ОБЗОР ПРОДУКТОВ ПО УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ

(Vulnerability Management)

Аналитическое сравнение российских продуктов по управлению уязвимостями

Введение

Эксплуатация уязвимостей продолжает оставаться одним из самых популярных и эффективных методов реализации кибератак. Причем зачастую эксплуатируются не 0-Day или 1-Day уязвимости, а даже те, которые были опубликованы несколько лет назад и для которых уже давно есть патчи. Управление уязвимостями - один из базовых процессов кибербезопасности, который, тем не менее, осложнен организационной неразберихой в различных реестрах уязвимостей и тем, что в крупных компаниях может быть большое число инсталляций различного софта, который нельзя пропатчить вне согласованных технологических окон. Особенно острый вызов в текущих российских реалиях - это отсутствие технической поддержки от ушедших зарубежных вендоров и невозможность легально обновить импортное ПО. Поверхность кибератак увеличивается и за счет устаревающего западного софта, и за счет импортозамещающих отечественных решений, которые пилотируются организациями и активно развиваются российскими вендорами, иногда не успевающими за создателями эксплойтов. Широкое использование Open Source с его сложными программными зависимостями также предъявляет всё больше требований к казалось бы простому и давно описанному процессу vulnerability management. Вывод прост - без использования средств автоматизации будет очень сложно управлять всем зоопарком различного импортного и отечественного софта, учитывать экземпляры, контролировать версии, ставить обновления. Ранее мы подготовили обзор рынка систем оценки уязвимостей https://securitymedia.org/info/obzor-rynka-sistem-upravleniya-uyazvimostyami.html , а сегодня вниманию читателей предлагается аналитическое сравнение российских систем управления уязвимостями.

Уход зарубежных решений для управления уязвимостями - Qualys, Nexpose, Nessus и других - не привел к появлению вакуума в данном сегменте ИБ. Производители известных сканеров и новые игроки VM-сегмента активно включились в процесс импортозамещения, поэтому сегодня мы можем наблюдать интересную конкурентную борьбу. Для данного сравнения мы выбрали следующие on-prem (локальные) решения для управления уязвимостями:

- MaxPatrol 8
- MaxPatrol VM
- R-Vision VM
- RedCheck
- ScanFactory VM
- ScanOVAL
- Security Vision VM
- Сканер-ВС 7

Методология оценки и сравнения функциональных возможностей продуктов включала в себя разработку перечня основных критериев, которые были сформированы авторами обзора 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.

Для всех продуктов оценивались последние актуальные на момент анализа версии. Для "Сканер-ВС" производителем была продемонстрирована версия 7, которая еще не была официально представлена. Решение ScanFactory было добавлено в сравнение позже, поскольку в конце октября была представлена версия продукта для локальной установки, а ранее он предлагался только в виде облачного сервиса для управления поверхностью атак.

В настоящем обзоре используются следующие термины и определения:

- Решение – система для управления активами, уязвимостями, соответствием.
- Модули решения – модуль управления активами, модуль управления уязвимостями, модуль управления соответствием.
- Low-code – метод разработки программного обеспечения, при котором разработка упрощается за счет использования графического конструктора, при этом частичное написание кода требуется.
- No-code – метод разработки программного обеспечения, при котором разработка выполняется за счет использования графического конструктора, написание кода не требуется.

Основные критерии

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
1. Общие технические характеристики								
1.1. Технические требования к платформе и среде внедрения решения (системные требования к аппаратному и программному обеспечению, окружению);	Установка со встроенной БД: MaxPatrol Server: 4 ЦПУ, 10 Гб ОЗУ, 300 Гб дискового пространства; MaxPatrol Scanner: 4 ЦПУ, 8 Гб ОЗУ, 50 Гб дискового пространства. Установка с внешней СУБД на одном сервере: MaxPatrol Server: 4 ЦПУ, 16 Гб ОЗУ, от 90 Гб дискового пространства (зависит от количества сканируемых узлов и частоты сканирования в месяц); MaxPatrol Consolidator: 4 ЦПУ, 16 Гб ОЗУ, от 120 Гб дискового пространства (зависит от количества сканируемых узлов и частоты сканирования в месяц); MaxPatrol Scanner: 4 ЦПУ, 8 Гб ОЗУ, 50 Гб дискового пространства. Установка с внешней СУБД на отдельном сервере: MaxPatrol Server: 4 ЦПУ, 10 Гб ОЗУ, 200 Гб дискового пространства; MaxPatrol Consolidator: 4 ЦПУ, 16 Гб ОЗУ, 200 Гб дискового пространства; Сервер СУБД: 4 ЦПУ, 12 Гб ОЗУ, от 90 Гб дискового пространства (зависит от количества сканируемых узлов и частоты сканирования в месяц); MaxPatrol Scanner: 4 ЦПУ, 8 Гб ОЗУ, 50 Гб дискового пространства; MaxPatrol Local Update Server (LUS): 4 ЦПУ, 4 Гб ОЗУ, 50 Гб дискового пространства. Центр управления (MaxPatrol Console) устанавливается в виде "толстого клиента": 1 ЦПУ, 512 Мб ОЗУ, 150 Мб дискового пространства, разрешение экрана 1280 * 1024, ОС Microsoft Windows XP SP3, Microsoft Windows Server 2003 SP2 и выше. Поддерживается установка на ОС Microsoft Windows 8 / 10 / 11, Microsoft Windows Server 2012 / 2016 / 2019 / 2022; Встроенная СУБД: Microsoft SQL Server 2017 Express; Поддерживаются внешние СУБД: PostgreSQL 13.3-15.1, Postgres Pro Standard 14.4.1, Microsoft SQL Server 2005 SP4 / 2008 SP3 / 2008 R2 SP1 / 2012 / 2014 / 2016 / 2017 / 2019	Установка All-in-one - MP 10 Core, PT MC (Management and Configuration), MP 10 Collector, PT UCS (Update and Configuration Service) на одном сервере: 32 ЦПУ, 64 Гб ОЗУ, 4 дисковых накопителя по 1200 Гб и скоростью вращения 10000 об./мин. каждый (для Linux рекомендуется объединить диски в массив RAID 10), 2 сетевых адаптера со скоростью 1 Гбит/с каждый. Установка выделенного MP 10 Collector: От 4 ЦПУ, 4 Гб ОЗУ, 300 Гб дискового пространства, сетевой адаптер со скоростью не менее 1 Гбит/с. Установка выделенного PT UCS: 4 ЦПУ, 4 Гб ОЗУ, 300 Гб дискового пространства, сетевой адаптер со скоростью не менее 1 Гбит/с. Доступ к решению осуществляется через веб-интерфейс. Поддерживается установка на 64-разрядные ОС семейства Linux: Astra Linux Special Edition 1.7.5 (на базе ядра Linux версии 5.15), Debian 10.3-10.13, 11, 12 (на базе ядра Linux версии 5.10 и выше). Поддерживается установка MP 10 Collector на ОС Microsoft Windows Server 2012 / 2012 R2 / 2016 / 2019 / 2022	Для установки All-in-one (БД и коллектор на одном сервере): Минимальные требования: от 4 ЦПУ, 16 Гб ОЗУ, от 32 Гб дискового пространства. Для работы с 20000 активами: 16 ЦПУ, 20 Гб ОЗУ, от 250 Гб дискового пространства	От 4 ЦПУ, от 12 ГБ ОЗУ, от 100 ГБ дисковой подсистемы. ОС: AstraLinux, РедОС, SberLinux, Debian, Microsoft Windows	Поддерживается установка на российские ОС на базе Linux	Поддерживается только локальная установка на сканируемом устройстве. Требования для установки на ОС Windows: 1 ЦПУ, 1 Гб ОЗУ (для 32-разрядной системы) или 2 Гб ОЗУ (для 64-разрядной системы), 500 Мб дисковой подсистемы. Поддерживается установка на Microsoft Windows 7/8/8.1/10, Microsoft Windows Server 2008/2008R2/ 2012/2012 R2/ 2016. Требования для установки на ОС Linux: 1 ЦПУ, 500 Мб ОЗУ, 500 Мб дисковой подсистемы. Поддерживается установка на Astra Linux 1.7 SE, Astra Linux 1.6 SE, Альт Рабочая станция 9, Альт Сервер 9, Роса "Кобальт"	ОС: CentOS Stream 8 и выше, RHEL 8 и выше, Ubuntu 20.04/22.04/24.04, AlmaLinux 9, Debian 10/11/12, Oracle Linux 8/9, Astra Linux CE (Common Edition), Astra Linux SE (Special Edition), Альт Сервер 10 и выше, Альт 8 СП и выше, Oracle Linux 8 и выше, AlterOS 7.5 и выше, РЕД ОС 7/8 и выше, РОСА "ХРОМ", "КОБАЛЬТ", Microsoft Windows Server 2016 R2 и выше. СУБД: Microsoft SQL Server версии 2016 или выше, PostgreSQL версии 11 или выше, Postgres Pro версии 11 или выше, Jatoba. Аппаратные требования: От 8 ЦПУ, 12 Гб ОЗУ, 100 Гб дисковой подсистемы	ЦПУ не хуже Intel Core i7, ОЗУ от 16 Гб, дисковая подсистема 1 Тб. ОС Astra Linux Special Edition 1.7, ОС Windows
1.2. Технические требования к платформе и среде внедрения агента решения, влияние агента на производительность конечных точек (если применимо);	Безагентское сканирование. При удаленном сканировании Windows-узла рекомендуется, чтобы ЦПУ узла был загружен не более чем на 70%, свободной ОЗУ было не менее 256 Мб, свободного места на системном диске было не менее 50 Мб	Безагентское сканирование.	ОС: CentOS, RHEL, Debian, Astra SE, Astra CE, RED OS, ALT Server, ALT 8, SP Server. СУБД: PostgreSQL 14, Jatoba J4. Агентское сканирование не поддерживается по умолчанию. Агентское сканирование возможно при использовании продукта R-Vision Endpoint	Microsoft Windows, 1 ЦПУ, 2 ГБ ОЗУ, 500 МБ дисковой подсистемы. Агент постоянного влияния на производительность не оказывает	Безагентское сканирование	Поддерживается только локальная установка на сканируемом устройстве	Поддержка агентского и/или безагентского режима работы. Влияние агента на производительность конечных точек: Характеристика тестового АРМ: • ЦПУ 8 ядер, 3.4 GHz • ОЗУ 8 Гб Влияние процедуры сканирования хоста, при помощи механизмов Security Vision: В неактивном режиме утилизация ЦПУ менее 1%, ОЗУ менее 200 МБ	Безагентское сканирование.
1.3. Варианты поставки и инсталляции (аппаратный аплайнс, образ, контейнер, установка на "голое железо", установка on-prem, установка в облаке, наличие графических инсталляторов, поддержка виртуализации);	Графический инсталлятор. Установка на "голое железо" и в среде виртуализации. Поддержка виртуализации VMware ESXi 4.1 и выше, VMware Workstation 6.0 и выше, Hyper-V, KVM (с ядром Linux 2.6.18 и выше) с поддержкой подключения USB-ключей eToken, Rutoken	Поддержка виртуализации VMware vSphere версии 11 и выше, VMware ESXi версии 6.0 и выше	Поддерживаемые варианты установки: on-prem, виртуализация, контейнер. Поддержка виртуализации VMware, MS Hyper-V, Xen, Parallels, VirtualBox	On-prem лицензия с инсталлятором, возможно установить в облако или получить сервис сканирования от Партнеров	Установка в облаке (SaaS-режим), локальная установка (on-prem), контейнеры	Графический инсталлятор. Только локальная установка на сканируемом устройстве	Поддержка установки в виде контейнера, на голое железо, из ISO образа, из 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	Инсталлятор командной строки для ОС Astra Linux, графический инсталлятор для ОС Windows, установка на USB-носитель с предустановленной ОС Astra Linux и Сканер-ВС

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
1.4. Архитектурные особенности решения (стек технологий, возможность прямого доступа к внутренним структурам, возможность доступа покупателя к ОС/СУБД решения с правами администратора);	Трехуровневая архитектура, поддерживается установка All-in-one. Основные компоненты: MaxPatrol Server – модуль управления; MaxPatrol Scanner – сканер (в составе MP Server или на отдельной ноде) MaxPatrol Consolidation Server – сервер консолидации информации от всех серверов MP Server MaxPatrol Local Update Server (LUS) – локальный сервер обновлений MaxPatrol Console – консоль управления системой MaxPatrol 8. Возможен прямой доступ к СУБД с административными привилегиями	Поддерживается установка All-in-one всех компонент решения: MP 10 Core, PT MC, MP 10 Collector. Компонент PT UCS может быть установлен вместе с MP 10 Core или на выделенный сервер. В решении используются Docker-контейнеры, СУБД PostgreSQL, брокер сообщений RabbitMQ, SaltStack для управления конфигурацией решения. Данные текущего сканирования могут храниться во временной базе SQLite или в памяти узла MP 10 Collector. Особенности: если MP 10 Collector установлен на Linux, то MaxPatrol VM не сможет выполнять сценарии на удаленных узлах с помощью профилей PowershellExecutor и RemoteExecutor, не сможет собирать события с профилем CheckpointOpsecLog, использовать протокол Kerberos, выполнять поиск файлов в режиме пентеста. Производительность MP 10 Collector, установленного на Linux, в режиме пентеста в целом на 15-40% ниже, чем установленного на Microsoft Windows	Распределенная архитектура: сервер управления (управление системой, инвентаризация, хранение информации), коллекторы (сканеры). Используются СУБД PostgreSQL 14, Jatoba J4	Российское ПО, на основе открытого стандарта SCAP, OVAL, XCCDF с расширенными возможностями решения прикладных задач	Используются контейнеры под управлением Kubernetes, в решении объединены 21 сканер, включая несколько коммерческих сканеров и Open Source инструменты Nuclei, Nmap, Brute, Sdto, Dirsearch, Chrome crawler, Crawlergo, Fuzzuli, Grep, Waybackurls, Wpscan, x8, а также OSINT-утилиты amass, subfinder, goaltdns	На Windows используется Microsoft .NET Framework версии 4.8 или выше, интерпретатор языка OVAL 5.10.1 или выше (поставляется совместно с дистрибутивом ScanOVAL). Предварительно импортируются XML-файлы с OVAL-описаниями уязвимостей, выполненными в соответствии со стандартом "The OVAL Language Specification" версии не ниже 5.10.1. На Linux для обеспечения работы программы ScanOVAL необходимо ПО (для Astra Linux 1.7 SE): графический интерфейс пользователя Fly 2.0, Xorg версии 7.7, qt 5.11, libcurl3 (поставляется совместно с дистрибутивом программы ScanOVAL для Linux), openscap-scanner, openscap-common, openssl	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	Используемый язык разработки Go, СУБД sqlite. Поддерживается возможность прямого доступа к базе данных. Используется монолитная архитектура (один сервис), используется встроенный сервер аутентификации
1.5. Параметры масштабируемости, кластеризации, производительности;	Масштабирование достигается за счет распределения компонент СУБД, установки отдельных нод MaxPatrol Scanner, выноса MaxPatrol Server и MaxPatrol Consolidation Server на отдельные ноды	Масштабирование достигается за счет установки дополнительных компонент MP 10 Collector	Поддерживается установка дополнительных компонент (коллекторов) в распределенной инфраструктуре	Горизонтальное масштабирование и подключение сканеров	Масштабирование достигается за счет быстрого развертывания контейнеров	Поддерживается только локальная установка на сканируемом устройстве	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	Скорость сканирования: сетевое сканирование 50 узлов (Astra Linux, Windows), все TCP порты 1-65535, с определением версий сервисов, с настройкой 1000 пакетов в секунду – до 12 минут. Поиск уязвимостей на 50 узлах, до 1 минуты. Можно использовать LiteFS, что позволяет реплицировать данные SQLite на несколько узлов
1.6. Поддержка отказоустойчивости (реализация, требования вендора к инфраструктуре покупателя);	Реализуется за счет функционала ОС и СУБД	Реализуется за счет функционала ОС и СУБД	Реализуется за счет функционала ОС и СУБД	На уровне хранения данных - СУБД	Не поддерживается	Поддерживается только локальная установка на сканируемом устройстве	Поддерживается создание кластера высокой доступности, дублирование и резервирование всех элементов решения, возможность создания геокластера, поддержка отказоустойчивости для провайдеров MSS	Реализуется за счет функционала СУБД
1.7. Поддержка распределенной установки компонентов, включая возможность размещения СУБД на отдельной ноде;	Поддерживается размещение СУБД на отдельном сервере	Поддерживается установка выделенных нод MP 10 Collector, PT UCS	Поддерживается установка БД на отдельном сервере, установка коллекторов на отдельных серверах	Поддерживается, все службы могут размещаться отдельно	Не поддерживается	Поддерживается только локальная установка на сканируемом устройстве	Поддерживается возможность установки неограниченного количества нод каждого компонента	Не поддерживается
1.8. Возможность обнаружения, инвентаризации, сканирования, оценки соответствия активов в различных сетевых сегментах, включая частично изолированные, через отдельные ноды решения;	Поддерживается за счет установки отдельного выносного компонента MaxPatrol Scanner в сканируемую подсеть, за счет использования MaxPatrol Offline Scanner (запускается с флеш-носителя Guardant к сканируемому ПК, не требует установки), за счет использования MaxPatrol Mobile Server (устанавливается на ноутбуках, применяется для проверки территориально удаленных сетей и подразделений или физически изолированных сегментов)	Поддерживается за счет установки отдельной выносной ноды MP 10 Collector	Поддержка выполнения обнаружения, инвентаризации, сканирования активов в выделенных сетевых сегментах за счет установки отдельных коллекторов. Для взаимодействия коллекторов и сервера управления назначается один выделенный сетевой порт. Сканирование в изолированных сетях поддерживается только за счет разворачивания отдельной выделенной инсталляции решения	Поддерживается	Поддерживается работа в различных сетевых сегментах	Поддерживается только локальная установка на сканируемом устройстве	Поддерживается возможность установки компонентов решения (сервисов) на выделенные серверы в удаленных и изолированных сетях, с дальнейшим импортом результатов сканирования на основной сервер	Поддерживается за счет разворачивания дополнительной инсталляции либо использования Live-USB

