УДК 004.056.53

СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ И СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.И. Алейникова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Беларусь

Аннотация. Рассмотрены основные этапы функционирования SIEM-системы, ключевой фактор, влияющий на эффективность аналитики и работы детектирующей логики SIEM-системы. Рассмотрены примеры воздействия нарушителя на уровень сбора событий информационной безопасности и даны рекомендации по противодействию. Рассмотрены события, для которых необходимо осуществлять мониторинг и настройку корреляционных правил в первую очередь. Приведены примеры настройки корреляционных правил для выявления потенциальных инцидентов информационной безопасности или потенциальных уязвимостей в локальной сети организации. Даны рекомендации по снижению ложноположительных сработок SIEM-системы.

Ключевые слова: система мониторинга, SIEM-система, агрегация, корреляция, управление активами, мониторинг, выявление инцидентов, выявление уязвимостей, ложноположительные сработки.

INFORMATION SECURITY AND INFORMATION SECURITY EVENT MANAGEMENT SYSTEMS

D.I. Aleinikova

Belarusian State University of Informatics and Radio Electronics, Minsk, Belarus

Abstract. The main stages of the SIEM system functioning, a key factor influencing the effectiveness of analytics and the detection logic of the SIEM system, are considered. Examples of the attacker's impact on the level of information security event collection are considered and recommendations on counteraction are given. The events for which it is necessary to monitor and adjust the correlation rules in the first place are considered. Examples of setting up correlation rules to identify potential information security incidents or potential vulnerabilities in the organization's local network are given. Recommendations to reduce the false positive alarms of the SIEM system are given.

Keywords: monitoring system, SIEM, aggregation, correlation, asset management, monitoring, incident detection, vulnerability detection, false positive alarms.

Введение

В настоящее время информационная безопасность является одним из приоритетных направлений для любой организации. Для решения задач быстрого выявления инцидентов и своевременного реагирования на них применяются системы класса SIEM (Security Information and Event Management). Они позволяют анализировать большое количество событий информационной безопасности в локальной сети организации в режиме реального времени, оперативно выявлять угрозы, уязвимости или инциденты, повышая скорость реагирования и способствуя предотвращению или минимизации ущерба от реализации атак.

Основная часть

SIEM-система – ключевой компонент в архитектуре SOC (Security Operational Center), обеспечивающий централизованный сбор информации с различных источников информационной инфраструктуры организации, таких как рабочие станции пользователей, серверы приложений и веб-серверы, базы данных, почтовый и хостовой антивирусы, системы класса IDS/IPS (Intrusion Detection System/Intrusion Prevention System), межсетевые экраны, телекоммуникационное оборудование и другие. На рис. 1 представлены базовые модули классической SIEM-системы [1].

Рис. 1. Базовые модули SIEM-системы
Fig. 1. Basic modules of the SIEM system

После сбора и нормализации событий ключевыми этапами работы SIEM-системы являются агрегация и корреляция полученных событий информационной безопасности.

Агрегация представляет собой сбор и объединение однородных или повторяющихся событий информационной безопасности в единую структуру, которую затем можно использовать для дальнейшего анализа. Пример агрегации – объединение повторяющихся событий о неудачных попытках входа под одной учетной записью с определенного хоста.

Корреляция – анализ различных событий с целью выявления потенциальных инцидентов информационной безопасности. По заданным настройкам SIEM-система обрабатывает приходящие потоки событий информационной безопасности, выявляя взаимосвязи, которые в совокупности могут указывать на потенциальную атаку. Помимо выявления атак, грамотная настройка корреляций событий позволяет снизить число ложноположительных сработок SIEM-системы.

Следует отметить, что возможности аналитики и работы детектирующей логики данной системы напрямую зависят от полноты собираемой телеметрии (событий информационной безопасности) с хостов и средств защиты, составляющих информационную инфраструктуру организации. В основе эффективной работы SIEM лежит управление активами, их инвентаризация.

Учитывая этот факт, нарушители информационной безопасности могут оказывать воздействие на уровень сбора событий информационной безопасности, чтобы сокрыть свое присутствие в локальной сети.

Например, нарушитель может попытаться напрямую остановить сервис логирования событий на хосте, например, с помощью штатных системных средств (SC, PowerShell) или путем модификации соответствующих ключей реестра. В таком случае можно настроить корреляционные правила SIEM-системы учитывая такие события, как отключение службы логирования, очистка журнала мониторинга, а также осуществлять контроль содержимого командной строки в событиях запуска процессов.

Тем не менее, нарушитель может воспользоваться «слепым местом» в локальной сети, когда на некоторых хостах аудит информационной безопасности работает некорректно или не настроен. Стоит отметить, что передовые SIEM-системы оснащены функционалом, отслеживающим доступность подключенных источников, отсутствие определенного типа событий информационной безопасности, задержки в их получении. Использование этого функционала позволит своевременно обнаружить и устранить ошибки в настройках аудита или выявить потенциальную атаку на информационную инфраструктуру.

