОР;	Не поддерживается	Не поддерживается специализированный функционал для управления операционными рисками по требованиям ЦБ РФ (716-П), но поддерживается общий процесс управления	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается, возможна ручная, автоматическая и пакетная загрузка данных по событиям ОР. Поддерживается предоставление доступа всем сотрудникам организации для регистрации событий ОР с

		операционными рисками в модуле Archer Operational Risk Management				учетом ролевой модели доступа.
7.2. Возможность учёта потерь и возмещений по событиям ОР;	Не поддерживается	Не поддерживается специализированный функционал для управления операционными рисками по требованиям ЦБ РФ (716-П), но поддерживается общий процесс управления операционными рисками в модуле Archer Operational Risk Management	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается, с классификацией потерь и возмещений в соответствии с Положением Банка России от 8 апреля 2020 г. № 716-П
7.3. Возможность проведения качественной и количественной оценки уровня ОР;	Не поддерживается	Не поддерживается специализированный функционал для управления операционными рисками по требованиям ЦБ РФ (716-П), но поддерживается общий процесс управления операционными рисками в модуле Archer Operational Risk Management	Не поддерживается	Частично поддерживается с помощью функционала управления соответствием требованиям и проведением аудитов	Не поддерживается	Поддерживается, в соответствии с Положением Банка России от 8 апреля 2020 г. № 716-П
7.4. Возможность ролевой модели разграничения доступа для управления операционными рисками;	Не поддерживается	Поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается, наличие разграничения прав доступа на заведение, утверждение, расследование событий ОР.
7.5. Возможность импорта событий операционного риска из файлов;	Не поддерживается	Поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается (файловая загрузка, электронная почта, базы данных, получение данных из API внешних систем, импорт данных через API решения)
7.6. Возможность получения событий операционного риска по email;	Не поддерживается	Поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается
7.7. Возможность ведения и учёта ключевых индикаторов риска;	Не поддерживается	Не поддерживается специализированный функционал для управления операционными рисками по требованиям ЦБ РФ (716-П), но поддерживается общий процесс обработки ключевых индикаторов риска в модуле Archer Key Indicator Management	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается. Реализация жизненного цикла КИРа, регулярное обновление значений на основании данных от бизнес-подразделений, хранение и визуализация исторических данных по КИР, наличие сигнального и контрольного значений. Возможность создания мероприятий по управлению КИРом.
7.8. Возможность проведения самооценки уровня риска;	Не поддерживается	Поддерживается	Не поддерживается	Частично поддерживается с помощью функционала управления соответствием требованиям и проведением аудитов	Не поддерживается	Поддерживается, организация жизненного цикла процедуры самооценки, сбор данных и автоматизированный расчёт уровня риска, формирования плана мероприятий, согласование и утверждение результатов.
7.9. Поддержка формирования отчетности по операционным рискам (по формам ЦБ РФ, по внутренним формам).	Не поддерживается	Поддерживается, по внутренним формам	Не поддерживается	Частично поддерживается с помощью функционала создания отчетности, но отсутствует специализированный функционал	Не поддерживается	Поддерживается
Расширенные критерии	**АльфаДок**	**Archer Suite**	**ePlat4m SGRC (UDV ePlat4m SGRC)**	**R-Vision SGRC**	**SECURITM**	**Security Vision SGRC**
1. Общие технические характеристики:						
1.1. Возможность использования SGRC как услуги (SaaS-модель);	Поддерживается	Поддерживается	Поддерживается	Нет данных	Поддерживается	Поддерживается