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
1.9. Обеспечение безопасной работы решения (ограничение доступа, ролевая модель, ограничение используемых сетевых портов, защита канала связи, защита обрабатываемых данных, журналирование, способы аутентификации пользователей, контроль действий пользователей решения, шифрование критичных данных, контроль целостности исполняемых и вспомогательных файлов, возможность создания резервных копий, корректная обработка ошибок настройки решения);	Шифрование учетных записей для сканирования: 3DES с ключом SHA-1 (хранится в БД решения). Шифрование БД: AES-128 в режиме CCM. Ключ шифрования БД находится в защищенном хранилище в ОС. Взаимодействие между MaxPatrol Server и MaxPatrol Scanner осуществляется по порту 2002/TCP. Для защиты взаимодействия между компонентами решения используется протокол TLS (версии 1.0 – 1.2), поддерживаются самоподписанные или пользовательские сертификаты. Разграничение доступа реализуется за счет включения пользователя в определенную внутреннюю группу для разграничения доступа к объектам: задачи, учетный записи, справочник, профили, расписания, отчеты, стандарты. Возможно применение дополнительных ограничений (запрет на доступ к определенным сканерам, запрет создания задач на сканирование определенных узлов). Журналирование (типы журналов: инсталлятор, сканер, консоль, системные события), поддержка расширенного журналирования, журналирование работы определенных модулей решения (с помощью создания справочников). Поддержка хранения паролей в CyberArk Enterprise Password Vault, Total Privileged Account Management. Ограничение доступа учетной записи по типам протоколов (транспортов) для сканирования	Централизованное управление ролями пользователей решения и единый вход через PT MC. Присутствуют встроенные стандартные роли (администратор, оператор, пользователь), поддерживается создание пользовательских ролей, которые содержат наборы привилегий, определяющих доступные для пользователя разделы интерфейса, операции в системе, доступ к определенным активам, уязвимостям, задачам. Поддерживается синхронизация учетных записей пользователей с Microsoft Active Directory. Для защиты доступа по веб-интерфейсу поддерживаются самоподписанные и пользовательские сертификаты. Для защиты информации, передаваемой между RMQ Message Bus, MP 10 Core, MP 10 Collector, используется шифрование с поддержкой установки пользовательских сертификатов. Поддерживается журналирование работы компонента MP 10 Core на Linux, журналирование работы компонента MP 10 Collector на Microsoft Windows. Резервное копирование и восстановление производится с использованием встроенных bash-скриптов. Поддерживается автоматический мониторинг параметров жизнеспособности и целостности компонентов решения, отправка уведомлений по электронной почте (с поддержкой шифрования при подключении к SMTP-серверу)	Шифрование трафика между компонентами решения с помощью SSL. Ролевая модель доступа, дискреционный доступ, аутентификация пользователей (локальная, SSO). Поддерживается логирование изменений, вносимых пользователями. Применяется шифрование учетных данных, сохраненных в системе	Поддерживается	Не поддерживается	Цифровая подпись файла-инсталлятора (.msi), исполняемого файла (.exe), библиотек (.dll), импортируемых XML-файлов с OVAL-описаниями уязвимостей. Ведется журнал работы ПО с записью ошибок	Поддерживается ограничение доступа на основе IP-адресов, двухфакторная аутентификация, аутентификация по сертификатам для пользователей и компонентов решения (самоподписанные сертификаты, сертификатов от внутреннего центра сертификации), наличие SSO. Используется SSL/TLS для защиты доступа к веб-интерфейсу, поддерживается аудит попыток входа в систему, аудит действий пользователей и администраторов (включая факт просмотра карточек). Поддерживается ролевая модель управления доступом ко всем элементам решения. Поддерживается шифрование базы данных и отдельных критичных элементов (например, паролей для учетных записей). Система выполняет проверку целостности ПО и конфигурационных файлов во время функционирования и по команде пользователя. Система выполняет мониторинг состояния всех своих компонентов (сервисов) и выполняет оповещения пользователя при выявлении отклонений. Резервное копирование реализуется средствами ОС и СУБД. Ошибки решения доступны для просмотра в консоли решения с различным уровнем детализации	Поддерживаются следующие настройки безопасности: 1) Ограничение доступа: настройки CORS в HTTP сервере позволяют контролировать, с каких источников можно обращаться к серверу. Это ограничивает доступ к API только с доверенных доменов. 2) Ролевая модель: в разделе services определены роли (admin, user) и правила доступа для каждой роли. Это позволяет ограничивать доступ пользователей к различным частям системы в зависимости от их роли. 3) Ограничение используемых сетевых портов (HTTP и HTTPS): в конфигурации можно указать конкретные порты для HTTP сервера (например, 3300, 443). 4) Защита канала связи: включение TLS обеспечивает шифрование данных при передаче, защищая их от перехвата. Настройки включают использование сертификатов и указание минимальной версии TLS (1.3) 5) Журналирование (логирование): конфигурация логирования позволяет вести журналирование событий в файл с ротацией и консоль. 6) Способы аутентификации пользователей: интеграция с LDAP, внутренний pauth-сервер и возможность указать путь к конфигурации Kerberos; 7) Резервное копирование баз данных: есть возможность указать путь для резервной копии базы данных уязвимостей (backup-path), что важно для восстановления данных в случае сбоя. 8) Корректная обработка ошибок и настройки решения: настройки для повторных попыток подключения и выполнения команд могут помочь в обработке ошибок и повышении надежности
1.10. Локализация интерфейса, поддержка мультиязычности, возможность кастомизации интерфейса, возможность сквозного поиска по всем обрабатываемым данным.	Язык интерфейса: русский, английский, корейский	Русский и английский языки интерфейса	Поддерживается русская и английская локализации, настройка карточки интерфейса, поддержка тем (темная и светлая), кастомизация вкладок и дашбордов, сквозной поиск по объектам	Интерфейс на русском языке. Возможность поиска и фильтрации	Язык интерфейса: русский, английский. Поддерживаются темная и светлая темы	Язык интерфейса: русский	Поддерживается мультиязычность, локализация интерфейса и всех элементов на русском и английском с возможностью добавления других языков. Поддерживаются темы (темная и светлая), кастомизация интерфейса (брендирование, логотип). Поддерживается сквозной поиск	Язык интерфейса: русский, английский
2. Общие организационные характеристики								
2.1. Дата первого релиза, текущая версия;	Первый релиз – 2008 год, текущая версия 25.7	Первый релиз – 2021 год, текущая версия 2.7	Текущая версия 5.4	Государственная регистрация 12 декабря 2013 года Актуальные версии: RedCheck Windows 2.6.9 RedCheck NIX 2.7.0	2022 год	Первый релиз – 2018 год, текущая версия 1.5.0	Первый релиз - 2015, текущая версия – 5	Текущая версия 7, дата релиза – октябрь 2024 года
2.2. Наличие документации, наличие API;	Онлайн-документация на сайте, API не поддерживается	Онлайн-документация на сайте, поддерживается REST API через HTTPS	Документация поставляется с системой, API документирован	Документация присутствует, API поддерживается	Онлайн-документация на сайте, API поддерживается	Документация на сайте (pdf), API не поддерживается	Документация в виде интерактивной справки в решении, в виде PDF-файлов, поддержка API. Предоставляется документация на API	Поддержка API, документация через swagger

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
2.3. Наличие технической поддержки, режим работы, SLA-нормативы;	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 техподдержки уровня premium	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 техподдержки уровня premium	Выполнение работ осуществляется по заявкам, поступившим от Клиента по телефону и E-mail. Стандартная техническая поддержка (обработка обращений) предоставляется в будние дни в рабочее время с 9:00 до 18:00. Срок ответа на заявку Клиента составляет 24 часа с момента получения заявки. Расширенная поддержка включает реагирование на аварии в режиме 24/7. Поддержка "ПремиумПлюс" включает доработку и кастомизацию функционала по требованиям клиентов	Техническая поддержка предоставляется в рабочее время	Обращение в техническую поддержку через сайт, телефон, email	Не предоставляется	Техническая поддержка трёх уровней. Премиальная - 24/7. Показатели SLA для тарифа "Премиальный": время реакции: 4 часа, время предоставления решения: 24 часа. Поддерживается возможность согласования и подписания сжатых SLA-нормативов и условий предоставления услуг, индивидуальное ведение	Техническая поддержка 8/5
2.4. Наличие гарантии, срок предоставления гарантийного обслуживания, что включено в стандартное гарантийное обслуживание, возможность расширенной гарантии;	Предоставляются обновления описаний уязвимостей и стандарты, сервисное обслуживание, консультационные услуги, услуги экспертного центра кибербезопасности PT Expert Security Center (PT ESC)	Предоставляются обновления описаний уязвимостей и стандарты, сервисное обслуживание, консультационные услуги, услуги экспертного центра кибербезопасности PT Expert Security Center (PT ESC)	Предоставляется в соответствии с условиями гарантийного обслуживания на основании договора или сертификата на клиентскую (гарантийную) поддержку	Техническая поддержка включена в лицензию и действует согласно сроку действия лицензии. Возможна техническая поддержка с совместной работой по удаленной сессии	Предоставляется по запросу	ПО предоставляется "как есть" без каких-либо гарантий	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 сбору информации для определения неисправностей в работе программных продуктов, применению решений по устранению неисправностей и восстановлению работы программных продуктов	Гарантии в рамках оказания технической поддержки и поддержания сертификации
2.5. Лицензионная политика: стоимость дополнительных интеграций (ИТ/ИБ-системы, СЗИ, внешние сервисы и т.д.), лицензирование API, правила расчета лицензии (по пользователям, объектам / IP-адресам сканирования, интеграциям, числу параллельных сканирований, количеству нод решения и т.д.), отличие в стоимости при разных вариантах инсталляции, специальные условия для MSS-провайдеров;	Лицензируется по максимальному количеству сканируемых узлов, по модулям/сборкам (pentest, audit, compliance), по дополнительным ядрам сканирования	Лицензируется по максимальному количеству сканируемых узлов, по нодам MP 10 Collector	Предоставляется по запросу	Интеграции на стороне других решений (обычно включены в коробку), API входит во все редакции, кроме Base, лицензирование по хостам (есть безлимитная лицензия), индивидуальные условия для ИБ-провайдеров	Стоимость лицензии зависит от количества хостов, необходимости ручной верификации, предоставления отчетов на русском языке	В соответствии с лицензионным соглашением с конечным пользователем ПО на сайте bdu.fstec.ru/scanoval	Предусмотрены временные и бессрочные лицензии. Метрики лицензирования: 1) Количество конкурентных лицензий коннекторов для подключения к внешним системам; 2) Режим функционирования (количество дополнительных нод) – отказоустойчивость, режим мультинод; 3) Количество сканируемых IP-адресов (узлов); 4) Мультиарендность для MSSP провайдеров, холдингов, групп компаний. Других ограничительных метрик не предусмотрено. Количество активов, пользователей, сценариев, отчетов и дашбордов – все входит в неограниченном количестве. API и конструкторы не лицензируются дополнительно, включены в любую поставку решения	Лицензируется по количеству активов в базе данных, привязки к конкретным IP-адресам нет, старые активы могут быть перезаписаны на новые
2.6. Опыт внедрений;	Опыт внедрений во многих отраслях	Опыт внедрений во многих отраслях	Опыт внедрений во многих отраслях	Через партнерскую сеть	Нет данных	Нет данных	Опыт внедрения во многих отраслях экономики. Среди Заказчиков – Сбербанк России, Альфа-Банк, Тинькофф Банк, РосБанк, Норильский Никель, Северсталь, Уралхим, Евраз, ТГК-1, X5 Group, Магнит, ФСО России, Совет Федерации, ДомРФ, Мегафон MSSP, Центр киберустойчивости Angara SOC, РТ-Информационная безопасность (РОСТЕХ), МТС, Вымпелком Первый Канал и другие	Количество пользователей Сканер-ВС (версии 5, 6) – более 6000. Сканер-ВС (версии 7) – в процессе получения сертификата

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
2.7. Наличие сертификатов регуляторов, присутствие в реестре российского ПО.	Срок действия сертификата ФСТЭК России на MaxPatrol 8 закончился 08.07.2024, информации о повторной сертификации не имеется, решение работает только на ОС Windows, информации о планах по переводу MaxPatrol 8 на Linux не имеется. Оказание техподдержки допустимо по купленному продукту до 2029 года, кроме объектов КИИ. Новые продажи по старому сертификату под ОС Windows недопустимы. В соответствии с п.1 б) Указа Президента РФ №166 «О мерах по обеспечению технологической независимости и безопасности КИИ РФ» с 01.01.2025 на значимых объектах КИИ запрещено использование иностранного ПО (в том числе ОС Windows)	Сертификат соответствия ФСТЭК России № 3734 от 15.11.2023 (УД4). Присутствует в реестре российского ПО	Сертификат ФСТЭК России № 4782 (4 УД). Присутствует в реестре российского ПО	Сертификат ФСТЭК России №3172 (4УД). Присутствует в реестре российского ПО	Отсутствует Сертификат ФСТЭК и др. Присутствует в реестре российского ПО	Присутствует в реестре российского ПО	Заключение 8 Центра ФСБ России 149/3/6/908 от 01.10.2024; 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). Присутствует в реестре российского ПО	Нет
3. Общий функционал всех решений (управление активами, управление уязвимостями, оценка соответствия)								
3.1. Настройка правил и логики управления объектами решения (активами, уязвимостями, задачами, требованиями, документами, инцидентами);	Только в рамках преднастроенной неизменяемой логики решения (профили сканирования, задачи сканирования, настройка требований стандартов, настройка групп)	Поддерживается с помощью создания политик, состоящих из совокупности правил, автоматически изменяющих параметры объектов решения. Создание правил выполняется с помощью фильтров - запросов на языке PDQL	Поддерживается настройка профилей сканирования, настройка политик управления уязвимостями, настройка задач и расписания сканирования	Поддерживаются статичные хосты (цели сканирования) и группы (допускается пересечение хостов по группам), Задача сканирования включает хосты или группы, тип сканирования, расписание	Только в рамках логики используемых внутри решения сканеров	Не поддерживается	Поддерживается настройка правил и логики управления всеми объектами решения (включая произвольные пользовательские типы объектов) через графический low-code / no-code конструктор рабочих процессов	Для активов поддерживается возможность создания, редактирования и классификации активов; настройка автоматического обнаружения посредством сетевого сканирования и обогащения информации об активах. Для уязвимостей поддерживается настройка параметров обнаружения, возможность создания пользовательских уязвимостей
3.2. Разграничение доступа к объектам решения;	Поддерживается разграничение доступа за счет включения пользователя в определенную внутреннюю группу для разграничения доступа к объектам: задачи, учетный записи, справочник, профили, расписания, отчеты, стандарты	Поддерживается разграничение доступа к определенным активам, уязвимостям, задачам на сбор данных	Поддерживается ролевая модель доступа	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается гибкая ролевая модель доступа, ограничивающая доступ к объектам по любым условиям, с детализацией до доступа к свойствам объектов (например, отдельных полей в карточке)	Не поддерживается, пользователь имеет доступ ко всем активам в системе
3.3. Настройка прав доступа к инвентаризируемым, сканируемым и оцениваемым активам;	Для режимов сканирования Audit и PenTest настраиваются отдельные учетные записи	Поддерживается указание списка разрешенных и запрещенных команд для сканирования систем через терминал (протоколы SSH, Telnet). Учетная запись должна обладать правами на выполнение команд для сбора данных на различных типах активов. Поддержка аутентификации по логину, паролю, сертификату. Поддержка LAPS (только версия 6.2.), механизма sudo wrappers	Поддерживается настройка прав доступа к инвентаризируемым и сканируемым активам	Не поддерживается	Только в рамках функционала используемых внутри решения сканеров. Своего разграничения нет	Требуются права локального администратора (на Windows), учетная запись root или другая учетная запись с привилегиями суперпользователя (на Linux)	Поддерживается, используется принцип минимальных привилегий, отсутствие требований полных административных прав. Наличие описания необходимых прав доступа в документации	Используются учетные записи с правами администратора
3.4. Возможность задания отдельных УЗ для обнаружения, инвентаризации, сканирования, оценки соответствия;	Поддерживается через настройку профилей сканирования	Поддерживается задание отдельных УЗ для различных типов сканируемых узлов	Для режимов сканирования пентест и аудит настраиваются отдельные учетные записи для различных типов систем и протоколов	Поддерживается через менеджер учетных записей, УЗ назначаются в конкретной задаче сканирования	Только в рамках функционала используемых внутри решения сканеров. Своего разграничения нет	Не поддерживается	Поддерживается, возможно указать разные УЗ для различных задач. Поддерживается через настройку рабочих процессов в графическом low-code / no-code конструкторе	Все учетные записи (УЗ) создаются через подключение к активу. Каждое подключение привязано к секрету. Система поддерживает возможность временного отключения учетных записей для выполнения конкретных задач, таких как обнаружение, инвентаризация, сканирование и оценка соответствия на других УЗ.
3.5. Возможность задания отдельных УЗ для отдельных объектов обнаружения, инвентаризации, сканирования, оценки соответствия;	Поддерживается через настройку профилей сканирования и списка узлов в задачах сканирования	Поддерживается за счет создания пользовательских профилей сбора данных и сканирования	Поддерживается через настройку УЗ для задач сканирования для определенных сетевых диапазонов, отдельных IP-адресов (устройств)	Поддерживается через менеджер учетных записей, УЗ назначаются в конкретной задаче сканирования	Только в рамках функционала используемых внутри решения сканеров	Не поддерживается	Поддерживается через настройку рабочих процессов в графическом low-code / no-code конструкторе	Поддерживается настройка отдельных УЗ для отдельных активов

