УДК 004.056.5

С.В. Корякин, srgkoryakin1@gmail.com
Институт информационных технологий КГТУ им. И.Раззакова
Институт машиноведения автоматики и геомеханики НАН КР
С.У. Сураналиева, suranalieva.salta18@gmail.com
Институт информационных технологий КГТУ им. И. Раззакова

ОБЗОР МЕТОДОВ РЕАЛИЗАЦИИ ПОДСИСТЕМ РАССЛЕДОВАНИЯ И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SOAR (SECURITY ORCHESTRATION AUTOMATION AND RESPONSE) В СОСТАВЕ СИСТЕМ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В данной работе рассмотрены ключевые проблемы, с которыми сталкиваются центры мониторинга информационной безопасности (SOC), включая высокую нагрузку на персонал, длительное время реагирования на инциденты и разрозненность используемых инструментов и систем. Для решения этих проблем были проанализированы различные подходы и методы, направленные на повышение эффективности работы SOC. В результате исследования было установлено, что наиболее оптимальным решением является внедрение платформы SOAR (Security Orchestration, Automation, and Response), так как она позволяет устранить все выявленные недостатки.

Исследования, проведенные Palo Alto Networks и Rapid7, подтверждают эффективность SOAR: по их данным, применение данной технологии может сократить время реагирования на инциденты до 70% и повысить производительность аналитиков на 35%. SOAR повышает эффективность SOC за счет автоматизации рутинных задач, что позволяет аналитикам сосредоточиться на поиске угроз и расследовании инцидентов. Кроме того, SOAR оптимизирует рабочие процессы, предоставляя централизованную панель управления операциями по обеспечению безопасности, что сокращает время на поиск информации и принятие решений.

Помимо повышения оперативности реагирования, SOAR способствует сокращению затрат за счет автоматизации процессов, уменьшения необходимости в сверхурочной работе и предотвращения утечек данных, приводящих к крупным финансовым потерям. Дополнительным преимуществом является улучшение общей безопасности за счет глубокой интеграции аналитики угроз и автоматизированного реагирования. Таким образом, SOAR является стратегически важным инструментом для современных SOC, обеспечивая их эффективную и бесперебойную работу.

Ключевые слова: оркестровка безопасности, автоматизация, реагирование, центр управления безопасностью, кибербезопасность, реагирование на инциденты, управление угрозами.

Введение

В условиях стремительного роста числа кибератак и их усложнения центры операций безопасности (SOC) сталкиваются с рядом серьезных вызовов. Киберпреступники разрабатывают все более сложные методы атак, а компании вынуждены инвестировать значительные ресурсы в защиту своей цифровой инфраструктуры. Однако традиционные подходы к управлению инцидентами оказываются недостаточно эффективными, в связи с чем организации сталкиваются с такими большими проблемами как: 1) высокая нагрузка на персонал; 2) длительное время реагирования на инциденты; 3) разрозненность инструментов и систем. Эти проблемы необходимо решить самым оптимальным методом, так как при таких условиях ухудшается эффективность и увеличивается перегруженность самого SOC и персонала.

Высокая нагрузка на персонал

Современные SOC ежедневно обрабатывают огромное количество оповещений и событий безопасности. Специалисты вынуждены вручную анализировать и классифицировать множество инцидентов, значительная часть которых оказывается ложными срабатываниями. Это приводит к усталости, когнитивной перегрузке и выгоранию сотрудников. В результате критически важные угрозы могут оставаться без внимания, а общая эффективность работы SOC снижается. Нехватка квалифицированных специалистов еще больше усугубляет ситуацию, так как SOC испытывают кадровый дефицит, а существующие сотрудники вынуждены работать в условиях постоянного стресса.

Длительное время реагирования на инциденты

При отсутствии автоматизированных процессов расследование и устранение инцидентов требует значительных временных затрат. Вручную анализировать инциденты, собирать дополнительную информацию, сопоставлять данные из различных источников и разрабатывать стратегию реагирования — все это занимает слишком много времени. В условиях постоянных кибератак и растущего числа угроз такая задержка может привести к серьезным финансовым и репутационным потерям для организации. Время, затраченное на реагирование, напрямую влияет на эффективность SOC: чем быстрее инцидент выявляется и устраняется, тем меньше ущерб от атаки.