1.2. Поддержка работы в сетях, изолированных от Интернет;	Нет данных	Нет данных	Поддерживается	Поддерживается	Поддерживается, но нужен периодический доступ к серверу лицензирования вендора для проверки лицензии. Возможна поставка автономного экземпляра на дополнительных условиях.	Поддерживается, функционирование решения не требует доступа к сети Интернет. Дополнительно возможна установка выделенного сервиса коннекторов в изолированном сегменте сети для доступа в сеть Интернет
1.3. Поддержка работы в режиме multitenancy.	Нет данных	Поддерживается	Поддерживается	Поддерживается, с разграничением прав доступа на основе ролевой модели	Поддерживается: решение мультитенантное и один пользователь может переключаться между различными тенантами (командами). Данные в тенантах изолированы, тенанты могут объединяться в древовидную структуру.	Поддерживается, с разграничением доступа пользователей к объектам и справочникам на основе организационной структуры (разграничение доступа к объектам дочерних и головных организаций)
2. Общие организационные характеристики:						
2.1. Наличие авторизованного обучения от вендора, стоимость обучения;	Обучение в учебном центре «Альфа-Образование»	Обучение в авторизованных центрах	Присутствует (по запросу)	Обучение по курсам администрирования и использования решения, выдается сертификат вендора	В стоимость on-premise версии входят регулярные персональные обучающие вебинары	Проводится обучение в собственном учебном центре вендора с выдачей сертификата
2.2. Дорожная карта развития продукта (планируемый к внедрению функционал и ориентировочные сроки реализации, планируемые изменения в лицензионную политику).	Нет данных	Нет данных	Присутствует (по запросу)	Нет данных	Планируется выпуск модуля управления инцидентами, операционных рисков, операционной надежности, расширение прямых интеграций.	Планируется разработка и обновление следующих коробочных экспертных модулей: 1. Планирование непрерывности бизнеса 2. Риски кибербезопасности 3.Проведение оценки соответствия различным стандартам ИБ
3. Управление информационной безопасностью:						
3.1. Управление активами:						
3.1.1. Поддержка установки и визуализации связей между различными типами активов (интерактивные графы для отображения и управления связями между объектами), выполнение действий с активами из интерактивного отображения;	Поддерживается формирование и отображение графической схемы взаимодействия информационных систем (формирование автоматически по заполненным данным, с возможностью ручной правки элементов схемы), с поддержкой экспорта изображения в формате SVG	Визуализация поддерживается (таблицы, списки, географические карты, графы связей), с функционалом «drilldown»	Не поддерживается	Поддержка отображения связей между активами в виде графа, с возможностью выполнения действий по просмотру из графа (отображение связей с другими активами)	Поддерживаются интерактивные графы связей между различными типами активов и псевдографы (пути достижимости)	Поддерживается отображение иерархической (древовидной) структуры и графов связей между активами, поддерживается выполнение следующих действий с активами: переход в карточку актива для просмотра детальной информации, отображение связанных активов (родительский и дочерних), создание опросного листа по активу
3.1.2. Возможность выполнения действий с активом из карточки актива, количество действий, возможность кастомизации или доработки новых действий с применением подхода low-code / no-code;	Не поддерживается	Не поддерживается	Ограниченно поддерживается выполнение некоторых ручных действий с активом из карточки актива	Поддерживается возможность действий по просмотру из графа	Из карточки актива можно изменять его карточку, запускать его актуализацию у владельца актива или другого работника, создавать задачи, связанные с активом и т.д. Для воздействия на исходный актив (хост) можно создавать RPA автоматизации запускающие скрипты.	Поддерживается более 60 действий с активом, такие как выполнение действий по получению инвентаризационной информации (данные о программном и аппаратном обеспечении, залогиненные пользователи, запущенные процессы и т.д.) и выполнению активных действий в случае обнаружения киберугрозы (завершение процесса, блокирование сетевых коммуникаций, перезагрузка и т.д.). Возможность создания отчёта по карточке объекта (например, паспорт Актива). Поддерживается кастомизация вида карточки и создание новых действий с применением подхода low-code / no-code
3.1.3. Возможность создания пользовательских отчетов с применением подхода low-code / no-code для карточек активов.	Не поддерживается	Не поддерживается	Поддерживается, кастомизация отчетов возможна с помощью изменения шаблона документа	Поддерживается	Поддерживается создание кастомных метрик / дашбордов и присоединение их к карточке актива. Поддерживается выгрузка типового паспорта актива с отчетом по изменениям актива в формате DOC.	Поддерживается формирование отчетов произвольной формы с отображением хранящейся в решении информации об активах в любом виде. Настройка отчетов производится с применением подхода low-code / no-code
3.2. Управление уязвимостями:						
3.2.1. Поддержка визуализации связей						

между различными активами, уязвимостями, бюллетенями и т.д. (интерактивные графы для отображения и управления связями между объектами);	Не поддерживается	Визуализация поддерживается (таблицы, списки, географические карты, графы связей), с функционалом «drilldown»	Не поддерживается	Поддерживается отображение уязвимостей на графике (история изменения уязвимостей), на диаграммах (отображение групп активов с уязвимостями), на географической карте, на графе связей активов	Поддерживаются интерактивные графы связей между различными типами активов	Поддерживается отображение иерархической (древовидной) структуры и графов связей между устройствами, уязвимостями, ПО, СЗИ
3.2.2. Интеграция с сервисами получения и обогащения данных об уязвимостях (например, exploit-db, vulners, БДУ ФСТЭК, NVD и т.д.);	Поддерживается интеграция с БДУ ФСТЭК России	Поддерживается интеграция с NIST NVD	Не поддерживается	Поддерживается только интеграция с vulners.com	Поддерживается интеграция с базой CPE	Поддерживаются следующие источники данных для обогащения информации об уязвимостях: БДУ ФСТЭК, NVD, vulners.com, VulDB, OpenCVE, AttackerKB, бюллетени Microsoft.
3.2.3. Поддержка бюллетеней НКЦКИ, ФинЦЕРТ.	Поддерживается получение информации от НКЦКИ (ГосСОПКА)	Не поддерживается	Поддерживается, обработка бюллетеней об угрозах и уязвимостях от НКЦКИ	Не поддерживается. Получение и обработка бюллетеней НКЦКИ об угрозах реализовано в решении R-Vision TIP	Поддерживается только ручной ввод бюллетеней в систему в модуль контроля соответствия	Поддерживается работа с бюллетенями НКЦКИ, ФинЦЕРТ с получением, обработкой, созданием уязвимостей и заявок на устранение в решении
4. Управление киберрисками:						
4.1. Наличие, функционал, кастомизация процесса управления киберрисками (выбор методологии, этапов оценки, обеспечение совместной работы заинтересованных лиц, контроль выполнения принятого решения по обработке киберриска);	Не поддерживается	Поддерживается	Частично поддерживается, с возможностью изменения встроенной методологии управления киберрисками	Поддерживается	Поддерживается	Поддерживается кастомизация процесса оценки рисков с применением подхода low-code / no-code. Возможно изменение внешнего вида, атрибутики, методики, этапности, ролевой модели и т.д., с обеспечением совместной работы, контроля созданных задачи на устранение.
4.2. Поддержка проведения финансовой оценки киберрисков (с учетом оценочной стоимости активов, проведения атаки, реализации контрмер).	Не поддерживается	Поддерживается	Частично поддерживается во встроенной частной методологии одного из заказчиков	Поддерживается с помощью задания финансовой ценности актива, финансовых параметров мероприятий по обработке риска	Не поддерживается	Поддерживается учет финансового эффекта реализации киберриска (ущерба) с учетом стоимости актива
5. Управление аудитами и соответствием требованиям:						
5.1. Возможность сбора технических параметров (посредством интеграции с ИТ и ИБ инфраструктурой) с целью автоматического определения степени соответствия;	Не поддерживается	Не поддерживается	Частично, с ручным выполнением действий по сравнению конфигураций, полученных от интегрированных систем, с эталонными значениями	Поддерживается с помощью механизма проведения аудитов, но без специализированного функционала автоматического определения степени соответствия	Поддерживается: параметры, собранные с ИТ/ИБ-инфраструктуры, сохраняются в карточки активов, далее формируется телеметрия, из которой по кастомным формулам рассчитываются метрики, использующиеся для оценки соответствия требованиям.	Поддерживается как с помощью инвентаризации активов встроенными средствами решения с определением конфигураций активов и оценкой степени соответствия конфигураций требованиям, так и с использованием механизма получения данных из внешних систем и реализации пользовательской методики определения выполнения каждого требования.
						Поддерживается на основе следующих стандартов: · Положение Банка России от 4 июня 2020 г. № 719-П · Положение Банка России от 20 апреля 2021 г. № 757-П · Положение Банка России от 25 июля 2022 г. № 802-П ·Положение Банка России от 17 апреля 2019 г. N 683-П

5.2. Наличие механизма и кастомизация автоматического расчета степени соответствия в зависимости от конкретного требования ИБ.	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается	Для каждого требования расчет соответствия может проводиться по разным методикам. Каждый набор требований может быть оценен по-разному для различных, в том числе пересекающихся областей (скоупов).	·Приказ ФСТЭК России от 21 декабря 2017 г. N 235 · CIS Critical Security Controls® Version 8 ·Приказ ФСТЭК России от 14 марта 2014 г. N 31 ·Приказ ФСТЭК России от 11 февраля 2013 г. N 17 ·Приказ ФСТЭК России от 18 февраля 2013 г. N 21 ·Приказ ФСТЭК России от 25 декабря 2017 г. N 239 · ГОСТ Р 57580.1-2017 · PCI DSS