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
3.6. Возможность оффлайн-действий (обнаружение, инвентаризация, сканирование, оценка соответствия) в изолированных сегментах, например, с помощью отчуждаемого файла-скрипта, результаты которого можно импортировать в решение;	Поддерживается за счет использования MaxPatrol Offline Scanner (запускается с флеш-носителя Guardant к сканируемому ПК, не требует установки), за счет использования MaxPatrol Mobile Server (устанавливается на ноутбуках, применяется для проверки территориально удаленных сетей и подразделений или физически изолированных сегментов)	Поддерживается через механизм импорта / экспорта результатов выполнения задачи на сбор данных из компонента MP 10 Collector, установленного в изолированном сегменте	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается за счет возможности создания и экспорта отчетов с результатами сканирования	Поддерживается выполнение скриптов, поддерживаемых устройством, в том числе Bash, Shell скрипт Unix, cmd, bat, Python, Java, JavaScript на устройствах в изолированных сегментах с дальнейшим импортом результатов обнаружения, инвентаризации, сканирования, оценки соответствия на сервере управления решения	Поддерживается возможность создания и использования Live-USB версии для исследования в изолированных сегментах
3.7. Интеграция с внешними системами, содержащими данные по активам и уязвимостям (перечень поддерживаемых систем)	Импорт списка узлов из Active Directory, импорт xml-файлов (с настройкой xsl-преобразования)	Поддержка импорта активов из MP 8 (через xml-файл), импорт из csv-файлов, обнаружение активов на основе данных других просканированных активов типа MS Active Directory, MS SCCM, Kaspersky Security Center, VMware ESXi, Microsoft Hyper-V, сетевых устройств	Поддерживается интеграция со сканерами безопасности (MaxPatrol 8, MaxPatrol VM, RedCheck, Nessus, Nexpose, OpenVAS, Qualys, Tenable SC, Skybox). Поддерживается импорт файлов отчётов от сканеров (xml, csv)	Поддерживается импорт хостов из AD, CSV, поиск в сети	Интеграция через API	Не поддерживается	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	Реализована возможность отправки событий об обнаружении активов и уязвимостей в SIEM систему по syslog
3.8. Поддержка протоколов и механизмов для доступа к внешним системам: LDAP, SMB, SSH, ODBC, SQL, SOAP, API;	LDAP, SMB	LDAP, SMB, SSH, API, MSSQL, Telnet	LDAP, SMB, SSH, ODBC, SQL, SOAP, API	Поддерживается импорт хостов, авторизация в консоли из AD. Отправка отчетов по SMB, SMTP. Интеграции через REST API. Сканирование по протоколу сканируемой платформы	Не поддерживается	Не поддерживается	Поддерживается LDAP, SMB, SSH, ODBC, SQL, SOAP, API; Поддерживается 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)	Поддерживается SMB, FTP, SSH, WinRM, Telnet
3.9. Поддержка агентского или безагентского режима работы;	Безагентское сканирование. При сканировании Windows-устройств с использованием транспорта Remote Engine на сканируемое устройство загружается exe-файл, собирающий информацию локально, с последующей передачей информации на сервер MP и самоудалением exe-файла	Безагентский режим работы	Поддерживается только безагентский режим работы. Агентский режим возможен при использовании продукта R-Vision Endpoint.	Поддерживается агентский и безагентский режимы работы	Безагентское сканирование	Только локальная установка на сканируемом устройстве	Поддержка агентского и/или безагентского режима работы	Реализован полностью безагентский режим работы
3.10. Импорт контента и политик (форматы csv, xlsx, json, xml, yaml);	Импорт расписаний, задач, профилей, учетных записей, справочников, правил идентификации из xml-файлов	Поддержка импорта активов из MP 8 (через xml-файл), импорт из csv-файлов. Поддержка импорта пользовательских профилей в формате json	Поддерживается импорт файлов Excel с описанием уязвимостей	Поддерживаются OVAL и XCCDF	Не поддерживается	Импорт XML-файлов с OVAL-описаниями уязвимостей, выполненными в соответствии со стандартом "The OVAL Language Specification" версии не ниже 5.10.1	Поддерживается импорт в форматах csv, json, xml	Импорт шаблонов и правил аудита конфигурации в формате yaml
3.11. Экспорт контента и политик (форматы csv, xlsx, json, xml, yaml, docx, ods, odt, txt, pdf, html);	Экспорт отчетов, расписаний, задач, профилей, учетных записей, справочников, правил идентификации в xml-файлы. Поддержка экспорта отчетов в форматах mht, pdf, xml	Поддержка экспорта отчетов в файлы форматы pdf, mht, xlsx, docx, csv по активам, уязвимостям. Экспорт информации об активах и данных табличных виджетов в файлы форматов csv, xlsx, json, xml. Экспорт топологии сети в виде графического файла формата png, svg. Экспорт пользовательских профилей в формате json. Экспорт результатов сканирования, полученных в закрытом сегменте сети, в zip-архив. Экспорт данных с графического виджета в файлы формата png. Экспорт записей из табличных виджетов в файлы формата xlsx	Поддерживается экспорт объектов в формате json, xlsx	Поддерживаются только отчеты с результатами в форматах PDF, HTML, CSV, XML	Экспорт отчетов в форматах PDF, CSV	Экспорт отчетов в html. Выполняется сохранение xml-файлов в стандартном формате OVAL в каталоге с временными файлами решения	Поддерживается экспорт в форматах pdf, docx, odt, xlsx, ods, csv, json	Экспорт пользовательских скриптов, шаблонов и правил, результата всех задач, а также отчёта в формате yaml, lua/nse, csv, pdf, html
3.12. Встроенная, обновляемая вендором и пополняемая пользователями база знаний с рекомендациями, советами, лучшими практиками по эффективному обнаружению и инвентаризации активов, сканированию на наличие уязвимостей, оценке и приведению в соответствие;	Поддерживается в рамках периодических обновлений базы знаний – загрузка актуальной информации о появившихся уязвимостях и способах их устранения, новых стандартов, обновлений профилей сканирования и т.д.	Поддерживается в рамках периодических обновлений базы знаний – загрузка актуальной информации о появившихся уязвимостях, списков трендовых уязвимостей, данных по наличию эксплойтов, последствий эксплуатации уязвимостей, способах устранения уязвимостей, загрузка новых стандартов, рекомендаций	Не поддерживается	Поддерживаются, собственный репозиторий уязвимостей OVALdb вендора	Поддержка от вендора	Поддерживается в рамках формирования XML-файлов с OVAL-описаниями уязвимостей (раз в несколько дней)	Поддерживается ведение и регулярное обновление вендором базы лучших практик и рекомендаций по работе с активами, уязвимостями, несоответствиями.	Автоматическое обновление Базы уязвимостей

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
3.13. Возможность проверки ("прогона") интеграций и скриптов перед вводом в эксплуатацию без реального взаимодействия с инфраструктурой;	Частично поддерживается через функционал тестирования транспортов – выполняется проверка доступности сканируемого хоста, валидность учетных записей и их прав	Частично поддерживается проверка доступности узлов, конфигурации транспортов на узлах, проверка корректности указанной учетной записи для сканирования через выполнение задач проверки подключения	Не поддерживается	Не поддерживается. Контент верифицирован и применяется динамически во время сканирования на каждом хосте индивидуально	Не поддерживается	Не поддерживается	Поддерживается тестовый режим проверки интеграций и скриптов во встроенной в решение среде разработки	Не поддерживается
3.14. Формирование и контроль задач на получение инвентаризационной информации об активах, задач на устранение уязвимостей, задач на приведение активов в соответствие с требованиями;	Частично поддерживается формирование задач на приведение активов в соответствие через настройку сценария "Контроль за устранением уязвимостей" (настройка временных периодов на исследование и устранение уязвимостей) в планировщике. Частично поддерживается через выгрузку xml-отчетов о сканированиях и их загрузку в стороннюю ticketing/tracker-систему	Поддерживается задание регламентов сканирования инфраструктуры иустранения уязвимостей. Контроль защищенности инфраструктуры исроков устранения уязвимостей производится спомощью дашбордов	Не поддерживается	Поддерживается ручное назначение задач сканирования	Не поддерживается	Не поддерживается	Поддерживается ведение и управление задачами встроенными в решение средствами (с оповещениями, интеграцией со сторонними таск-трекерами, синхронизацией статусов)	Не поддерживается. Предполагается, что постановка задач на устранение уязвимостей осуществляется во внешнем трекере задач
3.15. Наличие различной логики формирования задач на устранение уязвимости (например, создавать задачи по каждому узлу или по каждой уязвимости);	Не поддерживается	Не поддерживается	Поддерживается в рамках настройки перечня выполняемых действий в зависимости от свойств активов и уязвимостей	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается возможность формирования задач по каждому хосту, ПО, уязвимости или их комбинации. Кроме того, возможна тонкая настройка логики формирования задач (заявок) через настройку рабочих процессов в графическом low-code / no-code конструкторе	Не поддерживается
3.16. Поддержка совместной работы ИБ / ИТ / бизнес-подразделений: чат, оповещения, возможность обработки email и приложенных файлов;	Частично, за счет встроенных информационных сообщений в интерфейсе решения, отправки отчетов о сканировании по email	Частично, за счет встроенных информационных сообщений в интерфейсе решения, отправки отчетов о сканировании по email	Поддерживается чат, оповещения, возможность отправки и обработки email	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживаются чаты по задачам (заявкам), уязвимостям, активам, несоответствиям. Поддерживается отправка оповещений через веб-интерфейс решения, через мессенджеры (Telegram), через API к любой системе. Поддерживается парсинг email с обработкой вложений	Не поддерживается
3.17. Возможность интеграции, включая двухстороннюю, с системами класса CMDB / ITAM;	Не поддерживается	Поддержка интеграции с MS SCCM, Kaspersky Security Center, другие системы – через API	Поддерживается интеграция с MS SCCM, Micro Focus UCMDB	Не поддерживается	Через API	Не поддерживается	Поддерживается интеграция с Security Vision AM/CMDB, MicroFocus Service Manager (HP Service Manager), CMDB iTop, MS SCCM, MS WSUS, Active Directory, Infoblox (IPAM), Skybox, Lansweeper, HP OneView, Microsoft Endpoint Configuration Manager	Не поддерживается
3.18. Возможность интеграции, включая двухстороннюю, со службами каталогов (Active Directory, FreeIPA / ALD Pro, Samba DC и т.д.);	Active Directory	Поддержка интеграции с MS Active Directory, другие системы – через API	Поддерживается интеграция с Active Directory	Поддерживается AD	Не поддерживается	Не поддерживается	Поддерживается интеграция с Active Directory, OpenLDAP, FreeIPA, Astra Linux Directory	Поддерживается интеграция с AD/LDAP сервером
3.19. Возможность интеграции, включая двухстороннюю, с системами класса ITSM / ServiceDesk;	Не поддерживается	Возможна интеграция через API	Поддерживается интеграция через REST API	Поддерживается через REST API	Через API	Не поддерживается	Поддерживается интеграция с Security Vision SD, One Vision SD, Jira, Naumen Service Desk, MicroFocus Service Manager (HP Service Manager), BPM Online (Creatio), OTRS, Redmine	Не поддерживается
3.20. Возможность интеграции, включая двухстороннюю, с системами класса SIEM;	Cisco MARS, Symantec SIM, ArcSight ESM, NetForensics SIM One, Skybox View, IBM Security QRadar SIEM, MaxPatrol 10	MaxPatrol SIEM, другие системы – через API	Поддерживается интеграция с R-Vision SIEM, с другими решениями – через REST API	Поддерживается через REST API	Через API	Не поддерживается	Поддерживается интеграция с Kaspersky KUMA, MaxPatrol SIEM, Pangeo RADAR, RuSIEM, NEURODAT SIEM, ArcSight SIEM, IBM QRadar, Splunk	Поддерживается интеграция с KOMRAD Enterprise SIEM. Поддерживается передача списка активов и уязвимостей по syslog
3.21. Возможность интеграции, включая двухстороннюю, с системами класса SOAR;	Не поддерживается	Возможна интеграция через API	Поддерживается интеграция с R-Vision SOAR, с другими решениями – через REST API	Поддерживается через REST API	Не поддерживается	Не поддерживается	Поддерживается интеграция с Security Vision SOAR, Security Vision NG SOAR, с другими решениями – через REST API	Не поддерживается
3.22. Возможность интеграции, включая двухстороннюю, с системами класса TIP;	Не поддерживается	PT Threat Analyzer, другие системы – через API	Поддерживается интеграция с R-Vision TIP, с другими решениями –через REST API	Поддерживается через REST API	Не поддерживается	Не поддерживается	Поддерживается интеграция с Security Vision TIP, с другими решениями – через REST API	Не поддерживается
3.23. Возможность интеграции, включая двухстороннюю, с системами класса NTA;	Не поддерживается	PT NAD, другие системы – через API	Поддерживается интеграция через REST API	Поддерживается через REST API	Через API	Не поддерживается	Поддерживается интеграция с PT Network Attack Discovery, с другими решениями – через REST API	Не поддерживается
3.24. Возможность интеграции, включая двухстороннюю, с системами класса EDR / XDR;	Не поддерживается	PT XDR, MaxPatrol EDR, другие системы – через API	Поддерживается интеграция через REST API	Поддерживается через REST API	Через API	Не поддерживается	Поддерживается интеграция с Kaspersky Symphony XDR, Kaspersky EDR, MS Defender EDR, RT Protect EDR	Не поддерживается
3.25. Возможность интеграции, включая двухстороннюю, с системами класса SGRC;	Не поддерживается	Возможна интеграция через API	Поддерживается интеграция с R-Vision SGRC, с другими решениями – через REST API	Поддерживается через REST API	Не поддерживается	Не поддерживается	Поддерживается интеграция с Security Vision SGRC/auto-SGRC, с другими решениями – через REST API	Не поддерживается

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
3.26. Возможность интеграции, включая двухстороннюю, с ИТ/ИБ-системами других классов;	Поддерживается интеграция со сканером безопасности приложений PT BlackBox	PT Sandbox, PT Application Firewall, PT ISIM, другие системы – через API	Поддерживается интеграция с R-Vision TDP, R-Vision UEBA, с другими решениями – через REST API	Поддерживается через REST API	Через API	Не поддерживается	Поддерживается интеграция с Security Vision BCP, Security Vision RM/ORM, Security Vision CM, Security Vision UEBA, Security Vision AD + ML. Поддерживается интеграция с Any.Run, Kaspersky KATA, One Vision, PT Sandbox, PT NAD, Trend Micro Deep Discovery Analyzer (DDA), Cisco StealthWatch, Zabbix, Microsoft Exchange, Veeam Backup, 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, 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), 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, Active Directory, OpenLDAP, FreeIPA, Astra Linux Directory и другими системами	Поддерживается интеграция со сканером безопасности приложений PT BlackBox
3.27. Поддержка параллельного выполнения задач обнаружения, инвентаризации, сканирования, оценки соответствия, максимальное число параллельных задач (потоков);	Настройка количества параллельных процессов сканирования в режиме PenTest (максимальное количество одновременных соединений для одного сканируемого узла – 64 потока), сканирования веб-приложений, сканирования с помощью Nmap	Поддерживается с ограничениями: MP 10 Collector может одновременно проводить аудит не более чем на 1000 клиентских компьютерах. По умолчанию для модуля Audit могут одновременно выполняться не больше 20 подзадач, а для встроенного модуля AuditCheck - не больше 40	Не поддерживается	Поддерживается, до 5 параллельных задач на каждый сканер	Не поддерживается	Не поддерживается	Поддерживается, максимальное число параллельных задач (потоков) ограничено вычислительной мощностью используемой аппаратной платформы. По умолчанию - 50 параллельных потоков. Количество потоков может быть изменено в зависимости от вычислительной мощности серверов	Поддерживается, максимально число параллельных задач устанавливается физическим количеством ядер на целевой машине, в конфигурации настраивается коэффициент параллельности.
3.28. Отчетность: разнообразные виды и форматы отчетов (doc, pdf и т.д.), возможность создания стратегических, оперативных, тактических, аналитических отчетов для различных групп потребителей решения, возможность отправки отчетов автоматически и по запросу по электронной почте, через мессенджеры и т.д.;	Кастомизация шаблонов отчетов с результатами сканирования. Настройка типов и перечней отображаемых блоков. Настройка задач и сканирований, по которым выпускается отчет. Поддерживаются типы отчетов: · Информация - отчет выпускается по одному выбранному скану; · Дифференциальный - отчет позволяет увидеть разницу между результатами двух сканов; · Сравнительный аналитический - позволяет определить скорость устранения уязвимостей; · Динамический аналитический - позволяет видеть динамику наличия уязвимостей; · Аналитический - отчет о соответствии указанному стандарту (PCI DSS 2.0, PCI DSS 3.2, 3GPP Security Requirements, ИБ ISO/IEC 27001/27002, АС РД ФСТЭК, СТО БР ИББС-1.0-2010, ГОСТ Р 57580.1-2017, GDPR Security Measures); · Диагностический - отчет позволяет продемонстрировать сводную статистику по проведенным сканированиям. Поддержка выгрузки отчетов в форматах mht, pdf, xml. Доставка отчетов по email, в сетевой каталог, на FTP-сервер. Кастомизация отчетов через MS SQL Reporting Services	Поддержка экспорта отчетов в файлы форматы pdf, mht, xlsx, docx, csv по активам, уязвимостям. Формирование отчетов с использованием пользовательских шаблонов (формат xlsx) и с помощью PDQL-запросов. Ручной и автоматический (по расписанию) выпуск отчетов и экспорт данных. Доставка отчетов по email	Поддерживается формирование отчетов в формате Microsoft Office (docx, xlsx, pptx), odt, pdf	Поддерживается, отчеты PDF, HTML, CSV, XML. Автоматическая доставка выбранным получателям по завершению задачи сканирования по SMTP или SMB, с применением шаблона Определение блоков отчета в шаблоне	Экспорт отчетов в форматах PDF, CSV. Отправка отчетов через Telegram, по email	Поддерживается формирование отчетов о сканировании в формате html	Поддерживается формирование отчетов в форматах pdf, docx, odt, xlsx, ods. Поддерживается отображение состояния объектов (активов, уязвимостей, несоответствий) в отчетах различного типа с элементами визуализации (таблицы, графики, диаграммы, географическая карта и т.д.)	Поддерживается формирование кратких и полных отчётов по всем последним результатам выполненных задач для выбранных активов. Формат: html, pdf

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
3.29. Встроенный функционал (среда разработки) для создания интеграций, политик и правил работы с объектами, настройки выполняемых действий по обработке уязвимостей, приведению в соответствие;	Не поддерживается	Не поддерживается	Поддерживается создание пользовательских интеграций через конструктор интеграций и написание Python-скриптов	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается встроенная в решение среда разработки с подсветкой синтаксиса, подсказками, проверкой синтаксиса, тестированием разработанных интеграций, политик, правил работы с объектами, со встроенной справкой и тестовым режимом для проверки	Поддерживается UI-конструктор для создания описания пользовательских уязвимостей и UI-сниппет со встроенным пустым шаблоном для написания правил аудита конфигурации. К каждому компоненту прилагается документация на UI по работе с полями yaml файла и описанием уязвимости
3.30. Наличие сообщества / маркетплейса для получения дополнительных интеграций, скриптов инвентаризации, скриптов сканирования на наличие уязвимостей, скриптов оценки соответствия и т.д.;	В рамках портала технической поддержки вендора, через официальные и неофициальные группы в Телеграм	В рамках портала технической поддержки вендора, через официальные и неофициальные группы в Телеграм	Информация предоставляется в рамках технической поддержки уровня "ПремиумПлюс"	Поддерживается OVAL и поддержка производителя	В рамках портала технической поддержки вендора, через группу в Телеграм	Не поддерживается	Присутствует веб-портал для клиентов с возможностью обмена информацией (экспертизой по реагированию, настройками интеграций, скриптами и сценариями реагирования)	Не поддерживается
3.31. Наличие, функционал, кастомизация средств отправки оповещений (электронная почта, мессенджеры, встроенные в решение средства и т.д.);	Встроенные информационные сообщения в интерфейсе решения, отправка отчетов о сканировании по email	Встроенные информационные сообщения в интерфейсе решения, отправка отчетов о сканировании по email.	Поддерживается отправка оповещений через электронную почту, через встроенные в решение средства, за счет интеграции через REST API.	Поддерживается чрез электронную почту (SMTP)	Отправка отчетов через Telegram, по email.	Не поддерживается	Поддерживается отправка оповещений через веб-интерфейс решения, через мессенджеры (Telegram), электронная почта, через API к любой системе.	Не поддерживается
3.32. Наличие базы шаблонов оповещений;	Предустановлены 12 шаблонов отчетов о сканировании	Не поддерживается	Поддерживается	Шаблон по умолчанию	Поддерживается через шаблоны оповещений сканеров, входящих в состав решения	Не поддерживается	Поддерживается	Не поддерживается
3.33. Настройка правил отправки оповещений (например, при обнаружении уязвимости, изменении свойств актива, принятом решении по задаче и т.д.);	Только в рамках настройки профилей сканирования	Поддерживается с помощью создания задачи на отправку уведомлений	Поддерживается через настройку политик управления сканированиями	Поддерживается, по завершению задачи сканирования	Поддерживается	Не поддерживается	Поддерживается через настройку рабочих процессов в графическом low-code / no-code конструкторе	Не поддерживается
3.34. Отображение связи объектов решения на интерактивном графе, переход от одного типа объекта к другому, выполнение действий с объектами из графа;	Не поддерживается	Поддерживается через интерфейс карты (топологии) сети с отображением активов и связей между ними, сетевой достижимости между активами. Поддерживается переход к работе с событиями и инцидентами с карты сети	Граф взаимосвязей строится отдельно для каждого актива, поддерживается построение карты сети для группы активов, поддерживается формирование схемы связей бизнес-процессов и активов	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается отображение всей ресурсно-сервисной модели инфраструктуре на графе связей с поддержкой выполнения интерактивных действий с объектами из графа	Поддерживается формирование карты сети
3.35. Отображение объектов на географической карте, схемах зданий и помещений;	Не поддерживается	Не поддерживается	Поддерживается отображение активов на географической карте	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается отображение объектов на карте, схемах, планах	Поддерживается отображения топологии сети с шлюзами и всеми активами, а также индикация максимального уровня опасности обнаруженных на активе уязвимостей (вкладка "Карта сети")
3.36. Отображение объектов на схемах сети уровней L1 / L2 / L3 для применимых объектов;	Не поддерживается	Отображение уровней L2 /L3 на карте сети	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Поддерживается формирование карты сети
3.37. Поддержка сквозного поиска, фильтрации, сортировки по свойствам объектов решения, возможность сохранения созданных фильтров и поисковых запросов;	Не поддерживается	Поддержка поисковых PDQL-запросов, поддержка создания фильтров	Поддерживается.	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
3.38. Работа с карточкой объекта: кастомизация полей, добавление комментариев, вложений и тегов, настройка отображаемых полей, настройка внешнего вида карточки в зависимости от пользователя или группы, возможность скрытия полей и их значений для различных пользователей или групп;	Не поддерживается	Поддерживается добавление пользовательских полей в модель актива с помощью изменения файла UserModel.xml	Поддерживается создание пользовательских полей для уязвимостей, активов, настройка внешнего вида карточек уязвимостей, активов	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается произвольная кастомизация карточек объектов по требованиям пользователя (добавление полей, элементов, вкладок, элементов управления и т.д.). Поддерживается настройка прав доступа к объектам и их свойствам, скрытие конфиденциальной информации (например, определенных свойств активов)	Поддерживается возможность создания и назначения тегов для активов
3.39. Поддержка выполнения автоматических действий с объектами: добавление, удаление, изменение, включая массовые операции;	Не поддерживается	Поддерживается автоматическое выполнение массовых операций над уязвимостями с помощью правил (возможность менять статусы, отмечать уязвимости как важные, применять правила обработки уязвимостей)	Массовые операции поддерживаются	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживаются автоматические действия и автоматические массовые операции	Не поддерживается

