

MaxPatrol VM

Система для управления
уязвимостями

ВОЗМОЖНОСТИ MaxPatrol VM

Постоянно актуализирует данные об IT-инфраструктуре. MaxPatrol VM получает наиболее полную информацию об активах за счет активного и пассивного сбора данных

Автоматизирует управление активами. Система автоматически идентифицирует активы, позволяет оценить их важность, распределить по группам, контролировать сканирование и устаревание

Выявляет и приоритизирует уязвимости. На основе постоянно обновляемой базы знаний MaxPatrol VM оценивает уровень защищенности активов

Выстраивает процесс управления уязвимостями. Позволяет задать политики сканирования и устранения уязвимостей и контролировать их соблюдение

Отслеживает трендовые уязвимости. Команда экспертов Positive Technologies предоставляет информацию о самых актуальных критически опасных уязвимостях в течение 12 часов

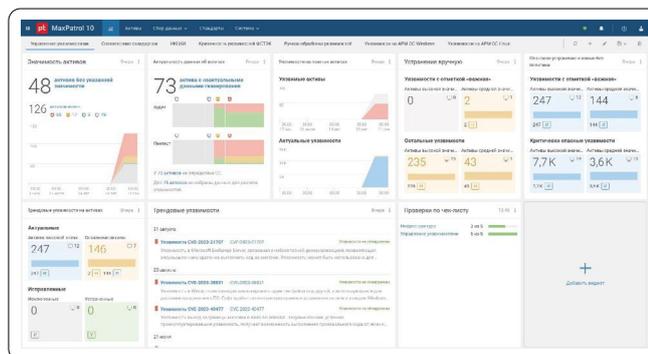
MaxPatrol VM — система, которая поможет выстроить полноценный процесс управления уязвимостями и сделать проникновение в сеть сложным и дорогим для злоумышленника. **Современное решение с гарантированным сроком доставки информации о трендовых уязвимостях — 12 часов.**

В основе MaxPatrol VM лежит уникальная технология управления активами, security asset management (SAM). С ее помощью MaxPatrol VM собирает данные в активном и пассивном режимах, идентифицирует активы по множеству параметров и на их основе строит актуальную модель IT-инфраструктуры. Таким образом, решение показывает специалисту по ИБ, как выглядит защищаемая IT-среда. Опираясь на это, он сможет выстроить и автоматизировать процесс управления уязвимостями, оценивая значимость компонентов сети для бизнес-процессов во всех системах компании и учитывая изменения инфраструктуры.

В MaxPatrol VM разделены сбор информации об активах и определение уязвимостей. Решение запоминает результаты предыдущих сканирований активов и на основе этого автоматически высчитывает применимость новой уязвимости к узлам сети.

Это позволяет без дополнительного сканирования обнаружить новые уязвимости и реагировать на них гораздо быстрее — сразу же приступать к устранению или применять компенсирующие меры.

Модуль MaxPatrol HCC в MaxPatrol VM позволяет проверить инфраструктуру на соответствие стандартам практической информационной безопасности. Благодаря ему можно отслеживать на динамических дашбордах выполнение самых важных требований в отношении активов, вносить изменения в проверки с учетом специфики компании, а также устанавливать сроки устранения несоответствий.



Интерактивный дашборд MaxPatrol VM



ПРЕИМУЩЕСТВА MaxPatrol VM

Глубокая интеграция

с продуктами классов SIEM и NTA и взаимное обогащение информацией об активах

Комплексное понимание

IT-среды благодаря уникальной технологии выявления активов

Оперативное выявление

уязвимостей без повторного сканирования за счет хранения информации об активах

Поддержка экспертов

и оповещение об особо опасных уязвимостях в течение 12 часов

Максимальная автоматизация

управления и анализа защищенности активов

ПРОВЕДИТЕ ПИЛОТНОЕ ВНЕДРЕНИЕ



Оцените возможности MaxPatrol VM на вашей инфраструктуре —

заполните заявку на сайте и начните выстраивать процесс управления уязвимостями

С помощью MaxPatrol VM можно:

- получать полные и актуализируемые данные о составе IT-инфраструктуры;
- учитывать значимость защищаемых активов;
- выявлять, приоритизировать и задавать правила обработки уязвимостей;
- оперативно выявлять новые опасные уязвимости;
- контролировать устранение уязвимостей и отслеживать общее состояние защищенности компании.

Как работает

Собирает и актуализирует базу активов

MaxPatrol VM собирает наиболее полную информацию об активах. База пополняется за счет сканирования в режиме черного и белого ящика и импорта данных из различных источников: внешних каталогов (Active Directory, SCCM, гипервизоров) и других средств ИБ (SIEM- и NTA-систем по результатам анализа событий и трафика). Запатентованный алгоритм идентификации активов позволяет сводить воедино информацию об одном и том же сетевом узле, даже если она получена из разных источников.

Оценивает и классифицирует активы

Классификация активов по уровню значимости помогает сконцентрироваться на работе с приоритетными узлами и отслеживать появление новых активов. Кроме того, система сообщает о неоцененных активах и подсказывает потенциально значимые.

Выявляет и приоритизирует уязвимости

MaxPatrol VM проводит глубокую проверку IT-инфраструктуры: выявляет уязвимости и ошибки конфигурации компонентов информационных систем, позволяет задавать способы устранения уязвимостей, учитывая уровень их опасности и другие характеристики (производителя, версию ОС, параметры актива, на котором они обнаружены).

Определяет политики

Политики сканирования и устранения уязвимостей в MaxPatrol VM позволяют автоматизировать выполнение различных операций с активами и найденными уязвимостями. Например, можно задать расписание сканирования или дату плановой обработки уязвимости на множестве активов.

Отслеживает трендовые уязвимости

Информация об актуальных уязвимостях, которую поставляют эксперты Positive Technologies в течение 12 часов, позволяет оперативно выявлять их в инфраструктуре, а также планировать приоритетное сканирование тех систем, где они могут присутствовать.

Контролирует управление уязвимостями

MaxPatrol VM отслеживает динамику показателей регулярных сканирований: эта информация помогает специалистам по ИБ контролировать качество сканирования. Кроме того, с помощью ретроспективного анализа можно оценить ход устранения уязвимостей, контролировать соблюдение политик и степень защищенности инфраструктуры.

ptsecurity.com
pr@ptsecurity.com

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400».

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 185 тысяч акционеров.

Следите за нами в соцсетях ([Telegram](#), [ВКонтакте](#), [Twitter](#), [Хабр](#)) и в разделе «Новости» на сайте ptsecurity.com, а также подписывайтесь на телеграм-канал [IT's positive investing](#).