



positive
technologies

MaxPatrol SIEM

Детально знает вашу инфраструктуру —
точно выявляет инциденты

ВОЗМОЖНОСТИ MAXPATROL SIEM



Регулярно получает свежие экспертные знания для выявления актуальных угроз



Контролирует актуальность данных об IT-инфраструктуре



Отслеживает состояние ИБ в крупных иерархических инфраструктурах



Контролирует качество настройки системы с помощью чек-листа



Позволяет создавать собственные правила корреляции с помощью гибкого конструктора



Контролирует работу источников событий ИБ



Оценивает уровень защищенности организации и эффективность процессов ИБ с помощью модуля PT SIP

MaxPatrol SIEM дает полную видимость IT-инфраструктуры и выявляет инциденты информационной безопасности. Он постоянно пополняется знаниями экспертов Positive Technologies о способах детектирования актуальных угроз и адаптируется к изменениям в защищаемой сети.

Выявляет самые актуальные угрозы

Система регулярно получает свежие знания о способах детектирования новых угроз в виде пакетов экспертизы. Это позволяет пользователям детектировать техники и тактики атак до наступления серьезных последствий.

Дает полную видимость IT-инфраструктуры

В основе MaxPatrol SIEM лежит уникальная технология управления IT-активами (security asset management). Благодаря ей MaxPatrol SIEM собирает данные обо всем, что есть в сети, в активном и пассивном режиме, делая IT-инфраструктуру прозрачной для оператора ИБ.

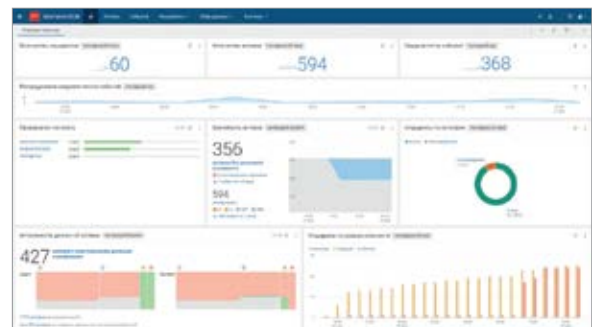
Учитывает изменения в инфраструктуре

Точно идентифицирует IT-активы даже в постоянно меняющемся ландшафте и адаптирует группы активов к изменениям в сети. Это помогает легко настраивать работу правил корреляции, постоянно отслеживать рабочие системы с необновленным ПО или одинаковыми уязвимостями.

Снижает порог входа в мир SIEM

Мы постоянно упрощаем продукт, чтобы развернуть MaxPatrol SIEM, работать с ним и выявлять угрозы мог даже новичок. Например, за последние два года в продукте появились регулярная поставка пакетов экспертизы, чек-лист настройки системы, конструктор правил корреляции и функциональность для быстрого снижения числа ложных срабатываний.

*Отслеживайте
общее состояние
ИБ в организации
с помощью гибких
дашбордов*





Проведите бесплатный пилот



Оцените возможности MaxPatrol SIEM на вашей инфраструктуре — заполните заявку на сайте и начните выявлять актуальные угрозы с помощью экспертизы Positive Technologies.

Чем MaxPatrol SIEM лучше конкурентов



Лидирующее отечественное SIEM-решение

Продукт внедрен более чем в 250 промышленных, транспортных, финансовых компаниях, в частном и государственном секторе, в органах власти. Согласно исследованию IDC, MaxPatrol SIEM входит в тройку лидеров российского рынка SIEM. Другие отечественные SIEM-системы занимают не более 6% рынка



Регулярно получает экспертизу для обнаружения угроз

Раз в два месяца MaxPatrol SIEM пополняется пакетами экспертизы с новыми правилами корреляции, индикаторами компрометации и плейбуками



Знает наиболее актуальные для России угрозы

Экспертиза в продукте — это результат наших расследований сложных инцидентов, изучения новых угроз и методов взлома российских компаний, а также мониторинга деятельности всех основных хакерских группировок на территории России и СНГ



Быстро развивается

Выпускаем два релиза в год, регулярно внедряем новые технологии и постоянно расширяем команду разработки продукта



Выполняет требования по защите информации

Помогает соответствовать требованиям законов № 152-ФЗ, 161-ФЗ, 187-ФЗ, приказов ФСТЭК № 21, 17 и 31, СТО БР ИББС, РС БР ИББС-2.5-2014, ГОСТ Р 57580.1-2017, международного стандарта PCI DSS



Дмитрий Якоб.
директор по информационным технологиям ТМК

«Трубная металлургическая компания»

Внедрение заняло полгода, подключено 16 типов источников

«Мы уже ощутили конкретную пользу от MaxPatrol SIEM во время роста количества атак в период карантинных мер, связанных с противодействием вирусу COVID-19. Благодаря проактивным действиям и внедренному решению мы успешно справились с этим вызовом».

ptsecurity.com
pr@ptsecurity.com

Positive Technologies — ведущий разработчик решений для кибербезопасности. Наши технологии и сервисы используют более 2300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Уже 20 лет наша основная задача — предотвращать хакерские атаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики.

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI).

Следите за нами в соцсетях (Telegram, ВКонтакте, Twitter, Хабр) и в разделе «Новости» на сайте ptsecurity.com, а также подписывайтесь на телеграм-канал IT's positive investing.