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
3.40. Поддержка выполнения ручных действий с объектами: добавление, удаление, изменение, включая массовые операции;	Не поддерживается	Поддерживается ручное выполнение массовых операций над уязвимостями (возможность менять статусы, отмечать уязвимости как важные, применять правила обработки уязвимостей)	Поддерживается	Поддерживается	Не поддерживается	Не поддерживается	Поддерживаются ручные действий и ручные массовые операции	Поддерживается
3.41. Поддержка выполнения ручных, автоматических действий с объектами в табличном представлении, включая массовые операции;	Не поддерживается	Поддерживается	Поддерживается	Поддерживается управление хостами через CSV-импорт	Не поддерживается	Не поддерживается	Поддерживается выполнение одиночных и массовых ручных и автоматических действий с объектами в табличном представлении	Не поддерживается
3.42. Возможность создания пользовательских типов объектов с кастомизацией свойств;	Не поддерживается	Поддерживается для активов через настройку пользовательских полей в модели актива с загрузкой xml-файла с описанием модели актива	Поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
3.43. Поддержка ведения и отображения истории изменений объектов и их свойств;	Только в рамках истории выполнения задач сканирования. Поддержка календарного представления выполненных задач сканирования	Поддерживается хранение истории изменений каждого актива в базе данных сервиса Temporal Read Model, ротация истории изменений может быть включена вручную	Поддерживается, с отображением истории и источника получения обогащающих данных об уязвимостях	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Поддерживается возможность просмотра результата задач из вкладки "История"
3.44. Расписание выполнения действий с объектами;	Поддерживается настройка расписания проведения задач сканирования, выпуска отчетов, импорта данных через встроенный планировщик. Настраивается частота повторения, дата и время начала и окончания запуска задач	Поддерживается запуск задач по расписанию (выпуск отчетов, экспорт записей, сканирование)	Поддерживается выполнение сканирований, формирование отчетов по расписанию	Поддерживается расписание задач сканирования	Не поддерживается	Не поддерживается	Поддерживается	При создании каждой задачи в интерфейсе поддерживается возможность задать расписание ее выполнения
3.45. Задание временных интервалов и расписаний, в течение которых действия с объектами не выполняются (ставятся на паузу автоматически);	Поддерживается создание недопустимых интервалов сканирования и действий при их наступлении (приостановить, перезапустить, отменить, выполнить сканирование заново)	Поддерживается настройка технических окон для сканирования, запрещенного времени сканирования	Поддерживается	Поддерживается настройка запрещенных интервалов сканирования	Не поддерживается	Не поддерживается	Поддерживается формирование расписаний, "запрещенных" временных интервалов	Не поддерживается
3.46. Возможность приостановки или полной остановки действий с объектами по команде оператора или автоматически при выполнении определенных условий (например, при ошибках аутентификации);	Поддерживается приостановка, перезапуск, отмена сканирования вручную и по расписанию	Не поддерживается	Поддерживается ручная и автоматическая остановка действий	Поддерживается ручная остановка, ограничивающая дата сканирования	Не поддерживается	Не поддерживается	Поддерживается выполнение ручной приостановки, остановки действий (по команде пользователя) и автоматической приостановки, остановки действий (через настройку рабочих процессов в графическом low-code / no-code конструкторе)	Поддерживается выполнение команд ("Пауза" и "Стоп")
3.47. Возможность задания таймаута, после которого действия с объектом останавливаются с записью ошибки таймаута и отправкой оповещения оператору;	Через настройку параметра Nmap "host-timeout <time>" - время, после которого необходимо перестать пытаться сканировать узел (таймаут)	Поддерживается настройка параметра таймаута простоя, аутентификации для соединений SSH, LDAP, WMI, Oracle, MSSQL, SAP RFC, API, OPSEC. Поддерживается настройка времени таймаута ответа портов TCP, UDP для сканирования, таймаут выполнения сценариев PowershellExecutor, RemoteExecutor	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается, оповещение отображается в консоли, отправляется через email или мессенджеры, по API в любую совместимую систему	Не поддерживается
3.48. Поддержка ведения и отображения статистики и бизнес-аналитики по объектам решения;	Статистика - в ограниченном объеме через настройку отчетов	Частично поддерживается за счет сохранения статистики собранных данных об активах, экспорта статистических данных по активам, уязвимостям, выполненным проверкам	Не поддерживается	Поддерживается через дашборды главной страницы	Поддерживается в рамках отчетности сканеров, входящих в состав решения	Не поддерживается	Поддерживается ведение и отображение информации в виде диаграмм, графиков, отчетов	Поддерживается отображение статистических данных по обнаруженным уязвимостям в рамках проекта, либо по каждому узлу на карте сети
3.49. Поддержка визуализации: дашборды, виджеты, функционал "drill down";	Статичные дашборды - в ограниченном объеме через настройку отчетов	Поддерживается создание дашбордов с виджетами по активам, уязвимостям, выполненным проверкам	Поддерживается	Поддерживается через дашборды и диаграммы в отчетах	Поддерживается	Не поддерживается	Поддерживается отображение состояния активов на виджетах (линейный график, столбчатая диаграмма, круговая диаграмма, спидометр, таблица, географическая карта), на графах связей, на дашбордах, в отчетах. Во всех графических элементах поддерживается функционал "drill down" для непосредственного перехода от визуальных элементов к данным, на основании которых было построено графическое отображение	Не поддерживается
3.50. Возможность пользовательской настройки элементов визуализации (дашборды, виджеты) с настройкой отображения под каждого пользователя или группы, поддержка сохранения пользовательской настройки отображения;	Статичные дашборды - в ограниченном объеме через настройку отчетов	Поддерживается создание пользовательских дашбордов, добавление виджетов на дашборды	Поддерживается создание пользовательских графиков, дашбордов	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается настройка произвольных графических элементов индивидуально под каждого пользователя и сохранение настроек	Не поддерживается

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
3.51. Встроенная веб-помощь в интерфейсе решения;	Не поддерживается	Поддерживается	Поддерживается	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается, включая контекстную помощь и ссылки на разделы документации с учётом текущего функционального блока пользователя	Для разделов "Пользовательские уязвимости" и "Шаблоны и правила аудита конфигурации" при создании объекта справа есть всплывающая документация. Кроме того, подробную информацию о работе с этими разделами можно найти на сайте с онлайн-документацией.
3.52. Наличие разных тем интерфейса решения;	Не поддерживается	Не поддерживается	Поддерживается (темная, светлая темы).	Не поддерживается	Поддерживаются темная и светлая темы	Не поддерживается	Поддерживаются темы (темная и светлая, индивидуальная).	Не поддерживается
3.53. Поддержка различных языков интерфейса решения.	Язык интерфейса: русский, английский, корейский	Русский и английский языки интерфейса	Поддерживается русская и английская локализации	Поддерживается только русский язык	Язык интерфейса: русский, английский	Язык интерфейса: русский.	Поддерживается мультиязычная локализация интерфейса и всех элементов на русском и английском с возможностью добавления других языков	Язык интерфейса: русский, английский
4. Управление активами								
4.1. Настройка правил и логики обнаружения, инвентаризации, классификации активов;	Не поддерживается	Поддерживается с помощью создания политик, состоящих из совокупности правил, автоматически изменяющих параметры объектов решения. Политики позволяют автоматически изменять свойства значимости активов, сроки актуальности и устаревания данных об активах. Создание правил выполняется с помощью фильтров - запросов на языке PDQL	Не поддерживается	Поддерживается через настройку профилей сканирования	Не поддерживается	Не поддерживается	Поддерживается настройка правил и логики обнаружения, инвентаризации, классификации активов через графический low-code / no-code конструктор рабочих процессов	Поддерживается запуск исследования сети по расписанию
4.2. Поддерживаемые типы активов (документы, базы данных, информационные системы, устройства, сети, компоненты, интерфейсы, организационные единицы и т.д., пользовательские типы активов) и проставление связей между ними в ручном и автоматическом режимах;	Не поддерживается	Поддерживаемые типы активов: рабочая станция, сервер, маршрутизатор, сетевой коммутатор, межсетевой экран, точка доступа, неизвестное сетевое устройство, сетевой принтер, узел, внутренняя сеть, пограничная сеть, служба каталогов Microsoft Active Directory, гипервизор, контроллер удаленного управления сервером. Пользовательские типы активов не поддерживаются. Связи между активами проставляются на карте сети автоматически	Поддерживаются типы активов: оборудование, подразделения, помещения, бизнес-процессы, информация, сети, персонал, ПО, группы ИТ-активов, лицензии, СКЗИ, мобильные устройства	Поддерживается тип "Хост" (IP, FQDN)	Не поддерживается	Не поддерживается	Поддерживаются произвольные типы активов, предустановлены типы "Информационная система", "Бизнес-процесс", "Приложение", "Оборудование", "Поставщики", "Продукты". Связи между объектами проставляются автоматически (в рамках построения ресурсно-сервисной модели и обнаружения взаимосвязей между объектами) и вручную	Сервер, рабочая станция, межсетевой экран, маршрутизатор, принтер, VoIP-адаптер, WAP, камера, виртуальная машина, общее назначение, мост, широкополосный маршрутизатор, игровая приставка, концентратор, балансировщик нагрузки, мультимедийное устройство, АТС, КПК, телефон, устройство питания, сервер печати, прокси-сервер, удалённое управление, устройство безопасности, специализированное, устройство хранения, коммутатор, устройство телекоммуникации, терминал, терминальный сервер и VoIP-телефон
4.3. Настройка правил и логики управления активами в рамках их жизненного цикла (например: планирование, закупка, разработка, внедрение, эксплуатация, поддержка, модификация, вывод в резерв, вывод из эксплуатации, уничтожение), включая настройку расписания обнаружения, инвентаризации, классификации активов, настройку глубины и частоты инвентаризации, классификации активов в зависимости от свойств активов, настройку SLA-метрик инвентаризации, классификации активов;	Не поддерживается	Поддерживается через настройку пользовательских полей в модели активов, правил, PDQL-запросов	Поддерживается настройка расписания обнаружения и инвентаризации (ПО, СЗИ, пользователи, технические характеристики), настройка глубины и частоты обнаружения, настройка правил классификации (установка критичности)	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается настройка правил и логики управления активами через графический low-code / no-code конструктор рабочих процессов. Настраивается расписание, частота, глубина обнаружения, инвентаризации, классификации активов	Не поддерживается
4.4. Контроль изменений свойств активов (изменение аппаратной и программной конфигурации);	В ограниченном объеме через контроль целостности, сканирование в режимах Compliance и Forensic, выпуск дифференциальных отчетов	Поддерживается ведение истории изменений конфигураций активов	Поддерживается ведение истории изменений свойств активов	Поддерживается через функционал инвентаризации и контроля	Не поддерживается	Не поддерживается	Поддерживается с накоплением статистики и последующей аналитикой, визуализацией, отчетностью	Поддерживается в рамках задачи "Инвентаризация"
4.5. Поддержка автоматического и ручного построения ресурсно-сервисной модели активов и инфраструктуры;	Не поддерживается	Частично поддерживается автоматическое построение топологии сети - связей между активами с отображением на карте сети	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается построение ресурсно-сервисной модели активов и инфраструктуры в ручном и автоматическом режимах	Не поддерживается

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
4.6. Визуализация ресурсно-сервисной модели;	Не поддерживается	Отображение топологии на карте сети	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается визуализация ресурсно-сервисной модели на графе связей, на географической карте, на схемах, планах	Не поддерживается
4.7. Возможность группирования активов: поддержка статических, динамических, пользовательских групп активов, настройка правил попадания активов в группы (например, по домену, установленной ОС, IP-адресу и т.д.), группирование активов в информационные системы, учет взаимного влияния активов;	Не поддерживается	Поддержка создания пользовательских статических и динамических групп активов. Динамические группы формируются с использованием фильтрации активов на языке PDQL с различными критериями запросов	Поддерживается группирование активов в группы IT-активов, включая пользовательские, через политики распределения активов по группам	Поддерживаются только статические группы	Не поддерживается	Не поддерживается	Поддерживается формирование статических, динамических, пользовательских групп активов, правил включения активов в группы с помощью графического low-code / no-code конструктора рабочих процессов	Поддерживается только по созданным пользователям тегам
4.8. Поддержка контроля выполнения инвентаризации и классификации активов, ведение и отображение истории изменений свойств активов;	Только в рамках истории выполнения задач сканирования	Поддерживается сравнение конфигураций активов. Экспорт истории изменений конфигураций активов поддерживается с ограничением - можно экспортировать историю изменений только одного актива в xml-файл	Поддерживается инвентаризация, классификация активов. Поддерживается ведение истории изменений свойств активов	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается, возможна настройка ведения истории изменений с детализацией до каждого свойства	Не поддерживается
4.9. Скоринг активов: расчет уровня критичности для активов, настройка правил установки критичности, возможность кастомизации формулы для расчета, непрерывный автоматический скоринг, перерасчет уровня критичности для уже учтенных активов при изменении формулы расчета;	Не поддерживается	Не поддерживается	Поддерживается выбор и назначение уровня критичности для активов	Поддерживается расчет уровня критичности в момент сканирования	Не поддерживается	Не поддерживается	Поддерживается скоринг, кастомизация формулы скоринга, автоматический перерасчет скоринг-балла	Не поддерживается
4.10. Возможности по обнаружению активов: активный (сетевое сканирование, опрос хостов) и пассивный (получение данных из ИТ/ИБ-систем, например, из SIEM, NTA, EDR, от сетевых устройств и т.д.) режимы;	Поддерживается активное обнаружение (сканер, Nmap) и пассивное за счет импорта списка узлов из Active Directory, импорта xml-файлов	Активное и пассивное (импорт активов из MP 8, импорт из csv-файлов, обнаружение активов на основе данных других просканированных активов типа MS Active Directory, MS SCCM, Kaspersky Security Center, VMware ESXi, Microsoft Hyper-V, сетевых устройств)	Поддерживается активное обнаружение, пассивное обнаружение реализуется за счет API-интеграций.	Поддерживается сетевое обнаружение хостов и импорт хостов через CSV или из AD	Поддерживается активное обнаружение (входящими в состав сканеры) и пассивное обнаружение за счет импорта из систем, интегрированных по API	Не поддерживается	Поддерживается активное обнаружение (агентский, безагентский способы), пассивный (получение данных об активах из совместимых систем)	Поддерживается активное обнаружение через возможность получать информацию о целях ("Исследование сети")
4.11. Поддерживаемые протоколы удаленного подключения к инвентаризуемым системам (SMB, WMI, WinRM, SSH, SNMP, ODBC, SQL и т.д.);	Поддерживаются DB2, FTP, LDAP, MongoDB, MSSQL, MySQL, Oracle, PostgreSQL, RPC, SAP HTTP, SAP RFC, SMB, SNMP, SSH, Sybase, Telnet, Tibero Database, VMware, WMI	Поддерживаются LDAP, MSSQL, ODBC, OPSEC, Oracle, RPC, SAP RFC, SNMP, SSH, Telnet, VMware, Web API, WMI	Поддерживается LDAP, MSSQL, MySQL, OracleDB, PostreSQL, REST API, SNMP, SOAP, SSH	Поддерживается инвентаризация Windows через агентскую инвентаризацию и протоколы WinRM, WMI; Linux - через протокол SSH; SQL - через протокол ODBC/SQL; сетевое оборудование - через протокол SSH; VMware - через протокол HTTPS	Не поддерживается	Не поддерживается	Поддерживается 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)	Поддерживаются SMB. WinRM, SSH, FTP, Telnet
4.12. Поддержка выполнения скриптов инвентаризации на конечных устройствах (batch, PowerShell, VBS, Python, bash и т.д.);	Не поддерживается	Поддерживается выполнение сценариев PowershellExecutor (скрипт Windows PowerShell), RemoteExecutor (сценарий командной оболочки Windows)	Поддерживается выполнение Python-скриптов	Поддерживается внутри OVAL/XCCDF, но не рекомендуется из-за высокой нагрузки и опасности таких скриптов	Не поддерживается	Не поддерживается	Поддерживается выполнение скриптов, поддерживаемых устройством, в том числе Bash, Shell скрипт Unix, cmd, bat, Python, Java, JavaScript	Поддерживается использование внутреннего bash и Powershell скриптов
4.13. Нормализация данных об активах (при импорте из разных источников), тонкая настройка правил нормализации;	Не поддерживается	Частично поддерживается за счет алгоритма идентификации при обнаружении активов	Не поддерживается	Поддерживается обновление хостов по группам через CSV или по OU AD	Не поддерживается	Не поддерживается	Поддерживается нормализация данных, тонкая настройка правил нормализации с помощью графического low-code / no-code конструктора рабочих процессов	Не поддерживается
4.14. Дедупликация данных об активах (при импорте пересекающихся данных об активах), тонкая настройка правил дедупликации (например, по совпадению FQDN, IP, MAC, наименованию ОС и т.д.);	Поддерживается через правила идентификации узлов с неизменяемыми ключами идентификации (IP-адрес, FQDN-имя, NetBIOS-имя, имя экземпляра MSSQL, имя экземпляра Oracle).	Поддерживается за счет алгоритма идентификации при обнаружении активов и сравнения идентификаторов просканированных активов	Не поддерживается	Поддерживается настройка при импорте	Не поддерживается	Не поддерживается	Поддерживается дедупликация данных, тонкая настройка правил дедупликации с помощью графического low-code / no-code конструктора рабочих процессов	Не поддерживается
4.15. Поддержка удаленного управления устройством из консоли решения (например, ручной и автоматический запуск обновления ОС / ПО, выполнение команд, перезагрузка, выключение и т.д.);	Не поддерживается	Частично поддерживается за счет возможности выполнения сценариев PowershellExecutor (скрипт Windows PowerShell), RemoteExecutor (сценарий командной оболочки Windows)	Поддерживается удаленное управление устройством через Python-скрипты	Поддерживается доступ через веб-консоль, доступна удаленно через браузер	Не поддерживается	Не поддерживается	Поддерживается удаленное управление устройствами, выполнение скриптов и команд на них, в том числе интерактивно из графического представления (графа связей)	Не поддерживается
4.16. Тегирование активов (исключения, напоминания, комментарии);	Не поддерживается	Поддерживается за счет функционала псевдонимов	Поддерживается указание комментариев, тэгов для активов	Поддерживается, с описанием хоста, членства в группе или группах	Не поддерживается	Не поддерживается	Поддерживается установка тегов, комментариев, добавление в исключения, создание напоминаний по активам	Поддерживается работа с тегами и удобная фильтрация всех активов по тегам