Разрозненность инструментов и систем

SOC используют широкий спектр решений для мониторинга, анализа и реагирования на угрозы, включая SIEM, EDR, NDR, TIP и множество других инструментов. Однако отсутствие интеграции между ними приводит к разрозненности данных, необходимости ручного анализа информации из разных источников и, как следствие, к снижению скорости и точности реагирования. Без централизованного управления инцидентами SOC теряют возможность эффективно координировать свои действия и оптимально использовать ресурсы

Из этих проблем наиболее критичной является высокая нагрузка на персонал, так как именно она становится причиной замедления всех процессов в SOC, увеличивает риск ошибок и снижает общую эффективность работы специалистов.

Принято считать, что для решения таких ключевых проблем, как высокая нагрузка на персонал, длительное время реагирования и разрозненность инструментов, используются следующие методы, направленные на повышение эффективности работы SOC: 1) улучшение процессов и оптимизация рабочих процедур; 2) автоматизированное управление угрозами без SOAR; 3) автоматизация с использованием скриптов и RPA; 4) искусственный интеллект и машинное обучение; 5) интеграция Threat Intelligence (TI); 6) интеграция SOAR системы (Security Orchestration, Automation and Response).

Улучшение процессов и оптимизация рабочих процедур

Один из способов оптимизации работы SOC заключается в улучшении процессов и рабочих процедур. Внедрение стандартов реагирования на инциденты, таких как Incident Response Playbooks, позволяет создать четко регламентированные процедуры обработки инцидентов. Использование международных стандартов, таких как NIST CSF, MITRE ATT&CK и SANS Incident Response, помогает унифицировать работу SOC, а также улучшает процессы эскалации инцидентов для более быстрого реагирования. Кроме того, подход Fusion SOC, который предполагает интеграцию SOC с другими подразделениями безопасности, такими как IT, DevOps, Risk Management и Threat Intelligence, способствует лучшей координации действий и повышению качества расследований за счет обмена данными между различными отделами. Однако этот метод требует значительных временных и кадровых ресурсов для внедрения и постоянного контроля. Кроме того, сложность регламентации может привести к затруднениям в адаптации сотрудников к новым процессам.

Автоматизированное управление угрозами без SOAR

Другой подход – автоматизированное управление угрозами без использования SOAR. Оптимизация правил корреляции в SIEM за счет настройки более точных алгоритмов снижает количество ложных срабатываний. Применение поведенческой аналитики позволяет выявлять аномалии в данных, а использование технологий XDR (Extended Detection and Response) объединяет данные из различных источников, таких как EDR, NDR и облачные решения, что повышает точность обнаружения угроз. Также автоматизируется выявление сложных атак, которые не фиксируются отдельными инструментами. Однако этот метод имеет свои ограничения: он требует значительных усилий на настройку и сопровождение, а

также оставляет необходимость в ручном реагировании. Без полноценной автоматизации многие угрозы по-прежнему будут требовать вмешательства аналитиков, что увеличивает нагрузку на персонал и может замедлять реакцию на инциденты.

Автоматизация с использованием скриптов и RPA

Автоматизация с использованием скриптов и RPA (Robotic Process Automation) представляет собой еще один способ оптимизации работы SOC. Использование скриптов на Python, PowerShell и Bash позволяет автоматизировать рутинные задачи, такие как блокировка IP-адресов, выгрузка логов и изоляция хостов. Внедрение RPA для SOC помогает автоматизировать обработку типовых инцидентов, генерацию отчетов и сбор данных. Однако скрипты требуют ручного обслуживания, сложно масштабируются и не обеспечивают централизованного управления процессами. Кроме того, при изменении инфраструктуры SOC может потребоваться постоянное обновление скриптов, что создает дополнительную нагрузку на команду.

Искусственный интеллект и машинное обучение

Еще одним современным решением является применение искусственного интеллекта и машинного обучения. Использование моделей машинного обучения позволяет предсказывать угрозы, анализируя прошлые инциденты и выявляя характерные паттерны атак. Это также способствует автоматическому снижению уровня ложных срабатываний. Технология User and Entity Behavior Analytics (UEBA) помогает обнаруживать аномальное поведение пользователей и устройств внутри сети, что позволяет выявлять сложные атаки, такие как компрометация учетных записей. Однако для эффективного функционирования подобных моделей требуются большие объемы данных и длительное обучение, а также настройка алгоритмов. Возможны ложные срабатывания, что требует дополнительного контроля со стороны аналитиков и увеличивает нагрузку на персонал.