Рассмотрим примеры событий, для которых необходимо осуществлять мониторинг и настройку корреляционных правил в SIEM-системе [2,3].

Последовательное появление события неудачной попытки авторизации в системе в течение небольшого промежутка времени может указывать на потенциальную атаку подбора пароля. Например, для операционной системы Windows событие с event ID 4625, в котором также указана причина неудачной попытки входа в виде кода или в поле «Failure Reason». Таким образом, можно настроить агрегацию 6 таких событий за 15 минут для одной и той же учетной записи с одного IP-адреса в локальной сети. Еще одним вариантом мониторинга такого события может быть настройка агрегации 4 событий за 15 минут для разных учетных записей, размещенных на одном хосте. Такая последовательность событий также может также указывать на потенциальный перебор учетных записей и паролей к ним.

Необходимо отслеживать изменение прав доступа для учетных записей, особенно на критически значимых активах организации. При использовании в локальной сети контроллера домена можно отслеживать добавление пользователей в сетевые группы. Например, для операционной системы Windows события с event ID 4728, 4732, 4756, 4729, 4733, 4757. Для осуществления контроля и обеспечения информационной безопасности организации предоставление прав доступ пользователям должно быть согласовано с подразделением, отвечающем за информационную безопасность. Обнаружение событий изменения прав доступа учетных записей не в соответствии с согласованным доступом может указывать на действия нарушителя или халатность работников, создающую потенциальную уязвимость в локальной сети организации.

Несогласованные внутренние сканирования локальной сети могут являться попытками нарушителя изучить сетевую архитектуру, следовательно, можно настроить правила корреляции на их обнаружение. Например, можно отслеживать наличие сетевого трафика с одного IP-адреса на множество других, по определенному набору портов или по всем.

Для обеспечения безопасности корпоративной сети применяется технология ее сегментации. Следует отметить, что тестовые подсети также должны находиться в изолированном сетевом контуре. Можно настроить корреляционное правило, которое будет отслеживать исходящий (входящий) трафик из (в) тестовых подсетей. Если обнаруженные исходящие или входящие телекоммуникационные доступы не были согласованными, то это может быть признаком действий нарушителя или халатности

работников, создающей потенциальную уязвимость в локальной сети организации. Также необходимо отслеживать наличие несогласованных сетевых доступов во внешнюю сеть из внутренней сети или из изолированных сегментов, для которых такой доступ не предусмотрен.

Отслеживание изменений в конфигурации сетевого оборудования, в частности маршрутизаторов и межсетевых экранов, поможет своевременно выявить нарушение в регламентированных настройках сетевого оборудования или обнаружить предоставление сетевого доступа (изменение списков контроля доступа), которого быть не должно. После создания корреляционных правил необходимо отслеживать правильность их функционирования и, при необходимости, дорабатывать их, в том числе снижать количество ложноположительных сработок SIEM-системы. Для этого можно воспользоваться списками исключений и подбором более точных условий агрегации событий. Следует отметить, что ведение списков исключений представляет собой постоянный процесс.

Заключение

Системы класса SIEM играют важную роль в обеспечении информационной безопасности. Внедрение таких систем в информационную инфраструктуру организации значительно упрощает процесс мониторинга, а также повышает скорость обнаружения и реагирования на инциденты информационной безопасности. SIEM-система позволяет в режиме реального времени анализировать и коррелировать события информационной безопасности, приходящие с хостов, а также многочисленных средств защиты информации, таких как почтовые и хвостовые антивирусы, межсетевые экраны, WAF (Web Application Firewall), DLP-системы (Data Link Prevention), системы класса IDP/IPS и другие. Данный подход особенно актуален для организаций, обладающих большой информационной инфраструктурой, например, банковский сектор, где количество хостов исчисляется тысячами.

Список использованных источников

1. Gonzalez Granadillo G., Gonzalez Zarzosa S., Diaz R. (2021) Security Information and Event Management (SIEM). *ResearchGate*. 34 (2). 1–2.

2. Ertugrul A. (2016) Log correlation SIEM rule examples and correlation engine performance data. *ResearchGate*. 2 (2). 1–2.

3. Таблица Attack Mitre. – Текст: электронный // Mitre: официальный сайт. – 2025. – URL: https://attack.mitre.org/ (дата обращения: 15.02.2025).

References

1. Gonzalez Granadillo G., Gonzalez Zarzosa S., Diaz R. (2021) Security Information and Event Management (SIEM). *ResearchGate*. 34 (2). 1–2.

2. Ertugrul A. (2016) Log correlation SIEM rule examples and correlation engine performance data. *ResearchGate*. 2 (2). 1–2.

3. Attack Mitre Table. – Text: electronic // Mitre: official web-site. – 2025. – URL: https://attack.mitre.org/ (date of request: 15.02.2025).

Сведения об авторе

Алейникова Д.И., магистрант кафедры защиты информации. Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники». alein.diana@yandex.ru

Information about the author

Aleinikova D., master student o fthe Department of Information Security. Belarusian State University of Informatics and Radio Electronics. alein.diana@yandex.ru.