К. С. Кручковский, А. М. Шабалин
Тюменский государственный университет, г. Тюмень
УДК 004.056.53

СПЕЦИФИКА РАЗРАБОТКИ И ПРИМЕНЕНИЯ ПРАВИЛ КОРРЕЛЯЦИИ ДЛЯ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ SIEM-СИСТЕМАХ (НА ПРИМЕРЕ MICROSOFT WINDOWS)

Аннотация. В статье представлены разработанные авторами правила корреляции, которые базируются на анализе реально проведенных компьютерных атак и соответствующих журналов событий и направлены на эффективное выявление угроз в среде Microsoft Windows, а также позволяют обеспечить более точное и оперативное обнаружение аномальных активностей для повышения эффективности SIEM-систем.

Ключевые слова: правила корреляции, события информационной безопасности, Microsoft Windows, SIEM-система, Sysmon, Winlogbeat, ELK.

Введение. Системы сбора и анализа информации о безопасности (Security information and event management, SIEM) играют ключевую роль в обнаружении кибератак и реагировании на них. Они собирают, агрегируют и анализируют логи событий различных компонентов информационной инфраструктуры. SIEM предоставляют мощный инструментарий для обработки и анализа данных, необходимых для обеспечения информационной безопасности. Эти решения становятся все более привлекательным средством мониторинга безопасности, однако нужно отметить, что многие компании при внедрении и последующей эксплуатации данных систем не обеспечивают их необходимым количеством эффективных правил корреляции, что приводит к нерациональному использованию. Так, проведенное в октябре 2023 года исследование компаниями TAdviser и Positive Technologies, в котором опросили более 100 различных организаций о внедрении SIEM-систем, показало, что третья часть респондентов планирует работать с преднастроенными готовыми правилами (правилами из «коробки»), а остальные либо занимаются донастройкой имеющегося функционала, либо разрабатывают собственные правила корреляции [1].

Обзор литературы по предмету исследования показал, что авторы ряда статей фокусировались преимущественно на разработке единичных дополнительных правил корреляции в «коробочных» решениях SIEM-систем, отмечая при этом недостаточную способность эффективного детектирования различных атак [2-5]. Другие исследователи анализируют современные методы разработки алгоритмов корреляции и приводят примеры практической разработки правил на основе выработанного алгоритма [6, 7].

В целом, все исследователи склоняются к тому, что преднастроенные правила корреляции SIEM-систем недостаточны, поэтому для обеспечения надежной защиты информационных ресурсов необходимо разрабатывать и редактировать правила корреляции, которые способны выявлять аномальные события и потенциальные угрозы в реальном времени.

Авторы данного исследования подтверждают острую необходимость в разработке и модификации правил для современных SIEM-систем и предлагают сфокусироваться на специфике эффективных правил корреляции для Microsoft Windows, которая на сегодняшний день является самой популярной клиентской операционной системой.

Также, авторами статьи рассматривался российский представитель SIEM-систем Komrad, разработанной НПО Эшелон. Это программное средство имеет следующий перечень предустановленных правил для операционной системы Windows: обнаружение неудачной попытки входа в систему, изменение конфигурации межсетевого экрана, отключение антивирусной защиты, обнаружение всех операций с учетными записями пользователей, изменение политики аудита системы, создание нового пользователя; использование истории SID, обнаружение передачи прав локального администратора пользователю.

Данные правила могут детектировать достаточно небольшой вектор нелегитимной активности, в то время как для детектирования каждой из техник в тактике необходимо создать как минимум 194 правила корреляции [8]. Злоумышленники используют в своих атаках на корпоративную инфраструктуру под управлением Microsoft Windows двенадцать базовых тактик и соответствующее им количество техник. Следовательно, рассчитывать только на предустановленные правила корреляции не приходится: необходимо осуществлять редактирование готовых и создание новых правил корреляции имеющимся функционалом SIEM-системы.

Проблема исследования. Эволюция кибератак характеризуется их возрастающей сложностью и разнообразием, постоянными изменениями тактик злоумышленников и проблемами ложных срабатываний, а также ограниченной доступностью информации о самих атаках.

Цель данного исследования — разработать правила корреляции для операционной системы Microsoft Windows средствами SIEM, способными эффективно выявлять атаки и снижать количество ложноположительных срабатываний. В ходе работы решался ряд задач:

- подготовить стенд и провести атаки с использованием инструментов, содержащиеся в сценариях Atomic Red Team, для реализации нелегитимной активности злоумышленника;
- проанализировать и выявить наиболее подходящие ID событий и их поля, логируемые Windows и Sysmon, для создания правил корреляции;
- разработать правила с подробным их описанием для каждого найденного события.

