КОМПЛЕКСНЫЙ АНАЛИЗ ПОВЕДЕНИЯ СИСТЕМЫ WINDOWS ДЛЯ ОБНАРУЖЕНИЯ КИБЕРУГРОЗ

Долгачев М. В.[1], Костюнин В. А.[2]

DOI: 10.21681/2311-3456-2025-2-71-77

Цель работы: *разработка и анализ методов обнаружения аномалий на конечных хостах системы Windows в рамках централизованного решения класса SIEM с использованием машинного обучение и комплексного подхода, для повышения эффективности и точности выявления потенциальных угроз безопасности в контексте современных кибератак.*

Метод исследования: *исследование основывается на теоретическом анализе существующих подходов к обнаружению аномалий, а также на практическом применении машинного обучения для анализа данных событий безопасности, собранных через SIEM-системы. Анализ включает изучение матрицы MITRE ATT&CK для определения ключевых событий, указывающих на возможные атаки и разработку алгоритмов для их обнаружения.*

Результаты исследования: *в исследовании показано, что разработанная методика обнаружения аномалий, основанная на анализе ключевых событий системы Windows и комплексном подходе к обнаружению аномалий, позволяет значительно повысить точность и эффективность обнаружения инцидентов информационной безопасности в сетевой инфраструктуре. Это способствует более быстрому и точному реагированию на угрозы безопасности. Применение полученных результатов может улучшить системы обнаружения аномалий в Security Operations Centers (SOC), укрепляя таким образом общую кибербезопасность организаций.*

Научная новизна: *работа предлагает новый взгляд на обнаружение аномалий, акцентируя внимание на необходимости комплексного анализа и использования машинного обучения для обработки больших объемов данных собранных с SIEM систем. Также подчеркивается важность адаптации методов обнаружения аномалий к специфике системы Windows и учета последних тенденций в области кибербезопасности.*

Ключевые слова: *SIEM, аномалия поведения, журнал событий, анализ инцидентов, мониторинг событий, матрица MITRE.*

Введение

В современном мире кибербезопасности, где атаки становятся все более сложными и инновационными, автоматизация процессов в SOC (Security Operations Center) и использование машинного обучения для поиска аномалий становятся критически важными. Одним из ключевых аспектов в этой области является обнаружение аномалий в различных аспектах работы системы Windows, включая запуск процессов, аутентификацию пользователей и сетевую активность. Применение машинного обучения позволяет аналитикам SOC создавать более точные и эффективные системы обнаружения аномалий, что, в свою очередь, способствует более быстрому и точному реагированию на угрозы безопасности.

Основной принцип, который лежит в основе современного подхода к обнаружению аномалий, заключается в том, что аномалии не следует искать только в одном месте. Вместо этого необходимо рассматривать аномалии как комплексное явление, которое может проявляться в разных формах и на разных уровнях системы. Это означает, что для обнаружения потенциальной угрозы может потребоваться накопление нескольких аномалий в разных областях, прежде чем можно будет говорить о реальной угрозе. Этот подход требует пересмотра традиционных средств к обнаружению аномалий на основе сигнатурных методов [2,3] и развития новых методов анализа, способных обрабатывать большое количество данных и выявлять сложные паттерны поведения, которые могут указывать на наличие угрозы.

Теоретический анализ

Разработка системы обнаружения аномалий в качестве модуля к SIEM (Security Information and Event Management) системе представляет собой логичное и эффективное решение, основываясь на принципах централизованного управления и анализа событий безопасности. SIEM решения агрегируют данные о событиях из различных источников внутри сетевой инфраструктуры, включая серверы, системы, устройства и приложения. Это позволяет не только собирать все события в одном месте, но и анализировать их в совокупности, а не по отдельности для выявления отклонений от установленных в организации правил поведения, что, в свою очередь, помогает идентифицировать потенциальные угрозы. Системы класса SIEM без сомнений являются отличным средством

1 Долгачев Михаил Владимирович, кандидат технических наук, доцент, ФГБОУ ВО «Тихоокеанский государственный университет», г. Хабаровск, Россия. E-mail: 007428@pnu.edu.ru, ORCID:0000-0003-1520-800X.,

2 Костюнин Владислав Александрович, аспирант, ФГБОУ ВО «Тихоокеанский государственный университет», г. Хабаровск, Россия. E-mail: 011783@pnu.edu.ru, ORCID: 0009-0006-1402-9084.

