MaxPatrol SIEM

мониторинг событий ИБ и выявление инцидентов в реальном времени

ВАШИ ВОЗМОЖНОСТИ С MAXPATROL SIEM

Выявляйте актуальные угрозы. Знания специалистов экспертного центра безопасности Positive Technologies (PT ESC) о способах обнаружения новых угроз регулярно передаются в MaxPatrol SIEM. Это помогает выявлять современные типы атак.

Управляйте рисками благодаря глубоким знаниям об активах. Подробная информация об активах помогает оператору ИБ выявлять и устранять проблемные зоны в инфраструктуре, тем самым снижая риск возникновения критически опасных инцидентов.

Выполняйте требования регуляторов. MaxPatrol SIEM помогает соответствовать требованиям законов № 152-ФЗ, 161-ФЗ, приказов ФСТЭК № 21, 17 и 31, СТО БР ИББС и РС БР ИББС-2.5-2014, международного стандарта PCI DSS.

в 2 раза

выросло в 2017 году количество компаний, столкнувшихся с целевыми атаками

197 дней

средний срок выявления злоумышленника в инфраструктуре

в 84% случаев

компрометация инфраструктуры занимает менее 24 часов

MaxPatrol SIEM обрабатывает события ИБ, собирает данные об активах и автоматически выявляет угрозы, в том числе ранее неизвестные. Служба ИБ моментально получает уведомления об инцидентах, что помогает оперативно отреагировать на атаку, провести детальное расследование и предотвратить репутационный и финансовый ущерб.

Получите полную картину IT-инфраструктуры

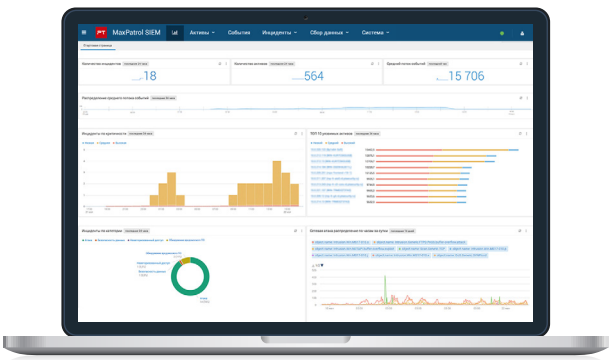
MaxPatrol SIEM строит точную модель инфраструктуры, используя методы активного и пассивного сбора, агенты для анализа трафика и данных на конечных точках.

Выявляйте инциденты вне зависимости от изменений в инфраструктуре

Изменения IT-инфраструктуры автоматически учитываются в работе правил, которые по заданным признакам выявляют инциденты. Это помогает избежать трудоемкой ручной перенастройки.

Расследуйте инциденты безопасности

Точная привязка детальных сведений о конфигурации активов, уязвимостях и событиях ИБ к соответствующему активу дает возможность изучить его состояние на любой момент в прошлом.



Дашборд отображает сводную информацию об инцидентах и уязвимостях активов в инфраструктуре и указывает на наиболее опасные из них.

25% **российского рынка SIEM**

занял MaxPatrol SIEM в 2017 году (согласно исследованию компании IDC)

100 **проектов внедрения**

MaxPatrol SIEM и MaxPatrol SIEM LE реализовано с 2015 года

230 **источников преднастроены**

Подключение любых других бизнес-систем, в том числе специфических и самописных, бесплатное

ПРОПИЛОТИРУЙТЕ РЕШЕНИЕ

Оцените возможности MaxPatrol SIEM на вашей инфраструктуре: заполните заявку на сайте и начните выявлять инциденты в режиме реального времени.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

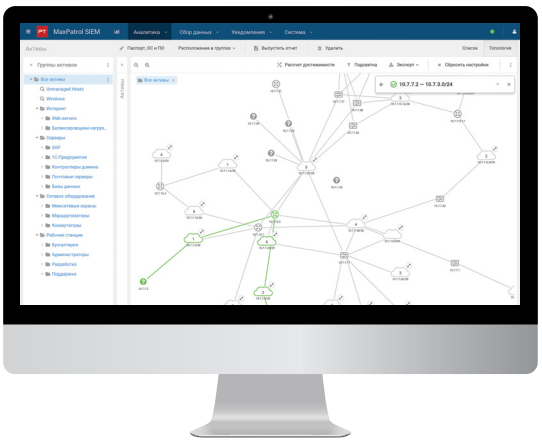
Эффективно выявляет инциденты благодаря управлению активами
Актив — ключевая сущность в MaxPatrol SIEM, которая идентифицируется по целому набору характеристик и не зависит от IP-адреса или сетевого имени. Построенные на активах правила корреляции беспроблемно адаптируются к изменениям в инфраструктуре.

Строит топологию сети
MaxPatrol SIEM автоматически строит топологию сети на основе полной модели инфраструктуры. Это помогает оператору лучше понимать защищаемую инфраструктуру и оценивать реализуемость атак, упрощает расследование инцидентов.

Выявляет новые типы угроз
Пользователи MaxPatrol SIEM оперативно получают свежие знания из Positive Technologies Knowledge Base о способах выявления новых типов атак, что помогает вовремя детектировать самые актуальные угрозы.

Помогает построить оптимальную модель мониторинга безопасности
Поскольку MaxPatrol SIEM лицензируется по количеству активов, а не по потоку событий, пользователи могут менять источники событий для мониторинга, выявляя наиболее важные источники, и подключать новые без дополнительных затрат.

Российская разработка
Продукт сертифицирован ФСТЭК России и Минобороны России и входит в реестр отечественного ПО.



Топология сети строится на основании модели IT-инфраструктуры и автоматически обновляется в случае изменений

«MaxPatrol SIEM позволил нам создать гибкую систему выявления инцидентов. В результате мы автоматизировали существующие процессы ИБ с минимальными временными затратами».

Сергей Рысин, советник директора по безопасности ПАО «ГТЛК»

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.

POSITIVE TECHNOLOGIES

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