POSITIVE TECHNOLOGIES

MaxPatrol 8 и MaxPatrol VM. Новый подход к управлению уязвимостями

Архитектурные и функциональные различия двух средств vulnerability management

MaxPatrol 8

Система контроля защищенности и соответствия стандартам безопасности.

В основе MaxPatrol 8 лежат механизмы тестирования на проникновение, системных проверок и контроля соответствия стандартам.

MaxPatrol 8 позволяет:

- своевременно обнаружить уязвимости информационной системы;
- провести комплексный анализ сетевого оборудования, операционных систем, СУБД, прикладных и ERP-систем, веб-приложений;
- контролировать соответствие основным стандартам информационной безопасности (ISO 27001, PCI DSS, стандарты CIS).

MaxPatrol VM

Система управления уязвимостями.

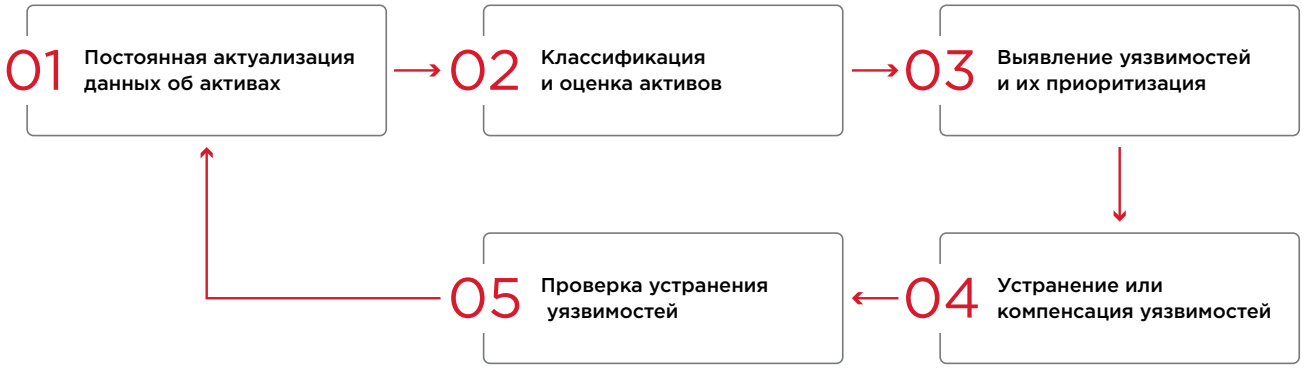
MaxPatrol VM позволяет контролировать защищенность IT-инфраструктуры в реальном времени. Выстраивает полноценный процесс управления уязвимостями и делает его более удобным для специалистов по ИБ. Стандартные процедуры занимают меньше времени.

С помощью MaxPatrol VM можно:

- полностью контролировать IT-инфраструктуру за счет регулярной актуализации данных;
- выявлять новые уязвимости без повторного сканирования;
- приоритизировать уязвимости и задавать правила их обработки для IT-отдела;
- контролировать устранение уязвимостей и отслеживать общее состояние защищенности корпоративной инфраструктуры;
- быть в курсе трендовых уязвимостей и учитывать их в работе. Эксперты Positive Technologies поставляют информацию о наиболее опасных уязвимостях, которые в данный момент используются злоумышленниками в атаках. Это помогает вовремя проводить проверку значимых активов компании.

Процесс управления уязвимостями в MaxPatrol 8 и MaxPatrol VM

На каждом этапе процесса у продуктов есть функциональные особенности. Рассмотрим их.



Этап 1. Инвентаризация IT-инфраструктуры

Помогает определить и просканировать все активы компании (элементы инфраструктуры, подключенные к сети).

	MaxPatrol 8	MaxPatrol VM
Что сканирует в инфраструктуре	▪ IP-адрес	▪ Актив. Более 3000 параметров (FQDN, MAC- и IP-адреса, тип ОС, имя сетевого узла, признаки виртуальности узла и т. п.) собираются и обрабатываются с помощью запатентованной технологии идентификации ▪ Хранит историю актива
Сбор информации об инфраструктуре	▪ Сканирует с профилями Host discovery и Pentest, а также в режиме Audit ▪ Импортирует данные из Active Directory ▪ Ручной ввод списка адресов для сканирования	▪ Непрерывное обогащение информации об активах ▪ Сканирует с профилями Host discovery и Pentest, а также в режиме Audit ▪ Импортирует данные из Active Directory, System Center Configuration Manager (SCCM), гипервизоров ▪ Ручной ввод списка адресов для сканирования ▪ Импортирует данные об активах из других средств защиты (результаты анализа событий — из SIEM-системы, трафик — из NTA-системы) ▪ Контролирует недавно обнаруженные активы, а также те, о которых давно не было информации

	MaxPatrol 8	MaxPatrol VM
Актуализация информации об инфраструктуре	▪ Сканирует в режимах Pentest и Audit ▪ Контролирует ошибки по задачам сканирования ▪ Создает расписание сканирования	▪ Сканирует в режимах Pentest и Audit ▪ Контролирует ошибки по задачам сканирования ▪ Создает расписание сканирования ▪ Импортирует данные из SCCM ▪ Задает политики частоты сканирования ▪ Контролирует активы с неполной информацией

Этап 2. Приоритизация активов

Дает возможность автоматизировать процесс работы с активами и выделить из них те, которые больше всего влияют на бизнес-процессы компании.

