МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.23670/IRJ.2022.124.8

ВСТРАИВАНИЕ ИНСТРУМЕНТОВ SOAR-ПЛАТФОРМ В ЭКОСИСТЕМУ SOC ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ

Научная статья

Селезнёв В.М.[1,] *, Боровская О.Е.[2]
[1] ORCID : 0000-0003-4521-0290;
[2] ORCID : 0000-0002-1682-8334;
[1, 2] Финансовый Университет, Москва, Российская Федерация

* Корреспондирующий автор (vmseleznyov[at]fa.ru)

Аннотация

Мир кибербезопасности полон инструментов информационной безопасности (далее – ИБ). Наиболее новый элемент постоянно прогрессирующих технологий – SOAR-платформа (Security Orchestration, Automation, and Response platform), которая, как обещают производители, сокращает время реагирования на инциденты, улучшает работу функций безопасности и облегчает жизнь командам безопасности [1]. Данная статья посвящена основным проблемам выстраивания процесса реагирования на инциденты информационной безопасности с помощью встраивания SOAR-платформ в экосистему SOC, выбора SOAR-платформы в соответствии с требованиями к системе управления инцидентами ИБ, взаимодействия SOAR-платформы и SIEM-системы, а также определению преимуществ интеграции SOAR-платформы с иными системами ИБ.

Ключевые слова: SOAR-платформа, инциденты информационной безопасности, SIEM-система, автоматизация реагирования, анализ событий, SOC.

INTEGRATING SOAR TOOLS INTO THE SOC ECOSYSTEM TO AUTOMATE THE IS INCIDENT RESPONSE PROCESS

Research article

Seleznyov V.M.[1,] *, Borovskaya O.Y.[2]
[1] ORCID : 0000-0003-4521-0290;
[2] ORCID : 0000-0002-1682-8334;
[1, 2] Financial University, Moscow, Russian Federation

* Corresponding author (vmseleznyov[at]fa.ru)

Abstract

The world of cybersecurity is full of information security ("IS") tools. The newest element of constantly evolving technology is the SOAR (Security Orchestration, Automation, and Response platform), which, as manufacturers promise, reduces incident response time, improves security functions, and makes life easier for security teams [1]. This article focuses on the main problems of building the information security incident response process by integrating SOAR platforms into the SOC ecosystem, choosing a SOAR platform in accordance with the requirements for the IS incident management system, the interaction between the SOAR platform and the SIEM system, and identifying the benefits of integrating the SOAR platform with other IS systems.

Keywords: SOAR platform, information security incidents, SIEM system, response automation, event analysis, SOC.

Введение

Security Orchestration, Automation and Response (далее – SOAR) – платформа, обеспечивающая сбор данных о событиях, инцидентах информационной безопасности (далее – ИБ) из нескольких источников, координацию (оркестрацию) и автоматизацию реагирования на выявленные инциденты ИБ [2]. Таким образом, платформа SOAR позволяет сводить воедино данные об угрозах безопасности из разных источников, выявлять риски, давать им оценку и автоматически обеспечивать на основе собранных сведений адекватный и своевременный ответ, защищая инфраструктуру на самой ранней стадии появления аномальной активности.

По данным Gartner, исследовательской и консалтинговой компании, к концу 2022 года 30% организаций с группой безопасности численностью более пяти человек будут использовать инструменты SOAR-платформ в своих операциях по обеспечению безопасности, по сравнению с менее чем 5% сегодня [3].

Исходя из названия, SOAR-платформы осуществляют 4 процесса.

Агрегация – сбор событий, инцидентов ИБ со всех источников: Security information and event management (далее – SIEM), средств защиты информации (далее – СЗИ), VirtualMachine (VM) tools, threat intelligence- (TI-) services/ Threat Intelligence Platform (далее – TIP), IT Service Management (далее – ITSM), e-mail;

Оркестрация – интеграция с различными ИТ- и ИБ-системами для выполнения отдельных задач в рамках соответствующего заданного алгоритма, подхода (workflow) реагирования на каждый тип инцидента ИБ;

Автоматизация – автоматизация отдельных задач реагирования на каждый тип инцидента ИБ в рамках соответствующего workflow;

Реагирование – определение workflow и задач реагирования на каждый тип инцидента ИБ с контролем SLA/OLA (далее – Service Level Agreement/Operational-level agreement) [4].

