Повышение киберустойчивости: Как платформа Logsign Unified SO опережает SIEM, SOAR и XDR

logsign.bakotech.com logsign@bakotech.com

Каковы ключевые различия между SIEM, SOAR, XDR и Logsign Unified SO Platform?

SIEM, SOAR, XDR и Logsign USO Platform — это технологии кибербезопасности, которые помогают организациям выявлять, расследовать киберугрозы и реагировать на них. Однако они отличаются по сфере применения, возможностям и направленности. Вот основные различия между ними:

SIEM

Решения Security Information and Event Management (SIEM) собирают и анализируют данные, связанные с безопасностью, из различных источников, таких как сетевые устройства, серверы и конечные точки. Инструменты SIEM сопоставляют данные и генерируют оповещения при обнаружении подозрительной активности. SIEM сосредотачивается на выявлении инцидентов безопасности и обеспечении видимости событий безопасности в IT-среде организации.

SOAR

Решения Security Orchestration, Automation and Response (SOAR) автоматизируют и оптимизируют процессы реагирования на инциденты. Инструменты SOAR интегрируются с другими технологиями безопасности, такими как SIEM и EDR, чтобы помочь командам безопасности управлять оповещениями, автоматизировать задачи реагирования на инциденты, а также эффективнее расследовать и решать инциденты безопасности.

XDR

Решение Extended Detection and Response — это усовершенствованная и более развитая версия EDR, которая расширяет сферу обнаружения и реагирования за пределы конечных точек, включая другие части IT-среды, такие как облачная инфраструктура и сетевые устройства. Решения XDR используют аналитику и машинное обучение, чтобы соотносить данные о безопасности из различных продуктов безопасности и генерировать оповещения при обнаружении угроз.

Logsign Unified SO Platform:

Logsign Unified SO Platform — это усовершенствованная платформа для управления безопасностью, обогащенная такими функциями, как управление логами, корреляция, обработка данных и обнаружение событий, анализ угроз, управление инцидентами, автоматизация и расширенные отчеты. Она использует расширенную аналитику для анализа данных о безопасности из различных источников, в частности с сетевых устройств, серверов, приложений и конечных точек. Logsign USO Platform интегрирует SIEM нового поколения, аналитику угроз, UEBA и SOAR и позволяет организациям оптимизировать и упорядочить свои операции по кибербезопасности.

Кроме того, платформа предлагает возможности беспрепятственной интеграции, что позволяет без труда интегрировать ссуществующие решения для безопасности и использовать обширную библиотеку интеграции, расширяя функциональность Logsign USO Platform и обеспечивая комплексный подход к управлению безопасностью. Благодаря этим широким возможностям она позволяет организациям улучшить свое состояние безопасности и обеспечить соответствие нормам и стандартам.

Диаграмма решений для SIEM, SOAR, XDR и Logsign Unified SO Platform

Решение	Ключевой функционал	Основные функции	Сценарии использования
SIEM	Собирает и агрегирует события безопасности из разных источников, анализирует события для выявления угроз безопасности, генерирует оповещения для расследования	Централизованное управление событиями безопасности	Выявление потенциальных инцидентов безопасности, обеспечение централизованного обзора событий безопасности, мониторинг соответствия нормативным требованиям
SOAR	Автоматизирует реагирование на инциденты с помощью плейбуков и рабочих процессов правил оповещения (alert rules) и правил действия (action rules)	Оркестрация и автоматизация операций по безопасности	Автоматизация расследования и исправления инцидентов безопасности, сокращение времени реагирования, улучшение согласованности мер реагирования
XDR	Обеспечивает комплексное обнаружение угроз и реагирование на них в разных доменах	Кроссдоменное обнаружение и реагирование на угрозы	Корреляция и анализ событий безопасности из разных источников, выявление продвинутых угроз на эндпойнтах, в сети и облаке
Logsign Unified SO Platform	Обеспечивает комплексную, унифицированную платформу для управления безопасностью, обнаружения угроз и реагирования на инциденты для предприятий любого размера	Управление безопасностью на интегрированной платформе	Сбор, корреляция и анализ данных из разных источников, обеспечение комплексной видимости, расследование, эффективное выявление потенциальных угроз, быстрое автоматическое реагирование на инциденты для их исправления и уменьшения последствий

Примечание: Определенные функции указанных технологий могут варьироваться в зависимости от вендора. Здесь рассмотрены общие возможности.

Сравнительная таблица для SIEM, SOAR, XDR и Logsign Unified SO Platform

Решение	SIEM	SOAR	XDR	Logsign Unified SO Platform
Управление логами	✓	✗	✗	✓
Мониторинг в реальном времени	✓	✓	✓	✓
Детализированное расследование	✗	✓	✓	✓
Анализ данных	✓	✗	✗	✓
Отчетность о комплаенсе	✓	✗	✗	✓
Управление кейсами и инцидентами	✗	✓	✓	✓
Выявление угроз и реагирование на них	✗	✓	✓	✓
Поддержка Mitre ATT&CK Mapping	✗	✓	✓	✓
Выявление аномалий	✗	✓	✓	✓
Наличие специфических знаний у специалистов	✓	✗	✗	✗
Автоматизированное реагирование	✗	✓	✓	✓
Автоматизация и оркестровка	✗	✓	✓	✓
Исследование угроз	✗	✓	✓	✓
UEBA (Аналитика поведения пользователей и субъектов)	✗	✗	✗	✓

Примечание: Определенные функции и кейсы использования упомянутых технологий могут варьироваться в зависимости от вендора. Здесь рассмотрены общие возможности.

Выводы

Logsign Unified SO Platform предоставляет все функции, упомянутые в диаграммах выше, на единой платформе в интегрированном виде, чтобы помочь организациям повысить уровень безопасности и снизить риск кибератак, предоставляя им интегрированную и эффективную платформу управления безопасностью, которая включает в себя все возможности SIEM, SOAR, XDR и многое другое. С помощью Logsign USO Platform организации смогут централизовать свои операции по безопасности, таким образом достигая повышенной эффективности с точки зрения времени и человеческих ресурсов в дополнение к значительно улучшенному уровню безопасности.

Logsign

Logsign — это международный поставщик, который специализируется на предоставлении комплексных решений по кибербезопасности, позволяющих организациям повысить свою киберустойчивость, снизить риски и оптимизировать процессы безопасности, уменьшив при этом хаос в HR- и операционном отделах. Logsign неизменно предлагает эффективную, удобную и безупречную платформу и использует новейшие технологии для создания безопасных, устойчивых и совместимых сред, предоставляя организациям комплексную видимость своей IT-инфраструктуры, расширяя возможности обнаружения угроз и оптимизируя усилия по реагированию на них. В современном сложном ландшафте угроз Logsign гарантирует, что компании имеют отличный процесс кибербезопасности, проактивно защищая свои системы, данные и цифровые активы. Компания Logsign представлена на четырех континентах, ее клиентская база насчитывает более 600 предприятий и государственных учреждений, уже два года подряд компания упоминается в магическом квадранте Gartner SIEM. Кроме того, Logsign имеет высокие рейтинги на сайтах Gartner Peer Insight и G2.

bakotech

BAKOTECH — международная компания, которая занимает лидирующие позиции в сфере фокусной Value Added IT-дистрибуции и поставляет решения ведущих мировых IT-производителей. Позиционируя себя как True Value-Added IT-дистрибьютор, BAKOTECH предоставляет профессиональную до- и постпродажную, маркетинговую, техническую поддержку для партнеров и конечных заказчиков.

logsign.bakotech.com

logsign@bakotech.com