positive technologies

MaxPatrol SIEM

Детально знает вашу инфраструктуру — точно выявляет инциденты

ВОЗМОЖНОСТИ MAXPATROL SIEM

Отслеживает состояние ИБ в крупных иерархических инфраструктурах

Видит IT-инфраструктуру

Контролирует качество настройки системы с помощью чек-листа

Позволяет создавать собственные правила корреляции с помощью гибкого конструктора

Автоматически заносит в белый список легитимные сработки

Помогает проверять гипотезы с помощью просмотра связанных корреляционных событий

Ищет данные в сторонних системах и сервисах прямо из карточки события

MaxPatrol SIEM выявляет инциденты ИБ, ведущие к реализации недопустимых событий, и попытки нарушения киберустойчивости компании.

Быстрый результат

Без дополнительных вложений и доработок. Оперативно разворачиваемся и запускаем мониторинг инфраструктуры за счет экспертизы из коробки.

Актуальная экспертиза

Каждый месяц MaxPatrol SIEM автоматически пополняется новым пакетом экспертизы. Плюс мы постоянно обновляем и улучшаем ранее загруженные правила.

Адаптация к изменениям

Продукт быстро адаптируется к изменениям в инфраструктуре и четко идентифицирует ИТ-активы. Классификация активов по группам облегчает настройку правил корреляции.

Помощь в принятии решений

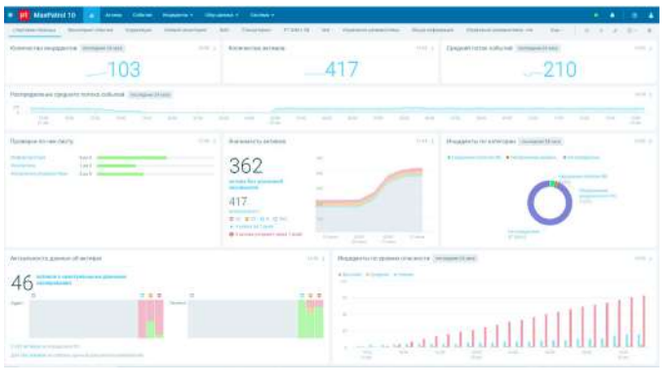
В MaxPatrol SIEM встроен ML-помощник BAD (Behavioral Anomaly Detection). Это система second opinion, повышающая эффективность обнаружения атак за счет альтернативного метода оценки событий.

Простота и удобство

Мы активно вкладываемся в Analyst Experience. Удобная карточка события позволяет просматривать связанные события, проверять потенциально опасные файлы и реагировать на инциденты в рамках единого окна.

Enterprise-мониторинг

MaxPatrol SIEM может обрабатывать 540+K EPS на одном ядре с полной экспертизой. В продукте используется разработанная нами СУБД LogSpace, которая потребляет в два раза меньше ресурсов, чем аналогичные Open Source решения.



Настраиваемые дашборды помогают отслеживать общее состояние ИБ в организации

ОСТАВЬТЕ ЗАЯВКУ НА ПИЛОТНЫЙ ПРОЕКТ

Оцените возможности MaxPatrol SIEM для вашей инфраструктуры.

Чем MaxPatrol SIEM лучше конкурентов

Лидирующее отечественное SIEM-решение	Продукт внедрен более чем в 600 промышленных, транспортных, финансовых компаниях, в частном и государственном секторе, в органах власти.
Регулярно получает экспертизу для обнаружения угроз	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.
Комьюнити и независимые разработки	В каталоге расширений представлены расширения, правила и коннекторы для MaxPatrol SIEM, разработанные экспертным сообществом, которые упрощают решение самых разных задач.
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, указу президента №250, стандартам ЦБ и международному стандарту PCI DSS

ГТЛК

Сергей Рысин,
советник директора
по безопасности ПАО «ГТЛК»

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

О компании
ptsecurity.com
pr@ptsecurity.com

Positive Technologies — ведущий разработчик решений для информационной безопасности. Уже 21 год наша основная задача — предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии и сервисы используют более 2900 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». 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.