Материалы и методы. Для данного исследования авторами проводились на виртуальном лабораторном стенде наиболее известные атаки на операционную систему Microsoft Windows, которые включали в себя использование различных тактик и техник по матрице Mitre Attack [8], такие как разведка, доставка, эксплуатация уязвимостей, установка и закрепление.

При проведении атак использовались инструменты для реализации нелегитимной активности злоумышленника, содержащиеся в сценариях Atomic Red Team [9], которые представляют собой библиотеку тестов, сопоставленных с техниками Mitre Attack. В ней содержатся множество утилит, powershell- и bash-скриптов, а также другие способы генерации подозрительных событий. Атаки были реализованы на подготовленном стенде в виртуальной среде GNS3 (см. рис. 1), в котором использовались следующие программные продукты:

- Host — целевая атакуемая система, использующая Windows 10 с установленными программными решениями Sysmon и Winlogbeat для фиксирования подозрительной активности;
- Attacker — компьютер, генерирующий вредоносный трафик;
- Server — система сбора событий ELK Stack (Elasticsearch, Logstash, Kibana) на базе операционной системы Ubuntu Linux.

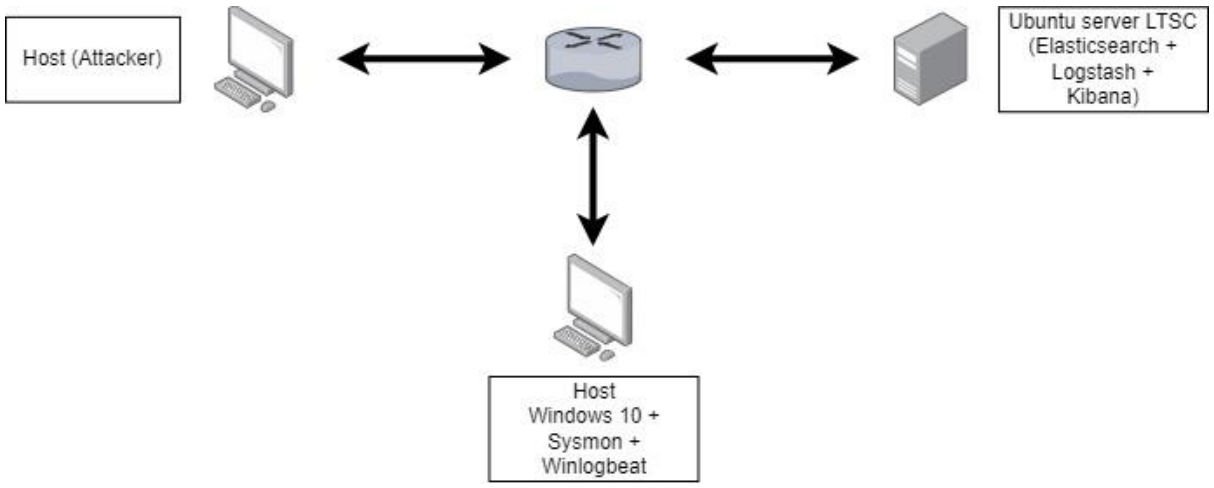

Рис. 1. Топология виртуального лабораторного стенда в среде GNS3

В процессе проведения атак были зафиксированы и систематизированы логи событий, которые впоследствии использовались для их анализа и разработки правил корреляции. Важным этапом работы было выявление основных событий и действий, которые могут свидетельствовать о наличии нелегитимных процессов.

Результаты. Операционная система Windows предоставляет богатый массив различных событий, связанных с активностью пользователей и системы в целом и представляющих собой ценный источник информации, который можно использовать для выявления угроз и аномалий. Операционная система обладает традиционными журналами Security, System, Application.

В данном исследовании авторы расширили перечисленный выше функционал специализированным программным решением Sysmon из комплекта утилит Sysinternals, который с 1996 года активно развивается под руководством Марка Руссиновича. Авторами были определены основные поля событий операционной системы Windows, на основе которых были разработаны базовые типы детектирующих правил (для корреляции SIEM-систем), созданных стандартными средствами журналирования операционной системы Microsoft Windows.

Утилита Sysmon расширяет возможности функционала журналирования операционной системы Microsoft Windows, что позволило авторам статьи разработать дополнительные типы детектирующих правил для SIEM-систем.

Представленные на сегодняшний день типы детектирующих правил выложены авторами на платформе Github и используются в организации учебного процесса с целью разработки правил корреляции для SIEM-систем в виртуальной лаборатории (https://github.com/defender7272/correlation-rules).

Разработанные авторами статьи правила корреляции могут быть расширены и за счет добавления индикаторов компрометаций, которые были найдены в общем доступе или отправлены специальными службами, например ФинЦЕРТ. Однако при их использовании необходимо учитывать специфику конкретной организации и отслеживать подключения к критичным хостам или осуществлять запрет использования нелегитимного программного обеспечения.

Подводя итог, нужно отметить, что «коробочные» правила корреляции обладают преимуществами в простоте и поддержке работоспособности, в то время как «авторские» правила

предоставляют уникальные возможности адаптации. Организации могут выбирать между этими подходами в зависимости от своих потребностей и ресурсов, стремясь к оптимальному балансу между готовыми решениями и гибкостью в обеспечении информационной безопасности.

Заключение. Предложенные авторами правила корреляции были протестированы на событиях, собранных в рамках тестовой информационной виртуальной инфраструктуры предприятия, но могут быть также адаптированы для специализированных продуктов безопасности класса Endpoint / Extended Detection and Response (EDR / XDR).

Таким образом, в данной статье представлен подход к разработке специфичных правил корреляции для SIEM на основе проведения и анализа различных атак на операционную систему Microsoft Windows, который может значительно улучшить эффективность обнаружения атак и сократить число ложноположительных срабатываний.

СПИСОК ЛИТЕРАТУРЫ

1. Исследование TAdviser и Positive Technologies: Рынок SIEM в России. — Текст: электронный // Positive Technologies: официальный сайт. — 2023. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/siem-market-in-of-russia/ (дата обращения: 02.04.2024).
2. Шишков С.А. Разработка методов обнаружения вредоносного воздействия на основе корреляционного анализа событий информационной безопасности в SIEM-системах / С.А. Шишков, М.М. Путято, А.С. Макарян // Цифровые технологии и защита информации в современном обществе: сборник докладов Международной научно-практической конференции, 29-30 ноября 2021 года. — Астрахань, 2021. — С. 36-40.
3. Чепайкин Р.Н. Методика подготовки правил корреляции событий для SIEM / Р.Н. Чепайкин // XXV Туполевские чтения (школа молодых ученых): Международная молодежная научная конференция, посвященная 60-летию со дня осуществления Первого полета человека в космическое пространство и 90-летию Казанского национального исследовательского технического университета им. А.Н. Туполева-КАИ. 10-11 ноября 2021 года. Том V. — Казань, 2021. — С. 695-699.
4. Миланкович М.Р. Разработка правил нормализации и корреляции для maxpatrol SIEM с целью выявления инцидентов безопасности при аутентификации пользователей в домене / М.Р. Миланкович, М.В. Малькова, Д.Ю. Селиванов // Сборник избранных статей научной сессии ТУСУР. — Томск, 2018. — № 1-1. — С. 169-171.
5. Сапожников О.Ю. Организация системы централизованного хранения и обработки событий средствами SIEM-системы „Komrad“ / О.Ю. Сапожников, А.М. Шабалин // Математическое и информационное моделирование: Материалы Всероссийской конференции молодых ученых, 18–20 мая 2023 года. Вып. 21. — Тюмень, 2023. — С. 233-237.
6. Москвичев А.Д. Алгоритмы корреляции событий информационной безопасности / А.Д. Москвичев, М.В. Долгачев // Автоматизация процессов управления. — 2020. — № 3 (61). — С. 50-59.
7. Шабанов В. . Алгоритм разработки правил нормализации и корреляции для SIEM-систем и его апробация / В.С. Шабанов // Нанотехнологии. Информация.радиотехника (НИР-23): материалы Всероссийской молодежной научно-практической конференции, 18 апреля 2023 года. — Омск, 2023. — С. 345-351.
8. Таблица Attack Mitre. — Текст: электронный // Mitre: официальный сайт. — 2024. — URL: https://attack.mitre.org/matrices/enterprise/windows/ (дата обращения: 09.04.2024).
9. Сценарии Atomic Red Team. — Текст: электронный // Atomic Red Team: официальный сайт. — 2024. — URL: https://atomicredteam.io/atomics/ (дата обращения: 16.04.2024).