



MaxPatrol SIEM

■ positive technologies

MaxPatrol SIEM

Система, обеспечивающая непрерывный мониторинг и результативное обнаружение событий ИБ в инфраструктурах любого масштаба

540 000+

событий обрабатывается
в секунду

360+

техник MITRE ATT&CK,
покрывает решение

10 000+

правил нормализации

400+

источников «из коробки»

1700+

правил корреляции

90+

ML-моделей для выявления
аномалий поведения

MaxPatrol SIEM знает



Что искать

Выявляет актуальные угрозы, аномалии в поведении, трендовые техники и инструменты атак



Где искать

Обеспечивает комплексный мониторинг ИТ-инфраструктуры — серверов, рабочих станций и сетевых устройств



Как искать

Работает в любых инфраструктурах, обеспечивая стабильную и надежную защиту



Что делать дальше

Строит список приоритизированных алертов с необходимым контекстом и поддержкой ИИ-помощника PT NAIRA для автоматизации рутины и активных действий



Ключевые возможности



Адаптивная конфигурация

Гибкая ролевая модель, возможность создания собственных правил и автоматический вайтлистинг для уменьшения числа ложных срабатываний



Возможности интеграции

Нативная поддержка решений Positive Technologies и возможность работы с другими решениями благодаря открытому API



Мониторинг состояния инфраструктуры

Дашборды, виджеты, мониторинг источников и состояния компонентов системы позволяют вести системный анализ и своевременно выявлять отклонения



Выполнение требований регуляторов

Обеспечение соответствия ключевым требованиям регуляторов для субъектов КИИ: ГосСОПКА, ФинЦЕРТ, приказ ФСТЭК России № 117 и т.д.*



Экспертиза

Обширная и непрерывно обновляющаяся база экспертизы MaxPatrol SIEM позволяет определить в событиях безопасности признаки реализации актуальных угроз



Повышение эффективности SOC

MaxPatrol BAD и PT NAIRA снижают порог входа и повышают эффективность работы с системой благодаря автоматизации рутинных операций и выявлению аномалий в поведении пользователей

* ГОСТ 57580-1-2017, ФСТЭК РФ от 18 февраля 2013 №21, 187-ФЗ, приказ ФСТЭК № 239 от 25 декабря 2017 г., ФСБ России № 196 от 6 мая 2019 г.



Сильный SOC начинается с **MaxPatrol SIEM**