	MaxPatrol 8	MaxPatrol VM
Группировка активов	▪ Статическая группировка активов	▪ Статическая группировка активов ▪ Динамические группы, с возможностью вложить их в статические ▪ Триггеры для отслеживания изменений в группах
Оценка активов	▪ Ручная оценка активов на основе статической группировки	▪ Возможность автоматизировать часть ручной работы за счет динамических групп и настройки степени важности активов ▪ Система контролирует оценку активов

Этап 3. Выявление уязвимостей

Системы проводят глубокую проверку IT-инфраструктуры — выявляют уязвимости компонентов и ошибки в их конфигурации.

	MaxPatrol 8	MaxPatrol VM
Принцип определения уязвимостей	Решение о том, есть ли на узле уязвимость, система принимает в момент сканирования	При сканировании инфраструктуры система строит модель сети, сохраняя для каждого актива информацию о его конфигурации (несколько тысяч параметров ОС, ПО, оборудования, сети). На основании этой информации система определяет уязвимости. При обновлении базы знаний система автоматически определяет новые уязвимости на ранее просканированных активах.
Определение уязвимостей	▪ Выявляет уязвимости на основании сканирования в режимах черного и белого ящика ▪ Выявляет версионные и конфигурационные ошибки ▪ Выявляет уязвимости на основании сканирования по правилам, заданным в базе знаний	▪ Выявляет уязвимости на основании сканирования в режимах черного и белого ящика ▪ Выявляет версионные и конфигурационные ошибки ▪ Выявляет уязвимости на основании сканирования по правилам, заданным в базе знаний ▪ Выявляет уязвимости без сканирования (рассчитывает их после обновления базы знаний) ▪ Выявляет уязвимости в пассивном режиме (на основе трафика)
Приоритизация уязвимостей	▪ Оценивает уязвимости по методологии CVSS v2 и CVSS v3 ▪ Выводит информацию о способе обнаружения уязвимости ▪ Сортирует уязвимости по опасности в рамках узла (в отчетах)	▪ Оценивает уязвимости по методологии CVSS v2 и CVSS v3 ▪ Выводит информацию о способе обнаружения уязвимости ▪ Сортирует уязвимости по опасности в рамках актива ▪ Сортирует уязвимости в зависимости от степени важности активов, на которых они обнаружены ▪ Информирует о трендовых уязвимостях — наиболее опасных уязвимостях из специального набора, обновляемого экспертами Positive Technologies; такие уязвимости требуют особого внимания

Этап 4. Устранение уязвимостей

Системы структурируют информацию о выявленных уязвимостях. Это помогает сделать более эффективным взаимодействие подразделений ИБ и IT.

	MaxPatrol 8	MaxPatrol VM
Задание правил обработки уязвимостей	—	▪ Можно настроить исключение уязвимостей ▪ Учитывает принятые компенсационные меры ▪ Задает политики определения опасности уязвимостей (по умолчанию опасными считаются все трендовые) ▪ Задает политики по способу обработки уязвимостей (ручной разбор, обновление ПО сотрудниками IT-отдела)
Устранение или компенсация уязвимостей	▪ Выгрузка и автоматическая передача отчета в IT-отдел	▪ Передает в IT-отдел отчет о трендовых уязвимостях ▪ Контролирует соблюдение политик (настраиваемый параметр для отслеживания соблюдения SLA по устранению уязвимостей) ▪ Передает в IT-отдел отчет о несоблюдении регламентов

Этап 5. Контроль устранения уязвимостей

Чем сильнее контроль уровня защищенности, тем меньше вероятность использования взломщиками найденных в инфраструктуре уязвимостей.

	MaxPatrol 8	MaxPatrol VM
Проверка устранения уязвимостей	▪ Сканирует по расписанию ▪ Дифференцированные отчеты для сравнения данных нескольких сканирований	▪ Сканирует по расписанию, также может проверить наличие новой уязвимости без дополнительного сканирования за счет ведения истории активов ▪ Автоматически задает рекомендуемые интервалы между сканированиями ▪ Настраиваемые виджеты для отслеживания устранения опасных и трендовых уязвимостей ▪ Контролирует соблюдение политик устранения уязвимостей ▪ Выполняет точечные проверки для контроля устранения

MaxPatrol 8 и MaxPatrol VM.
Новый подход к управлению уязвимостями

О компании

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

Positive Technologies уже 18 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.

MaxPatrol 8_vs_MaxPatrol VM_A4.RUS.0001.02.MAR.22.2021