мониторинга активности внутри инфраструктуры, но они имеют один серьезный недостаток – данные системы смогут обнаружить аномалию, только если предварительно написано специальное правило детектирования этой аномалии. Иными словами – аномалия или действия злоумышленника должны быть ранее обнаружены, разобраны и для них составлено правило детектирования. Ввиду всего вышеописанного становится актуальным вопрос поиска еще не известных аномалий или аномалий ранее не встречаемого поведения в рамках контролируемой сети. Опубликовано большое количество работ, где методы обнаружения аномалий успешно используются для обнаружений вторжений злоумышленника [1,5].

Использование SIEM в качестве основы для системы обнаружения аномалий обеспечивает несколько преимуществ.

Во-первых, обучение алгоритмов поиска аномалий требует больших выборок данных, больших чем информация с одного хоста, например, как в работе [6]. Чем больше набор данных – тем точнее система сможет «обучиться». SIEM уже обладает необходимой инфраструктурой для сбора, анализа и хранения большого объема данных о событиях безопасности, что позволяет автоматизировать процессы обнаружения аномалий и улучшить их точность и эффективность.

Во-вторых, на критичных серверах, как правило, не устанавливают дополнительное ПО, например, для поиска аномалий на хосте или ПО без сертификации, из соображений безопасности. Это означает, что любые изменения в системе, включая попытки обнаружения аномалий, могут представлять собой потенциальную угрозу как для безопасности, так и для бизнес-процессов, из-за утилизации серверных мощностей на анализ активности. Поэтому сбор событий без установки на хосте агента через SIEM представляет собой более безопасное и надежное решение, минимизирующее риск несанкционированного доступа или утечки данных. Это обеспечивает более эффективное и безопасное обнаружение аномалий, не внося изменения в саму систему или ее конфигурацию. Например, как в работе [4].

В-третьих, интеграция системы обнаружения аномалий в SIEM позволяет использовать существующие механизмы для установки корреляционных правил, управления ими и реагирования на сигналы безопасности, а не создавать отдельную инфраструктуру [7], что существенно упрощает процесс обнаружения и реагирования на аномалии.

Поиск аномалий на конечных хостах

Ввиду распространения ОС Windows дальнейшая речь пойдет о ней. Для проведения анализа была выбрана сетевая инфраструктура университета и некоторые отдельные хосты в сети университета для получения более точных данных о «живой» инфраструктуре.

Анализируя статью специалистов компании Positive Technologies, 10 наиболее популярных техник специалистов по тестированию на проникновение [9] (которые имитируют злоумышленника) можно детектировать по журналам приложений или журналам событий ОС, это и станет базой для механизма обнаружения аномалий.

Цель поиска аномалий на конечном хосте – обнаружить действия злоумышленника, который уже проник в информационную систему. В ином случае, злоумышленник не сможет иметь доступ к хосту внутри компании.

Обратившись к единому описанию техник (приемов) и тактик, которые используют злоумышленники при атаках на организации – матрице MITRE [9], можно оценить, на каких этапах совершения атаки можно постараться детектировать злоумышленника на конечных хостах.

Изучив все тактики злоумышленников для системы Windows и проанализировав техники, которыми пользуются злоумышленники, а также раздел Detection (Обнаружение) на странице каждой техники, можно сделать вывод, что подавляющее их число можно детектировать на основе нескольких ключевых событий операционной системы Windows [7,8,12] или с использованием Sysmon.

1. Запуск процессов
   - Windows, EventID: 4688
   - Sysmon, EventID: 1
2. Сетевая активность процесса
   - Sysmon, EventID: 3
   - Штатный аудит Windows не журналирует данное событие. Только события от Windows Filtering Platform, но они в данной работе не рассматриваются
3. Создание файлов на системе
   - Sysmon, EventID: 11
   - Windows, EventID: 4663 (с типом доступа к файлу: WriteData)
4. Создание потоков (CreateRemoteThread) к процессам:
   - Sysmon, EventID: 8
5. Аутентификация пользователя
   - Windows, EventID: 4624

Использование этих событий в сочетании с матрицей MITRE ATT&CK позволит специалистам по безопасности создавать эффективные системы обнаружения аномалий, способные идентифицировать широкий спектр угроз, включая как известные, так и новые техники атак.