Gartner в 2017 году определила, что SOAR-платформа – совокупность следующих платформ [5]:

– SAO (Security Automation and Orchestration) – платформа оркестрации и автоматизации операционных задач информационной безопасности; [6]

– IRP (Incident Response Platform) – платформа управления жизненным циклом инцидентов информационной безопасности;

– TIP – платформа управления данными киберразведки.

Таким образом, можно выделить следующие основные задачи, которые возможно реализовывать их с помощью SOAR-платформ:

Реагирование на инциденты из SIEM/СЗИ/ITSM – обработка инцидента по заданному workflow, автоматизация первичной обработки, обогащение инцидента ИБ, проверка на вредоносность с помощью Threat Services, автоматизация задач реагирования в инфраструктуре, отчетность;

Ретроспективный анализ событий ИБ – проверка событий ИБ в инфраструктуре на наличие полученных индикаторов компрометации (далее – IoC, Indicators of Compromise) от Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (далее – ФинЦЕРТ)/Национального координационного центра по компьютерным инцидентам (далее – НКЦКИ)/TI-services/TIP;

Обработка уязвимостей – приоритизация уязвимостей, обогащение, автоматизация задач устранения уязвимостей [7].

Методы и принципы исследования

Рисунок 1 систематизирует и отражает место SOAR-платформы в экосистеме операционного центра безопасности (далее – SOC, Security Operations Center) при решении задач управления инцидентами ИБ. В самой SOAR-платформе есть набор playbooks, сконфигурированный по личным предпочтениям, который представляет собой сущность, формализующую workflow обработки инцидента, скрипты автоматизации и отчетность. Эти инструменты позволяют автоматизировать рутинные задачи в рамках workflow [8].

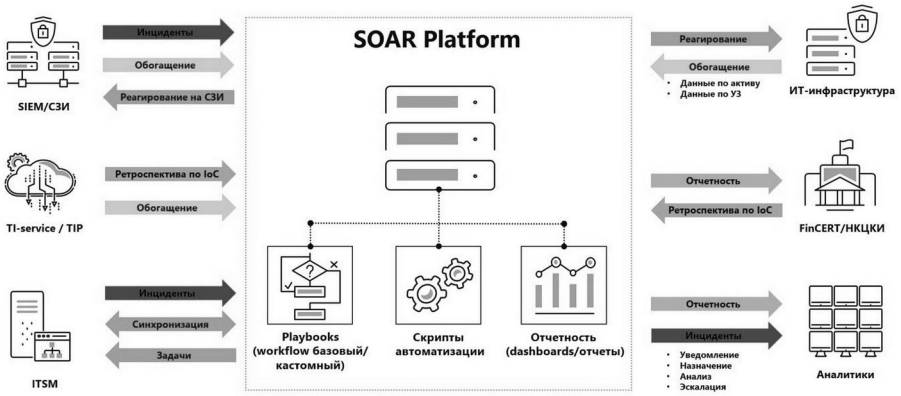

Рисунок 1 - Место SOAR-платформы в экосистеме ИБ
DOI: https://doi.org/10.23670/IRJ.2022.124.8.1

Примечание: УЗ – учетные записи

Стрелка «инциденты»: Важной особенность SOAR-платформы является оркестрация. Для реагирования на инциденты и автоматизированного выполнения задач необходима интеграция с различными средствами и технологиями инфраструктуры. Так, для получения инцидентов возможна интеграция с SIEM/СЗИ и ITSM.

Стрелка «обогащение», «ретроспектива по IoC»: Запуск playbooks (сценарии по обработке инцидентов) влечет за собой первичную обработку по playbooks (классификация и приоритизация инцидентов). На данном этапе возможно обогащение событий ИБ из SIEM/СЗИ и ИТ-инфраструктуры в зависимости от типа инцидентов, а также проверка выявленных IoC во внешних базах угроз.

Стрелка «инциденты»: К моменту привлечения аналитиков – команды SOC, имеющих на данном этапе полное понимание об инцидентах, данная информация нуждается в анализе и определении способов устранении.

Стрелка «синхронизация», «задачи»: Далее выбирается стратегия реагирования. Стоит учесть, что все задачи можно загрузить в SOAR-платформу и за счет скриптов автоматизации автоматизировать либо выполнение самих этих задач на СЗИ, ИТ-инфраструктуре, либо создать эти задачи в ITSM-системе и получать некую синхронизацию по статусам.

Стрелка «отчетность»: По итогам устранения инцидентов аналитикам предоставляется отчетность по проделанным действиям и характеристикам инцидентов. Дополнительно SOAR-платформа предоставляет возможность настройки интеграцию с внешними регуляторами (ФинЦЕРТ/НКЦКИ) для предоставления отчетности об инцидентах.

