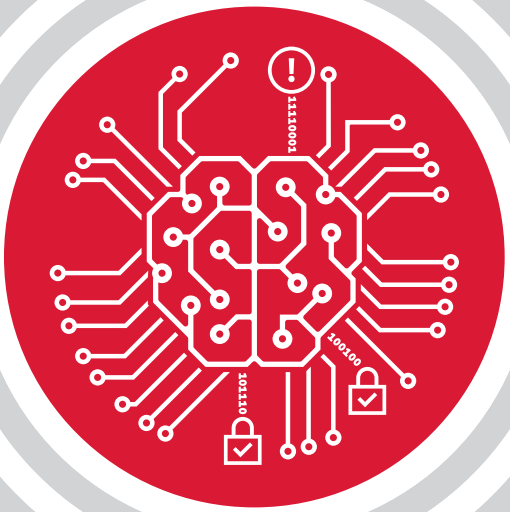
Система выявления инцидентов ИБ

MaxPatrol SIEM



КРАТКОЕ ОПИСАНИЕ ПРОДУКТА

POSITIVE TECHNOLOGIES

MAXPATROL SIEM

НОВАЯ ЭРА В МИРЕ SIEM

MAXPATROL SIEM ЭТО:

Выявление инцидентов ИБ и доступ к экспертизе Positive Technologies. Благодаря глубокому пониманию инфраструктуры, автоматической адаптации системы к изменениям и уникальному механизму передачи ИБ-экспертизы в продукт MaxPatrol SIEM эффективно выявляет новые угрозы и целенаправленные атаки.

Сокращение ресурсов эксплуатации. Требования к команде эксплуатации SIEM снижаются благодаря автоматизации процедур администрирования, построению полной модели инфраструктуры и топологии сети, жизнеспособности правил корреляции, использованию комплексной платформы MaxPatrol вместо множества разнородных решений ИБ.

Полноценная поддержка и ключевая экспертиза в России. Над созданием MaxPatrol SIEM работают десятки экспертов с опытом проведения тестов на проникновение и аудитов защищенности. Продукт имеет русскоязычный интерфейс и документацию, все уровни поддержки обеспечиваются специалистами в РФ.

В последние годы компании все чаще страдают от целенаправленных кибератак, целью которых является кража денежных средств или конфиденциальной информации, нарушение бизнес-процессов.

Несмотря на широкое распространение разнообразных решений для информационной безопасности, среднее время обнаружения вторжения по-прежнему составляет недопустимые 188 дней[1]. Кроме того, увеличивается и относительный разрыв между временем обнаружения атаки и временем, требуемым на компрометацию инфраструктуры[2].

Ключевое средство выявления сложных атак и инцидентов ИБ — решения класса Security Information and Event Management (SIEM).

На практике эффективность работы SIEM-систем оказывается низкой и их использование многими компаниями не меняет ситуацию с качеством и временем выявления инцидентов ИБ.

Основные причины низкой эффективности существующих SIEM-систем:

+ Сложность внедрения и большие трудозатраты при эксплуатации. При внедрении сложно оценить трудоемкость и сроки окончания работ по интеграции системы, а процесс поддержания работоспособности SIEM-системы и учета новых угроз продолжается и в ходе эксплуатации системы.
+ Отсутствие автоматизированной передачи экспертизы ИБ в продукт. Даже если производитель SIEM-системы имеет знания о новых угрозах и сценариях атак, он может поделиться ими только в ручном режиме — через специализированные форумы или рассылку бюллетеней.
+ Большое запаздывание в учете изменений инфраструктуры. Существующие средства ИБ адаптируются к изменениям с большой задержкой, так как процесс учета этих изменений слабо автоматизирован.

[1] 2015 Trustwave Global Security Report.
[2] Verizon 2016 Data Breach Investigation Report.

