positive technologies

MaxPatrol HCC

Ваш инструмент для комплаенс-контроля и харденинга инфраструктуры

Кроме уязвимостей в коде ПО и ОС, которые обнаруживают решения класса vulnerability management, киберугрозу несут и небезопасные настройки систем (избыточные права доступа, открытые порты, интерфейсы и т. п.). Злоумышленники используют их для проникновения в контур компании и продвижения внутри инфраструктуры.

40%
опасных уязвимостей
связаны с небезопасными настройками систем и недостатками контроля доступа

96%
компаний
не защищены от проникновения злоумышленника

Решение

Соблюдение базовых требований ИБ
при настройке операционных систем и ПО значительно повысит уровень защищенности инфраструктуры

Усиление защищенности (харденинг)
инфраструктуры увеличит время реализации атаки и сделает проникновение сложным и дорогим для злоумышленника

MaxPatrol HCC

Снижает риск реализации атак с использованием небезопасных настроек систем и уязвимостей нулевого дня (0-day), для которых еще не разработаны защитные механизмы

Сокращает время ИТ-специалистов на корректную настройку систем

Позволяет проверить инфраструктуру на соответствие внутренним и регуляторным требованиям безопасности

Модуль позволяет

Проверять активы на соответствие требованиям безопасности

Определяйте необходимые стандарты для технических и программных средств компании, а MaxPatrol HCC проконтролирует их выполнение на активах сети

Управлять безопасностью конфигураций систем

Выявляйте ошибки в конфигурации ИТ-активов, настраивайте параметры устройств и отображение актуальных данных о них, чтобы обезопасить компанию от проникновения

Уменьшить поверхность атаки

Выявляйте некорректные настройки активов (слабые пароли, незащищенные системы, неконтролируемый гостевой доступ и т. п.), чтобы снизить уязвимость инфраструктуры

Защитить от 0-day-уязвимостей

Корректная настройка основных систем и ПО позволяет снизить вероятность использования злоумышленниками уязвимостей, для которых пока не выпущены исправления

Преимущества

Глубокий мониторинг ИТ-инфраструктуры

Технология Asset Management предоставляет полную информацию об активах в инфраструктурах любого размера. Это помогает избавиться от теневых сегментов сети, отслеживать параметры конфигураций и вовремя исправлять ошибки

Создание политик безопасности с нуля

Не довольствуйтесь требованиями «из коробки» — создавайте собственные стандарты безопасности, актуальные для вашей компании, или кастомизируйте существующие и проверяйте инфраструктуру на соответствие им

Стандарты PT Essentials

По опыту пентестов и изучения мировых стандартов мы знаем, что можно закрыть до 80% уязвимых мест инфраструктуры, выполнив всего 20% самых важных требований безопасности. Использование PT Essentials существенно сэкономит время и ресурсы на разработку политик безопасности

Проверка конечных устройств

Благодаря возможности подключения хостового агента можно сканировать компьютеры сотрудников, в том числе удаленных, а после — проверять их на соответствие самым важным требованиям безопасности

Контроль важных метрик

Удобные дашборды показывают актуальное состояние инфраструктуры: сколько активов не соответствует требованиям безопасности, какие из них относятся к критически важным и требуют внимания в первую очередь

Интеграция с MaxPatrol VM

Модуль подключается к MaxPatrol VM за считаные минуты и позволяет из одной панели обнаруживать не только уязвимости ПО, но и небезопасные настройки систем

Узнать больше про MaxPatrol VM и модуль MaxPatrol HCC

Узнать про написание собственных требований для MaxPatrol HCC