Данные события и возьмем за основу методик поиска аномалий на конечных хостах.

Определение возможных аномалий на конечных АРМ

Исходя из анализа представленных тактик и техник в матрице MITRE можно выделить несколько направлений обнаружения аномалий на конечных хостах.

1. Аномалии аутентификаций пользователей.

1.1. Аномалия времени аутентификации пользователя по типу входа 10 (удаленно подключение по протоколу RDP) или 2 (Пользователь ввел пароль с клавиатуры – Interactive).

Например, за компьютером работает сотрудник, рабочий день которого начинается в 08:00 утра и заканчивается в 18:00 вечера. Мы имеем большую выборку данных, при которой сотрудник аутентифицируется на хосте в 7:45–08:10 утра и завершает свою работу в 17:45–18:15. Имеющееся расхождение в данных 25–30 минут принимаем за нормальное. В таком случае аутентификация пользователя на компьютере в 05:00 утра будет явной аномалией поведения, которая будет указывать на возможную компрометацию данных.

График аутентификаций одного пользователя в течение 2-х месяцев (рис. 1).

По матрице MITRE: Этап атаки: Resource Development, Техника: T1586 – Compromise Accounts

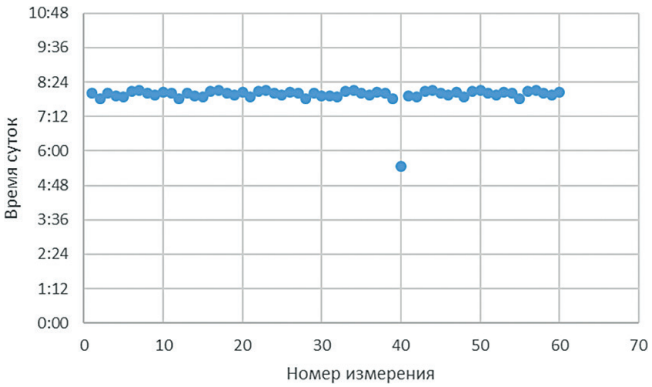

Рис. 1. Графическое отображение аномалии аутентификаций пользователя по времени

1.2. Аномалия по назначению аутентификации пользователя, по типу входа 3 (сетевой).

Зачастую тип входа 3 события 4624 используется для доступа к общим сетевым папкам в инфраструктуре, однако, если мы имеем статистическую выборку того, что пользователь по данному типу входа аутентифицируется только на определенных серверах (где развернута директория общего пользования), то аутентификация по 3 типу входа на стороннем сервере или на каком-либо конечном пользовательском хосте будет явной аномалией, указывающей на возможную реализацию атаки NTLM Relay или выполнение команд через протокол SMB (атака SMB Relay).

По матрице MITRE: Этап атаки: Lateral Movement / Credential Access. Техника T1021.002 – Remote Services: SMB/Windows Admin Shares / T1557.001 – Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay

На рисунке 2 представлено количество подключений одной технической учетной записи (учетная запись для работы приложения, живой пользователь не должен ее использовать) с разделением по серверам назначения за 1 месяц. Из рисунка видно, что распределение количества подключений близко к нормальному и при появлении нового хоста аномалия будет очевидной.

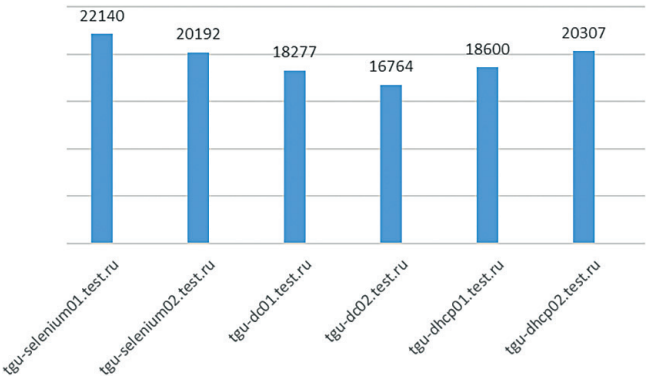

Рис. 2. Аномалия запуска процессов

2. Наиболее часто рассматриваемый способ обнаружения аномалий на хосте – по запускам процессов [10].