Интеграция Threat Intelligence (TI)

Интеграция Threat Intelligence (TI) также играет важную роль в повышении эффективности SOC. Использование платформ Threat Intelligence позволяет автоматически обновлять индикаторы компрометации (IoC) и проводить корреляцию с SIEM. Это значительно ускоряет выявление атак на основе глобальных данных о киберугрозах. Однако данный метод требует ручного анализа полученной информации и ее применения в защитных механизмах SOC. Автоматическое обновление данных TI может привести к перегрузке системы большим количеством ложных индикаторов, что может затруднить эффективное реагирование на реальные угрозы.

Интеграция SOAR системы (Security Orchestration, Automation and Response)

SOAR объединяет преимущества всех вышеперечисленных методов, обеспечивая автоматизацию реагирования на инциденты, интеграцию различных систем и сокращение нагрузки на персонал. Он позволяет автоматизировать анализ инцидентов, исключая рутинные задачи для аналитиков, и использовать плейбуки для быстрого реагирования без участия человека. Глубокая интеграция с SIEM, XDR, EDR, NDR и TIP создает централизованное управление инцидентами, а автоматическая корреляция данных снижает время анализа угроз. Дополнительным преимуществом SOAR является фильтрация ложных срабатываний, автоматизированная эскалация только важных инцидентов и уменьшение риска человеческих ошибок. Хотя SOAR требует первоначальной настройки и разработки сценариев реагирования, его преимущества в значительном снижении нагрузки на персонал и ускорении процесса реагирования делают его оптимальным выбором для современных SOC. Инвестиции в SOAR окупаются за счет повышения эффективности работы аналитиков, минимизации времени реагирования и улучшения общего уровня безопасности организации.

Несмотря на многообразие методов, используемых для решения указанных задач, наиболее эффективным подходом считается внедрение системы SOAR, которая

обеспечивает автоматизацию рутинных процессов, снижение числа ложных срабатываний и оперативную, координированную реакцию на инциденты.

Основы SOAR

SOAR (Security Orchestration Automation and Response) — это класс решений, предназначенный для оркестрации, координации и централизованного управления СЗИ, а также системами безопасности. SOAR обогащает данными инциденты ИБ, получаемые из SIEM системы или иных источников, обрабатывает инциденты ИБ и автоматизирует механизм реагирования, т.е. предлагает готовые инструкции реагирования на инциденты [1].

Что напрямую относится к работе SOAR [1]:

- Оркестровка (Orchestration) — интеграция технологий и инструментов для принятия решений на основе информации об уровне риска и состоянии системы.
- Автоматизация (Automation) — для замещения задач, которые ранее выполняли «вручную», автоматическими действиями со стороны системы по заготовленным сценариям (playbooks).
- Управление киберинцидентами и совместная деятельность (Incident management and collaboration) — сквозной подход по работе с «назначением приоритета», «протоколированием действий» и «принятием решений на основе политик компании».
- Формирование отчетов (Dashboards and reporting) — визуализация информации по ключевым метрикам и составление сводок для трех типов сотрудников — аналитиков, руководителей SOC и директоров по ИБ (Chief Information Security Officer, CISO).

На рисунке 1 представлена функциональная структурная схема SOAR системы.

Рисунок 1 — Основные функции SOAR-систем

SOAR обладают функциональностью, позволяющей сократить время расследования значимых инцидентов в сфере ИБ [2]. Это, в частности:

- интеграция технологий / инструментов, необходимых для принятия решений на основе отчетов о состоянии системы безопасности и оценки возможного уровня риска;
- автоматизация процессов;
- управление инцидентами с использованием сквозного подхода (определение приоритетов, регистрация всех действий по реагированию на инциденты, принятие решений в соответствии с политикой компании);
- визуализация данных, связанных с ключевыми показателями, отчетами сотрудников и документацией.

