Электронный научный журнал "Математическое моделирование, компьютерный и натурный эксперимент в естественных науках" http://mathmod.esrae.ru/
URL статьи: **mathmod.esrae.ru/49-204**
Ссылка для цитирования этой статьи:
Коклянов А.Е. Применение SIEM-систем для обеспечения информационной безопасности автоматизированных систем // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2025. №1

УДК 004.056 DOI:10.24412/2541-9269-2025-1-46-52

ПРИМЕНЕНИЕ SIEM-СИСТЕМ В ХОДЕ ПРОВЕДЕНИЯ УЧЕНИЙ НА ПЛАТФОРМЕ КИБЕРПОЛИГОНА

Коклянов А.Е.
Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов, moderncreed34@gmail.com

APPLICATION OF SIEM SYSTEMS DURING EXERCISES ON THE CYBER RANGE PLATFORM

Koklyanov A.E.
Yuri Gagarin State Technical University of Saratov, Russia, Saratov, moderncreed34@gmail.com

Аннотация. В статье рассматривается архитектура SIEM-систем и их основные компоненты, вопросы применения SIEM-систем на платформе киберполигона и влияния использования SIEM-систем при подготовке специалистов наступательной безопасности и специалистов службы мониторинга и реагирования на инциденты информационной безопасности в ходе киберучений, а также тенденции на рынке киберполигонов в России.

Ключевые слова: SIEM-система, мониторинг и реагирование на инциденты, киберполигон, киберучения.

Abstract. The article discusses the architecture of SIEM systems and their main components, the issue of using SIEM systems on a cyber range platform, the impact of using SIEM systems in training offensive security specialists and specialists in the service for monitoring and responding to information security incidents during cyber exercises, as well as trends in the cyber range market in Russia.

Keywords: SIEM system, monitoring and incident response, cyber training ground, cyber exercises.

SIEM (Security Information and Event Management) — это класс программных решений, предназначенных для централизованного сбора, анализа и управления данными о событиях безопасности в ИТ-инфраструктуре организации. SIEM объединяет две ключевые функции: управление информацией о безопасности (SIM) и управление событиями безопасности (SEM).

Главная задача SIEM-систем — анализ данных, поступающих из различных источников. На основе этого анализа выявляются отклонения от нормального режима работы, заданного критериями безопасности, и в случае обнаружения таких отклонений система уведомляет администратора безопасности. [1]

Типовая SIEM-система также может использоваться для следующих целей:

− анализа данных, поступающих из разных источников;

− формирования доказательной базы при расследовании инцидентов информационной безопасности;

− предоставления структурированной информации для аудита информационной безопасности;

− обеспечения непрерывности работы сервисов путем выявления сбоев;

− структуризации информационно-телекоммуникационной системы. [2]

Основные задачи, которые решает SIEM-система в области информационной безопасности, включают:

− сбор и хранение журналов событий;

− анализ событий и расследование инцидентов;

− обработку и корреляцию событий;

− уведомление об инцидентах и управление ими.

Обычно SIEM-система состоит из следующих ключевых компонентов (рис. 1):

− агенты, которые собирают данные из различных источников;

− серверы-коллекторы, накапливающие информацию от агентов;

− сервер корреляции;

− сервер баз данных.

Рис.1.

Киберполигон – это искусственно сконструированная виртуальная среда, которая имитирует реалистичные сети и системы и может применяться для обучения, тестирования, проведения учений или исследований в киберпространстве. Киберполигон имитирует инфраструктуры операционных технологий, критические инциденты безопасности в информационных системах и используемые в обучении информационной безопасности, тренировках и учениях по кибербезопасности. Основное преимущество использования киберполигона заключается в возможности протестировать в безопасной и изолированной виртуальной среде ситуации и стратегии обороны/нападения от кибератак. [3]

В киберучениях принимают участие две команды: атакующих («Red Team») и защитников («Blue Team»).

Команда атакующих проводит тестирование на проникновение информационной системы, представленной на киберполигоне. Это является примером наступательной безопасности (Offensive Security) — стратегии, направленной на применении активных мер взлома с целью нахождения уязвимостей компьютерных систем.

Тестирование на проникновение представляет собой тестирование системы на наличие критических уязвимостей и проблем. Данная методика позволяет определить уровень безопасности и оценить устойчивость информационной системы за счет полноценного моделирования атаки хакеров. Пентест проводит атакующая сторона, применяя специализированные программные средства, уязвимости серверов, операционных сред и пр.

Команда защитников занимается вопросом обнаружением, анализом инцидентов кибербезопасности, оперативным реагированием, предотвращением их возникновения и составлением отчетности, также ее называют командой SOC (Security Operation Center/Центр обеспечения безопасности). Необходимостью обучения сотрудников SOC является то, что специалисты получают опыт только из реальных инцидентов, количество которых может быть не так велико.

Функции центра мониторинга безопасности могут отличаться в зависимости от масштаба предприятия и его организационной структуры. Обычна они состоят из этапов, продемонстрированных на рисунке 2.