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
4.17. Возможность управления активами (создание, изменение, удаление) через API решения;	Не поддерживается	Поддерживается перенос и удаление активов, групп активов, выполнение PDQL-запросов, управление задачами сканирования (запуск, остановка, проверка состояния), управление профилями сканирования (создание, удаление, получение статуса)	Поддерживается	Поддерживается через REST API	Не поддерживается	Не поддерживается	Поддерживается	Поддерживается
4.18. Возможность настройки прав доступа при взаимодействии с активами посредством API.	Не поддерживается	Поддерживается, API-доступ предоставляется с привилегиями пользователя, запросившего API-токен доступа	Поддерживается	Поддерживается через ролевую модель REST API	Нет данных	Не поддерживается	Поддерживается	Не поддерживается
5. Управление уязвимостями								
5.1. Настройка правил и логики политик сканирования на наличие уязвимостей, политик обработки уязвимостей, правил контроля устранения уязвимостей и постановки задач на обработку уязвимостей в ИТ/ИБ/бизнес-подразделения, включая настройку расписания сканирований, настройку глубины и частоты сканирования в зависимости от свойств активов, настройку SLA-метрик обработки уязвимостей;	Поддерживается настройка задач обнаружения и сканирования узлов, профилей сканирования, фильтров при сканировании. Частично поддерживается контроль устранения уязвимостей, SLA и постановка задач на обработку уязвимостей через настройку сценария "Контроль за устранением уязвимостей" (настройка временных периодов на исследование и устранение уязвимостей) в планировщике. Поддерживается настройка расписания проведения задач сканирования через встроенный планировщик. Настраивается профиль сканирования, частота повторения, дата и время начала и окончания запуска задач сканирования	Поддерживается с помощью создания политик, состоящих из совокупности правил, автоматически изменяющих параметры объектов решения. Политики позволяют автоматически изменять статусы экземпляров уязвимостей, проставлять отметку "важная" для некоторых уязвимостей, определять срок устранения, откладывать обработку уязвимостей на определенный срок. Создание правил выполняется с помощью фильтров - запросов на языке PDQL. Правила политик перестают действовать для уязвимостей, параметры которых менялись вручную	Поддерживается настройка профилей сканирования, настройка политик управления уязвимостями, настройка задач и расписания сканирования, критериев действий в зависимости от свойств уязвимостей, перечня выполняемых действий (например, создание заявок на устранение)	Поддерживается формирование расписания сканирования для каждой задачи, включая запрещенные интервалы и момент остановки задачи. Применение профилей сканирования: Полный, Быстрый, Пользовательский	Только в рамках логики используемых внутри решения сканеров	Не поддерживается	Поддерживается настройка правил и логики политик сканирования на наличие уязвимостей, политик обработки уязвимостей, правил контроля устранения уязвимостей и постановки задач на обработку уязвимостей через графический low-code / no-code конструктор рабочих процессов. Настраивается расписание, частота, глубина сканирования на наличие уязвимостей	Поддерживается возможность использовать различные источники при создании задачи "Поиск уязвимостей", в том числе и пользовательскую базу уязвимостей. Запуск по расписанию доступен для всех типов задач
5.2. Настройка правил и логики управления уязвимостями в рамках их жизненного цикла (например: новая, обрабатывается, ложное срабатывание, исключена, принята, минимизирована, устранена, закрыта), поддержка ручного и автоматического изменения статуса для отдельной уязвимости и группы уязвимостей;	Не поддерживается	Поддерживается статусная модель уязвимостей (новая, исключена, в работе, запланировано устранение, устранена, истек срок устранения, устаревшая). Статус изменяется автоматически через правила, вручную, с использованием запросов PDQL	Поддерживается за счет настройки профилей сканирования, политик управления уязвимостями	Не поддерживается	Только в рамках логики используемых внутри решения сканеров	Не поддерживается	Поддерживается настройка правил и логики управления уязвимостями через графический low-code / no-code конструктор рабочих процессов	Поддерживается возможность отмечать уязвимость как ложное срабатывание. Для пользовательских уязвимостей есть возможность добавлять их в архив для поддержки просмотра уже пройденных задач и исключения поиска по данной уязвимости для новых
5.3. Поддержка методов сканирования: аутентифицированный (метод "белого ящика" с использованием административных полномочий на сканируемом активе), частично аутентифицированный (метод "серого ящика" с использованием ограниченных полномочий на сканируемом активе, например, УЗ с правами пользователя), неаутентифицированный (метод "черного ящика" без использования УЗ);	Поддерживается проведение неаутентифицированного сканирования (режим PenTest), аутентифицированного и частично аутентифицированного сканирования (режимы Audit, Compliance). Уровень полномочий сканирующей УЗ определяет достоверность и количество собранной информации	Аудит активов выполняется модулем audit (белый ящик) и pentest (черный ящик)	Поддерживается аутентифицированный и неаутентифицированный методы сканирования.	Поддерживается, полные и ограниченные права в "белом ящике", анонимно в "черном ящике"	Поддерживается проведение неаутентифицированного, аутентифицированного сканирования и сканирования Gray Box с авторизацией (для веб-приложений)	Поддерживается проведение только аутентифицированного сканирования с максимальными привилегиями на устройстве	Поддерживается аутентифицированное сканирование (с максимальными привилегиями на конечном устройстве), частично аутентифицированное (с минимально необходимыми привилегиями на конечном устройстве), неаутентифицированное (без УЗ)	Поддерживаются все три метода. Для методов "белый ящик" и "серый ящик" необходимо задать УЗ для актива и провести инвентаризацию, для метода "черный ящик" необходимо провести исследование сети. На основе собранных данных об установленном программном обеспечении запускается задача "поиск уязвимостей"
5.4. Поддержка сканирования файлов на сканируемом активе;	Поддерживается выполнение файловых проверок для Windows (через RPC, WMI), Linux (через SSH, Telnet) по всем объектам файловой системы. Поддерживается проведение контроля целостности файлов	Поддерживается в модуле Pentest: поиск файлов по метаданным, по содержимому, с использованием регулярных выражений, указанием условий поиска. В модуле Audit поддерживается поиск файлов (приложений) по метаданным, с использованием регулярных выражений	Поддерживается	Поддерживается сканирование уязвимостей, конфигураций, расчет контрольных сумм	Нет данных	Поддерживается выполнение файловых проверок	Поддерживается сканирование файловой системы на конечных точках, выявление и определение уязвимостей portable-версий ПО	Не поддерживается
5.5. Настройки сканирования: выбор и исключение диапазонов подсетей, IP-адресов, сетевых портов и протоколов, выбор УЗ для каждого метода сканирования (аутентифицированное, частично аутентифицированное, неаутентифицированное);	Поддерживается	Поддерживается	Поддерживается через настройку задач сканирования для определенных сетевых диапазонов, IP-адресов, поддерживается назначение УЗ для определенных задач сканирования	Поддерживается сканирование хостов и/или групп, выбор УЗ, выбор типа аудита	Только в рамках логики используемых внутри решения сканеров	Не поддерживается	Поддерживается выбор подсетей, групп активов, конкретных активов, включая внесение исключений. Возможно указание используемых методов и УЗ, включая автоматическое определение УЗ для актива из списка созданных УЗ. Поддерживается настройка правил и логики проведения сканирований через графический low-code / no-code конструктор рабочих процессов, с назначением определенных УЗ для определенных узлов/диапазонов	Поддерживается, параметры настраиваются пользователем в задаче "Исследование сети"

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
5.6. Поддержка ведения и отображения истории сканирований, использование собранных данных (версии ПО, ОС, СЗИ) для проактивной оценки эксплуатируемости новых уязвимостей;	Поддерживается частично через выпуск дифференциальных, аналитических (сравнительных, динамических) отчетов	Поддерживается ведение истории сканирований активов, собранные данные (версии ПО, ОС) используются для анализа применимости новых уязвимостей без проведения дополнительного сканирования	Поддерживается только ведение истории сканирования	Поддерживается только ведение истории сканирования.	Поддерживается частично через формирование отчетов	Поддерживается частично через формирование отчетов.	Поддерживается, в режиме ретро-скан производится поиск уязвимостей по полученным ранее данным из активов (включая контейнеры), без подключения к ним и ожидания окон сканирования. Поддерживается ведение истории с накоплением статистики и последующей аналитикой, визуализацией, отчетностью, оценкой трендов уязвимостей	Поддерживается ведение истории через вкладку "История" для всех типов задач
5.7. Поддержка выявления типов уязвимостей по ГОСТ Р 56546-2015: уязвимость кода, уязвимость конфигурации, уязвимость архитектуры, организационная уязвимость (уязвимость в процессах), многофакторная уязвимость;	Частично поддерживается: выявляются уязвимости кода, конфигурации	Частично поддерживается: выявляются уязвимости кода, конфигурации	Не поддерживается	Поддерживается	Не поддерживается	Не поддерживается	Поддерживаются все типы уязвимостей по ГОСТ Р 56546-2015. Для типов уязвимостей, которые определяются нетехническими методами (например, организационная уязвимость), предоставляется возможность заведения их в ручном режиме с установкой связей с бизнес-процессами, персоналом, уязвимыми информационными системами	Поддерживается
5.8. Поддержка различных методов обработки уязвимостей: принятие уязвимости (включая процесс согласования), минимизация рисков эксплуатации (применение СЗИ и компенсирующих мер), устранение (установка обновлений, применение временных обходных путей), избегание (отключение уязвимых компонентов, вывод уязвимого актива из эксплуатации);	Не поддерживается	Поддерживается за счет создания политик, состоящих из совокупности правил, которые автоматически изменяют статус экземпляров уязвимостей, определяют срок их устранения, откладывают их обработку на определенный срок, отмечают уязвимость как "важную"	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживаются различные методы, включая формирование логического "дерева решений", учитывающего свойства актива и уязвимостей, с установкой сроков, ответственных, формированием задач в решении и отправкой информации о задачах в интегрированные системы таск-трекинга. Возможна настройка произвольной логики через графический low-code / no-code конструктор рабочих процессов	Не поддерживается
5.9. Настройка правил и логики обработки и приоритизации уязвимостей с учетом свойств уязвимости, свойств уязвимого актива, других релевантных факторов (например, наличие выявленных несоответствий требованиям на активе, наличие незакрытых инцидентов ИБ на активе);	Не поддерживается	Поддерживается за счет создания политик и правил с использованием PDQL-запросов	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживаются различные методы, включая формирование логического "дерева решений", учитывающего свойства актива и уязвимостей, наличия инцидентов или рисков на активе, свойств зависимых бизнес-процессов. Возможна настройка произвольной логики через графический low-code / no-code конструктор рабочих процессов	Не поддерживается
5.10. Ведение и отображение идентификаторов уязвимостей из различных реестров уязвимостей (например, БДУ, CVE, NVD, VND, OSV, вендорские реестры);	Поддерживаются классификаторы уязвимостей БДУ, CVE, OSVDB, Bugtraq, вендорские (Cisco, RedHat RHSA, SuSE, Ubuntu, AIX, SAP)	Поддерживаются классификаторы уязвимостей БДУ, CVE	Поддерживается отображение идентификаторов CVE, БДУ	Поддерживается отображение всей доступной информации и информации из собственной базы вендора	Только в рамках функционала используемых внутри решения сканеров	Поддерживаются классификаторы уязвимостей БДУ, CVE, вендорские, бюллетени НКЦКИ, ФинЦЕРТ	Поддерживаются реестры БДУ, CVE, NVD, VND, OSV, информация из вендорских бюллетеней и реестров (Microsoft, Red Hat, Cisco и т.д.)	Поддерживаются классификаторы уязвимостей БДУ ФСТЭК России, NIST NVD, вендорские реестры (ОС Microsoft, Linux)
5.11. Поддержка CVSS-метрик версий 2 / 3 / 4;	Поддерживаются метрики CVSS v2 и v3	Поддерживаются метрики CVSS v2 и v3	Поддерживаются CVSS-метрики версий 2, 3, 4	Поддерживаются CVSS-метрики версий 2, 3	Только в рамках функционала используемых внутри решения сканеров	Поддерживаются метрики CVSS v2 и v3, в отчете отображаются уровни (критический, высокий, средний, низкий) в соответствии с CVSS v3, с отображением базового вектора уязвимости	Поддерживаются CVSS-метрики версий 2, 3, 4	Поддерживаются метрики CVSS v2, v3, v4
5.12. Поддержка нотации OVAL (Open Vulnerability and Assessment Language) для описания уязвимостей;	Поддерживается	Поддерживается	Поддерживается	Поддерживается	Только в рамках функционала используемых внутри решения сканеров	Поддерживается в соответствии со стандартом "The OVAL Language Specification" версии не ниже 5.10.1	Поддерживается	Не поддерживается
5.13. Поддерживаемые протоколы удаленного подключения к сканируемым системам (SMB, WMI, WinRM, SSH, SNMP, ODBC, SQL и т.д.);	Поддерживаются DB2, FTP, LDAP, MongoDB, MSSQL, MySQL, Oracle, PostgreSQL, RPC, SAP HTTP, SAP RFC, SMB, SNMP, SSH, Sybase, Telnet, Tibero Database, VMware, WMI	Поддерживаются LDAP, MSSQL, ODBC, OPSEC, Oracle, RPC, SAP RFC, SNMP, SSH, Telnet, VMware, Web API, WMI	Поддерживается LDAP, MSSQL, MySQL, OracleDB, PostreSQL, REST API, SNMP, SOAP, SSH	Поддерживается сканирование Windows через агентское сканирование и протоколы WinRM, WMI; Linux - через протокол SSH; SQL - через протокол ODBC/SQL; сетевое оборудование - через протокол SSH; VMware - через протокол HTTPS	Только в рамках функционала используемых внутри решения сканеров	Не поддерживается	Поддерживается 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)	Поддерживаются WinRM, SSH, FTP, Telnet
5.14. Поддержка выполнения скриптов сканирования на конечных устройствах (batch, PowerShell, VBS, Python, bash и т.д.);	Не поддерживается	Поддерживается выполнение сценариев PowershellExecutor (скрипт Windows PowerShell), RemoteExecutor (сценарий командной оболочки Windows)	Поддерживается выполнение Python-скриптов	Поддерживается внутри OVAL/XCCDF, но не рекомендуется из-за высокой нагрузки и опасности таких скриптов	Не поддерживается	Не поддерживается	Поддерживается выполнение скриптов, поддерживаемых устройством, в том числе Bash, Shell скрипт Unix, cmd, bat, Python, Java, JavaScript	Поддерживаются lua-скрипты: в задаче "Исследования сети" можно выбрать пользовательский или системный lua-скрипт для поиска уязвимостей актива.

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
5.15. Скоринг уязвимостей: расчет рейтинга опасности уязвимости, возможность кастомизации формулы для расчета, непрерывный автоматический расчет рейтинга уязвимостей, перерасчет рейтинга опасности для старых уязвимостей при изменении формулы расчета;	Оценивается только средний уровень уязвимостей в указанном наборе хостов через выпуск отчетов с некастомизируемой метрикой "Интегральная уязвимость"	Поддерживается выборка уязвимостей по их свойствам с помощью настраиваемых PDQL-запросов. Поддерживается расчет уровня опасности уязвимостей на активах по методике ФСТЭК России (методический документ "Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств", утвержденный ФСТЭК России 28.10.2022)	Поддерживается расчет уровня критичности уязвимости по методике (формуле) ФСТЭК. Поддерживается вендорская формула расчета рейтинга уязвимости. Поддерживается возможность кастомизации формулы для расчета	Поддерживается расчет уровня критичности в момент сканирования	Не поддерживается	Оценивается уровень опасности уязвимости с отображением уровня (критический, высокий, средний, низкий) в соответствии с CVSS v3, с отображением базового вектора уязвимости	Поддерживается скоринг, кастомизация формулы скоринга, автоматический перерасчет скоринг-балла	Поддерживается расчет рейтинга по методике ФСТЭК России (2022), без кастомизации формулы
5.16. Поддержка возможности контролируемой проверки эксплуатируемости уязвимости, ссылка на PoC / эксплойт;	Частично поддерживается за счет сканирования в режиме PenTest для веб-приложений (настройка "Искать уязвимости")	Поддерживается в модуле Pentest с помощью стандартных профилей для тестирования на проникновение (Safe PenTest, Unsafe PenTest). Поддерживается для веб-приложений (запрос для проверки на эксплуатабельность из карточки уязвимости). Поддерживается подтверждение наличия уязвимости скриптами с последующей простановкой признака "Эксплойт подтвержден"	Контролируемая проверка (запуск) эксплойта не поддерживается. Ссылка на PoC / эксплойт предоставляется (при наличии информации). В рамках режима "Пентест" поддерживается перебор словарных паролей (Bruteforce)	Поддерживается, отображается ссылка на доступную информацию об эксплойте	Не поддерживается	Не поддерживается	Поддерживается сканирование Web-приложений на наличие XSS, CSRF, SQL-инъекций, RFI, Code injection, раскрытие внутренней информации и настроек сайтов, подбор слабых паролей, перебор пользователей, а также проверка эксплуатации специфичных Web-уязвимостей и т.д. Поддерживается режим пентест для обнаружения и проверки возможности эксплуатации сетевых уязвимостей, возможности применения наиболее серьезных эксплойтов, подборы слабых паролей, проверка устаревших/ уязвимых алгоритмов шифрования и т.д. Поддерживается отображение информации об эксплойте в карточке уязвимости (наличие, уровень, эксплуатация в реальных атаках)	Поддержка отображения наличия эксплойта: в случае наличия опубликованного эксплойта, в карточке уязвимости выводится соответствующая информация
5.17. Поддерживаемые режимы сканирования: активный (с помощью встроенного сканера) и пассивный (получение данных из ИТ/ИБ-систем, например, из SIEM, NTA, EDR, от сетевых устройств и т.д.) режимы;	Только активный режим.	Поддерживаются активный и пассивный режимы (интеграция с MaxPatrol SIEM, PT NAD, PT XDR, MaxPatrol EDR)	Поддерживается активное сканирование (через встроенный nmap). Пассивное сканирование не поддерживается	Поддерживается активный режим	Поддерживается активное сканирование (входящими в состав сканеры) и пассивное сканирование за счет импорта из систем, интегрированных по API	Только активный локальный режим.	Поддерживается активное сканирование (агентский, безагентский способы), пассивный (получение данных об активах из совместимых систем). Используется сканер собственной разработки	Только активный режим через "Исследование сети"

