Что такое SIEM и приоритет подачи журналов в SIEM

Что такое 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.

Типы данных:

- Логи/журналы
- EDR - телеметрия
- Сетевая телеметрия

Возможности:

- Обогащение контекстной информацией о пользователях, активах, угрозах, уязвимостях
- Анализ корреляции, формирования отчетов, графиков
- Ретроспективный поиск, расследование инцидентов
- Проверка соответствия законодательству

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

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)

Эффективное логирование направлено на:

Отправку оповещений о событиях критических изменений в конфигурации программного обеспечения или развертывание новых программных решений;

Выявление событий, указывающих на инцидент кибербезопасности, например, методы Living off the Land (LOTL) или боковое перемещение после компрометации;

Поддержку реагирования на инциденты путем выявления масштаба и степени компрометации;

Мониторинг соответствия учетных записей организационным политикам, сокращение шума по оповещениям;

Предоставление возможности принимать гибкие и обоснованные решения на основе приоритизации оповещений и аналитики;

Гарантирование того, что журналы будут пригодными для аналитиков.

Хранение журнала событий

Сроки хранения журналов должны быть основаны на оценке рисков для данной системы. При оценке рисков для системы следует учитывать, что в некоторых случаях может потребоваться до 18 месяцев, чтобы обнаружить инцидент кибербезопасности, а некоторые вредоносные программы могут находиться в сети от 70 до 200 дней, прежде чем нанести явный вред.

Сроки хранения журналов также должны соответствовать любым нормативным требованиям и структурам кибербезопасности, которые могут применяться в юрисдикции организации. Журналы, которые имеют решающее значение для подтверждения вторжения и его последствий, должны быть приоритетными для более длительного хранения.

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 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 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 СРК (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.*

Подход для корпоративных сетей на основе рисков

1. Критические системы и хранилища данных, которые, вероятно, будут атакованы;
2. Интернет-сервисы, включая удаленный доступ к ним, сетевые метаданные и их ОС; серверы управления идентификацией и доменами;
3. Любые другие критические серверы;
4. Пограничные устройства, такие как граничные маршрутизаторы и фаерволы;
5. Административные рабочие станции;
6. Высокопривилегированные системы, такие как управление конфигурацией, мониторинг производительности и доступности (в случаях, когда используется привилегированный доступ), CI/CD, службы сканирования уязвимостей, управление секретами и привилегиями;
7. Хранилища данных;
8. Системы связанные с ИБ и критически важное ПО;
9. Пользовательские компьютеры;
10. Журналы пользовательских приложений;
11. Веб-прокси, используемые пользователями организации и сервисные учетные записи;
12. DNS-сервисы (используемые пользователями организации), серверы электронной почты, серверы DHCP;
13. Устаревшие ИТ-активы (которые ранее не были зафиксированы в критических или интернет-сервисах).
14. Журналы с более низким приоритетом:
    1. Базовая инфраструктура, например, хосты гипервизора;

2. ИТ-устройства, например, принтеры
3. Сетевые активы, например, шлюзы приложений.

Revision #7
Created 2023-10-24 11:42:58 UTC by Boris Rzr
Updated 2026-07-13 15:05:35 UTC by Dmitry Borisov