Огромным преимуществом использования SOAR является то, что они позволяют автоматизировать процессы управления инцидентами, начиная с назначения приоритетов и заканчивая, собственно, реагированием. Благодаря заранее созданным планам действий («плейбукам») система способна самостоятельно среагировать на то или иное происшествие, тем самым повысив точность и скорость выполнения операций. При этом следует обратить внимание на то, что автоматизация процессов реагирования при всей своей сложности и витиеватости должна быть гибкой и предусматривать включение человека в рабочий процесс, а иногда и вообще останавливаться, ожидая решения аналитика.

За счет оркестровки SOAR обеспечивает скоординированный автоматический ответ на выявленную несанкционированную активность. Конечно, полностью решить проблему в автоматическом режиме не всегда представляется возможным, но SOAR должна быть способна переводить средства защиты в более строгие режимы работы, своевременно начинать сбор подробной статистики либо ограничивать операции, которые потенциально могут привести к утечкам данных. Кроме того, важно, чтобы SOAR умела обрабатывать и сортировать оповещения, поступающие от внешних систем (например, SIEM), вести детальный журнал, быть источником для создания базы знаний о возможных атаках, предоставлять данные для аналитики и расследования инцидентов и к тому же была готова к интеграции с платформами киберразведки (Threat Intelligence).

SOAR может интегрировать данные об угрозах, поступающие из разных источников. Это достигается с помощью трех основных модулей, перечисленных далее [2]:

- Модуль реагирования на инциденты в области безопасности (Security Incident Response, SIR) облегчает процесс выявления происшествий. Он также импортирует информацию из других применяемых решений и настраивает ИБ-процедуры.
- Для приоритизации уязвимостей продукты класса SOAR используют модуль Response Vulnerability. Он помогает определить степень подверженности бизнес-систем угрозам.
- Модуль анализа угроз на основе данных киберразведки предназначен для выявления признаков возможной компрометации, а также для углубленного отслеживания угроз. Его основное преимущество заключается в том, что он поддерживает различные стандарты, применяемые для обмена данными об угрозах. Кроме того, этот модуль позволяет добавлять пользовательские источники и обмениваться информацией с внешними системами.

SOAR не заменяет, а дополняет другие системы, помогая автоматизировать рутинные задачи. В таблице 1 представлены все вышеперечисленные методы, их преимущества и недостатки.

Таблица 1 — Сравнение методов для решения ключевых проблем

Метод	Какие проблемы решает	Какие проблемы остаются нерешенными
Улучшение процессов и оптимизация рабочих процедур	+ Ускоряет реагирование за счет стандартизации процедур + Повышает координацию между командами + Облегчает расследование инцидентов	- Требует значительных кадровых и временных ресурсов для внедрения и поддержки - Процессы все еще зависят от человеческого фактора
Автоматизированное управление угрозами без SOAR	+ Снижает количество ложных срабатываний в SIEM + Улучшает обнаружение сложных атак благодаря XDR и поведенческому анализу	- Не автоматизирует реагирование на угрозы, требуется ручное вмешательство - Высокая сложность настройки и поддержки
Автоматизация с использованием скриптов и RPA	+ Автоматизирует рутинные задачи (блокировка IP, сбор логов, изоляция хостов) + Ускоряет выполнение типовых операций	- Скрипты требуют ручного обслуживания и доработки - Сложно масштабируется и централизуется

Искусственный интеллект и машинное обучение	+ Обнаруживает аномальное поведение и сложные угрозы + Снижает число ложных срабатываний + Анализирует прошлые атаки для предсказания новых	- Требует больших объемов данных и ресурсов на обучение моделей - Возможны ложные срабатывания
Интеграция Threat Intelligence (TI)	+ Позволяет быстро выявлять угрозы на основе глобальных данных + Автоматически обновляет индикаторы компрометации (IoC)	- Требует ручного анализа и адаптации данных под конкретные сценарии SOC
SOAR (Security Orchestration, Automation and Response)	+ Автоматизирует реагирование на инциденты и исключает рутинные задачи для аналитиков + Объединяет SIEM, XDR, EDR, NDR и TIP в единую систему + Использует плейбуки для быстрого реагирования + Оптимизирует работу аналитиков, снижает количество ложных срабатываний + Улучшает продуктивность SOC и снижает риск человеческих ошибок	- Требует времени и ресурсов на настройку интеграций и плейбуков - Может быть сложным в развертывании

При сравнении всех перечисленных методов самым оптимальным выходит применение SOAR системы в SOC. Этому может быть подтверждением растущее количество исследований.

