POSITIVE TECHNOLOGIES

MaxPatrol SIEM

Детально знает вашу инфраструктуру — точно выявляет инциденты

ВОЗМОЖНОСТИ MAXPATROL SIEM

Автоматически получает свежие экспертные знания для выявления актуальных угроз

Видит в сетевом трафике действия злоумышленников

Строит топологию сети и автоматически обновляет ее в случае изменений

Контролирует работу источников событий ИБ

Проверяет передаваемые файлы на вирусные угрозы

Позволяет создавать собственные правила корреляции с помощью гибкого конструктора

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.

Снижает трудозатраты экспертов по ИБ

В основе пакетов экспертизы — непрерывный мониторинг новых угроз, изучение атак и расследование сложных инцидентов. Это снижает потребность ваших специалистов по ИБ в мониторинге актуальных атак и написании собственных правил. Пакеты экспертизы сопровождаются подробными инструкциями по настройке работы правил и реагированию на инциденты.

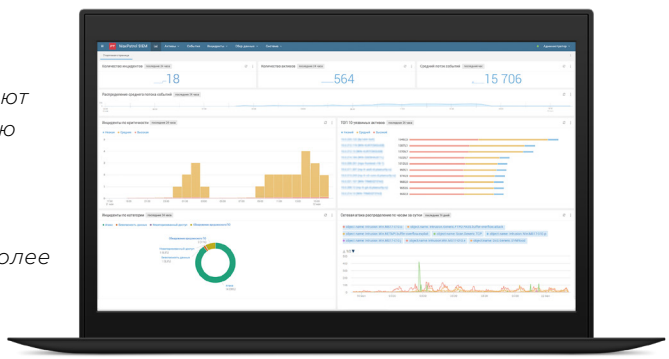
Дает полную видимость IT-инфраструктуры

Технология детальной инвентаризации, созданная на базе системы контроля защищенности MaxPatrol 8, дает MaxPatrol SIEM подробную информацию о каждом активе и уязвимых местах, 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.

Настраиваемые дашборды отображают сводную информацию об инцидентах и уязвимостях в инфраструктуре и указывают на наиболее опасные из них



25%
российского рынка SIEM
занял MaxPatrol SIEM в 2017 году (согласно исследованию компании IDC)

150
проектов внедрения
MaxPatrol SIEM и MaxPatrol SIEM All-In-One реализованы с 2015 года

300
источников поддерживаются
Среди них популярные системы российских вендоров — «1С», «Кода безопасности», «Лаборатории Касперского», InfoWatch. Подключение любых других бизнес-систем, в том числе специфических и самописных, бесплатное

Проведите пилотное внедрение

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

Преимущества

Регулярно получает экспертизу для обнаружения угроз

Не реже раза в месяц база знаний PT Knowledge Base пополняется пакетами экспертизы с новыми правилами корреляции и плейбуками. Пользователи MaxPatrol SIEM автоматически получают пакеты экспертизы из PT KB.

Экспертиза Positive Technologies
- Аудиты безопасности
- Расследования инцидентов ИБ
- Исследования угроз
- Пентесты

PT Knowledge Base
- Новые правила
- Рекомендации по реагированию
- Репутационные списки

MaxPatrol SIEM
- Выявление актуальных угроз

Знает наиболее актуальные для России угрозы

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

Быстро развивается

Мы выпускаем два релиза в год, регулярно внедряем новые технологии и постоянно расширяем команду разработки.

Выполняет требования законодательства

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

Имеет оптимальную модель лицензирования

MaxPatrol SIEM лицензируется по количеству активов, а не по потоку событий, поэтому его стоимость не зависит от изменения количества событий в секунду и объема получаемых данных из источников.

«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

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

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.

MP-SIEM_PB_A4.RUS.0014.17.AUG.2.2019