В некоторых научных работах рассматривается метод обнаружения аномалий в процессах только на основе связки «родительский процесс – дочерний процесс», однако, цепочки запусков процессов могут быть намного шире и включать в себя и 6, и 20 звеньев, рассматривать одну только связку из всей цепочки – не верно.

Единичной аномалией запуска процессов на хосте можно считать следующую активность:

2.1. Аномалия в запуске процессов в связке «родитель – дочерний».

Например, процесс порождает не ожидаемый процесс, word.exe (Microsoft Word) —> cmd.exe (Командная оболочка Windows), такое может быть произойти преимущественно при заражении системы [11].

2.2. Аномалия в запуске всей цепочки процессов целиком [12].

2.3. Аномалия запуска процесса с участием пользователя.

В данном пункте можно выделить 3 варианта:

2.3.1. Известный пользователь запускает неожиданный известный процесс.

Например, за компьютером бухгалтера, под учетной записью бухгалтера все время открываются процессы браузера, 1С, калькулятор и в один день открывается процесс powershell.exe. Данную активность точно можно считать аномалией и можно предположить, что учетная запись скомпрометирована.

2.3.2. Неожиданный пользователь запускает процесс.

Например, злоумышленник завладел рядом учетных записей (УЗ) в сети организации и при распространении внутри компании пробует применить УЗ на разных хостах, куда удалось получить доступ, для определения их привилегий.

2.3.3. Известный пользователь запускает неожиданный неизвестный процесс.

Например, злоумышленник завладел учетной записью бухгалтера и загрузил на хост собственное ПО.

Данный вариант аномалии следует рассматривать с более высоким приоритетом, так как появление на хосте нового ПО, без заявки в отдел IT, обычно не происходит.

По матрице MITRE: подходит большое количество этапов атак и техник.

Анализируя запуски процессов на исследуемом хосте за месяц (рис. 3), удалось выстроить 315 пар родитель-дочерний процесса, распределение запусков пар процессов на рисунке 4.

Исходя из графиков, наибольшей проблемой в механизме обнаружения аномалий будет отличить цепочки и процессы, у которых количество появлений в сети близится к нулю и малочисленные запуски процессов злоумышленником. Данный вопрос будет решаться в будущих работах.

3. Аномалия в сетевой активности процесса.

Количество процессов на конечном АРМ, которые создают какой-то сетевой трафик ограничено, при стандартной работе пользователя можно

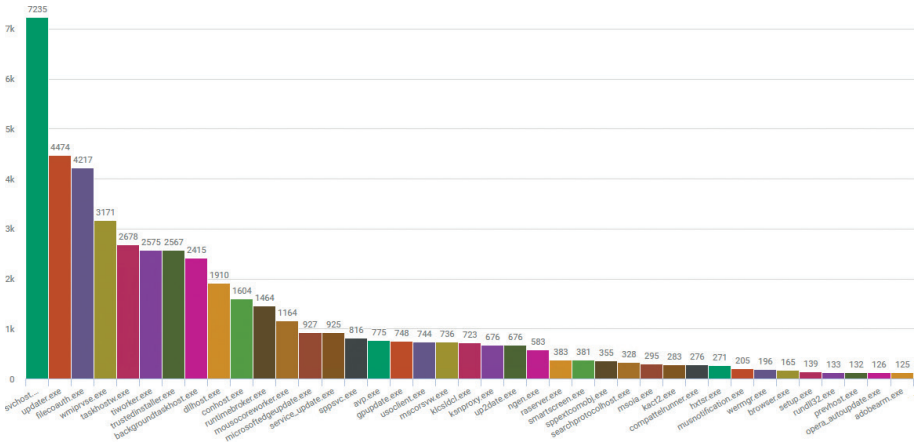

Рис. 3. Распределение запусков процесса от одной учетной записи за один месяц на одном хосте

