

PT SECURITY INTELLIGENCE PORTAL

ОТ АНАЛИЗА ИНЦИДЕНТОВ
К ЭФФЕКТИВНОМУ УПРАВЛЕНИЮ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТЬЮ



КЛЮЧЕВЫЕ ЗАДАЧИ

- + Мониторинг и оценка процессов управления ИБ и ИТ на основе KPI и трендов ИБ
- + Мониторинг и анализ предпосылок возникновения инцидентов ИБ
- + Оценка эффективности технических средств защиты информации
- + Оценка работы и достаточности персонала для достижения целей ИБ и ИТ

ДЛЯ КОГО ПРЕДНАЗНАЧЕН

- + Бизнес-руководители
- + Руководители ИБ и ИТ
- + Аналитики ИБ
- + Специалисты ИБ и ИТ

ЧТО ТАКОЕ PT SECURITY INTELLIGENCE PORTAL

PT Security Intelligence Portal — это удобный и эффективный инструмент для управления информационной безопасностью организации на стратегическом и тактическом уровнях, который осуществляет:

- + оценку текущего состояния информационной безопасности;
- + прогнозирование возможных инцидентов ИБ;
- + исследование инцидентов ИБ и выявление их причин;
- + анализ эффективности процессов ИБ.

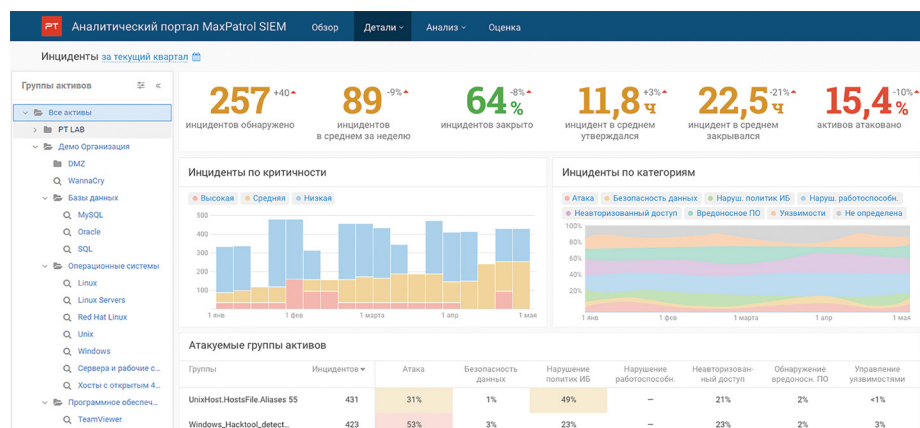
PT Security Intelligence Portal — модуль MaxPatrol SIEM, который позволяет выстроить диалог ИБ и бизнеса на основе информации из системы выявления инцидентов, поднимая данные с оперативного уровня на уровень оценки эффективности подразделений и процессов. В основе PT Security Intelligence Portal:

- + знания, накопленные в ходе разработки и развития PT Reporting Portal — портала аналитической отчетности для MaxPatrol 8;
- + многолетний опыт экспертного центра безопасности PT ESC;
- + результаты тесного сотрудничества с нашими ключевыми клиентами — компаниями с высоким уровнем зрелости ИБ.

ВОЗМОЖНОСТИ

Благодаря глубокой многоуровневой аналитике PT Security Intelligence Portal позволяет взглянуть на защищенность ИТ-инфраструктуры компании под разными углами зрения и с необходимой степенью детализации.

С помощью PT Security Intelligence Portal вы можете построить процесс управления информационной безопасностью, оценить и оптимизировать эффективность уже существующих процессов и используемых защитных систем, а также работу ИБ и ИТ-подразделений.



КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

- + Помогает принимать решения на стратегическом и тактическом уровнях управления
- + Предоставляет полную картину состояния ИБ- и IT-процессов и ресурсов в компании любого масштаба
- + Анализирует данные средств защиты и любых других систем, подключенных к MaxPatrol SIEM
- + Позволяет быстро начать работу благодаря готовым наборам показателей эффективности (KPI) и метрик
- + Помогает снизить операционные издержки
- + Позволяет гибко настраивать визуализацию и показатели KPI
- + Построен на основе быстрой и удобной BI-платформы

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ С PT SECURITY INTELLIGENCE PORTAL

PT Security Intelligence Portal обеспечивает мониторинг и оценку защищенности IT-инфраструктуры, контроль и оптимизацию процесса управления инцидентами на всех этапах.

	Шаг 1	
	Сбор данных об активах, уязвимостях и инцидентах из MaxPatrol SIEM для получения представления об инфраструктуре	
Проактивное выявление	Шаг 2	Руководители ИБ и IT Специалисты ИБ
	Оценка и мониторинг состояния инфраструктуры с использованием метрик, показателей и трендов, отображающих уровень ее защищенности	
	Шаг 3	Специалисты ИБ Специалисты IT Аналитики ИБ
	Выявление предпосылок к возникновению и развитию инцидентов ИБ, определение их опасности для осуществления превентивных действий и понимания потенциальных причин актуальных инцидентов	
Реагирование на инциденты и анализ	Шаг 4	Специалисты ИБ Специалисты IT Аналитики ИБ
	Исследование обнаруженных инцидентов ИБ, вовлеченных в них активов, назначенных приоритетов, возможных причин возникновения, а также принимаемых мер по реагированию	
	Шаг 5	Руководители ИБ и IT Специалисты ИБ Специалисты IT
	Отслеживание состояния и сроков проведения расследований по инцидентам ИБ для понимания наличия, своевременности и полноты мер по сдерживанию, устранению и восстановлению после инцидентов ИБ	
Накопление экспертизы	Шаг 6	Руководители ИБ и IT Аналитики ИБ
	Анализ и контроль эффективности построенных процессов ИБ и используемых ресурсов (средств защиты и персонала) для планирования мер по оптимизации работы с инцидентами	

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.