ENERGY SOAR

bako tech®

SOAR ДЛЯ НАЧИНАЮЩИХ

Устраните проблемы безопасности с помощью решений SOAR
(Security Orchestration, Automation, and Response)

www.energylogsoar.com

Что такое SOAR?

Высокая частота атак, сложность IT-сетей и отсутствие квалифицированных специалистов подвергают многие компании риску потери данных, финансового и репутационного ущерба. SOAR – это решение, позволяющее автоматизировать процессы реагирования на инциденты безопасности.

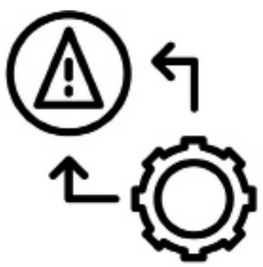
Аббревиатура «SOAR» расшифровывается как Security Orchestration, Automation, Response, и каждый компонент этой платформы играет определенную роль в процессе реагирования на инцидент безопасности:

Оркестрация (Orchestration)

Оркестрация в SOAR подразумевает координацию действий и интеграцию различных инструментов, систем и япроцессов для эффективного реагирования на инциденты безопасности. Этот компонент позволяет создавать автоматизированные процессы реагирования на инциденты и улучшает сотрудничество между различными командами, вовлеченными в работу с кибервторжениями.

Автоматизация (Automation)

Автоматизация является ключевым элементом SOAR, поскольку позволяет легче и эффективнее реагировать на атаки. Благодаря автоматизации можно ускорить запуск соответствующих процедур обнаружения и изолирования угроз, а также быстрее отправлять сообщения об инцидентах. И это еще не полный перечень возможностей!



Реагирование (Response)

Компонент реагирования в SOAR предусматривает оперативное принятие мер по минимизации ущерба в результате инцидента безопасности. Это включает идентификацию и классификацию инцидентов, изоляцию и нейтрализацию угроз, а также анализ и документирование инцидентов.

Когда вам стоит задуматься о внедрении SOAR?

Когда не хватает соответствующих ресурсов

Многие организации борются с нехваткой квалифицированного персонала, способного эффективно реагировать на инциденты безопасности. SOAR автоматизирует процессы реагирования, экономя время и человеческие ресурсы и одновременно обеспечивая мощную реакцию на инциденты.

Когда стоит острая потребность в соблюдении нормативных требований

Многие секторы экономики подпадают под строгие нормативные требования по кибербезопасности. SOAR позволяет организациям соответствовать этим требованиям путем автоматизации процессов реагирования на инциденты и отчетности о результатах.

Когда необходимо быстро реагировать на инциденты

В современном ландшафте ответ на угрозы должен быть быстрым и эффективным. SOAR заботится об оперативном обнаружении вредоносных действий и реагировании на них, минимизируя ущерб в результате атак.

Когда есть потребность в постоянном совершенствовании

Современные организации должны постоянно улучшать свои процедуры и процессы в сфере кибербезопасности, чтобы противостоять большему количеству угроз. SOAR способствует непрерывному совершенствованию процессов реагирования на инциденты и улучшает работу команды по IT-безопасности. Он интегрируется с различными IT-системами и системами безопасности в организации, такими как SIEM, электронная почта, облачные среды, системы продаж билетов, брандмауэры и т.д. Эта интеграция позволяет собирать информацию из разных источников, обеспечивая комплексное управление инцидентами.

Архитектура

Серверы MISP и коммерческие списки угроз занимают ведущее место в архитектуре SOAR. С их помощью система получает наиболее актуальную информацию о подозрительных IP- и URL-адресах, файлах и IoC, и это способствует быстрому реагированию на угрозы.

SOAR также позволяет выполнять некоторые автоматизированные действия на основе собранной информации. Он может проводить анализ вложений, блокировать хосты, IP-адреса и файлы песочницы, а также оповещать назначенных лиц в организации.

Архитектура Energy SOAR состоит из центральной точки, которая собирает всю информацию, связанную с инцидентами безопасности и интеграцией с разными системами. Используя серверы MISP и коммерческие списки угроз, SOAR может получать новейшую информацию об опасностях, обеспечивая быстрое реагирование на инциденты.

Интеграции

Energy SOAR запускает автоматизированные действия в IT-системах и системах безопасности посредством интеграции с их API. Он настраивает действия, которые будут производиться в ответ на определенные события или инциденты, например выявление подозрительной активности или атаки.

Когда SOAR обнаруживает угрозу или инцидент, он может инициировать определенные действия: например, автоматически отправить всю систему в карантин или заблокировать IP-адрес в брандмауэре. Он также может посылать уведомления другим решениям или командам, информируя их об инциденте и побуждая их принять меры.