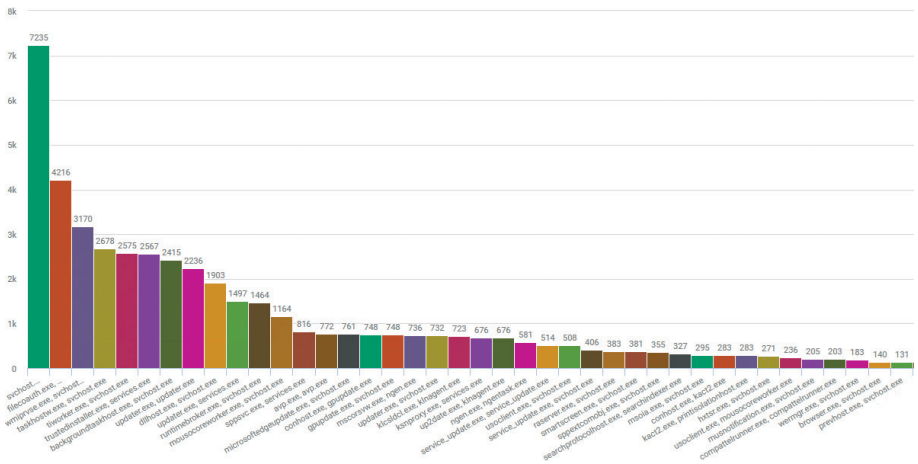

Рис. 4. Распределение запусков пар родитель-дочерний процесса за один месяц на одном хосте

составить профиль (список) подобных процессов, а также конечные адреса, куда процесс создает сетевое соединение. Однако, имея массив данных с множества АРМ и о процессах, создающих сетевую активность внутри компании, появляется шанс обнаружить аномалию, когда злоумышленник начнет «изучать» сеть при помощи собственного ПО.

По матрице MITRE: Этап атаки: Discovery / Lateral Movement. Подходит большое количество техник.

Однако появляется проблема с мимикрированием злоумышленника под легитимный процесс, то есть, когда ПО злоумышленника называется так же, как и стандартный процесс. В таком случае пригодится оперирование полными путями процесса, хеш суммами и метаданными процессов, как способ идентификации процесса.

object.process.fullpath	object.process.meta
c:\kaskad\kaskad_c\kaskad_udp.exe	CCleaner Installer
c:\windows\system32\cmd.exe	Windows Command Processor
c:\kaskad\kaskad_c\kaskad_udp.exe	CCleaner Installer

Рис. 5. Отображение параметров запуска процесса и Description процесса в системе MaxPatrol SIEM

object.name	object.hash
cmd.exe	935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2
cmd.exe	275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F

Рис. 6. Отображение имени процесса и его хеш суммы

Еще одним примером мимикрирования злоумышленника может служить переименование процесса. На рисунке 6 можно увидеть 2 процесса cmd.exe, однако нижняя хеш-сумма не принадлежит cmd.exe, а является хеш-суммой файла eicar.exe, который используют для проверки работоспособности АВПО.

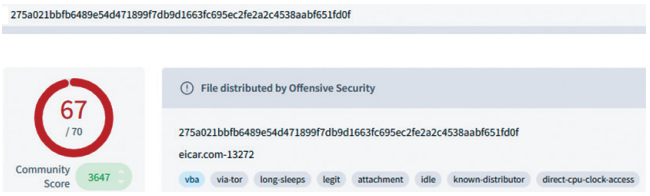

Рис. 7. Показатель обнаружения вредоносного файла вендорами АВПО на сайте VirusTotal

4. Аномалии в создании файлов процессами.

4.1. Файл создается в неожиданном месте известным процессом.

4.2. Файл создается, хотя процесс не должен этого делать.

Данные активности могут указывать на компрометацию процесса или стороннее влияние на работу процесса.

Комплексный поиск аномалий

Наиболее целесообразно искать не точечные аномалии в конкретных действиях, а рассматривать всю активность в совокупности для определения степени критичности происходящего на конечном АРМ.