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
5.18. Список поддерживаемых для сканирования систем/ решений;	Более 1500 систем, включая Windows, Linux, ERP, СУБД, сетевое оборудование. Полный писок на сайте вендора help.ptsecurity.com	Поддержка сканирования в режиме пентеста, идентификации узлов, обнаружения уязвимостей: системы АСУ ТП, ОС, сетевое оборудование, СУБД, серверное ПО, системы безопасности, СКЗИ, приложения. Полный список на сайте вендора help.ptsecurity.com	Поддержка основных зарубежных и отечественных дистрибутивов ОС Linux, поддержка ОС Windows (Windows 7 - 11, Windows Server 2008 R2 - 2022), поддержка более 50 типов ПО. Поддерживаемые СУБД: MS SQL, PostreSQL, Oracle, MySQL,ClickHouse	Поддерживаются ОС Microsoft Windows, Linux, отечественные ОС на базе Linux, сетевое оборудование, системы виртуализации, СУБД, АСУ ТП, ПЛК. Полный список на сайте вендора redcheck.ru	Нет данных	Поддерживаются ОС Microsoft Windows 7/8/8.1/10, Microsoft Windows Server 2008/ 2008R2/2012/ 2012 R2/2016. Поддерживаются ОС Linux: Astra Linux 1.7 SE, Astra Linux 1.6 SE, Альт Рабочая станция 9, Альт Сервер 9, Роса "Кобальт"	Поддерживаются "РЕД ОС", AlmaLinux, ALT Linux, Astra Linux CE, Astra Linux SE, CentOS Linux, Debian Linux, Red Hat Enterprise Linux, Microsoft Windows, Oracle Enterprise Linux, Ubuntu Linux, Alpine, openSUSE Leap, openSUSE Tumbleweed, SUSE Enterprise Linux (включая все возможные системы на его основе), настольные и серверные версии Windows, прикладное программное обеспечение (включая Microsoft Office с версиями "click-to-run", Exchange, SharePoint), базы данных (ClickHouse, MariaDB, Microsoft SQL Server, MongoDB, MySQL, Oracle Database, PostgreSQL, Redis, Elasticsearch и др.), сетевые устройства (Cisco, Juniper, CheckPoint, PaloAlto, Sun, F5, Brocade, Arista, CITRIX, A10 и др.). Поддерживается серверное ПО: Apache HTTP Server, Apache Tomcat, Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint Foundation, Microsoft SharePoint Server, Nginx, VMware vCenter Server, Squid HTTP Proxy Server, OpenResty и др. Поддерживаются приложения: 7-Zip, Adobe Acrobat, Adobe Acrobat Reader, AnyDesk, Apache Struts, Google Chrome, Mozilla Firefox, Mozilla Firefox ESR, Nessus, Notepad++, OpenOffice, LibreOffice, Skype for Windows, TeamViewer, Thunderbird, VirtualBox, VLC Media Player, VMware Tools, VMware Workstation, VMware Player, VMware ESXi, WinRAR, Zabbix Agent, Zabbix Server, Zoom, Hyper-V, Microsoft Edge, Microsoft Edge (Chromium), Microsoft Excel, Microsoft Excel Viewer, Microsoft Internet Explorer, Microsoft Office, Microsoft Visual Studio, Microsoft Visual Studio Code, Microsoft Windows Media, Microsoft Word Viewer, Microsoft .NET Framework, Microsoft .NET Core, Microsoft Lync, Microsoft OneDrive, Microsoft OneNote, Microsoft Outlook, Microsoft PowerPoint, Microsoft PowerPoint Viewer, Microsoft Project, Microsoft Publisher, Microsoft Remote Desktop Connection Client, Microsoft SharePoint Services, Microsoft Silverlight, Microsoft Visio, Microsoft Visio Viewer, Microsoft Office Compatibility Pack, Microsoft Word, Microsoft Word Viewer, Microsoft PowerShell Core, Microsoft PowerShel, Microsoft Teams, Microsoft XML Core Services, Microsoft Windows Remote Management, Microsoft Pragmatic General Multicast, Microsoft Terminal Services (Remote Desktop Service), Microsoft Office InfoPath, Windows Defender, Windows Media Center, Microsoft Dynamics 365, Microsoft Power BI, Docker, Apache Log4j, SaltStack, KeePass, RabbitMQ, Node.js, Postfix, Oracle Java SE Development Kit, Git, Openssl, Python, PHP, Proxmox (Virtual Environment,, Backup Server, Mail Gateway), Kubernetes, PuTTY, WinSCP, Telegram Desktop, Wireshark, Jenkins, Adobe Flash Player, TightVNC Server, TightVNC Viewer, Foxit PDF Reader, Mattermost, Kaspersky Security Center, Kaspersky Anti-Virus, Kaspersky Endpoint Security, GitLab Community Edition (GitLab CE), GitLab Enterprise Edition (GitLab EE), IrfanView, Ruby, Kibana, Logstash и др. Поддерживается сканирование и поиск уязвимостей в Docker-контейнерах	Поддерживаются ОС семейств Windows и Linux
5.19. Поддержка интеграции с внешними сканерами уязвимостей (привести список сканеров);	Только Nmap.	Max Patrol 8	Поддерживается интеграция со сканерами безопасности: MaxPatrol 8, MaxPatrol VM, RedCheck, Nessus, Nexpose, OpenVAS, Qualys, Tenable SC	Не поддерживается	В составе решения применяется 21 внешний сканер	Не поддерживается	Поддерживаются Kaspersky Security Center, RedCheck, MaxPatrol 8, MaxPatrol VM, Qualys, Nessus, Nexpose (Rapid7), OpenVAS, Tenable.io, Tenable.sc	Не поддерживается
5.20. Поддержка указания источника данных об уязвимости в карточке уязвимости (название сканера, внешнего сервиса, реестра уязвимостей);	Поддерживается указание сканера, реестра уязвимостей	Поддерживается указание сканера, реестра уязвимостей	Поддерживается	Поддерживается через отображение свойств задачи сканирования в отчете (сканер)	Только в рамках функционала используемых внутри решения сканеров	Поддерживается указание реестра уязвимостей, описание уязвимости, описание возможных мер по устранению уязвимости, ссылок на рекомендации по устранению, ссылок на бюллетени НКЦКИ, ФинЦЕРТ	Поддерживается ведение истории получения данных об уязвимости, включая название источника, сканера, сервиса	Поддерживается отображение подробной информации об источнике в карточке уязвимости

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
5.21. Поддержка агрегации информации в карточке уязвимости из множества источников с тегированием (обозначением) той или иной информации от того или иного источника;	Не поддерживается	Поддерживаются данные из классификаторов уязвимостей БДУ, CVE	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Поддерживается
5.22. Поддержка ведения и отображения истории изменения свойств уязвимостей;	Не поддерживается	Поддерживается через историю изменения активов – ведется история состояния уязвимостей, найденных на активах	Поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
5.23. Нормализация данных об уязвимостях (при импорте из разных источников), тонкая настройка правил нормализации;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается нормализация данных, тонкая настройка правил нормализации с помощью графического low-code / no-code конструктора рабочих процессов	Не поддерживается
5.24. Дедупликация данных об уязвимостях (при импорте пересекающихся данных об уязвимостях), тонкая настройка правил дедупликации (например, по совпадению идентификатора, уязвимого ПО, описанию уязвимости и т.д.);	Поддерживается через правила идентификации узлов с неизменяемыми ключами идентификации (IP-адрес, FQDN-имя, NetBIOS-имя, имя экземпляра MSSQL, имя экземпляра Oracle)	Поддерживается вручную за счет выполнения запроса на языке PDQL	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается дедупликация данных, тонкая настройка правил дедупликации с помощью графического low-code / no-code конструктора рабочих процессов	Не поддерживается
5.25. Интеграция с внешними сервисами учета уязвимостей и эксплойтов (БДУ ФСТЭК России, NIST NVD, Microsoft, Vulners.com, VulDB.com, OpenCVE.io, AttackerKB, Exploit-DB и т.д.), получение от них обогащающих, актуализированных данных по уязвимостям (наличие эксплойта, ссылка на патч или исправленную версию ПО, рекомендации по минимизации риска эксплуатации, рекомендации от вендоров и ИБ-экспертов по устранению уязвимости и т.д.);	Поддерживаются сервисы учета уязвимостей БДУ, CVE, OSVDB, Bugtraq, вендорские (Cisco, RedHat RHSA, SuSE, Ubuntu, AIX, SAP)	Поддерживается интеграция с классификаторами уязвимостей БДУ, CVE. Указываются признаки "Эксплойт" (наличие публичного эксплойта для уязвимости), "Эксплойт подтвержден" (наличие подтвержденного эксплойта для веб-приложений). Указываются типы последствий, к которым может привести эксплуатация уязвимости: удаленное выполнение кода (RCE), повышение привилегий (LPE), отказ в обслуживании (DoS)	Интеграции с внешними сервисами и обогащение настраиваются отдельно	Поддерживается через свою базу, производится агрегация всех доступных источников для каждой уязвимости	Только в рамках функционала используемых внутри решения сканеров	Поддерживаются сервисы учета уязвимостей БДУ, CVE, вендорские, бюллетени НКЦКИ, ФинЦЕРТ	Поддерживаются следующие источники данных для обогащения информации об уязвимостях: БДУ ФСТЭК, NIST NVD, vulners.com, VulDB, OpenCVE, AttackerKB, Exploit-DB, бюллетени Astra Linux, Microsoft, RedHat, Ubuntu	Поддерживаются БДУ ФСТЭК России, NIST NVD, Microsoft, Exploit-DB
5.26. Поддержка работы с наиболее эксплуатируемыми уязвимостями: перечень трендовых уязвимостей от вендора, "Наиболее опасные уязвимости" БДУ ФСТЭК России, CISA "Known Exploited Vulnerabilities" и т.д., периодичность обновления и срок доставки перечня трендовых уязвимостей;	Не поддерживается	Поддерживается доставка информации о трендовых уязвимостях за 12 часов (на основе экспертизы вендора)	Поддерживается	Не поддерживается	Только в рамках функционала используемых внутри решения сканеров	Не поддерживается	Поддержка получения данных об опасных и популярных уязвимостях из БДУ ФСТЭК России, из списка CISA "Known Exploited Vulnerabilities"	Поддерживается импорт наиболее опасных уязвимостей из БДУ ФСТЭК, CISA KEV. Один раз в 3 часа формируется новый пакет уязвимостей
5.27. Функционал карточки уязвимости: отображение уровня критичности (по CVSS и по пользовательскому скорингу), статуса, применяемых политик обработки, идентификаторов (из различных реестров уязвимостей), связь с затронутым активом, оценка возможности эксплуатации (в том числе интерактивно из карточки уязвимости);	Отображение уровня критичности по CVSS, идентификаторов уязвимости	Поддерживается отображение уровня опасности, типа, описания уязвимости, способов устранения, метрик CVSS (v2, v3), ссылок на публичные базы данных (CVE, БДУ). Проставляются отметки "Важная", данные об имеющихся эксплойтах и возможных последствиях эксплуатации	Поддерживается настройка полей карточки уязвимости, отображение уровня критичности, статуса, применяемых политик обработки, идентификаторов (из БДУ, CVE), связь с затронутыми активами. Интерактивная оценка возможности эксплуатации не поддерживается, предоставляется только информации о наличии эксплойта / PoC по данным бюллетеней	Поддерживается	Не поддерживается	Отображение уровня критичности по CVSS, идентификаторов уязвимости, описания, ссылок на рекомендации по устранению	Поддерживается отображение всей доступной информации, идентификаторов, поддерживается переход к затронутым активам. Поддерживается оценка возможности эксплуатации из карточки уязвимости	Поддерживается отображение уровня критичности (по CVSS последней доступной версии), статуса, конфигурации уязвимости, рекомендаций, информации об эксплойте, маппинга на другие уязвимости и таблицы связанных активов, на которых данная уязвимость уже была найдена
5.28. Тегирование уязвимостей (исключения, напоминания, комментарии);	Не поддерживается	Поддерживается за счет функционала псевдонимов. Поддерживается присвоение меток уязвимостям для быстрого поиска, идентификации, категоризации	Поддерживается указание комментариев, тэгов для уязвимостей	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Поддерживается установка тегов, реализован механизм работы с ложными срабатываниями
5.29. Наличие механизма и методики автоматического подтверждения устраненных технических уязвимостей;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается в автоматическом режиме за счет повторного анализа актива после устранения уязвимостей.	Не поддерживается
5.30. Наличие преднастроенного механизма и методики проведения сканирования узлов только в определённые временные промежутки времени ("окна сканирования");	Поддерживается создание недопустимых интервалов сканирования и действий при их наступлении (приостановить, перезапустить, отменить, выполнить сканирование заново)	Поддерживается с помощью установки расписания задач сканирования	Промежутки сканирования настраиваются через расписания сканирования	Поддерживается указание расписаний заданий и запрещенные интервалы	Не поддерживается	Не поддерживается	Поддерживается задание расписаний, окон сканирования, с возможностью ожидания наступления и завершения сканирования в указанное окно. Поддерживается ограничение максимального времени сканирования актива	Поддерживается через настройки расписания задачи

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
5.31. Возможность управления уязвимостями (создание, изменение, удаление) и процессом сканирования через API решения;	Не поддерживается	Поддерживается выполнение PDQL-запросов, управление задачами сканирования (запуск, остановка, проверка состояния), управление профилями сканирования (создание, удаление, получение статуса)	Поддерживается	Поддерживается управление заданиями через REST API	Не поддерживается	Не поддерживается	Поддерживается	1) Возможность создавать и редактировать уязвимости в формате JSON, используя стандарты CPE 2.2 и 2.3, что обеспечивает совместимость с различными версиями программного обеспечения. 2) Поддержка задания условий для обнаружения уязвимостей через алгебраические выражения и логические операторы (например, AND, OR), что позволяет создавать сложные сценарии для более точного определения уязвимостей. 3) Возможность детализированного указания версий программного обеспечения, на которые распространяется уязвимость, для точного контроля диапазона версий. 4) Графический интерфейс для создания и редактирования условий проверки уязвимостей, который позволяет легко добавлять и удалять такие параметры, как "Название ПО", "Оператор" и "Версия". 5) Документация API доступна по адресу 0.0.0.0. При необходимости можно по API управлять сервисом поиска уязвимостей.
5.32. Возможность настройки прав доступа при взаимодействии с уязвимостями посредством API.	Не поддерживается	Поддерживается	Поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
6. Управление соответствием								
6.1. Настройка правил и логики проведения оценки соответствия активов, приведения в соответствие, проверки результатов приведения в соответствие;	Не поддерживается	Поддерживается с помощью политик для соответствия стандартам и для статусов несоответствий в модуле HCC	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается настройка правил и логики проведения оценки соответствия активов, приведения в соответствие, проверки результатов приведения в соответствие через графический low-code / no-code конструктор рабочих процессов. Настраивается расписание, частота, глубина сканирования на наличие уязвимостей	Поддерживается через функционал "Аудит конфигурации": 1) Возможность создания и редактирования правил аудита конфигурации в формате YAML, с указанием проверяемых параметров и используемых команд для проверки. 2) Поддержка различных операционных систем и сетевых устройств через универсальные команды (например, bash для Linux, PowerShell для Windows). 3) Возможность использования регулярных выражений и логических операторов для создания сложных условий проверки
6.2. Поддерживаемые стандарты: ГОСТ 57580, ГОСТ/ISO 27001, документы ФСТЭК России (Приказы 17, 21, 31, 235, 239), документы ФСБ РФ (Приказы 378, 367, 196), Положения ЦБ РФ (683-П, 716-П, 719-П, 757-П, 802-П), PCI DSS v.4 и т.д.;	Поддерживаются PCI DSS 2.0, PCI DSS 3.2.1, 3GPP Security Requirements, ИБ ISO/IEC 27001/27002, ИБ ISO/IEC 27002:2013, АС РД ФСТЭК, СТБ 34.101.68, приказ ФСТЭК № 239, СТО БР ИББС-1.0-2010, ГОСТ Р 57580.1-2017, GDPR Security Measures	Нет данных	Не поддерживается	Поддерживаются ГОСТ 57580, Приказы ФСТЭК 17,21,31,239, Методический документ ФСТЭК от 25.12.2022, PCI DSS 3.2.1	Не поддерживается	Не поддерживается	Поддерживаются стандарты, документы: 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	Не поддерживается