Процесс выстраивания одного общего базового workflow для всех типов инцидентов состоит из следующих компонентов:

Регистрация:

1. Классификация инцидента;
2. Определение критичности инцидента;
3. Обогащение (сбор необходимой информации);
4. Заведение карточки инцидента;
5. Назначение ответственного.

Как только в SOAR-платформу передалась информация о событии ИБ, – потенциальном инциденте – запускается общий playbook по обработке инцидента, создается карточка инцидента по заданным критериям: определяется тип инцидента и его критичность. Это можно реализовать при помощи скриптов автоматизации.

В зависимости от определенного типа инцидента и его критичности инцидент обогащается (заполняются все необходимые поля для данной карточки инцидента с использованием скриптов интеграции под каждый тип инцидента). Для этого могут использоваться обращения в SIEM, СЗИ, Active Directory, CMDB (база данных управления конфигурацией) и др.

Если в рамках обогащения были выявлены IoC, то SOAR-платформа автоматизирует задачу проверки IoC на вредоносность, отправляя выявленные IoC во внешние базы угроз, с которыми настроена интеграция. Если проверка дала положительный результат, – IoC был выявлен базе угроз – дополнительно запускается поиск аналогичных инцидентов в ИТ-инфраструктуре.

Далее SOAR-платформа отправляет все данные по инциденту и назначает ответственное лицо за этот инцидент с соответствующим уведомлением.

Рисунок 2 отражает детализацию этапа «регистрация».

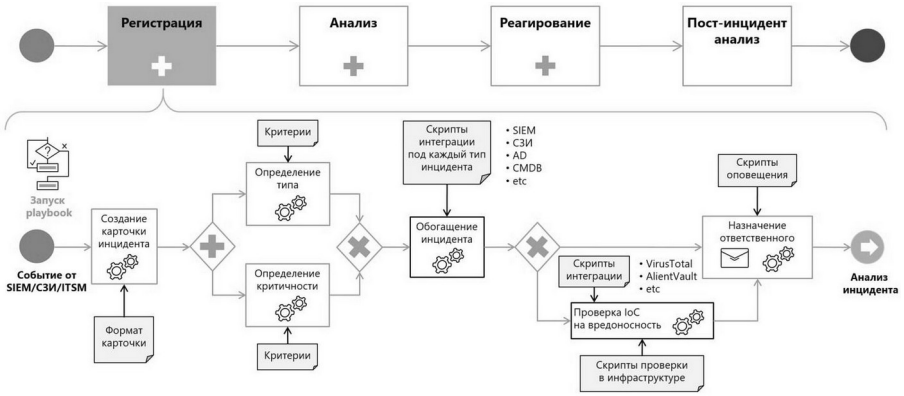

Рисунок 2 - Детализация этапа «регистрация»
DOI: https://doi.org/10.23670/IRJ.2022.124.8.2

Анализ:

1. Оповещение об инциденте ИБ;
2. Запрос на легитимность.

К этапу «анализ инцидента» аналитик получает полную информацию об инциденте. Далее аналитик фокусируется на базовом анализе, проверяя, является ли событие ИБ ложным срабатыванием. Здесь возможны следующие варианты:

– аналитик классифицирует событие ИБ как «ложное срабатывание» и переходит на этап «пост-инцидент анализ»;

– аналитик классифицирует событие ИБ как «легитимная активность» и переходит на этап «пост-инцидент анализ»;

– аналитик классифицирует событие ИБ как «инцидент», оповещает об инциденте при помощи скриптов оповещения и переходит на этап «реагирование на инцидент». В случае, если инцидент вызван легитимным действием пользователя в ИТ-инфраструктуре, аналитик отправляет запрос на подтверждение легитимности. Если легитимность не подтверждена, аналитик переходит на этап «пост-инцидент анализ».

Рисунок 3 отражает детализацию этапа «анализ».