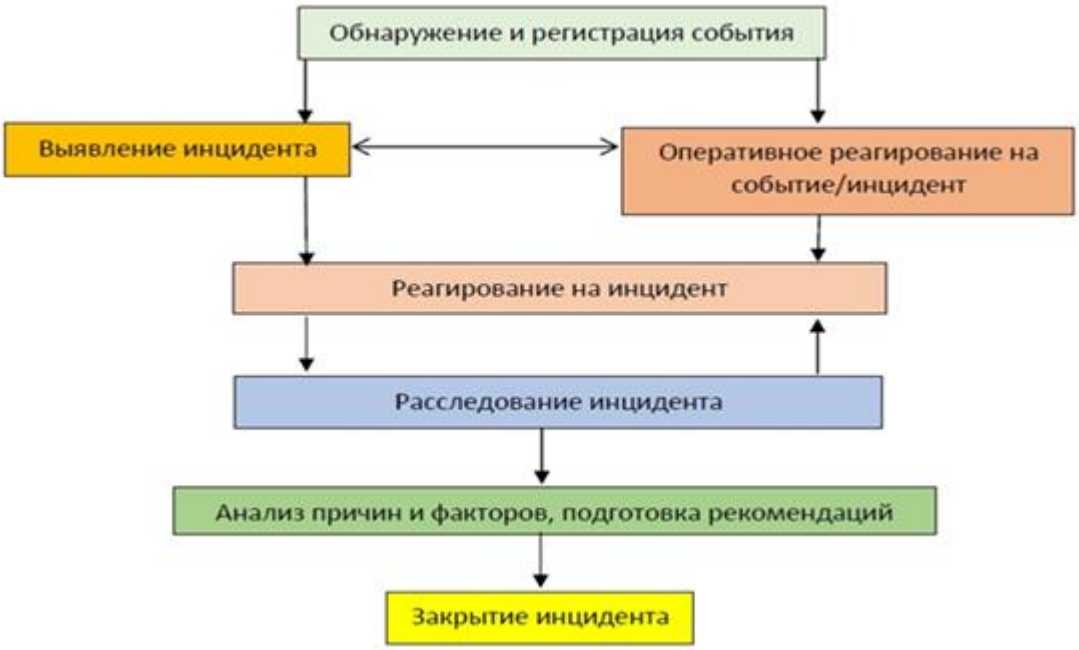

Рис. 2.

Основным инструментом команды по расследованию инцидентов является SIEM-система, к которой подключается посредством агентов конкретной системы каждый узел киберполигона: сервера, сетевые устройства, АРМ и т.д.

SIEM-система на киберучениях поможет команде мониторинга отследить цепочку атаки, узлы инфраструктуры, на которые идут попытки атаки команд пентестеров, для своевременного реагирования на инциденты и устранения брешей в безопасности инфраструктуры, представленной на киберполигоне. При помощи специальных фильтров поиска в индексах SIEM-системы можно найти сработки определенных правил. Можно использовать фильтры на поиск конкретного правила, либо на поиск по подстроке в логе, например, логине учетной записи, которую удалось скомпрометировать. Функционал SIEM может позволить команде мониторинга оперативно работать в условиях координации нескольких человек в ограниченном временном промежутке.

Логирование действий пользователей поможет определить не только скорость реагирования на инцидент Blue team и её порядок действий, были действия удачными или нет, но и порядок действий Red team, правильно ли был выбран вектор атаки, какие инциденты были реализованы и т.д.

В целом, киберучения и SIEM-системы могут помочь в таких аспектах, как:

- обнаружение несогласованных действий между участниками команд;
- выявление недостатков в коммуникациях между участниками;
- обнаружение ошибок в текущих бизнес-процессах и документации, которая их описывает;
- выявление ошибок и уязвимостей в настройке инструментов и систем, включая системы защиты информации. [4]

Но также, проведение киберучений может помочь соблюсти следующие требования нормативно-правовых документов Российской Федерации. Так, обязательность проведения киберучений для предприятий в настоящее время закреплена в п. 10 Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации (утв. приказом ФСБ России от 19.06.2019 № 282):

субъект, имеющий значимые объекты КИИ, не реже одного раза в год организует и проводит тренировки по отработке мероприятий Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак;

организация и проведение тренировок возлагаются на подразделения и должностных лиц субъекта КИИ, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак. [5]

Кроме того, нормативно-правовые акты, регламентирующие требования по безопасности значимых объектов КИИ (утвержденные приказами ФСТЭК России от 21.12.2017 № 235 и 25.12.2017 № 239), содержат нормы по информированию и обучению работников субъектов КИИ.