В случае генерации инцидента на основе одного из описанных в предыдущем пункте признаков инженер информационной безопасности столкнется с большим количеством False Positive сработок (сработка детектора на легитимную активность).

Рассмотрим несколько примеров.

- Использование нового ПО на хосте.

Сотрудник всегда пользовался notepad.exe (блокнот), но в какой-то момент скачал и начал пользоваться notepad++.exe (блокнот с дополнительными возможностями). С точки зрения аномалии запуска процессов (п. 2.1.) это будет инцидентом, так как ранее такой процесс не запускался, однако активность не представляет опасности и ни одна из остальных обозначенных аномалий не детектируется.

- Запуск нового ПО администратором сети на хосте.

Сотрудник всегда пользовался VPN клиентом ciscoanyconnect.exe (Cisco Any Connect), в рамках обновления продукта администратор под собственной УЗ запускает новый VPN клиент ngate.exe (Infotecs Crypto Pro). В таком случае, в данной активности обнаружится несколько аномалий:

- Аномалия в запуске процессов в связке «родитель – дочерний».
- Известный пользователь запускает неожиданный неизвестный процесс.

Данная активность, несомненно, требует анализа со стороны инженера информационной безопасности, однако, активность по-прежнему не представляет опасности для сети предприятия.

- Компрометация учетной записи.

Злоумышленник завладел учетной записью пользователя, подключился к хосту, на котором получилось аутентифицироваться по протоколу RDP, далее для осуществления своей деятельности скачал на хост собственное ПО для сканирования сети. В таком случае, в данной активности обнаружится несколько аномалий:

- Аномалии аутентификаций пользователей.
- Аномалия в запуске процессов в связке «родитель – дочерний».
- Аномалия запуска процесса от имени неожиданного пользователя.
- Аномалия в сетевой активности процесса.

Описанный случай уже требует более детального анализа инженера ИБ, так как активность представляет прямую опасность для сети предприятия.

Таким образом, механизм обнаружения каждой аномалии в деятельности пользователей должен присваивать активности коэффициенты опасности, на основе совокупности которых можно будет оценить результирующую опасность для сети организации.

Заключение

В данной работе были рассмотрены ключевые аспекты разработки и интеграции системы обнаружения аномалий в SIEM систему, что представляет собой целесообразный подход к обеспечению безопасности информационных систем. Этот подход позволяет максимально эффективно использовать уже существующие ресурсы и инфраструктуру, минимизируя риски и затраты на внедрение отдельных продуктов для обнаружения аномалий.

Также были рассмотрены события, на основе которых можно строить детектирование, покрывающее большую часть матрицы MITRE, что позволяет создавать мощные системы обнаружения аномалий. Эти события включают в себя аутентификацию пользователей, запуск процессов, сетевую активность процессов и создание файлов на системах, что обеспечивает широкий спектр обнаружения потенциальных угроз.

В статье также проанализированы ситуации, когда выявление аномалий в совокупности приводит к более продуктивному заключению о наличии угрозы. Это подчеркивает важность комплексного подхода к обнаружению аномалий, который учитывает множество различных аспектов работы системы и позволяет более точно идентифицировать потенциальные угрозы. Такой подход позволяет не только реагировать на инциденты безопасности, но и прогнозировать возможные угрозы, что является ключевым фактором для эффективного управления рисками в современных условиях кибербезопасности.