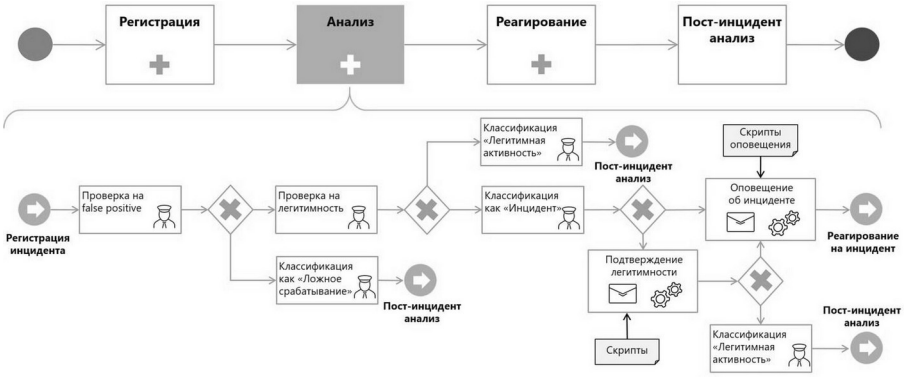

Рисунок 3 - Детализация этапа «анализ»
DOI: https://doi.org/10.23670/IRJ.2022.124.8.3

Реагирование:

1. Реализация мер реагирования;
2. Постановка задач в ITSM-систему.

Как только инцидент переходит на этап «реагирование на инцидент», формируется список задач (большой список/список, специально предназначенный под тип инцидента). Либо аналитик выбирает эти задачи по реагированию (автоматизация с участием человека) и подтверждает их реализацию, либо SOAR-платформа выполняет действия, внедрив их в ITSM и синхронизовав связь выполнения задач, настроенные на данный тип инцидента (полная автоматизация). Как только задачи были выполнены, осуществляется проверка реализации устранения инцидента. Если удалось – SOAR-платформа оповещает об этом всех необходимых лиц и осуществляется переход на этап «пост-инцидент анализ».

В случае, если проверка показала, что инцидент не устранен, может запуститься playbook по расследованию. К моменту, когда аналитик начинает анализировать инцидент и способ реакции, SOAR-платформа может выгрузить все логи для разбора. Далее – аналогичные этапы по реагированию: полностью автоматизированные или автоматизированные с участием человека. Окончательными действиями будет дополнительная проверка на устранение инцидента и оповещение об устранении инцидента, после чего происходит переход на этап «пост-инцидент анализ».

Рисунок 4 отражает детализацию этапа «реагирование».

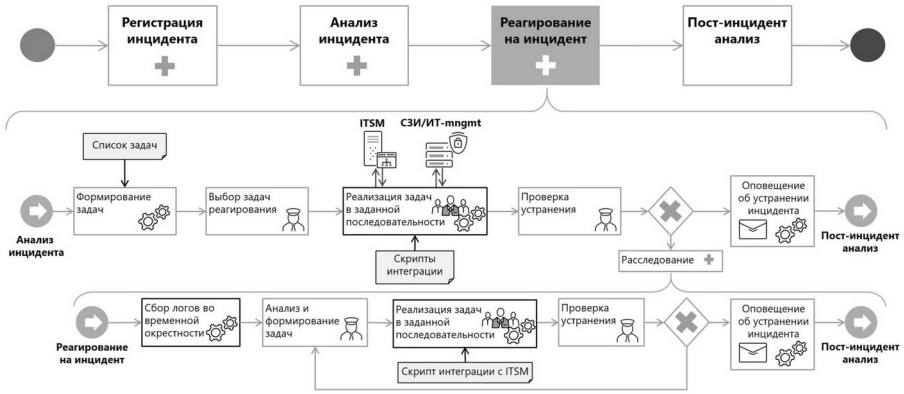

Рисунок 4 - Детализация этапа «реагирование»
DOI: https://doi.org/10.23670/IRJ.2022.124.8.4

Пост-инцидент анализ:

1. Формирование отчетов.

Процесс выстраивания кастомного workflow под определенный тип инцидента на практике заключается в следующем:

Имеющийся файрвол веб-приложений (далее – WAF, Web Application Firewall) фиксирует попытку web-атаки на внешнем web-сервисе, являющимся критичным для бизнеса. Таким образом, запускается playbook по обработке данного инцидента.

Первым этапом формируется содержание карточки (тип инцидента, критичность, детали инцидента из WAF, IoC: IP внешний) при помощи интеграции с WAF.

Вторым этапом осуществляется обогащение инцидента – сбор данных по веб-сервису, поиск событий по IP внешнему, фиксирование артефактов. SOAR-платформа находит ранее зафиксированное событие (выявленный артефакт): попытка неуспешной авторизации на веб сервисе из-под УЗ сотрудника.

В следующем этапе реализуется проверка нахождения этого внешнего IP-адреса в базе угроз. В данном примере данный внешний IP-адрес был замечен во вредоносной активности, что фиксируется в карточку инцидента.