Таким образом, планирование и реализация киберучений обеспечивает выполнение требований:

п. 25 Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (утв. приказом ФСТЭК России от 21.12.2017 № 235);

п. 13 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утв. приказом ФСТЭК России от 25.12.2017 № 239), а также следующих видов мер по обеспечению безопасности значимого объекта: ДНС.2, ИПО.2, ИПО.3. [6]

В целом, на рынке информационной безопасности формируется устойчивое понимание, что для эффективного повышения уровня защиты недостаточно просто установить оборудование и настроить программное обеспечение. [7] Необходимо заниматься информационной безопасностью предприятий систематически, в чем и могут помочь SIEM-системы. При помощи них можно реализовывать самые различные мероприятия, контролировать внешний периметр, проводить сканирования оборудования и программного обеспечения на уязвимости, собирать все события в одном месте, формировать отчеты и т.д.

В этом контексте киберполигоны, набирающие популярность, становятся ключевым инструментом для внедрения регулярной практики и формирования культуры ИБ. Они охватывают широкий спектр аспектов безопасности: пентестинг, OSINT, мониторинг, реагирование на инциденты и многое другое.

Разнообразие форматов, таких как Blue Team, Red Team, CSIRT и их взаимодействие, позволяет отрабатывать различные тактики атак и защиты, изучать уязвимости и методы их устранения.

Особенно востребованы киберполигоны в высших учебных заведениях, которые стремятся перейти от теоретического подхода к практическому обучению. Например, в ряде технических вузов студенты регулярно занимаются на базе киберполигонов, используют их в курсовых и дипломных проектах, сдают зачеты по реальным сценариям. Это позволяет им получить практические навыки, близкие к реальным условиям, и лучше подготовиться к работе в ИБ-компаниях. Более того, с появлением киберполигонов для детей к этому процессу подключаются и общеобразовательные школы, что указывает на долгосрочную тенденцию.

Киберполигоны также привлекают внимание предприятий топливно-энергетического комплекса и финансовых организаций. Заказчики заинтересованы в проведении киберучений на цифровых двойниках, чтобы сотрудники могли тренироваться в условиях, максимально приближенных к реальным. Однако создание таких двойников — сложная задача из-за специфического ПО и оборудования, что замедляет распространение киберполигонов в этих отраслях по сравнению с вузами. Тем не менее, спрос на такие решения продолжает расти, так как существующие платформы активно развиваются, а создание собственного киберполигона требует значительных ресурсов.

Одним из направлений развития киберполигонов является сотрудничество с отраслевыми научными институтами для создания специализированных шаблонов. Например, в 2023 году совместными усилиями НТЦ МЭИ и «Перспективного мониторинга» был разработан цифровой двойник энергосистемы, интегрированный в киберполигон. В нем моделируются атаки, перехватывающие управляющие сигналы к релейной защите и автоматике (РЗА), что приводит к коротким замыканиям на подстанциях. Особенность таких атак в том, что оператор SCADA-системы не видит изменений до момента возникновения аварии. Другим примером является сценарий, представленный на фестивале PHDays, где участники кибербитвы атаковали инфраструктуру двух виртуальных государств, что приводило к остановке нефтеперекачки, транспортному коллапсу и другим последствиям, визуализированным на физических макетах.

Рынок киберполигонов находится на стадии активного роста. Пока что такие решения внедрены лишь в небольшой части организаций, заинтересованных в повышении уровня ИБ, но их доля на рынке будет увеличиваться. На данный момент прямых аналогов киберполигонов не существует. Самостоятельное развертывание подобных комплексов крайне сложно и дорого, поэтому тенденция роста рынка киберполигонов сохранится в ближайшие годы и окажет значительное влияние на образование в сфере ИБ.

Литература

1. Бурмакин, А. О. Применение SIEM-систем для обеспечения безопасности корпоративных сетей / А. О. Бурмакин, Э. А. Воробьев, В. А. Гохович // Синергия Наук. – 2020. – № 44. – С. 485-490. – EDN MNHNXE.
2. Матвеев, Д. В. Управление SIEM системами / Д. В. Матвеев // Тенденции развития науки и образования. – 2024. – № 115-6. – С. 107-110. – DOI 10.18411/trnio-11-2024-261. – EDN DUJJGV.
3. Киберполигон – мультифункциональный комплекс для проведения киберучений // Habr : сайт – URL: https://habr.com/ru/articles/80586/ (дата обращения: 08.02.2025)
4. Киберучения и киберполигоны для безопасности КИИ // itsec.ru : сайт. – URL: https://www.itsec.ru/articles/kiberucheniya-i-kiberpoligony-dlya-bezopasnosti-kii (дата обращения: 09.02.2025)
5. Приказ Федеральной службы безопасности Российской Федерации от 19.06.2019 № 282 "Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информацио // Официальное опубликование правовых актов : сайт. – URL: http://publication.pravo.gov.ru/Document/View/0001201907170025 (дата обращения: 11.02.2025)
6. Приказ ФСТЭК России от 25 декабря 2017 г. N 239 // ФСТЭК России : сайт. – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 11.02.2025)
7. Мелихов, Г. Киберполигоны в стадии роста: преимущества и перспективы / Г. Мелихов // Connect : электронный журнал. – URL: https://www.connect-wit.ru/izdaniya-connect.html#flipbook-df_97612/62/ (дата обращения: 11.02.2025).