Литература

1. Добкач, Л.Я. Анализ методов распознавания компьютерных атак / Л.Я. Добкач // Правовая информатика. – 2020. – № 1. – С. 67–75.
2. Шабля В.О., Коноваленко С.А., Едунов Р.В. Анализ процесса функционирования SIEM-систем // E-Scio. – 2022. – № 5 (68). – С. 284–295.
3. Практические аспекты выявления уязвимостей при проведении сертификационных испытаний программных средств защиты информации / В.В. Вареница, А.С. Марков, В.В. Савченко, В.Л. Цирлов // Вопросы кибербезопасности. – 2021. № 5(45). С. 36–44. DOI:10.21681/2311-3456-2021-5-36-44.
4. Шелухин, О.И. Обнаружение аномалий больших данных неструктурированных системных журналов / О.И. Шелухин, В.С. Рябинин // Вопросы кибербезопасности. 2019. – № 2(30). – С. 36–41. DOI:10.21681/2311-3456-2019-2-36-41.
5. Москвичев А.Д., Долгачев М.В. Алгоритмы корреляции событий информационной безопасности // Автоматизация процессов управления. 2020. № 3. С. 50–59.
6. Выявление сетевых аномалий в системных журналах операционной системы Microsoft Windows с использованием методов машинного обучения / Павлычев А.В. [и др.] // Доклады ТУСУР. 2021. Т. 24. № 4. – С. 27–32. DOI: 10.21293/1818-0442-2021-24-4-27-32.
7. Гурина А.О., Гузев О.Ю., Елисеев В.Л. Обнаружение аномальных событий на хосте с использованием автокодировщика // International Journal of Open Information Technologies. Том 8, № 86, 2020 г., с. 26–36.
8. Мирошниченко Е.Л., Калач А.В., Зенин А.А. Разработка модели сбора информации о состоянии защищаемой системы для решения задач управления системой обнаружения, предупреждения и ликвидации последствий компьютерных атак // Вестник Воронежского института ФСИН России. – 2020. – № 1. – С. 102–107.
9. Навацкая Е.А. Сравнительный анализ методологий Cyber kill chain и MITRE ATT&CK // Управление информационными ресурсами: Материалы XIX Международной научно-практической конференции, Минск, 22 марта 2023 года. – Минск: Академия управления при Президенте Республики Беларусь, 2023. – С. 248–249.
10. Эдриан Прутяну. Как стать хакером: Сборник практических сценариев, позволяющих понять, как рассуждает злоумышленник / Эдриан Прутяну; пер. с англ. Д.А. Беликова. М.: ДМК Пресс, 2020.– 379 с.
11. Антонов С.Г., Гвоздева Г.А., Климов С.М. Методика повышения устойчивости функционирования информационно-управляющих систем при информационно-технических воздействиях // Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. – 2019. – С. 6–11.
12. Королев И.Д., Литвинов Е.С., Пестов С.В. Анализ потоков данных о событиях и инцидентах информационной безопасности, поступающих из разнородных источников // Результаты современных научных исследований и разработок. Сборник статей VIII Всероссийской научно-практической конференции. – 2020. – С. 26–34.

COMPREHENSIVE ANALYSIS OF WINDOWS SYSTEM BEHAVIOR FOR CYBER THREAT DETECTION

Dolgachev M. V.[3], Kostyunin V. A.[4]

3 Mikhail V. Dolgachev, Ph.D., Associate Professor, Pacific National University, Khabarovsk, Russia. E-mail: 007428@pnu.edu.ru ORCID:0000-0003-1520-800X.
4 Vladislav A. Kostyunin, Postgraduate Student, Pacific National University, Khabarovsk, Russia. E-mail: 011783@pnu.edu.ru ORCID: 0009-0006-1402-9084

Keywords: *SIEM, anomaly behavior, event log, incident analysis, event monitoring, MITRE matrix.*

Purpose of the article: *development and analysis of anomaly detection methods on Windows system end hosts within a centralized solution of SIEM class, using machine learning and integrated approach, to improve the efficiency and accuracy of detection of potential security threats in the context of modern cyberattacks.*

Method: the research *is based on a theoretical analysis of existing anomaly detection approaches, as well as a practical application of machine learning to analyze security event data collected through SIEM systems. The analysis includes studying the MITRE ATT&CK matrix to identify key events indicative of possible attacks and developing algorithms to detect them.*

Results: *the results of the study show that the developed anomaly detection methodology, based on the analysis of key events of the Windows system and an integrated approach to anomaly detection, allows to significantly improve the accuracy and efficiency of detection of information security incidents in the network infrastructure. This facilitates faster and more accurate response to security threats. Application of the findings can improve anomaly detection systems in Security Operations Centers (SOCs), thus strengthening the overall cybersecurity of organizations.*

