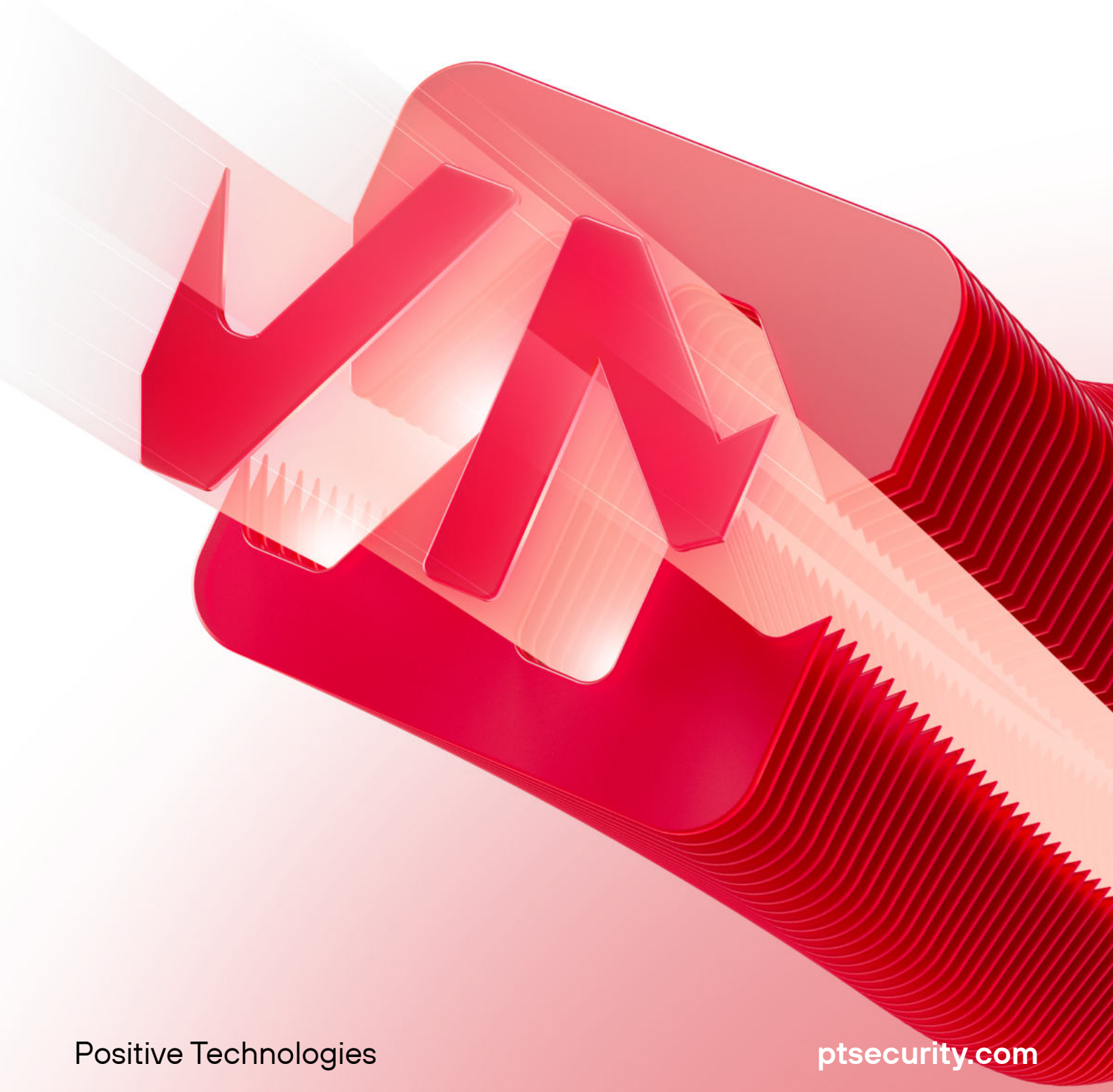
Сценарии использования MaxPatrol VM



Positive Technologies

ptsecurity.com

MaxPatrol VM — система управления уязвимостями, которая позволяет контролировать защищенность инфраструктуры в реальном времени и быть в курсе самых опасных уязвимостей.

Какие задачи позволяет выполнять MaxPatrol VM?

Управление активами

Инвентаризация активов

Если данные обо всех узлах инфраструктуры отсутствуют, специалист по ИБ проводит сканирование только известных активов. В итоге он может пропустить уязвимости на важных активах из-за недостатка информации.