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
6.3. Поддерживаемые рекомендации: NIST SP 800-171, NIST SP 800-53, CIS Critical Security Controls, CIS Benchmarks, рекомендации Microsoft ("Recommended security configuration baselines" из пакета "Microsoft Security Compliance Toolkit"), рекомендации "Security Technical Implementation Guides" (STIGs), частные рекомендации производителей (ОС, ПО, оборудования, сетевых устройств), собственная экспертиза вендора;	Рекомендации из пакетов собственной экспертизы вендора, лучшие практики и стандарты безопасности CIS, SAP, VMware, всего более 180 технических стандартов безопасности	Стандарты PT Essentials (на основе экспертизы вендора). Стандарты для ОС (включая Astra Linux, ALT Linux, РЕД ОС, Windows, RHEL), гипервизоров (VMware), СУБД (MSSQL, Oracle, MariaDB, MySQL), сетевых устройств (Cisco, CheckPoint), контейнеров (Docker), прикладных систем (MS Exchange, 1C-Bitrix)	Не поддерживается	Поддерживаются вендорские рекомендации, рекомендации CIS, собственные экспертные рекомендации вендора (АЛТЭКС-СОФТ)	Не поддерживается	Не поддерживается	Поддерживаются CIS Critical Security Controls, CIS Benchmarks, рекомендации Microsoft, рекомендации вендоров, собственная экспертиза вендора	Поддерживаются шаблоны на базе рекомендаций CIS Benchmarks, Astra Linux, собственная экспертиза вендора
6.4. Поддержка добавления произвольных пользовательских требований, стандартов, рекомендаций;	Поддерживается добавление пользовательских стандартов	Поддерживается за счет написания пользовательских требований в файле формата YAML для модуля HCC	Не поддерживается	Частично, через XCCDF	Не поддерживается	Не поддерживается	Поддерживается добавление пользовательских требований, стандартов, рекомендаций, для которых можно проводить оценку соответствия	Поддерживается добавление произвольных требований в шаблоны и правила аудита конфигурации
6.5. Поддержка добавления произвольных пользовательских скриптов оценки выполнения требований;	Не поддерживается, соответствие требованиям оценивается только встроенными средствами (анализ реестра, файлов, конфигураций)	Поддерживается за счет скриптов расширения сбора данных в режиме Audit (Audit Extension)	Не поддерживается	Частично, через XCCDF	Не поддерживается	Не поддерживается	Поддерживается выполнение скриптов Batch, Bash, Java, JavaScript, PowerShell, Python	Поддерживается создание уникальных правил с помощью команд, условий и предусловий
6.6. Возможность изменения встроенных скриптов оценки выполнения требований;	Не поддерживается	Поддерживается за счет переопределения существующих требований, изменения значений по умолчанию в системных требованиях	Не поддерживается	Частично, через XCCDF	Не поддерживается	Не поддерживается	Поддерживается	Поддерживается возможность редактировать шаблоны (на базе старых создавать новые) и правила аудита конфигурации
6.7. Поддержка добавления произвольных пользовательских скриптов приведения актива в состояние соответствия;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
6.8. Возможность изменения встроенных скриптов приведения актива в состояние соответствия;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
6.9. Поддержка контроля множества допустимых значений параметра в рамках одной итерации оценки соответствия (например, проверить значения ключа реестра из множества значений {0,1,2} в рамках одной операции чтения соответствующей ветки реестра);	Не поддерживается, проверяется только одно значение в рамках одной итерации	Поддерживается за счет скриптов расширения сбора данных в режиме Audit (Audit Extension)	Не поддерживается	Частично, через XCCDF	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
6.10. Поддержка задания приоритета (веса) контролируемых параметров при расчете результирующей оценки соответствия;	Не поддерживается	Не поддерживается	Не поддерживается	Частично, через XCCDF	Не поддерживается	Не поддерживается	Поддерживается, формула расчета оценки соответствия корректируется в соответствии с требованиями пользователя.	Не поддерживается
6.11. Возможность указания определенных требований для определенного актива, информационной системы;	Поддерживается	Поддерживается	Не поддерживается	Частично, через профиль для конфигурации	Не поддерживается	Не поддерживается	Поддерживается, возможна корректировка набора требований из шаблона для конкретных активов и групп активов без необходимости создания нового набора требований	Не поддерживается
6.12. Возможность кастомизации существующих требований относительно определенного актива, информационной системы;	Поддерживается	Поддерживается	Не поддерживается	Частично, через профиль для конфигурации	Не поддерживается	Не поддерживается	Поддерживается, возможно изменение целевых значений для конкретных активов без необходимости создания нового требования	Не поддерживается
6.13. Возможность выполнения точечной переоценки по активу – по требованию, по группе требований;	Поддерживается	Не поддерживается	Не поддерживается	Частично, через профиль для конфигурации	Не поддерживается	Не поддерживается	Поддерживается выполнение оценки по конкретному требованию, группе требований, внутреннему стандарту (набор требований)	Не поддерживается

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
6.14. Скоринг соответствия: расчет оценки соответствия выбранным требованиям для каждого актива в отдельности, информационной системы, всей инфраструктуры в целом, возможность кастомизации формулы для расчета, непрерывный автоматический расчет оценки соответствия, перерасчет оценки соответствия для уже оцененных активов, информационных систем, инфраструктуры при изменении формулы расчета;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается расчет уровня критичности в момент сканирования	Не поддерживается	Не поддерживается	Поддерживается скоринг, кастомизация формулы скоринга, автоматический перерасчет скоринг-балла.	Не поддерживается
6.15. Поддержка ведения и отображения истории оценки соответствия (например, отображение истории изменения параметров реестра), использование собранных данных для проактивной оценки соответствия новым требованиям;	Поддерживается через выпуск дифференциальных, аналитических (сравнительных, динамических) отчетов	Поддерживается ведение истории данных о рассчитанных на активах требованиях	Не поддерживается	Поддерживается ведение истории сканирований	Не поддерживается	Не поддерживается	Поддерживается, с накоплением статистики и последующей аналитикой, визуализацией, отчетностью, оценкой трендов соответствия	Не поддерживается
6.16. Поддержка ведения и отображения истории выполненных действий (ручных, автоматических) по приведению в соответствие;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается, изменения на хост не вносятся сканером	Не поддерживается	Не поддерживается	Поддерживается	Поддерживается через вкладку "История" в задаче "Аудит конфигурации"
6.17. Возможность отмены действия (ручного, автоматического) по приведению в соответствие;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается, изменения на хост не вносятся сканером	Не поддерживается	Не поддерживается	Поддерживается в ручном и автоматическом режимах	Поддерживается только остановка действий через операторы действий ("Пауза" и "Стоп") для работы с запущенной задачей "Аудит конфигурации"
6.18. Возможность управления оценкой соответствия (создание, изменение, удаление, управление процессом оценки соответствия) через API решения;	Не поддерживается	Поддерживается выполнение PDQL-запросов, управление задачами сканирования (запуск, остановка, проверка состояния), управление профилями сканирования (создание, удаление, получение статуса)	Не поддерживается	Поддерживается управление заданиями через REST API	Не поддерживается	Не поддерживается	Поддерживается	Поддерживается управление сервисом аудита конфигурации по API
6.19. Возможность настройки прав доступа при взаимодействии с оценкой соответствия посредством API.	Не поддерживается	Поддерживается, API-доступ предоставляется с привилегиями пользователя, запросившего API-токен доступа	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается

Расширенные критерии

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"8	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
1. Общие технические характеристики								
1.1. Возможность использования решения как услуги (SaaS-модель);	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается, услуги предоставляют Партнеры с использованием RedCheck.	Поддерживается	Не поддерживается	Поддерживается	Не поддерживается
1.2. Поддержка работы решения в сетях, изолированных от Интернет;	Поддерживается за счет установки отдельного MaxPatrol Scanner в изолированном сегменте	Поддерживается за счет установки отдельного компонента MP 10 Collector в изолированном сегменте	Частично. Поддерживается только установка полной отдельной инсталляции в изолированном сегменте без возможности интеграции с основной инсталляцией	Поддерживается,офлайн активация и обновления	Поддерживается	Поддерживается только локальная установка на сканируемом устройстве	Поддерживается, для установки и функционирования решения не требуется доступ в сеть Интернет. Дополнительно, имеется возможность установки компонентов решения (сервисов) на выделенные серверы в изолированных сетях, с дальнейшим импортом результатов сканирования на основной сервер	Поддерживается работа в изолированных сетях. Обновление базы уязвимостей возможно через импорт архива, что позволяет поддерживать актуальность данных без непосредственного подключения к интернет
1.3. Открытость скриптов, алгоритмов, логики, моделей машинного обучения в решении, возможность их доработки и адаптации под требования конечного пользователя (в части подключения к проверяемым хостам, сбора данных, обработки и анализа данных, выполнения проверок и т.д.);	Не поддерживается	Поддерживается доработка PDQL-запросов, скриптов Windows PowerShell, сценариев командной оболочки Windows	Поддерживается настройка Python-скриптов	Поддерживается: инструменты, реализующие поиск уязвимостей и соответствие конфигураций безопасности, реализованы в соответствии с SCAP-стандартом, включающим стандартизированные языки описаний OVAL и XCCDF, возможна доработка и загрузка лент безопасности с доверенной подписью	Не поддерживается	Поддерживается загрузка пользовательских подписанных XML-файлов с OVAL-описаниями уязвимостей, выполненными в соответствии со стандартом "The OVAL Language Specification" версии не ниже 5.10.1	Поддерживается тонкая пользовательская настройка всех механизмов, скриптов, моделей машинного обучения с использованием механизмов low code / no code	Поддерживается возможность загрузки, изменения пользовательских скриптов на языке Lua. Поддерживается кастомизация формулы для расчета оценки влияния уязвимостей на информационную систему по методике ФСТЭК России

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"8	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
1.4. Поддержка работы решения из внешней / облачной инфраструктуры (возможность размещения выносного компонента сканера в DMZ, интернете, частном облаке для проведения инвентаризации и сканирования инфраструктуры извне);	Поддерживается за счет установки отдельного MaxPatrol Scanner в выделенных сегментах	Поддерживается за счет установки отдельного компонента MP 10 Collector в выделенных сегментах	Поддерживается возможность работы в выделенных сетевых сегментах, частных облаках, DMZ за счет установки отдельных коллекторов в них	Поддерживается, сервер сканирования может быть размещен в различных сегментах сети	Поддерживается	Поддерживается только локальная установка на сканируемом устройстве	Поддерживается возможность установки компонентов решения (сервисов) на выделенные серверы в облачных инфраструктурах	Поддерживается работа из внешней или облачной инфраструктуры, поддерживается настройка прокси-сервера для доступа к обновлениям баз уязвимостей. Поддерживается инсталляция в средах контейнеризации
1.5. Поддержка работы решения в режиме multitenancy: наличие встроенного функционала по разграничению данных по тенантам, возможность присвоения тенанта пользователю, возможность присвоения тенанта данным (активам, уязвимостям, проверкам, несоответствиям, задачам и т.д.), построение иерархии тенантов, возможность переключения пользователя между доступными тенантами, возможность присвоения пользователям разных тенантов одной функциональной роли.	Не поддерживается	Не поддерживается	Частично, средствами разграничения прав доступа на основе ролевой модели	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается, доступна иерархическая модель тенантов без ограничения глубины иерархии. Разграничение доступа пользователей к объектам и справочникам на основе организационной структуры (разграничение доступа к объектам дочерних и головных организаций). Возможность присвоения тенанта пользователям и данным. Возможность в интерфейсе пользователя переключаться между доступными тенантами. Возможно назначение пользователем одной роли разных тенантов	Не поддерживается
2. Общие организационные характеристики								
2.1. Наличие авторизованного обучения от вендора, стоимость обучения, длительность курса;	Обучение в учебных центрах на основе курсов от вендора	Обучение в учебных центрах на основе курсов от вендора	Обучение по курсам администрирования и использования решения, выдается сертификат вендора	Авторизованные курсы в специализированных учебных центрах	Не поддерживается	Не поддерживается	Поддерживается. Проводится бесплатное обучение в собственном учебном центре вендора с выдачей сертификата	Проводится обучение на коммерческом авторизованном курсе "Комплексное тестирование защищенности информационных систем с применением Сканер-ВС и Инспектор" в собственном учебном центре "Эшелон". Проводятся открытые бесплатные курсы по работе с решением для заказчиков и партнёров 1 раз в 3-4 месяца
2.2. Поддержка работы MSS-провайдеров с решением;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается, услуги предоставляют Партнеры с использованием RedCheck	Поддерживается	Не поддерживается	Поддерживается, предоставляются специальные лицензионные условия для провайдеров MSSP	Поддерживается через партнерскую сеть
2.3. Дорожная карта развития решения (планируемый к внедрению функционал и ориентировочные сроки реализации, планируемые изменения в лицензионную политику).	Закрытая	Закрытая	Закрытая	Планируется добавление компонентов: - аналитики/VM; - повышение производительности; - расширение сканируемых платформ, российские сетевые устройства, контейнеризация; - сегментационная модель управления; - использование нескольких УЗ в одной задаче; - настраиваемый повтор сканирования недоступных хостов	Закрытая	Закрытая	Планируется расширение использования технологий машинного обучения и искусственного интеллекта для предиктивной аналитики по уязвимостям и несоответствиям, для выдачи рекомендаций по оптимальным методам их обработки, автоматическому устранению уязвимостей и несоответствий	Планы на начало 2025 г.: создание дистрибутивов под РедОС, ОС Альт Сервер
3. Общий функционал всех решений (управление активами, управление уязвимостями, оценка соответствия)								
3.1. Минимизация прав доступа к инвентаризируемым, сканируемым и оцениваемым активам, использование технологий ограничения доступа (например, LAPS, sudo wrappers) и скриптов настройки конечных активов для сканирования с ограниченными правами доступа;	Поддерживается за счет тонкой настройки прав доступа на конечных устройствах с помощью vbs-скриптов от вендора (для Windows) и sudo-оберток для Linux	Поддерживается LAPS (только версии 6.2), технология sudo wrappers	Поддерживается за счет тонкой настройки прав доступа на конечных устройствах	Поддерживается использования sudo, возможно сканирование с минимальными правами и ограничением результата (не рекомендуется). Изменения на сканируемые хосты не вносятся, производятся только чтение и аудит	Только в рамках функционала используемых внутри решения сканеров	Не поддерживается	Поддерживается за счет тонкой настройки прав доступа на конечных устройствах. Для работы решения не требуются полные / администраторские права. Наличие документации по требуемым правам доступа	Не поддерживается
3.2. Гибкость механизмов фильтрации: возможность составлять сложные поисковые запросы (разные условия по различным атрибутам, объединение через логические операторы "И" или "ИЛИ"), поддержка языков запроса в решении (SQL-подобные, скриптовые);	Не поддерживается	Поддерживается создание, сохранение, использование PDQL-запросов ко всем объектам решения	Поддерживается фильтрация, составление SQL-запросов при построении отчетности	Поддерживается частично: имеются развернутые статичные механизмы фильтрации и отбора, предоставляется возможность экспорта в CSV для работы редакторах таблиц и средствах анализа	Не поддерживается	Не поддерживается	Поддерживается фильтрация и составление поисковых запросов в графическом интерфейсе с low-code / no-code конструктором запросов	Не поддерживается
3.3. Возможность создания кастомизированных отчетов с применением подхода low-code / no-code (в рамках единого интерфейса, без использования внешних утилит);	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается через применение шаблона отчета выборки и фильтрацию параметров в интерфейсе	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
3.4. Возможность создания пользовательских типов объектов в графическом конструкторе, с применением подхода low-code / no-code;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"8	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
3.5. Возможность кастомизации визуализации дашбордов, виджетов, меню интерфейса с применением подхода low-code / no-code;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
3.6. Поддержка использования подхода low-code / no-code для настройки правил и логики управления объектами решения (активами, уязвимостями, задачами, требованиями, документами, инцидентами);	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается, доступна только базовая настройка расписания выполнения задач через параметры в интерфейсе
3.7. Возможность создания персонального рабочего окружения исходя из процессов и бренда организации: кастомизация гридов, быстрых фильтров, карточек и жизненного цикла активов, уязвимостей, несоответствий с применением подхода low-code / no-code;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается кастомизация интерфейса, брендирование, добавление логотипов в графическом интерфейсе с low-code / no-code конструктором	Не поддерживается
3.8. Возможность создания произвольной структуры и наименования разделов основного меню решения для любой роли пользователя;	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается для ролей и отдельных пользователей	Не поддерживается
3.9. Наличие функционала "Рабочий календарь" (учет только рабочих дней / часов при создании различных задач и установки сроков их выполнения), формирование актуального производственного календаря на текущий год за счет интеграции с внешними интернет-сервисами;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается функционал рабочего календаря с учетом количества рабочих часов, выходных и праздников. Возможность указания параметров рабочего календаря для разных тенантов	Не поддерживается
3.10. Возможности технической экосистемы (единой технологической платформы): наличие опции совместной установки на одной платформе других модулей, например: модуля управления инцидентами, управления киберрисками, управления информацией о киберугрозах и т.д. (перечислить);	Не поддерживается	Поддерживается интеграция с MaxPatrol SIEM, PT NAD, PT XDR, MaxPatrol EDR	Поддерживается совместная работа на единой платформе в рамках экосистемы R-Vision EVO, включая решения TDP, UEBA, SOAR, SGRC, TIP, SIEM	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается совместная работа на единой платформе в рамках экосистемы Security Vision в составе модулей Security Vision SOAR, SGRC, TIP, UEBA, AD + ML, BCP, CM, RM	Поддерживается возможность передачи информации об активах и уязвимостях по протоколу syslog в SIEM
3.11. Выявление уязвимостей и несоответствий на основе внутреннего аналитического движка;	Поддерживается	Поддерживается	Не поддерживается	Не поддерживается	В решении используется 21 внешний сканер	Поддерживается, используется собственный движок для локального поиска уязвимостей на основе OVAL-описаний.	Поддерживается использование встроенного аналитического движка.	Не поддерживается
3.12. Наличие функционала и кастомизации механизма статистического анализа свойств объектов;	Не поддерживается	Поддерживается с использованием PDQL-запросов	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
3.13. Применение методов машинного обучения (наличие и количество предварительно настроенных и обученных моделей машинного обучения), возможность подстройки параметров моделей под конкретную инфраструктуру;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается использование преднастроенных и обученный моделей машинного обучения, с возможностью переобучения, ручного и автоматического подбора параметров моделей	Не поддерживается
3.14. Применение методов обработки Big Data.	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается за счет интеграции с "озерами данных" на основе Kafka, Hadoop, Elasticsearch и др	Не поддерживается
4. Управление активами								
4.1. Поддержка нотации Common Platform Enumeration (CPE) для описания обнаруженного программного и аппаратного обеспечения;	Поддерживается	Поддерживается	Поддерживается	Поддерживается	Только в рамках функционала используемых внутри решения сканеров	Поддерживается	Поддерживается	Поддерживается использование нотации Common Platform Enumeration (CPE) для описания программного обеспечения в процессе поиска уязвимостей
4.2. Поддержка использования подхода low-code / no-code для настройки правил и логики обнаружения, инвентаризации, классификации активов;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
4.3. Поддержка использования подхода low-code / no-code для настройки правил и логики управления активами в рамках их жизненного цикла (например, планирование, закупка, разработка, внедрение, эксплуатация, поддержка, модификация, вывод в резерв, вывод из эксплуатации, уничтожение);	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается, возможность формирования жизненного цикла и связанных процессов за счёт механизмов рабочих процессов. Возможно создание отдельного жизненного цикла для каждого типа актива	Не поддерживается