Исследование, проведенное американской компанией, оказывающей услуги в области информационной безопасности Palo Alto Networks, показало, что SOAR может сократить время реагирования на инциденты до 70% [8]. Другое исследование, проведенное Rapid7, показало, что SOAR может повысить производительность аналитиков на 35% [9].

SOAR повышает эффективность SOC несколькими способами. Во-первых, SOAR может автоматизировать задачи, которые в настоящее время выполняются аналитиками вручную. Это позволяет аналитикам сосредоточиться на более сложных задачах, таких как поиск угроз и расследование инцидентов.

Во-вторых, SOAR может оптимизировать рабочие процессы, предоставляя единую панель для управления операциями по обеспечению безопасности. Это может помочь сократить время, необходимое аналитикам для поиска нужной информации и принятия мер в случае инцидентов.

Кроме того, помимо решения ключевых проблем, SOAR также может помочь сократить расходы за счет автоматизации задач, снижения необходимости в сверхурочной работе и улучшения общего состояния безопасности, что может помочь предотвратить утечки данных. Внедрение SOAR системы позволяет улучшить общее состояние безопасности, обеспечивая лучшую видимость событий безопасности, автоматизируя реагирование на инциденты и улучшая интеграцию аналитики угроз.

Согласно исследованиям одной из ведущих компаний в сфере кибербезопасности — Palo Alto Networks SOAR, система может автоматизировать такие задачи, как сортировка, расследование и устранение инцидентов, что может помочь сократить время реагирования на инциденты до 70% [8]. На рисунке 2 представлено процентное соотношение времени реагирования на инциденты до и после внедрения SOAR.

Рисунок 2 — Время реагирования на инциденты

Автоматизируя задачи и оптимизируя рабочие процессы, SOAR может освободить аналитиков, чтобы они могли сосредоточиться на более сложных задачах, повышая их производительность до 35% [9]. На рисунке 3 представлено процентное соотношение влияния SOAR на эффективность SOC до и после внедрения SOAR.

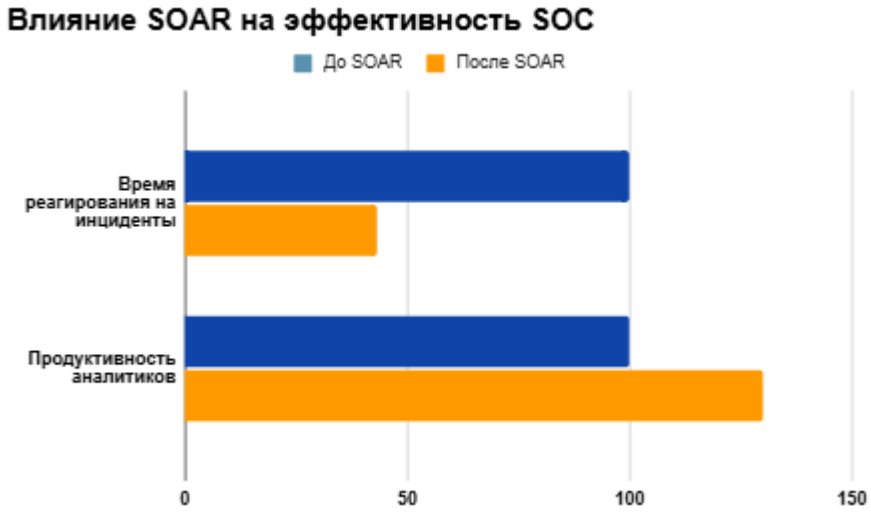

Рисунок 3 — Продуктивность аналитиков

SOAR может помочь снизить затраты за счет автоматизации задач, сокращения необходимости сверхурочной работы и улучшения общего состояния безопасности, что может помочь предотвратить дорогостоящие утечки данных [10]. На рисунке 4 представлено процентное соотношение затрат до и после внедрения SOAR.

Рисунок 4 — Снижение затрат

Заключение

Таким образом, в настоящее время компании внедряют SOAR как решение, обеспечивающее максимальную эффективность работы информационных систем, учитывая представленные выше преимущества. Данный подход подтверждается реальными примерами успешного применения.

