УДК 004.056.53

Алейникова Д.И.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

Научный руководитель:
Белоусова Е.С.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

МЕТОДИКА КОНФИГУРАЦИИ SIEM-СИСТЕМ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛЬНЫХ ДЕЙСТВИЙ В КОРПОРАТИВНОЙ СЕТИ

Аннотация. В статье представлена методика конфигурации SIEM-системы для обнаружения аномальных действий в корпоративной сети. Приведены примеры аномальных действий в корпоративной сети. Рассмотрены отличия сигнатурных правил корреляции от правил, основанных на поведенческом анализе, разработанных на основе данных базы знаний Mitre Att&ck.

Ключевые слова: система мониторинга, SIEM-система, методика конфигурации, корреляция, выявление инцидентов, Mitre Att&ck.

Введение

В настоящее время информационная безопасность является одним из приоритетных направлений для любой организации. Для своевременного выявления угроз и инцидентов применяются системы класса SIEM (Security Information and Event Management). Следует отметить, что эффективность работы SIEM-системы определяется правильностью ее конфигурации с учетом специфики конкретной информационной инфраструктуры.

Основная часть

SIEM-система – ключевой компонент в архитектуре SOC (Security Operational Center), обеспечивающий централизованный сбор событий информационной безопасности, мониторинг, выявление аномальных действий в корпоративной сети и оповещение команды реагирования о выявленных инцидентах [1].

К аномальным действиям могут относиться любые отклонения от штатной работы автоматизированных систем и поведения пользователей. Среди наиболее распространенных примеров таких действий можно выделить:

– попытки авторизации в локальной сети работниками в нерабочее время или из нетипичных геолокация, например, другой страны;

– несанкционированное повышение привилегий пользователем, не имеющим соответствующих полномочий;

– попытки доступа к конфиденциальной информации с устройств, с которых такой доступ не предусмотрен;

– запуск PowerShell или командной строки пользователем, работа которого не подразумевает использование данных инструментов;

– создание и изменение учетных записей без согласования с работниками отдела информационной безопасности и отдела информационных технологий;

– несогласованное с работниками отдела информационной безопасности и отдела информационных технологий изменение конфигураций оборудования.

Для своевременного выявления подобных угроз информационной безопасности можно эффективность конфигурации SIEM путем проведения анализа информационной инфраструктуры организации, определения критически важных активов, использования адаптивных правил корреляции, комбинировании сигнатурных правил корреляции и основанных на поведенческом анализе, а также использования актуальных баз знаний по техникам нарушителей, например, Mitre Att&ck [2].

Mitre Att&ck – это открытая база знаний о моделях поведения нарушителей информационной безопасности, основанная на реальных данных о кибератаках. Также она классифицирует тактики, техники и процедуры, которые применяются при проникновении в информационные системы и развитии кибератаки внутри сети.

Методика конфигурации SIEM-систем включает в себя следующие основные этапы:

1 Анализ информационной инфраструктуры организации. На данном этапе необходимо определить критически важные активы, используемые средства защиты, а также пользователей, обладающих повышенными привилегиями.

2 Подключение источников событий к SIEM-системе. На данном этапе необходимо настроить отправку логов оборудования, систем аутентификации, используемых в организации приложений и средств защиты в SIEM-систему. Следует отметить, что современные SIEM-системы обладают функционалом по нормализации получаемых логов – приведение их к единому формату для дальнейшего анализа.

3 Построение профиля нормального поведения пользователей и работы автоматизированных систем локальной сети. На данном этапе необходимо провести анализ штатной активности автоматизированных систем и пользователей локальной сети.

4 Настройка правил корреляции в SIEM-системе. На данном этапе существует несколько подходов к разработке правил корреляции – сигнатурные и с использованием поведенческого анализа.

