Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.056.5

Никита Федорович ЧАГАН

СИСТЕМА МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СЕТИ ОРГАНИЗАЦИИ

Автореферат
на соискание степени магистра
по специальности 1-98 80 01 Информационная безопасность

Научный руководитель
д. техн. н., профессор
Тимофей Валентинович БОРБОТЬКО

Минск 2024

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научной, научно-технической и инновационной деятельности

Тема диссертационной работы соответствует разделу 6 «Обеспечение безопасности человека, общества и государства» приоритетных направлений научной, научно-технической и инновационной деятельности в Республике Беларусь на 2021–2025 годы, утвержденных Указом Президента Республики Беларусь от 7 мая 2020 г. № 156. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке и апробации системы мониторинга событий информационной безопасности в информационной сети организации на основе SIEM и IDS.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

изучить методологическую базу и опыт базы знаний MITRE ATT&CK;

составить модель нарушителя и определить индикаторы его присутствия в информационной сети организации;

изучить особенности построения систем мониторинга;

сформировать систему мониторинга событий информационной безопасности на основе SIEM и IDS;

разработать правила корреляции для выявления нарушителя по определенным индикаторам компрометации;

апробировать разработанную систему мониторинга событий информационной безопасности.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на XXI Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, 2023).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 2 статьи в сборниках материалов конференций:

XXI Белорусско-российская научно-техническая конференция «Технические средства защиты информации» (Минск, 6 июня 2023 г.);

60-я юбилейная научная конференция аспирантов, магистрантов и студентов (Минск, 22–26 апреля 2024 г.).

Личный вклад соискателя

Содержание диссертации отображает личный вклад автора. Основные результаты, изложенные в диссертационной работе, получены соискателем самостоятельно.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем доктором технических наук, профессором Тимофеем Валентиновичем БОРБОТЬКО.

Проверка на уникальность

Проведена экспертиза диссертации Чагана Никиты Федоровича «Система мониторинга событий информационной безопасности в информационной сети организации» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: https://antiplagiat.ru) в онлайн режиме 17.06.2024 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 78,7%).

ВВЕДЕНИЕ

На современном этапе развития человеческой цивилизации бесспорным является факт базирования экономики на такой отрасли высоких технологий, как компьютерные системы, разветвленные по всей планете и объединяющие в единое целое практически все государства мира. В то же время динамичное внедрение новейших высокотехнологичных систем и средств в различные сферы жизнедеятельности современного человека не только привело к развитию положительных процессов и явлений, но и обозначило целый ряд проблем негативного характера, а нередко и социально опасного. Сегодняшняя действительность богата примерами явного преступного использования высоких технологий.

Одним из актуальных направлений в сфере информационной безопасности является мониторинг событий. В научном мире и прикладной деятельности он показывает нерешенность вопросов недостаточного покрытия данных, низкой точности обнаружения, отсутствия автоматизации, анализа, метрик и оценки, недостаточности взаимодействия с другими системами безопасности, а также отражает положения стратегического развития данного направления, что непосредственно связано с темой исследования.

Объектом исследования является автоматизированная информационная система мониторинга событий информационной безопасности, основанная на базе системы, предназначенной для обнаружения несанкционированных действий или вторжений в сеть или компьютерную систему, а также платформы для сбора, анализа и корреляции логов и событий безопасности из различных источников.

Предмет исследования: технологии двух важных компонентов в экосистеме кибербезопасности, которые используются для мониторинга, обнаружения и реагирования на потенциальные угрозы безопасности, обеспечивают раннее предупреждение о потенциальных кибератаках и несанкционированной деятельности.

Целью исследования является разработка и апробация системы мониторинга событий информационной безопасности в информационной сети организации на основе SIEM и IDS.

Для достижения цели поставлен следующий ряд задач:

– изучить методологическую базу и опыт базы знаний MITRE ATT&CK;

– составить модель нарушителя и определить индикаторы его присутствия в информационной системе организации;

– изучить особенности построения систем мониторинга;

– сформировать систему мониторинга событий информационной безопасности на основе SIEM и IDS;

– разработать правила корреляции для выявления нарушителя по определенным индикаторам компрометации;

– апробировать разработанную систему мониторинга событий информационной безопасности.