Вся информация об инциденте, а именно анализ сформированной карточки, классификация как инцидент и подтверждение реализации базовых мер, передается аналитику. В рамках обогащения инцидента было выявлено, что инцидент связан с потенциальной компрометацией УЗ сотрудника. Исходя из всего этого, аналитик формирует набор мер – добавление IP-адреса в black list, блокировка УЗ сотрудника, оповещение о необходимости смены пароля.

Последний этап – подготовка всей отчетности по результатам устранения инцидента (заполнение карточки инцидента).

Рисунок 5 систематизирует и отражает процесс выстраивания кастомного workflow.

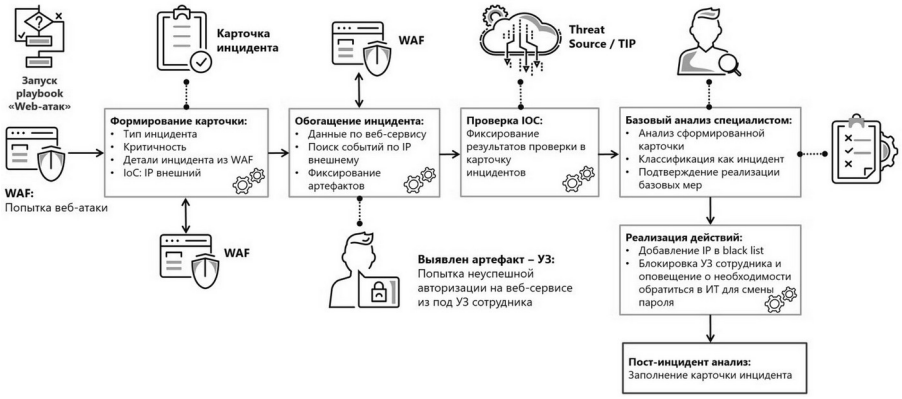

Рисунок 5 - Кастомный workflow
DOI: https://doi.org/10.23670/IRJ.2022.124.8.5

Основные результаты

Создаваемые или развивающиеся в настоящее время SOC строятся на базе SIEM-систем, упуская из виду события, происходящие на уровне сети или на уровне оконечных устройств. Ввиду изменения ландшафта угроз и появления новых технологий, SIEM-системы недостаточно для полноценной защиты информационной инфраструктуры. В качестве дополнения к SIEM-системам могут выступать следующие платформы:

– NTA (или NFT) (Network traffic analysis/Network forensics tool) - Средства анализа сетевого трафика и/или расследования сетевых инцидентов;

– EDR (Endpoint Detection & Response) - решения для обнаружения и изучения вредоносной активности на конечных точках;

– UEBA (User and Entity Behavior Analytics) - технологии анализа поведения пользователей и организаций;

– SOAR-платформы.

Построению моделей зрелости SOC и SIEM посвящено значительное количество литературы [9] при этом, как сказано выше, использование SOAR в них остается за пределами анализа.

Мы предлагаем упрощенную модель зрелости SOC, определяющую отличия SOCов разных уровней зрелости по пяти ключевым параметрам: инструментарий, функции, Threat Intelligence, метрики и персонал. Что поможет оценить существующий SOC и определить дальнейшее его развитие (Табл. 1).

Таблица 1 - Упрощенная модель зрелости SOC

DOI: https://doi.org/10.23670/IRJ.2022.124.8.6

Уровень	Инструментарий	Функции
1	SIEM	Базовый мониторинг событий
2	SIEM+базовый сетевой мониторинг	Мониторинг событий, тюнинг контента
3	SIEM+NTA	Базовое обнаружение аномалий, периодические пентесты
4	SIEM+NTA+EDR	Анализ ВПО, базовый threat hunting, киберучения red/blue team
5	SIEM+NTA+EDR+UEBA+SOAR	Интегрированные мониторинг и реагирование, threat hunting, продвинутая аналитика для обнаружения аномалий, red team

SOC высшего уровня зрелости, который должен состоять из множества платформ, определенных в зависимости от входа/выхода информации, изображен на Рисунок 6.

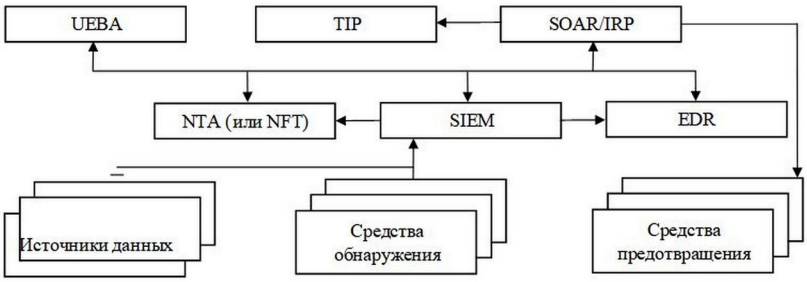

Рисунок 6 - Платформы SOC высшего уровня зрелости
DOI: https://doi.org/10.23670/IRJ.2022.124.8.7

Таким образом, SOAR-платформа является неотъемлемой частью полноценного SOC.