Сигнатурные правила корреляции основываются на известных шаблонах событий, которые указывают на конкретные типы кибератак. Такие правила срабатывают при наличии точного совпадения настроенных в правиле параметров с данными из агрегируемых логов, таких как: идентификаторы событий, хэши вредоносных файлов, имена и пути расположения вредоносных процессов, обращения на IP-адреса и доменные имена, связанные с вредоносной активностью, точные команды с определенными параметрами, запускаемые в PowerShell. Преимущество сигнатурных правил: высокая точность при обнаружении уже известных угроз. Недостаток: не позволяют выявлять новые или модифицированные атаки.

Правила, основанные на поведенческом анализе, ориентированы на анализ отклонения от штатной работы систем и пользователей локальной сети, обычно подразумевают реализацию определенных цепочек событий, отражающих логику действий нарушителя информационной безопасности. Для построения таких цепочек событий можно использовать открытую базу знаний Mitre Att&ck. Преимущество правил, основанных на поведенческом анализе: позволяют выявлять новые или модифицированные атаки. Недостаток: большое количество ложных сработок, требующих проведения повторного анализа цепочки событий и правила корреляции, его корректировки.

5 Тестирование и корректировка. На данном этапе происходит тестирование настроенных правил корреляции, анализ ложных срабатываний SIEM-системы, корректировка и доработка созданных правил корреляции. Для снижения количества ложных срабатываний можно воспользоваться списками исключений и подбором более точных условий агрегации событий, доработкой логики работы правила.

6 Непрерывное обновление и обогащение SIEM-системы. Необходимо регулярно пересматривать правила корреляции и актуализировать их для своевременного выявления новых угроз, а также обновлять используемые списки исключений и базы сигнатур. Необходимо на постоянной основе отслеживать наличие логов оборудования, систем аутентификации, используемых в организации приложений и средств защиты в SIEM-системе, по мере увеличения информационной инфраструктуры подключать новые источники.

Следует отметить, что после обнаружения аномальных действий в корпоративной сети важно обеспечить своевременное реагирование. Для этого необходимо разработать сценарии реагирования на инциденты, возможно, настроить интеграцию со специализированными средствами автоматизации для повышения эффективности реагирования.

Заключение

Эффективная конфигурация SIEM-системы – это непрерывный процесс, подразумевающий комплексный подход, учитывающий особенности информационной инфраструктуры организации, модели

поведения нарушителей информационной безопасности и легитимных пользователей локальной сети, а также особенности архитектуры используемой SIEM-системы и ее механизмы сбора, обработки и анализа событий информационной безопасности. Использование базы знаний Mitre Att&ck при конфигурировании SIEM-системы позволяет существенно обогатить логику ее работы, так как в таком случае правила корреляции основаны на логике реализации атаки, ее последовательных этапах, а не только на использовании сигнатур. Дополнение сигнатурных правил корреляции правилами, основанными на поведенческом анализе позволяет выявлять более сложные или неизвестные ранее атаки, что значительно повышает уровень защищенности корпоративной сети.

Список использованных источников:

1. Алейникова Д.И. Системы управления информационной безопасностью и событиями информационной безопасности // Технические средства защиты информации: материалы XXIII Международной научно-технической конференции, Минск, 08 апреля 2025 г. Минск: БГУИР, 2025. С. 51–54.

2. Таблица Attack Mitre. // Mitre: официальный сайт. 2025. URL: https://attack.mitre.org/ (дата обращения: 22.04.2025).

Aleinikova D.I.
Belarusian State University of
Informatics and Radioelectronics, Minsk

Scientific supervisor:
Belousova E.S.
Belarusian State University of
Informatics and Radioelectronics, Minsk

THE METHODOLOGY FOR CONFIGURING SIEM SYSTEMS TO DETECT ABNORMAL ACTIVITY IN A CORPORATE NETWORK

Abstract. The methodology for configuring a SIEM system to detect abnormal activity in a corporate network is considered. Examples of abnormal actions in the corporate network are given. The differences between the signature rules of correlation and the rules based on behavioral analysis, developed on the basis of data from the Mitre Att&ck knowledge base, are considered.

Keywords: monitoring system, SIEM system, configuration methodology, correlation rules, incident detection, Mitre Att&ck.