Например, известная финансовая организация внедрила SOAR в свою IT-инфраструктуру в 2018 году [11]. Перед внедрением SOAR команде SOC требовалась помощь, чтобы справиться с объемом предупреждений и инцидентов, что приводило к задержке реагирования на инциденты и повышенному риску компрометации [12].

После внедрения SOAR в организации сократилось время реагирования на инциденты на 60 %, а производительность аналитиков выросла на 20 % [11]. SOAR помог автоматизировать многие ручные задачи, которые ранее выполняли аналитики, такие как сортировка и расследование инцидентов [11]. Это позволило аналитикам сосредоточиться на более сложных задачах, таких как поиск угроз и управление уязвимостями [11].

Организация также значительно улучшила общий уровень безопасности [11]. SOAR предоставил команде SOC единую панель для управления всеми данными безопасности, что упростило выявление угроз и реагирование на них [11].

В ходе проведенного исследования были рассмотрены ключевые проблемы, влияющие на эффективность работы SOC: высокая нагрузка на персонал, длительное время реагирования на инциденты и разрозненность используемых инструментов и систем. Для решения этих проблем были изучены различные подходы, включая оптимизацию процессов, применение автоматизированных решений без SOAR, использование скриптов и RPA, внедрение технологий машинного обучения и интеграцию Threat Intelligence. Каждый из этих методов обладает своими преимуществами и ограничениями, позволяя частично устранить выявленные проблемы.

Однако самым оптимальным решением для повышения эффективности SOC является внедрение SOAR. Данный подход объединяет преимущества всех рассмотренных методов, обеспечивая автоматизацию реагирования на инциденты, интеграцию различных систем и снижение нагрузки на персонал. Использование SOAR позволяет значительно ускорить процесс обработки инцидентов, минимизировать рутинные задачи для аналитиков, улучшить корреляцию данных между различными решениями (SIEM, XDR, EDR, NDR, TIP) и повысить общую продуктивность SOC.

Таким образом, применение SOAR становится стратегически важным шагом для организаций, стремящихся к повышению уровня кибербезопасности, снижению времени реакции на угрозы и оптимизации работы аналитиков. Несмотря на необходимость

первоначальной настройки и поддержки системы, долгосрочные выгоды от использования SOAR значительно превосходят вложенные ресурсы, делая его наиболее эффективным решением для современных центров мониторинга информационной безопасности.

Литература

1. https://www.securityvision.ru/blog/tekhnologiya-soar-i-ee-mesto-v-soc/ (дата обращения 01.02.2025)
2. https://www.anti-malware.ru/analytics/Market_Analysis/Security-Orchestration-Automation-and-Response-SOAR-Solution-Overview (дата обращения 01.02.2025)
3. Symantec (2019). SOAR: The Future of Security Operations. (дата обращения 05.02.2025)
4. McAfee (2018). SOAR: A New Approach to Security Operations. (дата обращения 05.02.2025)
5. Forrester Research (2018). SOAR: The Missing Piece of the Security Automation Puzzle. (дата обращения 05.02.2025)
6. McAfee (2018). SOAR: A New Approach to Security Operations (дата обращения 05.02.2025)
7. Pulyala, S. R., Desetty, A. G., & Jangampet, V. D.. (2019). The Impact of Security Orchestration, Automation, and Response (SOAR) on Security Operations Center (SOC) Efficiency: A Comprehensive Analysis. Turkish Journal of Computer and Mathematics Education (TURCOMAT). https://doi.org/10.61841/turcomat.v10i3.14323 (дата обращения 13.02.2025)
8. Palo Alto Networks (2019). SOAR Automation: A Game-Changer for SOC Efficiency (дата обращения 13.02.2025)
9. Rapid7 (2019). SOAR: A New Paradigm for Security Automation (дата обращения 13.02.2025)
10. Symantec (2019). SOAR: The Future of Security Operations (дата обращения 13.02.2025)
11. Palo Alto Networks (2019). SOAR Automation: A Game-Changer for SOC Efficiency (дата обращения 13.02.2025)
12. IBM (2018). SOAR: Orchestrating Security Automation for a More Efficient SOC (дата обращения 13.02.2025)