The scientific novelty: *work offers a new perspective on anomaly detection, emphasizing the need for complex analysis and the use of machine learning to process large amounts of data collected from SIEM systems. It also emphasizes the importance of adapting anomaly detection techniques to Windows system specifics and taking into account recent trends in cybersecurity.*

References

1. Dobkach, L. Ja. Analiz metodov raspoznavanija komp'juternyh atak / L. Ja. Dobkach // Pravovaja informatika. – 2020. – № 1. – S. 67–75.
2. Shablja V. O., Konovalenko S. A., Edunov R. V. Analiz processa funkcionirovanija SIEM-sistem // E-Scio. – 2022. – № 5 (68). – S. 284–295.
3. Prakticheskie aspekty vyjavlenija ujazvimostej pri provedenii sertifikacionnyh ispytanij programmnyh sredstv zashhity informacii / V. V. Varenica, A. S. Markov, V. V. Savchenko, V. L. Cirlov // Voprosy kiberbezopasnosti. – 2021. № 5(45). S. 36–44. DOI:10.21681/2311-3456-2021-5-36-44.
4. Sheluhin, O. I. Obnaruzhenie anomalij bol'shih dannyh nestrukturirovannyh sistemnyh zhurnalov / O. I. Sheluhin, V. S. Rjabinin // Voprosy kiberbezopasnosti. – 2019. – № 2(30). – S. 36–41. DOI:10.21681/2311-3456-2019-2-36-41.
5. Moskvichev A. D., Dolgachev M. V. Algoritmy korreljacii sobytij informacionnoj bezopasnosti // Avtomatizacija processov upravlenija. 2020. № 3. S. 50–59.
6. Vyjavlenie setevyh anomalij v sistemnyh zhurnalah operacionnoj sistemy Microsoft Windows s ispol'zovaniem metodov mashinnogo obuchenija / Pavlychev A. V. [i dr.] // Doklady TUSUR. 2021. – T. 24. – № 4. – S. 27–32. DOI: 10.21293/1818-0442-2021-24-4-27-32.
7. Gurina A. O., Guzev O. Ju., Eliseev V. L. Obnaruzhenie anomal'nyh sobytij na hoste s ispol'zovaniem avtokodirovshhika // International Journal of Open Information Technologies. Tom 8, № 8b 2020 g., sju 26–36.
8. Miroshnichenko E. L., Kalach A. V., Zenin A. A. Razrabotka modeli sbora informacii o sostojanii zashhishhaemoj sistemy dlja reshenija zadach upravlenija sistemoj obnaruzhenija, preduprezhdenija i likvidacii posledstvij komp'juternyh atak // Vestnik Voronezhskogo instituta FSIN Rossii. – 2020. – № 1. – S. 102–107.
9. Navackaja E. A. Sravnitel'nyj analiz metodologij Cyber kill chain i MITRE ATT&CK [Jelektronnyj resurs]. – Rezhim dostupa: https://elibrary.ru/download/elibrary_53928687_43554665.pdf (data obrashhenija: 07.03.2024).
10. Jedrian Prutjanu. Kak stat' hakerom: Sbornik prakticheskih scenariev, pozvoljajushhih ponjat', kak rassuzhdaet zloumyshlennik / Jedrian Prutjanu; per. s angl. D. A. Belikova – M.: DMK Press, 2020.– 379 s.
11. Antonov S. G., Gvozdeva G. A., Klimov S. M. Metodika povyshenija ustojchivosti funkcionirovanija informacionno-upravljajushhih sistem pri informacionno-tehnicheskih vozdejstvijah // Bezopasnye informacionnye tehnologii. Sbornik trudov Desjatoj mezhdunarodnoj nauchno-tehnicheskoj konferencii. – 2019. – S. 6–11.
12. Korolev I. D., Litvinov E. S., Pestov S. V. Analiz potokov dannyh o sobytijah i incidentah informacionnoj bezopasnosti, postupajushhih iz raznorodnyh istochnikov // Rezul'taty sovremennyh nauchnyh issledovanij i razrabotok. Sbornik statej VIII Vserossijskoj nauchno-prakticheskoj konferencii. – 2020. – S. 26–34.