Обсуждение

Из нормативно-правовых актов РФ можно выделить следующие требования к системе управления инцидентами ИБ:

Централизованный сбор и хранение информации по инцидентам ИБ, автоматизация процесса реагирования на инциденты;

- Интеграция со смежными системами и СЗИ;
- Управление жизненным циклом ИТ-активов и их взаимосвязями;
- Управление жизненным циклом уязвимостей на контролируемых объектах ИТ-инфраструктуры;
- Хранение и контроль срока действия документов, регламентирующих деятельность по ИБ;
- Визуализация информации в различных форматах представления данных, включая отображение различных диаграмм, графиков и интерактивных схем;
- Формирование различной отчётности;
- Централизованное управление параметрами работы компонентов системы, включая их обновление.

Неправильный выбор SOAR-платформы может повлечь за собой следующие риски:

1. Нанесение ущерба компании за счет неэффективного реагирования на инциденты ИБ. Факторы риска:
1) простои в работе критичных для бизнеса систем и сервисов;
2) утечки конфиденциальной и другой критичной для бизнеса информации;
3) уничтожение / утрата критичных для бизнеса данных и систем;
4) нанесение вреда деловой репутации компании.
2. Причина низкой эффективности существующего процесса реагирования на инциденты ИБ:
1) отсутствие актуальной информации об ИТ-активах (данные разрознены по нескольким системам);
2) отсутствие автоматизированного контроля жизненного цикла управления инцидентами ИБ и уязвимостями;
3) отсутствие средств автоматизации реагирования на инциденты;
4) отсутствие полноценной и оперативной отчетности для принятия эффективных управленческих решений.

В связи с этим был проведен сравнительный анализ следующих решений SOAR-платформ: R-Vision IRP/ SOAR (Россия), Security Vision (Россия), КСУИБ (ICL) (Россия), Forti SOAR (США), IBM Resilient (США), отраженный в Табл. 2. Хотя в научной литературе указывается на возможность создания SOAR систем с использованием продуктов Open-Source [10], подобный подход требует высокого уровня зрелости компании в области ИТ и сопряжен со значительным количеством трудностей. Поэтому данный подход в анализе не рассматривался.

Таблица 2 - Сравнение решений SOAR-платформ

DOI: https://doi.org/10.23670/IRJ.2022.124.8.8

Критерии выбора решения	R-Vision IRP/ SOAR	Security Vision	КСУИБ (ICL)	Forti SOAR	IBM Resilient
Наличие функционала по управлению инцидентами ИБ	Да	Да	Да	Да	Да
Наличие интеграции с внешними системами и	Да	Да	Нет	Да	Да

СЗИ для автоматизации реагирования					
Наличие функционала по управлению уязвимостями	Да	Да	Нет	Нет	Нет
Наличие функционала по управлению активами	Да	Да	Нет	Нет	Нет
Наличие сертификации ФСТЭК или в процессе ее получения	Да	Да	Нет	Нет	Нет
Присутствие в реестре отечественного ПО	Да	Да	Нет	Нет	Нет
Поддержка взаимодействия с ФинЦЕРТ	Да	Да	Нет	Нет	Нет

Для дальнейшего сравнения необходимо использовать персонализированные весовые критерии выбора решения в соответствии с инфраструктурой компании:

- Критерии соответствия регуляторным требованиям;
- Критерии соответствия архитектурным требованиям;
- Критерии соответствия требованиям по ИБ;
- Критерии соответствия требованиям по контролю и мониторингу;
- Критерии соответствия требованиям по управлению инцидентами;
- Критерии соответствия требованиям по управлению активами;
- Критерии соответствия требованиям по управлению уязвимостями;
- Критерии соответствия требованиям по визуализации и отчетности.

Совместная работа SIEM-системы и SOAR-платформы будет выглядеть следующим образом [11]:

1. SIEM-система собирает логи с сетевых устройств и запускает на нем корреляции для генерации предупреждений.

2. Аналитик L1 оценивает эти предупреждения, чтобы определить, какие из них являются реальными инцидентами, а какие – ложными. Эти действия могут занять несколько часов, прежде чем аналитик сможет перейти к глубокому интеллектуальному реагированию на инциденты.