В качестве **методов исследований** применяются:

– анализ литературы. Метод включает обзор и анализ литературы, научных статей, публикаций и других источников по теме информационной безопасности. Он помогает изучить наработанный уровень знаний в области, выявить проблемы и недостатки, а также идентифицировать возможные направления исследования;

– экспериментальные исследования, что подразумевает проведение экспериментов и практических исследований, с тем чтобы проверить гипотезы и получить определенные данные. Для настоящего исследования может включать тесты на проникновение, анализ уязвимостей и т. д.;

– моделирование и симуляция. Использование моделей и симуляций дает возможность исследовать различные сценарии и прогнозировать поведение систем мониторинга. Так, например, определить уязвимости и обнаружить нарушителя возможно с помощью смоделированной атаки;

– кейс-исследования. Проведение кейс-исследований (детальный анализ конкретных случаев) позволяет получить глубокое понимание проблем, причин их возникновения и необходимых решений в области событий информационной безопасности. Изучение конкретных ситуаций и реальных примеров будет способствовать разработке рекомендаций и оценке эффективности решений;

– мета-анализ. Позволяет суммировать и анализировать результаты предыдущих исследований, выявить общие тенденции, противоречия и пробелы в области мониторинга событий информационной безопасности.

Исходными данными для разработки темы являются информация о текущих и возникавших ранее угрозах на основе базы данных угроз, включая типы атак, их характеристики и методы обнаружения; детализированные описания атак, которые использовались известными хакерскими группировками; информация об известных уязвимостях в используемом программном и аппаратном обеспечении; результаты проверок и аудитов безопасности, выявленные уязвимости и рекомендации по их устранению.

Практическая значимость результатов исследования заключается:

– в совершенствовании системы безопасности в информационной сети организации. Результаты исследования мониторинга событий информационной безопасности помогут в выявлении уязвимостей, аномалий и потенциальных угроз в системе безопасности, что даст возможность принять меры по улучшению защиты и предотвращению инцидентов в будущем. Основываясь на полученных данных, можно определить образцы поведения и паттерны атак, что впоследствии будет способствовать разработке эффективных стратегий защиты;

– в раннем обнаружении инцидентов. Мониторинг событий информационной безопасности позволит выявлять инциденты в режиме реального времени или близком к нему. Результаты исследования помогут определять индикаторы компрометации (Indicators of Compromise, IoC), которые подтверждают наличие атаки или нарушение безопасности. Это дает возможность оперативно реагировать на инциденты, минимизировать нанесенный ущерб и восстанавливать работоспособность системы;

– в оптимизации ресурсов. Результаты исследования мониторинга помогут в определении наиболее значимых, требующих особого внимания событий, что позволит оптимизировать использование ресурсов, направлять их на мониторинг и анализ наиболее критических моментов, а также на основе полученных данных упростит принятие решений;

– в совершенствовании стратегий реагирования на инциденты. Результаты исследования мониторинга будут способствовать разработке

более эффективных стратегий реагирования на инциденты информационной безопасности. Анализ полученных данных поможет определить наиболее эффективные методы и инструменты для обнаружения, анализа и устранения инцидентов, что повлечет сокращение времени реагирования, снижение последствий инцидентов и более эффективное восстановление работоспособности системы;

– в предотвращении будущих инцидентов. Результаты исследования мониторинга событий могут быть использованы для предотвращения будущих инцидентов информационной безопасности. Анализ прошлых инцидентов и образцов атак дает возможность разработать меры предосторожности, усилить защиту и обновить политику безопасности. Это снизит риск и вероятность возникновения инцидентов в будущем.

Результаты исследований опубликованы в статьях и сборниках [1-А, 2-А].

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрены проблемы необходимости проведения исследования по данной тематике.

В **общей характеристике работы** показана связь работы с приоритетными направлениями научных исследований, цель и задачи исследования, личный вклад соискателя ученой степени, апробация результатов диссертации.

В первой главе мы рассмотрели процесс выбора и анализа организованных преступных групп на основе базы знаний MITRE ATT&CK. Эта база знаний предоставляет ценную информацию о тактиках, техниках и процедурах, используемых киберпреступниками, что позволяет проводить более глубокий и информированный анализ.

В результате анализа базы знаний MITRE ATT&CK мы смогли выделить характеристики различных преступных групп, их цели, методы и инструменты, оценить их способности и уровень угрозы. Это помогло в выборе конкретной группы для дальнейшего исследования. Такой подход позволил принимать обоснованные решения и представить аргументированные выводы на основе объективных фактов и данных. В итоге использование базы знаний MITRE ATT&CK при выборе и анализе организованных преступных групп позволило проводить более глубокое и информированное исследование. Такой подход повысил эффективность действий в области кибербезопасности и способствовал предотвращению

угроз, минимизации рисков и защите систем и данных.

Важным результатом данного анализа является составление обобщенной модели нарушителя.

Определение индикаторов компрометации на основе базы знаний ATT&CK является значимым шагом для обеспечения безопасности. Анализ тактик, техник и процедур, применяемых нарушителями, позволил выделить характерные признаки компрометации и создать обобщенные правила и сигнатуры для обнаружения атак. Это необходимо для повышения эффективности обнаружения и реагирования на угрозы информационной безопасности.