MaxPatrol VM:

- осуществляет обнаружение и идентификацию активов вместо традиционного сканирования IP-адресов. Это позволяет получить информацию обо всей инфраструктуре и контролировать ее в режиме реального времени;
- собирает информацию о более чем 3000 параметрах активов (FQDN, MAC- и IP-адреса, тип ОС, имя сетевого узла, признаки виртуальности узла и т. п.) с помощью запатентованной технологии;
- импортирует данные из других средств ИБ и внешних систем;
- актуализирует информацию об инфраструктуре благодаря таким возможностям, как расписание сканирования и политики частоты сканирования.

Приоритизация активов

Для полного контроля над инфраструктурой недостаточно инвентаризации активов — необходимо приоритизировать узлы и сфокусироваться на работе с самыми важными из них. При большом количестве активов сложно делать это самостоятельно, нужна автоматизация процесса.

MaxPatrol VM:

- позволяет ранжировать активы по значимости для IT-инфраструктуры, учитывая их важность для бизнес-процессов, влияние на конфиденциальность и целостность данных, время безотказной работы и другие факторы;
- автоматизирует оценку активов путем их динамической группировки и настройки степени важности;
- контролирует оценку важности активов для бизнес-процессов компании.

Управление уязвимостями

Быстрое выявление новых уязвимостей

Каждый раз сканировать инфраструктуру для обновления информации об уязвимостях — долго и сложно. А в случае нерегулярного сканирования можно пропустить появление новой опасной уязвимости.

MaxPatrol VM:

- автоматически определяет после обновление базы уязвимостей, насколько новые уязвимости опасны для узлов сети, — без необходимости в повторном сканировании инфраструктуры;
- выявляет версионные и конфигурационные ошибки;
- выявляет уязвимости в пассивном режиме.

Приоритизация уязвимостей

При большом количестве уязвимостей сложно понять, какие из них наиболее опасны и что стоит устранять в первую очередь. К опасным уязвимостям можно отнести трендовые — те, что популярны у киберпреступников на текущий момент или могут начать массово использоваться в ближайшее время.

MaxPatrol VM:

- предоставляет информацию о трендовых уязвимостях в течение 12 часов,
- позволяет приоритизировать уязвимости по уровню опасности для бизнес-процессов компании,
- позволяет приоритизировать уязвимости согласно методике оценки уровня критичности уязвимостей программных, программно-аппаратных средств (утв. Федеральной службой по техническому и экспортному контролю 28 октября 2022 г.),
- оценивает уязвимости по методологиям CVSS v2 и CVSS v3.

Контроль устранения уязвимостей

Без выстроенного процесса взаимодействия с IT-отделом сложно добиться отсутствия критически опасных уязвимостей в инфраструктуре. Каждый раз требуется доказывать IT-специалисту, зачем устранять уязвимость и почему это важно.

MaxPatrol VM:

- повышает эффективность совместной работы отделов ИБ и ИТ: передает в ИТ отчет о трендовых уязвимостях, фиксирует регламенты регулярного обновления ОС и ПО, контролирует устранение уязвимостей, отслеживает общее состояние защищенности компании;
- позволяет установить регламенты сканирования инфраструктуры и устранения уязвимостей, а также автоматически задает рекомендуемые интервалы сканирования;
- позволяет контролировать защищенность инфраструктуры и сроки устранения уязвимостей с помощью дашбордов (настраиваемых виджетов для отслеживания устранения трендовых и опасных уязвимостей);
- выполняет точечные проверки для контроля устранения уязвимостей.

Комплаенс-контроль

Контроль соответствия стандартам и политикам безопасности

В обширном списке стандартов безопасности сложно выделить самые важные и значимые для инфраструктуры. А в случае несоответствия активов требованиям сложно приоритизировать работу с исправлениями и выстроить процесс комплаенс-контроля.

Модуль MaxPatrol HCC в MaxPatrol VM:

- содержит стандарты PT Essentials — оптимальный набор проверок для повышения уровня защищенности IT-систем,
- проверяет конфигурации систем в IT-инфраструктуре на соответствие стандартам ИБ и внутренним политикам компании,
- хранит информацию об активах и позволяет быстро реагировать на изменение требований,
- гибко настраивается, позволяя создавать собственные стандарты безопасности на основе существующих проверок.