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"8	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
4.4. Поддержка использования подхода low-code / no-code для построения ресурсно-сервисной модели активов и инфраструктуры;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
4.5. Возможность инвентаризации docker-контейнеров;	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается аудит docker-образов	Не поддерживается	Не поддерживается	Поддерживается, как активных, так и остановленных контейнеров	Не поддерживается
4.6. Возможность инвентаризации выделенных сетевых сегментов посредством выносных коллекторов;	Поддерживается за счет установки отдельных компонент MaxPatrol Scanner	Поддерживается за счет установки отдельных компонент MP 10 Collector	Поддерживается за счет установки отдельных коллекторов	Поддерживается за счет установки дополнительного модуля сканирования.	Поддерживается	Поддерживается за счет установки отдельных локальных инсталляций решения.	Поддерживается за счет возможности установки компонентов решения (сервисов) на отдельные серверы в выделенных сегментах, с дальнейшим импортом результатов сканирования на основной сервер	Не поддерживается
4.7. Возможность выполнения офлайн-инвентаризации;	Поддерживается через функционал MaxPatrol Offline Scanner	Поддерживается за счет функционала мобильного сканера	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается за счет запуска отчуждаемых скриптов инвентаризации на конечных точках и импорта результатов, за счет агентской инвентаризации	Поддерживается возможность выполнения офлайн-инвентаризации через Live-USB для локальной инвентаризации активов без необходимости подключения к сети (специальная редакция Сканер-ВС 7)
4.8. Возможность управления "белыми" и "чёрными" списками ПО;	Поддерживается	Поддерживается	Поддерживается частично	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
4.9. Отслеживание вышедших из эксплуатации хостов (контроль устаревания).	Не поддерживается	Поддерживается	Поддерживается частично	Поддерживается в рамках функции "Аналитика"	Не поддерживается	Не поддерживается	Поддерживается, с возможностью настройки периода неактивности	Не поддерживается
5. Управление уязвимостями								
5.1. Возможность настройки в соответствии с положениями ГОСТ Р 56546-2015 "Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем" в части предустановленной в решении классификации уязвимостей по типам и возможным местам возникновения (проявления);	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Поддерживается настройка в соответствии с ГОСТ Р 56546-2015
5.2. Возможность настройки в соответствии с положениями Методического документа ФСТЭК России от 17 мая 2023 г. "Руководство по организации процесса управления уязвимостями в органе (организации)" в части настройки процесса управления уязвимостями, предустановленного в решении;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Частично поддерживается за счет предоставления информации для оценки рисков на основе метрики EPSS, наличия эксплойта и рекомендаций по устранению от БДУ ФСТЭК. Отслеживание процесса устранения и контроля эффективности мер возможно через повторный запуск задач инвентаризации и поиска уязвимостей и визуального сопоставления
5.3. Возможность настройки в соответствии с положениями Методического документа ФСТЭК России от 28 октября 2022 г. "Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств" в части порядка оценки уровня критичности уязвимостей, предустановленного в решении;	Не поддерживается	Поддерживается формула расчета критичности по методике ФСТЭК (с помощью настраиваемого PDQL-запроса)	Поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Поддерживается расчёт показателя "Оценка влияния уязвимостей на ИС" в соответствии с методическим документом ФСТЭК России "Методика оценки уровня критичности уязвимостей программных и программно-аппаратных средств" от 28 октября 2022 года
5.4. Возможность поддержки создания инцидентов на основе обнаруженных уязвимостей, отправка сформированных инцидентов в сторонние системы (SIEM), синхронизация статусов инцидентов;	Не поддерживается	Поддерживается за счет интеграции с MaxPatrol SIEM	Поддерживается создание инцидентов в системе R-Vision SOAR, поддерживается отправка информации, синхронизация статусов с совместимыми SIEM: ArcSight ESM, ArcSight Logger, IBM QRadar, MaxPatrol SIEM	Поддерживается запрос результатов по API и создание триггеров на инциденты	Через API	Не поддерживается	Поддерживается создание инцидентов в системе Security Vision SOAR/NG SOAR, поддерживается отправка информации, синхронизация статусов с совместимыми SIEM: Kaspersky KUMA, MaxPatrol SIEM, Pangeo RADAR, RuSIEM, NEURODAT SIEM, ArcSight SIEM, IBM QRadar, Splunk	Поддерживается отправка информации об уязвимостях в SIEM через syslog, что позволяет формировать инциденты на основе обнаруженных уязвимостей
5.5. Возможность указывать ограничение максимального времени проведения сканирования активов на наличие уязвимостей;	Поддерживается	Поддерживается	Не поддерживается	Поддерживается настройка запрещенных интервалов сканирования (пауза) и завершение сканирования (остановка) по истечению указанного времени	Не поддерживается	Не поддерживается	Поддерживается задание таймаутов для каждого хоста. Возможно указание разных таймаутов в рамках разных задач сканирования.	Не поддерживается
5.6. Наличие механизма и методики автоматического возвращения закрытых задач на устранение уязвимостей обратно в работу;	Не поддерживается	Поддерживается	Поддерживается через настройку политик управления уязвимостями	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается через графический low-code / no-code конструктор рабочих процессов	Не поддерживается

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"8	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
5.7. Создание задач на основе обнаруженных уязвимостей, отправка сформированных задач в сторонние системы (Service Desk, ITSM), синхронизация статусов задач;	Не поддерживается	Поддерживается через API	Поддерживается создание задач в решении и отправка, синхронизация с совместимыми таск-трекинговыми системами	Не поддерживается	Через API	Не поддерживается	Поддерживается создание задач в решении и отправка, синхронизация с совместимыми таск-трекинговыми системами	Не поддерживается
5.8. Поддержка ретроспективного анализа: ведение и отображение динамики уязвимостей, соблюдения политик обработки, устранения и сканирования, соблюдения SLA-метрик;	Поддерживается через формирование аналитических, дифференциальных отчетов	Поддерживается через PDQL-запросы	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
5.9. Поддержка детальной работы с критичными уязвимостями: проверка эксплуатируемости (в реальных условиях) и приоритизация уязвимостей, обнаруженных на периметре, для которых есть работающий эксплойт, эксплуатируемых удаленно, трендовых, Zero Day;	Поддерживается частично путем проверки уязвимостей в режиме "Pentest"	Поддерживается частично путем проверки уязвимостей в режиме "Pentest", путем проверки эксплуатируемости веб-уязвимостей	Поддерживается	Поддерживается отображение ссылок на публично известные эксплойты (информация об эксплойтах) в обнаруженных уязвимостях	Нет данных	Не поддерживается	Поддерживается	Поддерживается: в карточке уязвимости приводится информация о наличии эксплойтов, оценке EPSS, включения в каталог KEV (CISA Known Exploited Vulnerabilities)
5.10. Экспертные рекомендации по управлению уязвимостями, включая интерактивные подсказки оператору;	Не поддерживается	Поддерживается отображение рекомендаций по устранению уязвимостей, в том числе вендорские рекомендации	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается отображение рекомендаций по устранению уязвимостей в карточке уязвимости	Поддерживается формирование и отображение экспертных рекомендаций пользователю	Не поддерживается
5.11. Возможность сопоставления выявленных уязвимостей с тактиками и техниками атакующих по фреймворку MITRE ATT&CK;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
5.12. Возможность сопоставления выявленных уязвимостей с индикаторами компрометации и индикаторами атак;	Не поддерживается	Поддерживается за счет интеграции с PT Threat Analyzer, PT Feeds	Поддерживается за счет интеграции с функционалом R-Vision TIP	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается за счет интеграции с функционалом Security Vision TIP.	Не поддерживается
5.13. Возможность сопоставления сведений об уязвимостях с релевантной информацией об инцидентах на просканированном активе, корректирование способа и приоритета обработки уязвимости;	Не поддерживается	Поддерживается за счет интеграции с MaxPatrol SIEM	Поддерживается за счет интеграции с функционалом R-Vision SOAR, SIEM	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается за счет интеграции с функционалом Security Vision SOAR	Не поддерживается
5.14. Возможность учета сетевой достижимости активов с уязвимостями, оценка возможности реальной эксплуатации;	Не поддерживается	Поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
5.15. Возможность поддержки технологии динамических сценариев обработки уязвимостей;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается частично за счет применения динамических профилей к сканированию или построению отчета по уязвимостям	Не поддерживается	Не поддерживается	Поддерживается через графический low-code / no-code конструктор рабочих процессов	Не поддерживается
5.16. Возможность создания политик допустимых действий по обработке уязвимостей в отношении определенных объектов (активов, информационных систем);	Не поддерживается	Поддерживается настройка глобальных исключений для всех задач	Не поддерживается	Поддерживается применение профиля уязвимостей для исключения при построении отчета	Не поддерживается	Не поддерживается	Поддерживается через графический low-code / no-code конструктор рабочих процессов	Не поддерживается
5.17. Поддержка использования подхода low-code / no-code для настройки правил и логики политик сканирования на наличие уязвимостей, политик обработки уязвимостей, правил контроля устранения уязвимостей и постановки задач на обработку уязвимостей в ИТ/ИБ/бизнес-подразделения, включая настройку расписания сканирований, настройку глубины и частоты сканирования в зависимости от свойств активов, настройку SLA-метрик обработки уязвимостей;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается частично за счет возможности в интерфейсе определять сканирование с помощью применения статических и динамических профилей уязвимостей, настройки расписания сканирования и запрещенных интервалов	Не поддерживается	Не поддерживается	Поддерживается через графический low-code / no-code конструктор рабочих процессов	Не поддерживается
5.18. Поддержка использования подхода low-code / no-code для настройки правил и логики управления уязвимостями в рамках их жизненного цикла (например: новая, обрабатывается, ложное срабатывание, исключена, принята, минимизирована, устранена, закрыта), поддержка ручного и автоматического изменения статуса для отдельной уязвимости и группы уязвимостей;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается через графический low-code / no-code конструктор рабочих процессов	Не поддерживается

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"8	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
5.19. Возможность интеграции с ФинЦЕРТ, ГосСОПКА (получение и обработка уведомлений об уязвимостях);	Не поддерживается	Поддерживается при наличии дополнительного продукта "ПТ Ведомственный центр"	Поддерживается	Поддерживается частично за счет обработки отдельных меток FinCERT и NKCKI на выявленных уязвимостях	Нет данных	Поддерживается	Поддерживается	Не поддерживается
5.20. Визуализация и отчетность по задачам на устранение уязвимостей для ИТ-подразделений, с учетом метрик и положений ITIL, CoBIT, ITSM и т.д.;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается в рамках функционала составления отчетности	Не поддерживается	Поддерживается	Не поддерживается
5.21. Возможность офлайн-сканирования на наличие уязвимостей при отсутствии доступа к сканируемым хостам;	Не поддерживается	Поддерживается за счет функционала мобильного сканера	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается за счет запуска отчуждаемых скриптов сканирования на конечных точках и импорта результатов, за счет агентского сканирования	Не поддерживается
5.22. Возможность сканирования на уязвимости docker-контейнеров;	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается аудит образов docker	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
5.23. Возможность сканирования как запущенных, так и не запущенных контейнеров;	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается аудит образов docker, контейнеры не поддерживаются	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
5.24. Возможность автоматического обновления версии уязвимого ПО.	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается запуск файла-установщика обновленной версии ПО на конечных точках	Не поддерживается
6. Управление соответствием								
6.1. Поддержка ретроспективного анализа: ведение и отображение динамики соответствия требованиям, приведения в соответствие, проверки результатов приведения в соответствие, соблюдения SLA-метрик;	Поддерживается через формирование аналитических, дифференциальных отчетов	Поддерживается через PDQL-запросы	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается за счет накопления истории и аналитики динамики изменения свойств объектов, статистической информации о состоянии инфраструктуры	Не поддерживается
6.2. Поддержка детальной работы с критичными несоответствиями: проверка эксплуатируемости и приоритизация несоответствий, выявленных на периметре, эксплуатируемых удаленно;	Поддерживается частично путем проверки несоответствий в режиме "Pentest"	Поддерживается частично путем проверки несоответствий в режиме "Pentest"	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается проверка эксплуатируемости несоответствий, их приоритизация	Не поддерживается
6.3. Поддержка восстановления конфигураций активов в эталонные безопасные значения в ручном и автоматическом режимах для соответствия требованиям;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживаются в ручном и автоматическом режиме за счет запуска скриптов на конечных точках	Не поддерживается
6.4. Возможность создания политик допустимых действий по устранению несоответствий в отношении определенных объектов (активов, информационных систем);	Не поддерживается	Не поддерживается	Не поддерживается	Частично, через профиль конфигурации безопасности на основе существующих со своими эталонными значениями или импорт собственной конфигурации XCCDF	Не поддерживается	Не поддерживается	Поддерживается через графический low-code / no-code конструктор рабочих процессов.	Не поддерживается
6.5. Возможность поддержки технологии динамических сценариев устранения несоответствий;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
6.6. Возможность сопоставления выявленных несоответствий с тактиками и техниками атакующих по фреймворку MITRE ATT&CK;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается за счет интеграции с базой MITRE ATT&CK	Не поддерживается
6.7. Возможность сопоставления выявленных несоответствий с индикаторами компрометации и индикаторами атак;	Не поддерживается	Поддерживается за счет интеграции с PT Threat Analyzer, PT Feeds	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается за счет интеграции с функционалом Security Vision TIP	Не поддерживается
6.8. Возможность сопоставления сведений о несоответствии с релевантной информацией об инцидентах на просканированном активе, корректирование способа и приоритета устранения несоответствия;	Не поддерживается	Поддерживается за счет интеграции с MaxPatrol SIEM	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается за счет интеграции с функционалом Security Vision SOAR/NG SOAR	Не поддерживается
6.9. Поддержка использования подхода low-code / no-code для настройки правил и логики проведения оценки соответствия активов;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается
6.10. Визуализация и отчетность по задачам на приведения в соответствие для ИТ-подразделений, с учетом метрик и положений ITIL, CoBIT, ITSM и т.д;	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается в рамках функционала составления отчетности	Не поддерживается	Поддерживаются рекомендации и метрики ITIL, CoBIT	Не поддерживается

Название продукта, производителя	MaxPatrol 8 АО "Позитив Текнолоджиз"8	MaxPatrol VM АО "Позитив Текнолоджиз"	R-Vision VM ООО "Р-Вижн"	RedCheck АО "Алтэкс-Софт"	ScanFactory VM ООО "СКАНФЭКТОРИ"	ScanOVAL Разработчик: АО "Алтэкс-Софт" Правообладатель: ФАУ "ГНИИИ ПТЗИ ФСТЭК России"	Security Vision VM ООО "Интеллектуальная безопасность"	Сканер-ВС 7 АО "НПО "Эшелон"
6.11. Возможность офлайн-сканирования на наличие несоответствий при отсутствии доступа к сканируемым хостам;	Не поддерживается	Поддерживается за счет функционала мобильного сканера	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается за счет запуска скриптов сканирования на конечных точках, за счет агентской инвентаризации	Не поддерживается
6.12. Автоматическое определение применимых требований для хостов.	Не поддерживается	Поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Не поддерживается

Выводы

В сравнении принимали участие продукты для управления уязвимостями, которые в большей или меньшей мере реализуют инвентаризацию активов, сканирование их на наличие уязвимостей, оценку конфигураций и выявление несоответствий требованиям ("комплаенс"). При этом были выявлены следующие особенности и ограничения:

- ScanOVAL: данное решение идет "вне конкурса", поскольку это бесплатный продукт для локального анализа наличия уязвимостей, которое, тем не менее, поддерживает работу на Windows и на самых популярных отечественных Linux-системах. Однако, ScanOVAL лишен большинства функций, которые можно ожидать от системы управления уязвимостями - отсутствует функционал работы с активами и управлением соответствием требованиям.
- MaxPatrol 8: данный продукт уже давно стал классикой во многих организациях, но сейчас производитель Positive Technologies сосредоточил свои усилия на развитии MaxPatrol VM. В решении MaxPatrol 8 отсутствует полноценное управление активами, и отсутствует режим multitenancy, при этом режим "Compliance" предоставляет достаточные возможности по созданию пользовательских проверок, а стандарты из пакетов экспертизы вендора позволяют оценить безопасность конфигураций широкого круга ПО. Однако, решение устанавливается только на ОС Windows и отсутствует информация о планах по переводу MaxPatrol 8 на Linux.
- ScanFactory VM: данное решение, по заверениям вендора, объединяет в себе функционал 21 различного сканера уязвимостей, поддерживает режим multitenancy, может быть использовано в виде SaaS. Однако, остается открытым вопрос с лицензионной чистотой подобного подхода с объединением различных сканеров, в том числе коммерческих, в один продукт. Кроме того, у решения нет сертификата ФСТЭК России, и его получение может быть осложнено ввиду использования "под капотом" ряда зарубежных сканеров.
- RedCheck: продукт от компании АЛТЭКС-СОФТ, которая ведет свой репозиторий ИБ-контента OVALdb. Сканером поддерживаются агентский и безагентский режимы работы, а также описания уязвимостей и требований в форматах OVAL и XCCDF. К сожалению, в решении отсутствует управление активами, а также нет полноценного функционала управления выявленными уязвимостями - например, назначения и контроля задач на устранение уязвимостей. В сканирующем ядре используется проверенный годами, но внешний сервис nmap, на продукт есть действующий сертификат ФСТЭК России.
- R-Vision VM: данное решение также использует в качестве сканирующего ядра внешний сервис nmap, сертифицировано ФСТЭК России, обладает функционалом API интеграций и является частью экосистемы R-Vision EVO. Однако, у решения отсутствует функционал управления соответствием (режим "Compliance"), нет возможности построения полноценной ресурсно-сервисной модели инфраструктуры, а также отсутствует функционал проведения инвентаризации и сканирования в изолированных сетевых сегментах и поиск уязвимостей в веб-приложениях.
- Сканер-ВС 7: в этом решении сбор информации об установленном на активе программном обеспечении возможен посредством сетевого сканирования, также реализована возможность создания пользовательских шаблонов для compliance-проверок различных ОС, СЗИ, сетевого оборудования. Имеются готовые шаблоны от вендора, которые позволяют оценить безопасность конфигураций широкого круга ПО. База уязвимостей обновляется несколько раз в сутки. Сертификат ФСТЭК России для Сканер-ВС 7 на момент написания обзора отсутствует.
- MaxPatrol VM: данное сертифицированное ФСТЭК решение интегрируется в экосистему продуктов Positive Technologies – продукты PT работают с продуктами PT, в этом есть и плюс, но есть и минус – если Заказчик использует продукты разных вендоров. Описания уязвимостей дополнены собственной экспертизой команды PT Expert Security Center. Кроме того, в течение 12 часов в решение поступают описания для наиболее критичных (трендовых) уязвимостей. Режим "Compliance" реализуется отдельным продуктом HCC (host compliance control) и позволяет выявлять несоответствия конфигураций лучшим практикам, количество профилей (проверок) небольшое – порядка 15. Отсутствует режим multitenancy, что делает невозможным использования в MSSP архитектуре. Также, большинство глубоких настроек в решении выполняется с помощью PDQL-запросов, что повышает уровень требований к администратору системы, а также отсутствует функционал автоматического устранения уязвимостей (например, через установку патча на уязвимом устройстве) и изменения небезопасных конфигураций.
- Security Vision VM: этот сертифицированный ФСТЭК продукт использует собственный движок для поиска уязвимостей, интегрируется в платформенную экосистему Security Vision и предлагает инструменты Low-code и No-code для кастомизации и создания своего функционала. Поддерживается интеграция с внешними аналитическими сервисами для получения дополнительной информации об уязвимостях, сканирование Docker-контейнеров и работа в изолированных сетях. Кроме того, решение позволяет выстраивать логику управления уязвимостями в зависимости от множества свойств активов, инфраструктуры и самих уязвимостей, а также автоматически устанавливать патчи для устранения уязвимостей и менять конфигурации устройств. Подобный функционал позволяет выстроить полноценный процесс управления уязвимостями – от инвентаризации и классификации активов, обнаружения уязвимостей и небезопасных конфигураций до принятия решения по уязвимости / несоответствию, автоматического патчинга, контроля результатов, визуализации и отчетности.

Редакция благодарит за помощь в подготовке обзора:

Дмитрия Чернякова, руководителя отдела по работе с партнерами и клиентами "АЛТЭКС-СОФТ", и команду "АЛТЭКС-СОФТ"

Романа Овчинникова, директора департамента внедрения Security Vision

Андрея Амираха, руководителя отдела технического пресейла Security Vision

Леднёва Данилу Владимировича, специалиста группы внедрения средств защиты информации ГК "Эшелон"

Лишке Николая Викторовича, директора центра кибербезопасности ГК "Эшелон"

Павла Попова, лидера практики продуктов для управления уязвимостями Positive Technologies

Дениса Матюхина, руководителя продукта MaxPatrol VM Positive Technologies

Андрея Селиванова, продакт-менеджера R-Vision VM