Исходя из изложенного сформулированы выводы о необходимости:

идентификации характерных признаков. Анализ информации о различных тактиках, техниках и процедурах, используемых нарушителями, позволил определить характерные признаки компрометации, которые могут указывать на наличие атаки или нарушителя;

создания обобщенных правил и сигнатур для обнаружения и определения атак на основе характерных индикаторов компрометации, что способствовало автоматизации процессов обнаружения и реагирования на атаки;

повышения эффективности обнаружения, что позволит улучшить эффективность обнаружения атак, сократить время реагирования, поможет предотвратить ущерб и минимизировать последствия компрометации данных и систем.

Во второй главе рассмотрены основные аспекты построения систем мониторинга, которые играют ключевую роль в обеспечении безопасности информационных ресурсов организации. Обозначена роль систем мониторинга, их значение для обнаружения угроз безопасности, а также значимость для обеспечения безопасности информационных систем.

Разобраны основные компоненты архитектуры систем мониторинга, включая сбор данных, нормализацию, анализ, хранение, интеграцию с другими системами безопасности и визуализацию результатов.

Рассмотрены различные средства мониторинга событий, включая SIEM, системы обнаружения вторжений, системы обнаружения компрометации и другое. Каждое из них имеет свои особенности и применение в области обеспечения безопасности информационных ресурсов.

Представлены алгоритмы функционирования систем мониторинга, включая процесс сбора данных, анализ аномалий, реагирование на инциденты и администрирование системы.

Подчеркнута значимость построения систем мониторинга событий

информационной безопасности для обнаружения и предотвращения угроз, а также повышения общего уровня безопасности информационных систем.

Исходя из проведенного анализа отмечено, что комбинация определенных SIEM- и IDS-систем позволит сформировать комплексный подход при создании системы мониторинга событий информационной безопасности в корпоративной сети. Данные системы играют ключевую роль в обеспечении защиты ИТ-инфраструктуры, так как они обеспечивают сбор, анализ и корреляцию данных для выявления и предотвращения инцидентов безопасности.

Таким образом, совмещение указанных систем позволит своевременно получить достоверные данные о нахождении нарушителя в информационной сети предприятия, а также экономить финансовые, временные и человеческие ресурсы при технической поддержке и сопровождении данного решения.

В целом представляется комплексное понимание о системах и средствах мониторинга событий информационной безопасности, их роли и важности в обеспечении безопасности информационных ресурсов организации.

В третьей главе проведена разработка и апробация системы мониторинга событий информационной безопасности, построенной на базе MaxPatrol SIEM и Suricata IDS. В результате проведенных исследований и экспериментов получены важные выводы, подчеркивающие эффективность и потенциал данной системы для защиты корпоративной сети от киберугроз.

Использование MaxPatrol SIEM в сочетании с Suricata IDS показало высокую эффективность в обнаружении и реагировании на различные киберугрозы. Suricata IDS успешно выявляет аномалии и подозрительный сетевой трафик, в то время как MaxPatrol SIEM анализирует события, собирает и обрабатывает данные из различных источников, обеспечивая комплексную картину происходящего в сети. Такое сочетание позволяет не только обнаруживать текущие угрозы, но и оперативно реагировать на инциденты безопасности, минимизируя потенциальные риски и ущерб.

Система успешно справляется с задачами обнаружения сложных киберугроз, таких как атаки, характерные для известных группировок APT35, APT37, APT41 и Lazarus. Однако выявленные в ходе апробации ложные срабатывания подчеркивают необходимость дальнейшей оптимизации настроек Suricata IDS и MaxPatrol SIEM для повышения точности и снижения количества ложных тревог. Это требует тщательной настройки сигнатур и алгоритмов обнаружения, а также адаптации системы к специфике конкретной корпоративной сети.

Апробация системы также подтвердила, что использование комбинации SIEM и IDS дает более глубокое и всестороннее видение возникающих

проблем. SIEM позволяет не только выявлять и анализировать инциденты безопасности, но и осуществлять аудит и контроль соблюдения политик безопасности, обеспечивая комплексное управление рисками и инцидентами. IDS, в свою очередь, обеспечивает оперативное обнаружение и предотвращение сетевых атак, что особенно важно для защиты от угроз, поступающих извне.

Результаты апробации указывают на необходимость продолжения работы по улучшению системы мониторинга. В частности, следует уделить внимание:

оптимизации параметров обнаружения в Suricata IDS для снижения ложных срабатываний;

расширению функциональности MaxPatrol SIEM для более глубокого анализа данных и совершенствованию механизмов реагирования на инциденты;

интеграции дополнительных источников данных в целях повышения точности и полноты анализа;

разработке и внедрению продвинутых методов машинного обучения и искусственного интеллекта для более точного прогнозирования и обнаружения сложных угроз.