3. SOAR-платформа способна автоматизировать эту рутинную работу, взаимодействуя с другими технологиями безопасности для автоматического выполнения начальных шагов реагирования на инциденты.

4. После получения предупреждения от SIEM-системы SOAR-платформа автоматизирует процесс обогащения и оценку предупреждения, создавая инциденты и удаляя ложные срабатывания. Затем SOAR-платформа создает и назначает заявку в системе отслеживания инцидентов. Таким образом SOAR-платформа автоматизирует деятельность L1.

5. Аналитик L2 получает первоначальное предупреждение вместе с другой информацией из внутренних и внешних источников. SOAR-платформа могут автоматизировать начальные шаги с помощью Digital Playbooks – шагов, которые необходимо заполнить для устранения инцидента. Таким образом, SOAR-платформа экономит драгоценное время отклика и служит ускорителем кибербезопасности.

Важно понимать, что SOAR-платформы выводят возможности реагирования SIEM-систем на новый уровень. Решения SOAR-платформ дополняют, а не заменяют SIEM-системы. Можно определить следующие ключевые отличия [12]:

- SIEM-системы не создаются для объединения людей, процессов и технологий в рамках SOC;
- SIEM-системы и SOAR-платформы могут собирать журналы напрямую;
- SIEM-системы запускают корреляцию для всех журналов, чтобы генерировать предупреждения. SOAR-платформы для этого не предназначены;
- SOAR-платформы поддерживает сторонние источники, такие как службы анализа угроз и другие внешние источники;
- SOAR-платформы могут интегрироваться с другими продуктами безопасности и сетями. SIEM-системы для этого не предназначены.

Заключение

Исходя из вышесказанного, можно выделить следующую пользу от внедрения SOAR-платформы в ИТ-инфраструктуру:

– Снижение времени реагирования на инцидент ИБ за счет автоматизации рутинных задач и задач реагирования;

– Фокус персонала на анализ инцидента ИБ за счет автоматизации первичной обработки и реагирования;

– Повышение зрелости процессов за счет их прозрачности и измеряемости (SLA/KPI (Key Performance Indicator – ключевые показатели эффективности));

– Автоматизация отчетности по инцидентам в рамках передачи в ФинЦЕРТ/НКЦКИ.

Конфликт интересов

Не указан.

Рецензия

Сообщество рецензентов Международного научно-исследовательского журнала
DOI: https://doi.org/10.23670/IRJ.2022.124.8.9

Conflict of Interest

None declared.

Review

International Research Journal Reviewers Community
DOI: https://doi.org/10.23670/IRJ.2022.124.8.9

Список литературы / References

1. What Is SOAR? [Electronic source] // Cyberpedia. – 2021. – URL: https://www.paloaltonetworks.com/cyberpedia/what-is-soar. (accessed: 24.07.22)

2. Security Orchestration, Automation And Response (SOAR) [Electronic source] // Cybersecurity 101. – 2021. – URL: https://www.crowdstrike.com/cybersecurity-101/security-orchestration-automation-and-response-soar/. (accessed: 24.07.22)

3. Neiva C. Market Guide for Security Orchestration, Automation and Response Solutions [Electronic source] / C. Neiva, C. Lawson, T. Bussa et al. // Gartner Research. – 2020. – URL: https://www.gartner.com/en/documents/3990720. (accessed: 24.07.22)

4. Рахметов Р. SOAR-системы [Электронный ресурс] / Р. Рахметов // Securityvision блог. – 2021. – URL: https://www.securityvision.ru/blog/soar-sistemy/. (дата обращения: 24.07.22)

5. Lawson C. Market Guide for Security Orchestration, Automation and Response Solutions [Electronic source] / C. Lawson, A. Price // Gartner. – 2022. – URL: https://www.gartner.com/reviews/market/security-orchestration-automation-and-response-solutions. (accessed: 24.07.22)

6. Horner M. Realizing the Benefits of Security Orchestration, Automation, and Response (SOAR) [Electronic source] / M. Horner // Threatconnect Insights. – 2020. – URL: https://threatconnect.com/blog/realizing-the-benefits-of-security-orchestration-automation-and-response-soar/. (accessed: 24.07.22)

7. What Is SOAR? [Electronic source] // Trellix. – 2020. – URL: https://www.trellix.com/en-us/security-awareness/operations/what-is-soar.html. (accessed: 24.07.22)