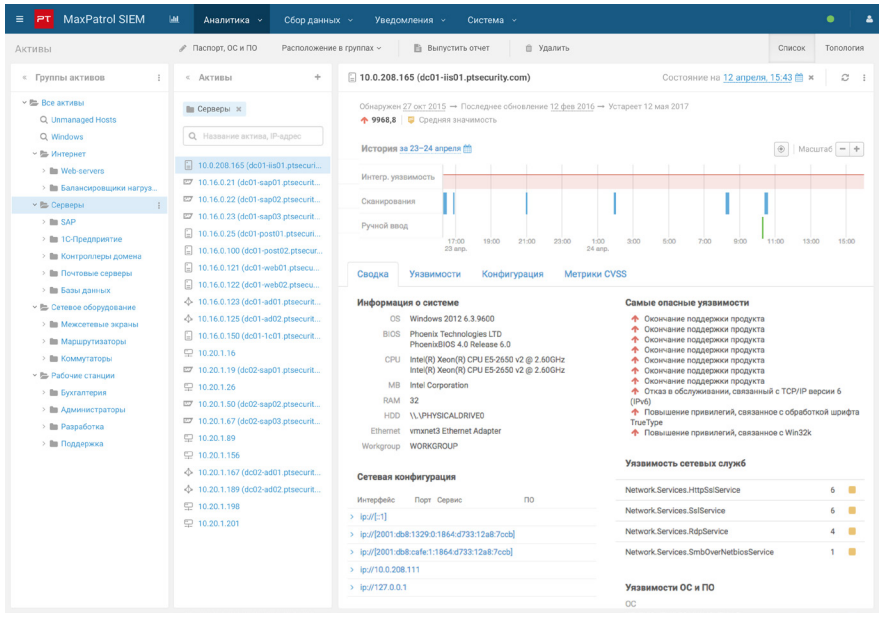
ПРЕИМУЩЕСТВА MAXPATROL SIEM

+ **Понимание инфраструктуры и стойкость правил корреляции к изменениям.** Изменения IT-инфраструктуры автоматически отображаются в модели инфраструктуры и учитываются в работе корреляционных правил, не требуя трудоемкой ручной перенастройки.
+ **Динамические группы активов.** MaxPatrol SIEM предлагает полноценную функциональность систем управления активами. Это позволяет создавать и автоматически обновлять группы активов по организационным, территориальным и функциональным признакам.
+ **Подключение актуальных источников.** В ходе реализации проектов компания Positive Technologies обеспечивает подключение актуальных источников данных без дополнительных затрат.
+ **Приоритизация с учетом важности актива.** Платформа MaxPatrol использует общепризнанный стандарт CVSS и позволяет приоритизировать активы, группы активов, события и уязвимости и присвоить им стандартизированные метрики в рамках единой платформы.
+ **Открытый API для быстрой интеграции.** MaxPatrol SIEM предлагает открытый стандартизированный API, предназначенный для загрузки или выгрузки информации на любом этапе работы системы. Это позволяет быстро решить ряд практических задач: выполнить интеграцию с SMS-шлюзом, корпоративным порталом, самописными приложениями и т. п.
+ **Развитая функциональность сбора данных.** В SIEM-систему включена широкая функциональность удаленного безагентного сбора данных с поддержкой основных видов транспорта. Помимо этого, используются дополнительные агенты для анализа сетевой активности и сбора низкоуровневой информации с конечных точек.
+ **Российское решение мирового класса.** MaxPatrol SIEM спроектирован в России на основе многолетнего опыта проведения тестов на проникновение и расследования инцидентов и учитывает требования российского законодательства в области ИБ. Продукт имеет русскоязычный интерфейс и документацию, сертифицирован ФСТЭК России и Министерством обороны РФ.

При создании SIEM-системы и новой платформы MaxPatrol компания Positive Technologies учла недостатки существующих систем и применила новые подходы для эффективного выявления инцидентов ИБ.

Внутри MaxPatrol SIEM информация об инфраструктуре постоянно обогащается данными из новых событий, результатов сканирований, сетевого трафика и агентов на конечных точках, создавая полную IT-модель предприятия. Благодаря этому правила корреляции могут оперировать не только отдельными IP-адресами или сетевыми именами, но и более высокоуровневыми категориями — активами и динамическими группами активов.

