

Что такое SIEM и Приоритет подачи журналов в SIEM

Вводная SIEM

Security information and event management (SIEM) – решение для консолидации и анализа данных о событиях, создаваемые системами безопасности, сетевой инфраструктурой конечными точками, приложениями и облачными сервисами.

Основной тип данных – логи/журналы, но SIEM может также обрабатывать иные типы данных, например, EDR-телеметрию или сетевую телеметрию (flows).

Данные события могут дополняться контекстной информацией о пользователях, активах, угрозах и уязвимостях. Параметры событий могут быть нормализованы, чтобы предоставить возможность единообразного анализа (корреляции, формирования отчётов и графиков) данных из разрозненных источников.

Решение обеспечивает анализ событий в режиме близком к реальному времени для мониторинга безопасности, ретроспективного поиска, расследования инцидентов и других задач, например, проверки соответствия законодательству или отчётность.

Термин SIEM был впервые введён Gartner в 2005.

В 2015, был представлен концепт "next-gen SIEM" или SIEM 2.0. Основное отличие – введение user behavioral analytics (UBA). Next-gen SIEM ориентированы в первую очередь на применение в очень крупном бизнесе (команды SOC 10+ сотрудников).

В 2020 SIEM остаётся ключевым инструментом для работы команд SOC или ИБ. SIEM предоставляет:

- Получение данных с различных уровней сети
- Централизованное хранение и просмотр различных данных в нормализованном виде
- Кросс-корреляцию данных

Стандартные возможности SIEM:

- Logs management (collection, normalization, storage)
- Detection (correlation)
- Reporting (dashboards, reports)
- Assets inventory (vulnerability management)

Новые запросы к SIEM:

- TI management - as a context about threats
- Threat Hunting support (quick advanced search, anomaly detection)
- Machine learning detection (UEBA/UBA)
- Response orchestration and automation

Сценарий применений SIEM

1. Предпроектное обследование (сбор информации об источниках, инфраструктуре), составление модели угроз, разработка сценариев выявления
2. Развёртывание и первоначальная настройка Подключение источников событий, интеграция с продуктами для реагирования и обогащения
3. Доработка и адаптация правил корреляции, дашбордов, отчётов
4. Инвентаризация и категоризация активов, групп пользователей
5. Штатная работа с системой (мониторинг безопасности, реагирование на инциденты, Threat Hunting)
6. [по мере необходимости] Подключение новых источников, обновление коннекторов, правил корреляции
7. [на регулярной основе] Оценка эффективности и актуализация сценариев выявления и правил корреляции
8. Остальные юзкейсы будут на этой странице (в разработке)

Приоритет журналов систем к подаче в SIEM

Приоритет подачи событий от определенных систем, прежде всего зависит от модели нарушителя и его возможностей на основе рисков. Если такого документа нет, то можно руководствоваться базовым подходом и акцентировать внимание на события следующих источников (при наличии) данных в порядке приоритета:

1. Периметровые/Пограничные решения (External facing Systems): *VPN порталы, WEB сервера, терминалы, точки доступа, роутеры, СКУД и др.*
2. Системы информационной безопасности (Security Devices): *МЭ, IPS/IDS, Email защита, NGFW, Антивирусная защита, EDR, WAF и др.*
3. Системы аутентификации (Authentication Systems): *PAM, MFA, LDAP/FreeIPA, RADIUS, CA Systems, SAML, AD и др.*

4. SaaS приложения/ПО как услуга (SaaS Apps): *Slack, Cloudflare, Microsoft Azure Active Directory, Zscaler и др.*
5. Системы под управлением ОС Windows (Windows Systems): *Сервера (AD, MS SQL, Exchange, DNS, DHCP, SCCM, WSUS, и др.), Рабочие станции и др.*
6. Системы под управлением ОС Linux (Linux Systems): *apache, nginx, mysql, fail2ban, bind, samba, exim, squid, postgres и др.*
7. Сетевые устройства (Network Devices): *Маршрутизаторы (Netflow полезно), коммутаторы, мосты, Wi-Fi, модемы, концентраторы и др.*
8. Системы виртуализации (Virtualization Systems): *VMware, Citrix, Hyper-V, KVM, ProxMox и др.*
9. Внутренние системы (Internal Systems): *Процессинг, Бизнес-приложения и др.*
10. Управления и работа с мобильными устройствами (Mobile Devices): *MDM, EMM, UEM и др.*
11. Системы хранения данных и БК (Storage/Backup Systems): *DELL EMC, HP 3PAR, NetApp, Veeam, CommVault и др.*
12. Узкоспециализированное ПО (COT: commercial off-the-shelf): *Собственные приложения, The Microsoft Office, Adobe Photoshop, SAP и др.*

Revision #3

Created 24 October 2023 11:42:58 by Boris RZR

Updated 28 November 2023 08:04:36 by Boris RZR