8. Security Orchestration Automation and Response (SOAR) Tools and Solutions [Electronic source] // Rapid7. – 2021. – URL: https://www.rapid7.com/solutions/security-orchestration-and-automation/. (accessed: 24.07.22)

9. Schlette D. The quest for mature, intelligence-driven security operations and incident response capabilities. / D. Schlette, M. Vielberth, G. Pernul // Computers & Security. – 2021. – № 111. – DOI: 10.1016/j.cose.2021.102482

10. Gibadullin R.F. Development of the System for Automated Incident Management Based on Open-Source Software. / R.F. Gibadullin, V.V. Nikonorov // International Russian Automation Conference (RusAutoCon). – 2021. – № 1. – DOI: 10.1109/RusAutoCon52004.2021.9537385

11. Ванерке Р. SOAR: автоматизация реагирования [Электронный ресурс] / Р. Ванерке // Информационная безопасность. – 2021. – URL: https://lib.itsec.ru/articles2/Oborandteh/soar-avtomatizatsiya-reagirovaniya. (дата обращения: 24.07.22)

12. Суслина А. Обзор решений UBA, SIEM и SOAR: в чем различие? [Электронный ресурс] / А. Суслина // Anti-Malware.ru . – 2018. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/UBA-SIEM-SOAR. (дата обращения: 24.07.22)

Список литературы на английском языке / References in English

1. What Is SOAR? [Electronic source] // Cyberpedia. – 2021. – URL: https://www.paloaltonetworks.com/cyberpedia/what-is-soar. (accessed: 24.07.22)

2. Security Orchestration, Automation And Response (SOAR) [Electronic source] // Cybersecurity 101. – 2021. – URL: https://www.crowdstrike.com/cybersecurity-101/security-orchestration-automation-and-response-soar/. (accessed: 24.07.22)

3. Neiva C. Market Guide for Security Orchestration, Automation and Response Solutions [Electronic source] / C. Neiva, C. Lawson, T. Bussa et al. // Gartner Research. – 2020. – URL: https://www.gartner.com/en/documents/3990720. (accessed: 24.07.22)

4. Raxmetov R. SOAR-sistemy' [SOAR-systems] [Electronic source] / R. Raxmetov // Securityvision blog. – 2021. – URL: https://www.securityvision.ru/blog/soar-sistemy/. (accessed: 24.07.22) [in Russian]

5. Lawson C. Market Guide for Security Orchestration, Automation and Response Solutions [Electronic source] / C. Lawson, A. Price // Gartner. – 2022. – URL: https://www.gartner.com/reviews/market/security-orchestration-automation-and-response-solutions. (accessed: 24.07.22)

6. Horner M. Realizing the Benefits of Security Orchestration, Automation, and Response (SOAR) [Electronic source] / M. Horner // Threatconnect Insights. – 2020. – URL: https://threatconnect.com/blog/realizing-the-benefits-of-security-orchestration-automation-and-response-soar/. (accessed: 24.07.22)

7. What Is SOAR? [Electronic source] // Trellix. – 2020. – URL: https://www.trellix.com/en-us/security-awareness/operations/what-is-soar.html. (accessed: 24.07.22)

8. Security Orchestration Automation and Response (SOAR) Tools and Solutions [Electronic source] // Rapid7. – 2021. – URL: https://www.rapid7.com/solutions/security-orchestration-and-automation/. (accessed: 24.07.22)

9. Schlette D. The quest for mature, intelligence-driven security operations and incident response capabilities. / D. Schlette, M. Vielberth, G. Pernul // Computers & Security. – 2021. – № 111. – DOI: 10.1016/j.cose.2021.102482

10. Gibadullin R.F. Development of the System for Automated Incident Management Based on Open-Source Software. / R.F. Gibadullin, V.V. Nikonorov // International Russian Automation Conference (RusAutoCon). – 2021. – № 1. – DOI: 10.1109/RusAutoCon52004.2021.9537385

11. Vanerke R. SOAR: avtomatizaciya reagirovaniya [SOAR: Response Automation] [Electronic source] / R. Vanerke // InformationSecurity. – 2021. – URL: https://lib.itsec.ru/articles2/Oborandteh/soar-avtomatizatsiya-reagirovaniya. (accessed: 24.07.22) [in Russian]

12. Suslina A. Obzor reshenij UBA, SIEM i SOAR: v chem razlichie? [Review of UBA, SIEM and SOAR solutions: what is the difference?] [Electronic source] / A. Suslina // Anti-malware.ru. – 2018. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/UBA-SIEM-SOAR. (accessed: 24.07.22) [in Russian]