Информация о состоянии актива

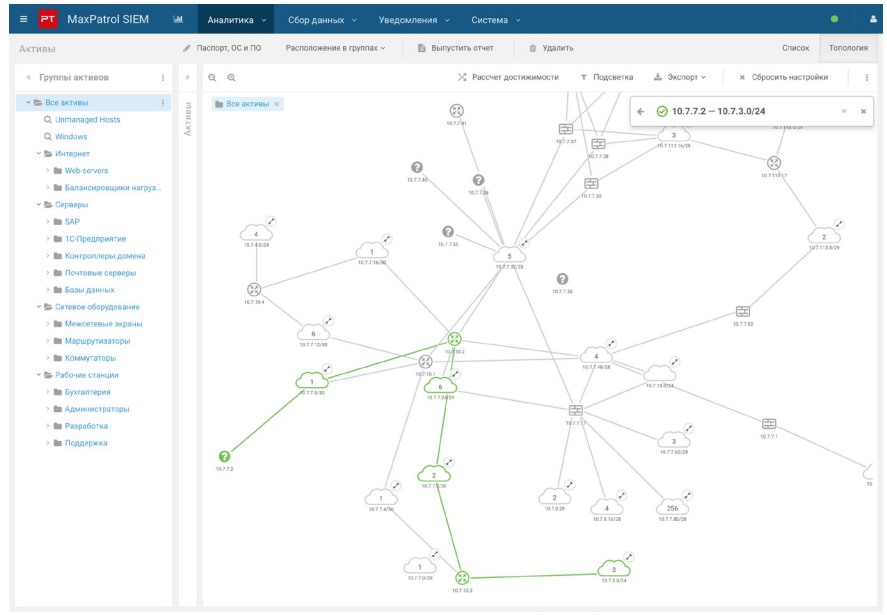


В MaxPatrol SIEM реализован механизм передачи в продукт экспертизы исследовательского центра Positive Research, основанный на базе знаний Positive Technologies Knowledge Base (PT KB). Это высокоуровневый, постоянно пополняемый набор данных, формируемый на основе 15-летнего опыта исследовательского центра, в том числе опыта тестов на проникновение и проведения аудитов защищенности.

MaxPatrol SIEM является неотъемлемой частью новой комплексной платформы MaxPatrol, обладающей изначальным пониманием природы угроз и уязвимостей и позволяющей заменить множество ИБ-решений (системы управления активами, уязвимостями, соответствия стандартам и др.). Все элементы MaxPatrol SIEM разработаны Positive Technologies как часть новой платформы MaxPatrol и используют единые принципы сбора и учета информации.

На основании полной модели инфраструктуры выполняется автоматическое построение топологии сети. Это позволяет лучше понимать защищаемую инфраструктуру и потенциальную достижимость атак, упрощает расследование инцидентов.

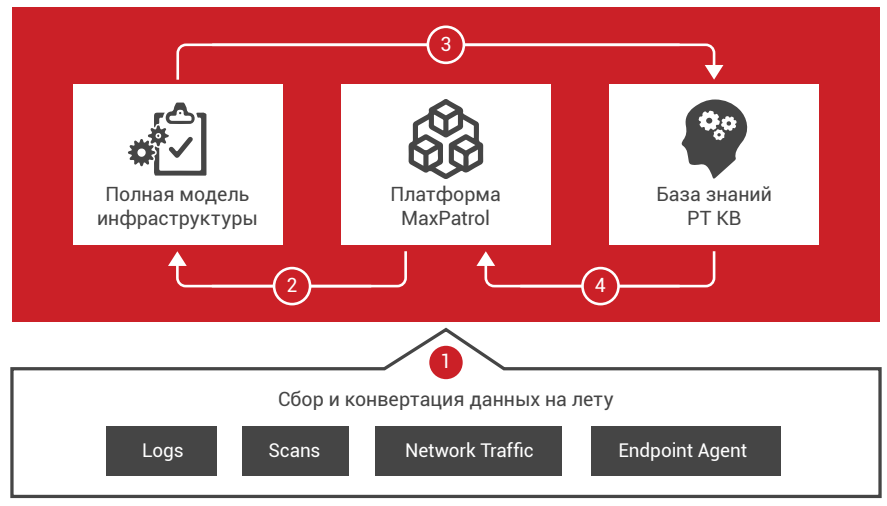
Топология сети и достижимость



Сбор, анализ и мониторинг событий для защиты инфраструктур любого масштаба

MaxPatrol SIEM использует специальный механизм для извлечения идентификаторов источника информации из трафика, событий или сканирований и их сопоставления с существующими активами. Таким образом, вся имеющаяся информация — конфигурация сетевого узла и его настройки, установленное ПО, сетевая активность, журналы — унифицируется и выстраивается вокруг каждого из активов.

После поступления в систему информация вначале проводится через модель инфраструктуры и привязывается к соответствующим активам и лишь после этого сохраняется в базе данных и попадает под действие правил корреляции. Благодаря этому изменение IP-адреса или имени актива не приведет к дублированию сущностей и появлению в системе нового актива.



Этап 1. Информация поступает в систему и проходит нормализацию.

Этап 2. Проводится через ядро и модель инфраструктуры для привязки к существующим активам.

Этап 3. Сопоставляется с данными базы знаний Positive Technologies Knowledge Base (PT KB).

Этап 4. Проводится через коррелятор с учетом всех данных, полученных на предыдущих этапах.

Страница **MaxPatrol SIEM**

Страница **MaxPatrol SIEM LE**

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». 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.

facebook.com/PHDays
facebook.com/PositiveTechnologies

ptsecurity.com pt@ptsecurity.com

POSITIVE TECHNOLOGIES

PT-SIEM_PB_A3.RUS.0007.08.SEP.08.2017_WEB