POSITIVE TECHNOLOGIES

MaxPatrol VM

Система нового поколения для управления уязвимостями

ВОЗМОЖНОСТИ MAXPATROL VM

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

Автоматизирует управление активами. Система автоматически идентифицирует активы, позволяет оценить 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 по сканированию и устранению уязвимостей, контролировать их соблюдение.

Отслеживает трендовые уязвимости. Команда экспертов PT поставляет информацию о самых актуальных критически опасных уязвимостях.

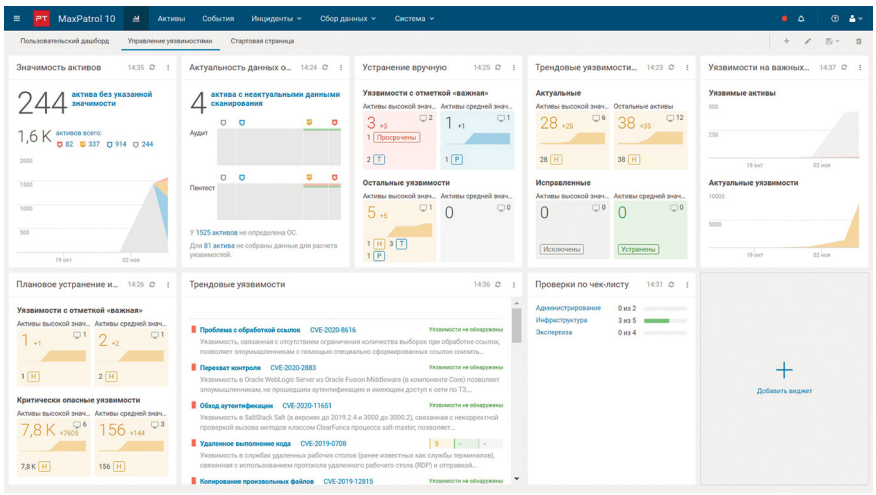
MaxPatrol VM позволяет построить полноценный процесс управления уязвимостями и контролировать защищенность IT-инфраструктуры в каждый момент времени.

В основе MaxPatrol VM лежит **уникальная технология управления активами** Security Asset Management (SAM). Благодаря ей 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 ИБ-специалисту, как выглядит защищаемая IT-среда. Опираясь на это, он сможет выстроить и автоматизировать процесс управления уязвимостями, оценивая значимость компонентов сети для бизнес-процессов и охватывая все системы компании, с учетом изменений инфраструктуры.

Система MaxPatrol VM построена на базе единой платформы MaxPatrol 10, которая объединяет продукты Positive Technologies для полной прозрачности сети и мониторинга безопасности. Продукты в составе MaxPatrol 10 обогащают друг друга данными об активах, что позволяет наиболее полно оценивать защищенность IT-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.



Интерактивный дашборд MaxPatrol VM

ПРЕИМУЩЕСТВА MAXPATROL VM

Часть единой платформы безопасности MaxPatrol 10 для глубокой интеграции с продуктами класса SIEM и NTA и взаимного обогащения информацией об активах

Глубокое понимание IT-среды за счет уникальной технологии выявления активов

Оперативное выявление уязвимостей без повторного сканирования за счет хранения информации об активах

Поддержка экспертов и оповещение об особо опасных уязвимостях

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 экспертизы Positive Technologies

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, гипервизоры) и других ИБ-решений (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. Также 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 параметры — производителя, версию ОС, параметры актива, на котором они обнаружены.

ОПРЕДЕЛЯЕТ ПОЛИТИКИ

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

ОТСЛЕЖИВАЕТ ТРЕНДОВЫЕ УЯЗВИМОСТИ

Информация об актуальных уязвимостях, которую поставляют эксперты Positive Technologies, позволяет оперативно выявлять особо опасные уязвимости в инфраструктуре, а также планировать приоритетное сканирование тех систем, где они потенциально могут присутствовать.

КОНТРОЛИРУЕТ УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

MaxPatrol VM отслеживает динамику показателей регулярных сканирований, эта информация помогает специалистам по ИБ контролировать качество сканирования. Также с помощью ретроспективного анализа можно оценить прогресс по устранению уязвимостей, контролировать соблюдение политик и степень защищенности инфраструктуры.

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies уже 19 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях (Facebook, ВКонтакте, Twitter), а также в разделе «Новости» на сайте ptsecurity.com.