Проведенная апробация системы мониторинга событий информационной безопасности на базе MaxPatrol SIEM и Suricata IDS подтвердила высокую эффективность данного решения в обеспечении защиты корпоративных сетей от современных киберугроз. Выявленные в ходе исследований результаты свидетельствуют о значительном потенциале в области развития и совершенствования системы, что позволит еще более эффективно противостоять угрозам информационной безопасности и обеспечивать надежную защиту корпоративных данных и ресурсов.

ЗАКЛЮЧЕНИЕ

В данном исследовании была проведена работа по разработке и реализации системы мониторинга событий информационной безопасности в информационной сети.

Осуществлен анализ, обоснование деятельности и выбор организованных преступных группировок по базе знаний MITRE ATT&CK, в ходе чего выбраны 4 преступные группировки (Lazarus, APT35, APT37, APT41), целями которых являются организации Беларуси и России.

На основании полученных данных, используя Unified Kill Chain, составлена обобщенная модель нарушителя. С помощью базы знаний MITRE

ATT&CK определены общие характеристики и профили нарушителей, их мотивация, цели, уровень сложности и доступные ресурсы, а также создана обобщенная модель, которая будет учитывать типичные характеристики группировок и предсказывать их возможные действия.

Определение индикаторов компрометации на основе базы знаний MITRE ATT&CK является важным шагом для обеспечения безопасности. Анализ тактик, техник и процедур, применяемых нарушителями, позволил выделить характерные признаки компрометации и создать обобщенные правила и сигнатуры для обнаружения атак в целях повышения эффективности обнаружения и реагирования на угрозы информационной безопасности.

Проведен анализ особенностей построения систем мониторинга в целях определения возможности сочетания нескольких систем для обеспечения всестороннего анализа событий информационной безопасности и последующего реагирования на них. Также рассмотрены различные источники информации о событиях информационной безопасности и проведен анализ средств мониторинга.

В результате были выбраны две системы – SIEM и IDS – для организации системы мониторинга событий информационной безопасности информационной сети.

Описана архитектура системы мониторинга на базе таких систем, как MaxPatrol SIEM и Suricata IDS. Построен алгоритм ее функционирования. Определен перечень событий информационной безопасности, подлежащих контролю, средства для его обеспечения.

Идентифицированы и категорированы возможные угрозы со стороны выбранных преступных группировок. Осуществлены сбор и агрегирование данных из разных источников для дальнейшего анализа и корреляции. Рассмотрены различные подходы для выполнения данных задач. Скоррелированы и проанализированы поступающие события. На основе результатов анализа сделаны прогнозы будущих событий и разработана стратегия управления рисками или принятия решений.

Проведена апробация и всесторонняя оценка построенной на базе MaxPatrol SIEM и Suricata IDS системы мониторинга событий информационной безопасности в корпоративной сети. Исследование включило в себя анализ теоретических аспектов информационной безопасности, практическую апробацию системы в реальных условиях и оценку ее эффективности в противодействии современным киберугрозам.

В ходе работы продемонстрированы преимущества комплексного подхода к информационной безопасности, заключающегося в интеграции

системы управления информационной безопасностью (SIEM) и системы обнаружения вторжений (IDS). MaxPatrol SIEM с его обширными возможностями по сбору и анализу данных в сочетании с Suricata IDS, обеспечивающей оперативное обнаружение сетевых атак, позволяет создавать многоуровневую эффективную защиту сетей организации. Такой подход способствует не только обнаружению текущих угроз, но и предотвращению потенциальных инцидентов безопасности, что существенно снижает риски для информационных систем.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Тезисы конференций

1-А. Чаган Н.Ф. База знаний MITRE ATT&CK для построения модели нарушителя информационной безопасности / Чаган Н.Ф. // XXI Белорусско-российская научно-техническая конференция : тезисы докладов XXI Белорусско-российской научно-технической конференции Республика Беларусь, Минск, 6 июня 2023 г. / редкол. : Т.В. Борботько [и др.]. – Минск : БГУИР, 2023. – 104 с.

2-А. Чаган Н.Ф. Система и средства мониторинга событий информационной безопасности / Чаган Н.Ф. // 60-я юбилейная научная конференция аспирантов, магистрантов и студентов : тезисы докладов 60-й юбилейной научной конференции аспирантов, магистрантов и студентов. Минск, 22–26 апреля 2024 г. / редкол. : Т.В. Борботько [и др.]. – Минск : БГУИР, 2024. –