Выводы

В классе SIEM-систем набор обязательных критериев и ожидаемого заказчиком функционала уже сформировался: клиентам требуется большое количество поддерживаемых протоколов и типов источников, наличие значительной базы правил корреляции "из коробки", возможность расширения функционала с помощью дополнительных приложений, регулярное обновление правил корреляции от экспертов вендора. Решение RuSIEM предлагает бесплатную версию своего продукта под названием RvSIEM (с функционалом, частично урезанным до Log Management), а также интересный модуль аналитики и обучения данных; с учетом того, что RuSIEM – это, скорее, нишевый игрок, данный функционал выглядит многообещающе. Продукт KUMA от Лаборатории Касперского гораздо известнее на рынке, и, благодаря бесшовной интеграции с множеством продуктов Kaspersky, он позволяет заказчикам выстроить логически связную, стройную ИБ-экосистему, при этом обеспечивая интеграцию с множеством других решений. Решение MaxPatrol SIEM также предоставляет и большой перечень поддерживаемых источников событий, и расширенные возможности по интеграции с линейкой продуктов от Positive Technologies, но дополнительно предлагает еще несколько "killer-фич": встроенная CMDB с контролем изменения свойств активов, функционал построения карты сети для оценки вероятности успешной атаки, фирменный SDK для создания и тестирования правил корреляции, функционал автоматического занесения ложноположительных событий в "белые списки", часто обновляемые пакеты экспертизы, фирменный маркетплейс и сообщество пользователей для обмена экспертизой, а также выявление аномалий и предсказание будущих инцидентов с помощью машинного обучения.

Среди рассмотренных SOAR-решений нам встретились продукты, в которых функционал управления инцидентами был надстроен над основными функциями продуктов вендора: так, Makves IRP реализует управление инцидентами, созданными исключительно в Windows-среде и в флагманском продукте Makves DCAP, а UserGate LogAnalyzer в составе экосистемы UserGate SUMMA лишь дополняет функционал NGFW (основного решения вендора) без полноценных возможностей по реагированию на инциденты. Продукты ePlat4m Orchestra и Innostage IRP интересны каждый по-своему: ePlat4m Orchestra, например, поддерживает создание сценариев реагирования в нотации Amazon States Language для повышения скорости создания плейбуков, но не допускает кастомизацию встроенных ролей, а Innostage IRP предоставляет возможность гибкой настройки ролевой модели и метрик реагирования, а также получения аналитики и рекомендаций от команды Innostage SOC CyberART, но обладает скромными возможностями по автоматизации обработки инцидентов (не поддерживается автоматическая приоритизация и триаж инцидентов) и рассылке оповещений (поддерживается только email). Решения R-Vision SOAR и Security Vision [NG]SOAR хорошо известны на рынке как два конкурента: оба обладают значительным функционалом и интеграцией со смежными продуктами тех же вендоров, оба предоставляют покупателям уже устоявшийся набор musthave-возможностей для данного класса: большое количество интеграций, тонкая настройка сценариев реагирования, визуализация инцидентов, отчетность. При этом R-Vision в определенной степени делает ставку на свою продуктовую экосистему R-Vision EVO (включает в себя продукты SOAR, SGRC, TIP, UEBA, SIEM, TDP и модуль управления активами и уязвимостями), а Security Vision [NG]SOAR выводит на рынок новую концепцию "NG-SOAR" с объектно-ориентированным подходом к реагированию, на основе технологии динамических плейбуков и экспертных рекомендаций. Концепция также подразумевает работу с инцидентами без привязки к SIEM-системе (которая сейчас чаще всего выступает основным источником инцидентов для SOAR), с использованием интегрированной в NG-SOAR логики выявления аномалий и инцидентов на основе событий, поступающих от различных СЗИ, и расширенным применением методов машинного обучения. Концепция "безSIEMного" SOAR и вообще отход от SIEM-систем как обязательных компонентов SOC-центров сейчас постепенно развивается на мировом рынке, и отрадно, что отечественные вендоры идут в авангарде этого тренда.

В классе TIP продукты разделились на облачные и on-prem: BI.ZONE ThreatVision и F.A.C.C.T. Threat Intelligence доступны исключительно "из облака", а у других вендоров платформа может разворачиваться локально в инфраструктуре (on-prem). У некоторых игроков (BI.ZONE, F.A.C.C.T., Kaspersky, PT) есть свои собственные TI-фиды, содержащие зачастую уникальные данные по угрозам, выявленным этими вендорами. Решение Kaspersky CyberTrace устанавливается on-prem, но функционирует в связке с облачным порталом Kaspersky Threat Intelligence Portal, который размещен в ЦОД вендора и является единственным предустановленным источником TI-данных для CyberTrace – в сравнении учтена такая взаимозависимость. Все решения (кроме продукта Kaspersky) поставляются с различными наборами подключенных по умолчанию источников TI-данных - как отечественных, так и зарубежных. Решение PT Cybersecurity Intelligence произвело впечатление непубличного продукта: нам не удалось найти расширенной информации о нем, а опрошенные эксплуатанты склонны считать этот продукт скорее дополнением к продуктам MP SIEM и PT NAD. Решения R-Vision TIP и Security Vision TIP опять идут в паре: оба вендора предлагают on-prem установку с поддержкой работы в изолированных от Интернет сетях (что является важным требованием для некоторых заказчиков), оба предлагают интеграцию с разнообразными сторонними TI-фидами, однако R-Vision TIP не поддерживает интеграцию с данными из БДУ ФСТЭК России (матрица техник и тактик нарушителей, база уязвимостей), не выявляет DGA-домены (популярная среди атакующих техника скрытия C&C-серверов) и не поддерживает проведение ретроспективного поиска IoC. Разработчики Security Vision делают ставку на выявление инцидентов и аномалий внутри Security Vision TIP, в том числе с использованием нейросетей и методов машинного обучения.

