MaxPatrol SIEM All-In-One

Программно-аппаратный комплекс для выявления инцидентов ИБ в реальном времени

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

- **MaxPatrol SIEM All-In-One** — самый быстрый и доступный способ начать использовать SIEM-систему корпоративного уровня и получить доступ к экспертизе Positive Technologies.
- **Лучшая возможность получить ответ на вопросы — кто, где, когда?** MaxPatrol SIEM осуществляет контроль и корреляцию событий в IT-инфраструктуре для выявления и расследования инцидентов.
- **Программно-аппаратный комплекс с единой поддержкой** — не требует длительного внедрения и высоких затрат на эксплуатацию.
- **Простой способ масштабирования существующей системы MaxPatrol SIEM** — комплекс может устанавливаться в территориальных подразделениях и работать как часть единой системы.
- **Полноценная поддержка и ключевая экспертиза в России.** Продукт имеет русскоязычный интерфейс и документацию. Все уровни поддержки обеспечиваются специалистами в РФ.
- **Быстрая миграция.** Благодаря поддержке Positive Technologies, а также заложенным в продукте техническим инновациям, переход с других решений на MaxPatrol SIEM осуществляется быстро и безболезненно для бизнес-процессов.
- **Практическое соответствие требованиям стандартов.**

Сбор, анализ и мониторинг событий из различных источников для защиты IT-инфраструктур малого и среднего масштаба

MaxPatrol SIEM All-In-One — высокопроизводительный программно-аппаратный комплекс на базе программного продукта MaxPatrol SIEM, включает в себя все необходимое для начала использования систем класса SIEM.

Особенности программно-аппаратного комплекса MaxPatrol SIEM All-In-One:

- Три модели — для организаций с общим количеством сетевых узлов 250, 500 или 1000*
- Переход между моделями (250→500→1000) через простой апгрейд лицензии
- Время хранения на встроенных дисках — до 15 месяцев в режиме оперативного хранения (при среднем потоке 3000 EPS)
- Время хранения с дополнительной опцией — до 5 лет в режиме архивного хранения
- Конфигурация «всё в одном», сбор данных с одной площадки
- Гарантийные обязательства на оборудование — 5 лет

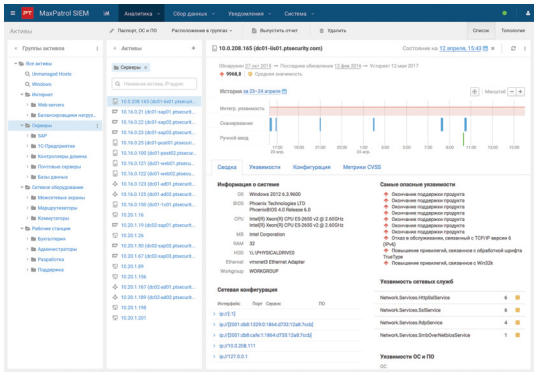
MaxPatrol SIEM — инновационный продукт, предлагающий новые подходы для эффективного выявления инцидентов ИБ и новых угроз с минимальными трудозатратами. Передовые характеристики MaxPatrol SIEM достигаются за счет создания и постоянного обновления полной модели инфраструктуры, а также за счет механизма передачи в продукт экспертизы исследовательского центра Positive Research.

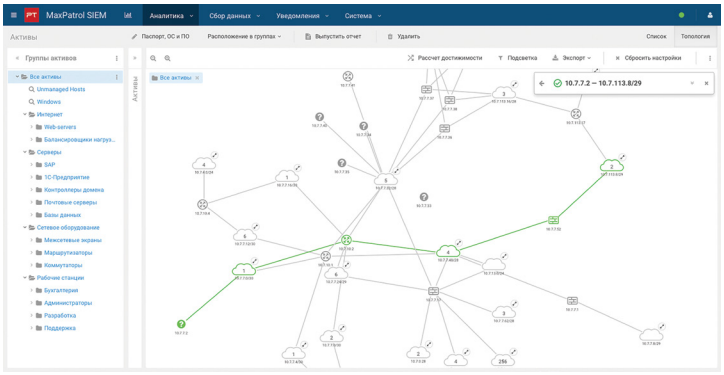
Внутри SIEM-системы информация об инфраструктуре постоянно обогащается данными из новых событий, сканирований, сетевого трафика и агентов на конечных точках, создавая полную IT-модель предприятия. Благодаря пониманию инфраструктуры правила корреляции могут захватывать не отдельные IP-адреса или hostname, но и более высокоуровневые категории — активы и динамические группы активов. В результате работоспособность правил сохраняется даже после изменений инфраструктуры.

Во всех элементах решения MaxPatrol SIEM заложены единые принципы сбора и учета информации. Модули сбора и анализа сетевого трафика, данных с конечных точек, средства управления уязвимостями и моделирования угроз изначально разрабатывались Positive Technologies как часть платформы MaxPatrol.

На основании полной модели инфраструктуры выполняется автоматическое построение топологии сети, учитывающей конфигурации сетевых устройств вне зависимости от производителя. Это позволяет лучше понимать защищаемую инфраструктуру и потенциальную достижимость атак, упрощает расследование инцидентов.

* Под сетевым узлом подразумевается любой элемент IT-инфраструктуры, подключенный к сети: серверы, компьютеры, принтеры, IP-телефония и т. п.





ХАРАКТЕРИСТИКИ АППАРАТНОЙ ПЛАТФОРМЫ

- 20 × Core 2,6 ГГц
- 128 ГБ ОЗУ
- 24 ТВ HDD
- 4 × 1 ГБ — сетевой интерфейс
- Резервируемый блок питания
- Возможность приобрести дополнительную опцию архивного хранения — СХД емкостью 40 ТВ

MaxPatrol SIEM: топология сети и достижимость, информация о состоянии сетевого узла

Для результативной эксплуатации MaxPatrol SIEM может быть достаточно одного специалиста: требования к команде эксплуатации SIEM-системы снижаются благодаря автоматизации процедур администрирования, построению полной модели инфраструктуры и топологии сети, жизнеспособности правил корреляции, использованию комплексной платформы MaxPatrol вместо множества разнородных решений ИБ.

При реализации проектов MaxPatrol SIEM обеспечивается полное покрытие актуальных источников данных и быстрое подключение новых источников. Компания Positive Technologies выполняет подключение источников без лишних затрат со стороны заказчика.

Сравнение MaxPatrol SIEM All-In-One и MaxPatrol SIEM	MP SIEM All-In-One	MP SIEM
Аппаратная платформа включена в состав продукта	✔	–
Конфигурация для организаций с общим количеством сетевых узлов 250 или 500	✔	–
Полная функциональность, доступ к экспертизе Positive Technologies	✔	✔
Без ограничений по количеству источников на узле	✔	✔
Подключение актуальных источников силами Positive Technologies	✔	✔
Не содержит ограничений по производительности (EPS)**	✔	✔
Масштабируемость, распределенная конфигурация	–	✔
Расширение лицензий на Scanner и Log Collector	–	✔
Конфигурация для организаций с общим количеством сетевых узлов больше 1000	–	✔
Увеличение хранилища для больших объемов данных и длительного хранения ***	✔	✔

** Производительность полностью определяется характеристиками оборудования.
*** Ограниченно доступно в виде опции архивного хранения.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays