DOI 10.37882/2223-2966.2024.9.32

АВТОМАТИЗАЦИЯ РАБОЧЕГО ПРОЦЕССА ОБРАБОТКИ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СВЯЗАННЫХ С ВИРУСНЫМ ЗАРАЖЕНИЕМ

AUTOMATION OF THE WORKFLOW FOR PROCESSING INFORMATION SECURITY INCIDENTS RELATED TO VIRUS INFECTION

E. Petkun

Summary. The purpose of this article is to improve the efficiency of the SOC (Security Operations Center).
The article described the possibilities of automating the processing of incidents related to virus infection using a SOAR (Security Orchestration, Automation and Response) class system.

Keywords: Information security, automation, SIEM, SOC, SOAR.

Петькун Егор Максимович
Аспирант, Финансовый университет при Правительстве РФ, Москва
petkun.egor@yandex.ru

Аннотация. Целью данной статьи является повышение эффективности работы SOC (Security Operations Center).
В статье были описаны возможности автоматизации обработки инцидентов, связанных с вирусным заражением с помощью системы класса SOAR (Security Orchestration, Automation and Response).
Актуальность данной статьи обусловлена тем, что с каждым годом все важнее, чтобы в крупных финансовых или государственных организациях была организована круглосуточная работа SOC, главным показателем работы которого является выявление и правильная обработка инцидентов. Одним из самых распространённых инцидентов является вирусное заражение. Важно отметить, что скорость реагирования и обработки напрямую влияет на эффективность процесса, для этого важно автоматизировать рутинные процессы.

Ключевые слова: защита информации, автоматизация, SIEM, SOC, SOAR.

Интерес злоумышленников с каждым годом растет к компаниям, располагающих большой базой персональных данных клиентов, КИИ, а также обладающие государственной и социальной значимостью. Для защиты этих чувствительных для компаний и для государства активов выстроен процесс работы SOC и аналитиков, без которых невозможно выстроить процесс. Аналитик должен на основе гипотез выстроить свой процесс и предугадать возможные действия злоумышленника. Но так как зачастую, не всегда вся подозрительная активность оказывается деятельностью злоумышленника и некоторые процессы могут для аналитика превратиться в рутину, требуется продумывать процессы автоматизированной обработки инцидентов. В данной статье будут предложены примеры процессов автоматизации инцидентов, связанных с вирусным заражением [1].

Центр мониторинга информационной безопасности (Security Operations Center, SOC) — структурное подразделение организации, отвечающее за оперативный мониторинг IT-среды и предотвращение киберинцидентов. Специалисты SOC собирают и анализируют данные с различных объектов инфраструктуры организации и при обнаружении подозрительной активности принимают меры для предотвращения атаки [2].

Событие, которое нарушает политику безопасности организации и подвергает конфиденциальные данные риску называется инцидент информационной безопасности. Инцидент информационной безопасности может включать в себя такие понятия, как утечка конфиденциальных данных, заражение вредоносным ПО, DDoS атаки, несанкционированный доступ, внутренние нарушения, нелегитимное повышение привилегий, фишинг.

Главные возможности SOAR систем это объединить оркестрацию (управление угрозами и уязвимостями), автоматизацию и реагирование на инциденты информационной безопасности. Системы класса SOAR необходимы для повышения эффективности аналитика информационной безопасности, который обрабатывает инциденты. С помощью SOAR сокращается время на реагирование, путем переноса на систему многих задач аналитика [3].

Важно отметить в чем отличие SIEM систем и SOAR. Управление информацией о безопасности и событиями (SIEM) помогает агрегировать данные из инфраструктуры в централизованное хранилище для дальнейшего анализа и аналитики. [4] Данные, которые поступают в SIEM являются журналами безопасности, события с различных СЗИ и сетевых устройств. Эти данные можно коррелировать в режиме реального времени для выявления аномалий, уязвимостей и инцидентов. Основное внимание уделяется данным входа в систему пользователей, обнаружение вредоносных программ. SIEM так же помогает визуализировать данные, что помогает при

анализе инцидентов. Таким образом, этот инструмент становится очень эффективным способом реагирования SOC на потенциальные угрозы. С помощью SIEM агрегируют данные с разных источников и с помощью правил корреляции, настраиваются паттерны на нелегитимную активность. С помощью SOAR настраиваются интеграции и продумывается логика обработки инцидента [5]. Хотя различные решения безопасности являются отличным арсеналом для SOC, каждое из решений использовать различные технологии и парадигмы для разработки, внедрения и эксплуатации.

Процесс реагирования на инциденты или его жизненный цикл можно разделить на несколько этапов, согласно Национальному институту стандартов и технологий (NIST): подготовка, обнаружение и анализ, устранение и восстановление, а также действия после инцидента [6]. Процесс реагирования на инциденты представляет собой непрерывный процесс, который циклически переключается между этими фазами.

Сложность общего процесса реагирования на инциденты снижается за счет унификации различных решений и процессов безопасности, интеграции в архитектуру безопасности организации компании, подключая системы обнаружения, безопасности сети и конечных точек, а также выполняя координацию инструментов безопасности, используемых компанией. Аналитика становится гораздо более эффективной, когда можно объединить различные решения безопасности. По отдельности различные решения безопасности могут быть «слепыми» и без связности и работы аналитика, не определять те или иные типы угроз. Благодаря оркестрации данные разведки об угрозах собираются из нескольких источников в единую базу данных.

При возникновении инцидента по вирусному заражению, аналитику необходимо вручную собирать данные об устройстве, собирать информацию о сигнатуре и продумывать процессы по минимизации последствий [7]. Рабочие процессы SOAR требуют стандартизированный процесс, включающий планирование реагирования на инциденты, выполнение политики, этапы расследования, ответные действия и процесс исправления, помогает собирать данные из окружающей среды и собирать их в едином пространстве [8].

Время аналитики может быть снижено благодаря автоматизации, поможет сосредоточиться на более глубоком анализе и разработке превентивных мер. Основное преимущество автоматизации безопасности заключается в освобождении аналитиков безопасности от трудоемких задач, чтобы они стали намного эффективнее в своей работе.

Сценарий обработки инцидента по вирусному заражению, проделываемый аналитиком.

1. Определить источник заражения, для этого аналитику требуется обратиться к серверу антивирусной защиты и найти IP адрес, на котором был найден нелегитимный файл.
2. Определить имя сервера или рабочей станции по исходному IP адресу, собрать информацию об владельце данного устройства.
3. Определить сигнатуру или метод, по которому антивирус нашел данный файл.
4. Достать данный файл с сервера антивирусной защиты или конечного устройства для анализа ручным или автоматизированным методом (использование средств защиты Sandbox).
5. Определить метод попадание данного файла на конечное устройство.
6. Собрать информацию о вердикте антивирусной системы.
7. Сделать вывод о вредоносности данного файла.

Начальный сбор информации у аналитика отнимает много времени и для этого начальный сбор информации нужно автоматизировать. Ниже представлена схема логики, заложенная в рабочий процесс SOAR системы, которая минимизирует время аналитика:

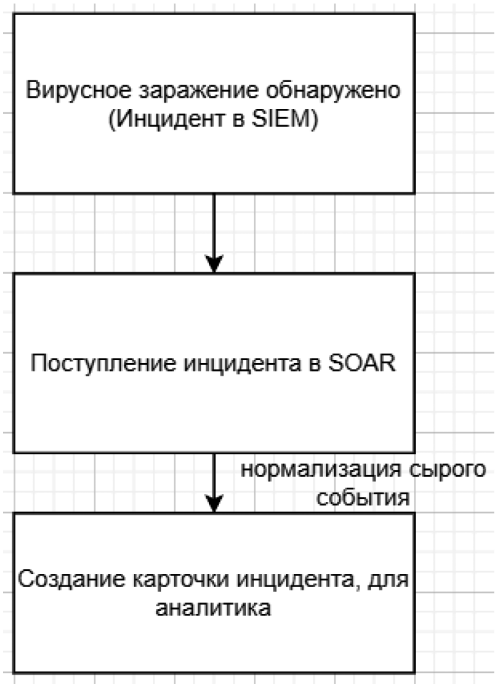

Рис. 1. Появление инцидента по вирусному заражению

Создание карточки инцидента, позволит привести в читаемый для аналитика вид сырой лог инцидента, обнаруженный SIEM системой с помощью корреляции. В продуманной логике с помощью регулярный выражений нам потребуется найти IP адрес зараженного устройства.

Следующий шаг представлен на рисунке 2:

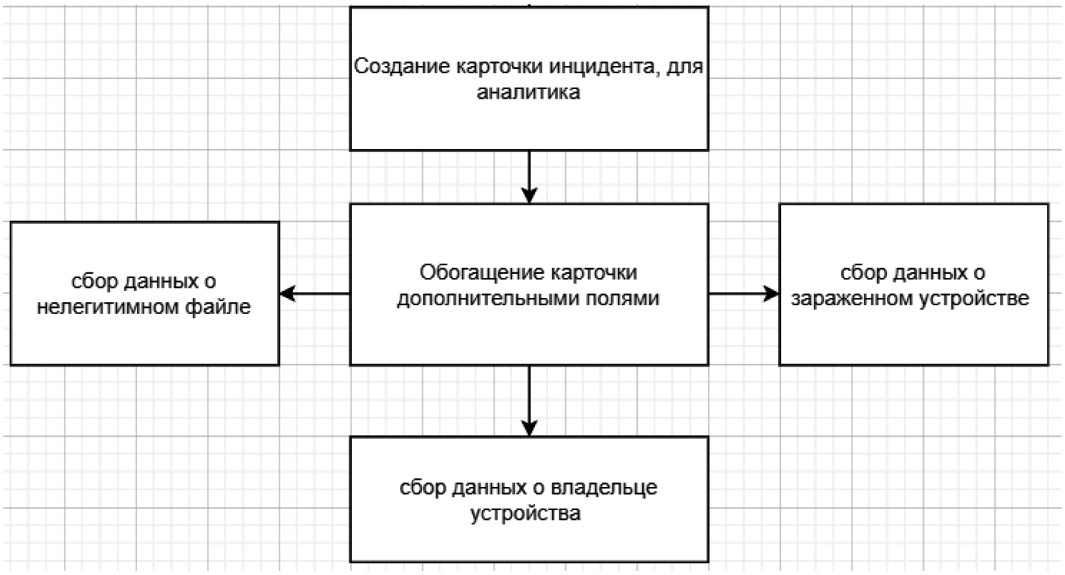

Рис. 2. Обогащение карточки дополнительными полями

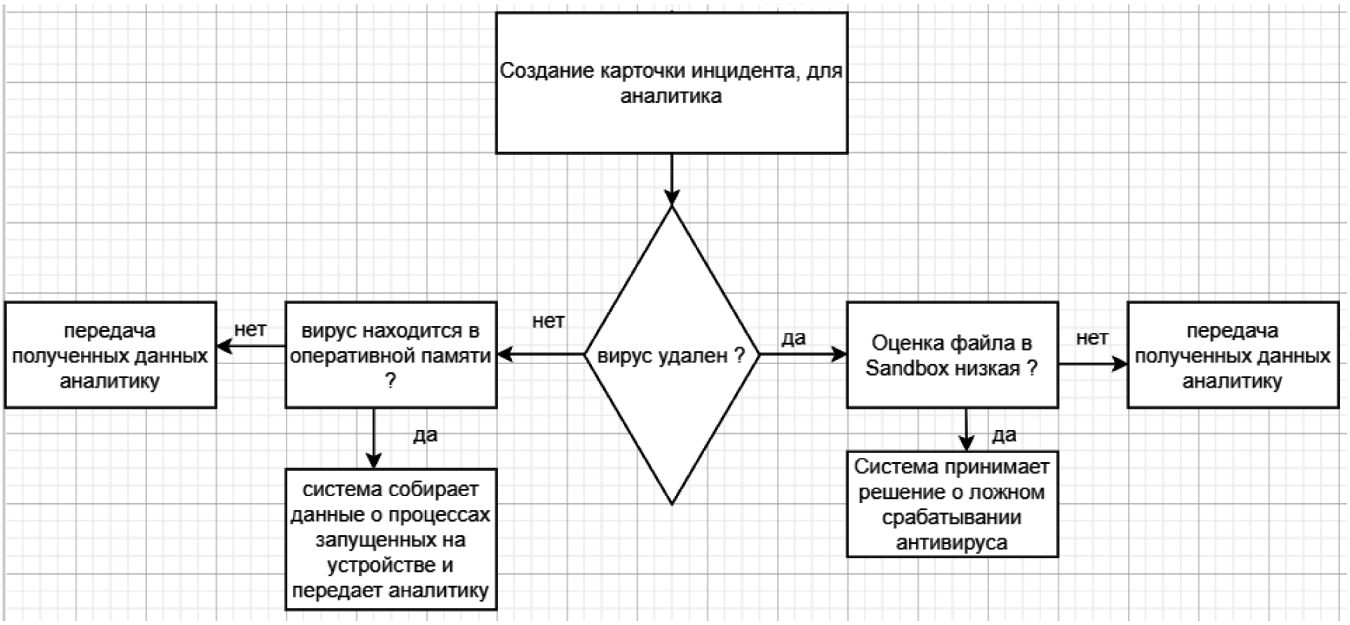

Рис. 3. Логика рабочего процесса

В рабочем процессе SOAR закладываем логику:

1. Сбор данных о зараженном устройстве, используя утилиту ping для сбора информации о имени хоста и операционной системе.
2. Сбор данных о владельце, используя обращения в Active Directory, используя Get-AdUser и манипулируя параметрами для получения информации о владельце устройства, руководителе владельца, последнем входе в систему.
3. В сбор данных о нелегитимном файле включаем подсчет хэш суммы используя утилиту CertUtil и отправку для проверки данной хэш суммы на общедоступных ресурсах, как сторонние Sandbox и антивирусные системы.

Далее в систему закладываем логику на основе вердикта антивирусной системы, который, так же с помощью регулярного выражения получаем в карточку инцидента [9].

По данной логике работа аналитика требуется, но сокращенно время на сбор первоначальной информации. Сокращается время, если антивирусного заражения не было, и система может сама сделать вывод об этом. Так же при наличии вирусного заражения, аналитик сразу приступает к минимизации последствий и не тратит время на сбор информации. В дальнейшем при каждом обработанном инциденте, логика дополняется и количество обрабатываемых инцидентов аналитиком уменьшается, путем добавления в логику правильных вопросов о прошлых инцидентах [10].

В дальнейшем для инцидентов продумываются меры минимизации последствий, которые в рамках автоматизации будут эффективнее расходовать время. Для вердикта, когда система делает вывод, что файл вредоносный, требуется сделать дополнительный этап. Без подключения аналитика реализовать превентивные меры по изоляции конечного устройства от сети и произвести блокировку учетных записей. Так как на первичном этапе все данные собраны, после вердикта системы злоумышленник и зараженное устройство уже заблокированы до вердикта аналитика. Данные действия позволят минимизировать риски распространения в инфраструктуре вредоносного ПО.

ЛИТЕРАТУРА

1. Аналитический отчет компании Headhunter https://ict.moscow/news/headhunter-s-ianvaria-po-noiabr-2023-goda-kolichestvo-vakansii-v-sfere-ib-vyroslo-na-27/ [Электронный ресурс] Дата обращения (14.08.2024)
2. Исследование TAdviser и Positive Technologies: Рынок SIEM в России https://www.ptsecurity.com/ru-ru/research/analytics/siem-market-in-of-russia/#:~:text=%D0%9E%D0%B1%D1%8A%D0%B5%D0%BC%20%D1%81%D0%B5%D0%B3%D0%BC%D0%B5%D0%BD%D1%82%D0%B0%20SIEM%2D%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%20%D0%B2,%D0%B2%D0%BD%D0%BE%D0%B2%D1%8C%20%D1%83%D1%81%D0%BA%D0%BE%D1%80%D1%8F%D1%82%D1%81%D1%8F%20%D0%BA%202026%20%D0%B3%D0%BE%D0%B4%D1%83. [Электронный ресурс] Дата обращения (12.08.2024)
3. Отчет Group-IB https://www.facct.ru/media-center/press-releases/critical-infrastructure-2021/ [Электронный ресурс] Дата обращения (03.08.2024)
4. Блог компании АйПиМатика Информационная безопасность https://habr.com/ru/companies/ipmatika/articles/584014/ [Электронный ресурс] Дата обращения (03.08.2024)
5. Блог компании OTUS Информационная безопасность https://habr.com/ru/companies/otus/articles/773430/ [Электронный ресурс] Дата обращения (05.08.2024)
6. Руслан Рахметов блог https://habr.com/ru/articles/704186/ [Электронный ресурс] Дата обращения (05.08.2024)
7. Журнал Sensor https://mdpi-res.com/d_attachment/sensors/sensors-21-04759/article_deploy/sensors-21-04759-v2.pdf%3Fversion%3D1626241362 [Электронный ресурс] Дата обращения (07.08.2024)
8. Блог компании Positive Technologies Информационная безопасность https://habr.com/ru/companies/pt/articles/791890/ [Электронный ресурс] Дата обращения (11.08.2024)
9. Селезнев В.М., Боровская О.Е. Встраивание инструментов SOAR-платформ в экосистему SOC для автоматизации процесса реагирования на инциденты ИБ [Электронный ресурс] Дата обращения (11.08.2024)
10. Jani Purujoki SOAR Playbook Implementation — Incident Deduplication and Its Effects [Электронный ресурс] Дата обращения (12.08.2024)

Журнал «Современная наука: актуальные проблемы теории и практики»