Среди рассмотренных SGRC-решений выделяются две "облачные" системы АльфаДок и SECURITM, которые предназначены скорее для помощи малому и среднему бизнесу: АльфаДок помогает автоматизировать соответствие законодательству в части "бумажной ИБ" и при необходимости позволяет установить платформу локально, а SECURITM предоставляет надежный фреймворк для выстраивания процессов управления ИБ, в том числе с предоставлением бесплатного доступа к веб-порталу SECURITM, а в платной версии поддерживает локальную (on-prem) инсталляцию. Платформа Security Vision SGRC предоставляет пользователям очень широкие возможности по кастомизации автоматизируемых процессов ИБ, от настройки типов и свойств активов до возможности автоматической установки заданной конфигурации ОС и ПО на конечные точки для соответствия корпоративным требованиям – по функционалу Security Vision SGRC ближе к "конструктору" зарубежного Archer Suite (прежнее название - RSA Archer) и поддержкой подхода "Low-code/No-code", и с дополнительными опциями по работе с инфраструктурой и с поддержкой базы российских нормативных требований. Решения ePlat4m SGRC и R-Vision SGRC уже давно известны на рынке, их отличает гибкость настройки с помощью графических редакторов и подхода "Low-code", а также интеграция с большим количеством инфраструктурных решений, но продукт R-Vision SGRC выглядит сильнее ePlat4m SGRC в части визуализации состояния ИБ, формирования отчетности и управления киберрисками (правда, без поддержки управления операционными рисками по требованиям ЦБ РФ).

В заключение отметим, что, сравнивая функционал российских решений для SOC-центров с импортными аналогами, у нас не сложилось ощущения какого-то отставания отечественных производителей – наоборот, они умело обходят уже известные подводные камни и архитектурно закладывают самые современные подходы, что позволяет разработчикам в дальнейшем не отвлекаться на поддержку "тяжелого наследия прошлого". С удовольствием отметили также, что всё больше наших производителей поддерживают мультиязычность (не только англ. язык) в интерфейсах своих продуктов, что поможет им выйти на иностранные дружественные рынки. Отечественные игроки достойно показали себя во всех рассматриваемых классах решений, и можно смело утверждать, что процесс импортозамещения, по крайней мере в отрасли кибербезопасности, идет успешно.

РЕДАКЦИЯ БЛАГОДАРИТ ЗА ПОМОЩЬ В ПОДГОТОВКЕ ОБЗОРА:

- **Тимофея Григорьева**, руководителя отдела технической поддержки продаж, UDV Group
- **Александра Позднякова**, менеджера продукта, UDV Group
- **Даниила Бородавкина**, менеджера продукта R-Vision SOAR, R-Vision
- **Валерию Чулкову**, менеджера продукта R-Vision TIP, R-Vision
- **Ксению Коляду**, менеджера продукта R-Vision SGRC, R-Vision
- **Илью Петрова**, руководителя направления продвижения собственных продуктов в области ИБ Департамента решений и развития бизнеса, Innostage
- **Альберта Насритдинова**, менеджера по продвижению собственных продуктов в области ИБ, Innostage
- **Николая Казанцева**, CEO SECURITM
- **Анну Олейникову**, директора по продуктам, Security Vision
- **Андрея Амираха**, руководителя отдела технического пресейла, Security Vision
- **Романа Овчинникова**, руководителя отдела исполнения, Security Vision
- **Сергея Сухорукова**, лидера продуктовой практики MaxPatrol SIEM, Positive Technologies
- **Ивана Прохорова,** руководителя продукта MaxPatrol SIEM, Positive Technologies
- **Максима Степченкова,** совладельца, RuSIEM
- **Даниила Вылегжанина**, руководителя отдела предпродажной подготовки, RuSIEM