Следует отметить, что SOAR обычно настроен таким образом, что позволяет администраторам выбирать, какие действия следует запускать при определенных условиях, в соответствии с установленными правилами безопасности и политикой организации.

Интеграция с CSIRT

Интеграция решения класса SOAR с внешней CSIRT (группой реагирования на инциденты компьютерной безопасности) предполагает содействие сотрудничеству и обмену информацией между компанией и внешним поставщиком услуг CSIRT.

SOAR может интегрироваться с внешней CSIRT, пересылая информацию, связанную с инцидентом (например, данные журнала) и результаты анализа, чтобы получить помощь в решении проблемы. SOAR автоматически передает эту информацию внешнему поставщику услуг CSIRT, ускоряя процесс реагирования на инциденты и повышая его эффективность.

Интеграция с внешним CSIRT также позволяет обмениваться данными о тенденциях и угрозах кибербезопасности, помогая компании повысить эффективность мер предосторожности в отношении будущих инцидентов.

Жизненный цикл SOAR в организации

Жизненный цикл SOAR – это непрерывный процесс, направленный на обеспечение эффективного функционирования системы и удовлетворение требований организации. Все этапы этого цикла одинаково важны и требуют надлежащего планирования и привлечения организационного персонала.

Ключом к успеху внедрения SOAR является надлежащее планирование и согласование с потребностями организации, а также постоянное развитие и адаптация к изменяющимся требованиям.

1 ПЛАНИРОВАНИЕ

Определяются цели и требования организации, а также наиболее распространенные типы инцидентов и процессы их обработки в организации. Проверяются возможности интеграции с другими решениями безопасности.

2 РЕАЛИЗАЦИЯ

На этом этапе система настраивается в соответствии с требованиями компании, интегрируется с существующими решениями и инструментами. Для оптимизации операций создаются автоматизированные процессы, а персонал, ответственный за их работу, проходит специальное обучение.

3 ЭКСПЛУАТАЦИЯ И РАЗВИТИЕ

Как и любое решение безопасности в сфере IT, SOAR нуждается в постоянном мониторинге, оценке и развитии. Это гибкая среда, обеспечивающая непрерывный рост организации и автоматизацию все более новых и передовых процессов.

Создание рабочих процессов

Пользователи могут создать рабочие процессы с помощью редактора, доступного в Energy SOAR. Редактор позволяет добавлять разные этапы в процесс, например, действия, решения, условия и интеграции. Пользователи также могут указать, как следует запускать рабочий процесс: вручную, автоматически в ответ на определенные события или в определенное время.

Каждый этап рабочего процесса можно настроить для запуска определенных действий в IT-системах и системах безопасности. Например, когда SOAR представляет угрозу, он может автоматически инициировать рабочий процесс, запускающий автоматизированные действия в других решениях (SIEM, IDS/IPS, антивирусах или системах управления событиями). Благодаря этой интеграции SOAR обеспечивает автоматизацию процессов и улучшает эффективность работы в случае инцидентов безопасности.

Как выглядит SOAR на практике

Что же представляет собой пошаговый процесс работы SOAR — от обнаружения инцидента до реагирования на него?

1. Первым шагом является интеграция SOAR с другими системами безопасности – SIEM, IDS, IPS, EDR и электронной почтой. Он получает данные об обнаруженных инцидентах и автоматизирует серию действий, которые обычно следует выполнять вручную.

2. После этого система выполняет анализ атрибутов полученного события (наблюдаемых), таких как IP-адреса, имена хостов, имена пользователей или URL-адреса. Каждому кейсу автоматически назначается уровень критичности и соответствующие теги. Кейсы можно назначать вручную или автоматически операторам, получающим определенные задания для выполнения. Каждый пользователь имеет доступ к четкому списку своих задач, а весь процесс рассмотрения дела фиксируется в истории.

Если выполняются конкретные условия для определенного типа кейса (например, определение соответствующего правила корреляции), SOAR выполняет весь процесс обработки без привлечения IT-специалистов. В таких случаях система не только собирает данные об инциденте, но и выполняет задачи, приводящие к блокированию IP-адреса на брандмауэре или изоляции компьютера в сети.

С помощью SOAR организация может быстро и эффективно реагировать на угрозы безопасности, обеспечивая защиту данных и предотвращение нарушений конфиденциальности.

Варианты использования

Анализ электронной почты

Если сотрудник заметит, что полученное электронное письмо выглядит подозрительным или неподходящим, он может переслать его в SOAR, который проанализирует его содержание и структуру.

SOAR использует различные механизмы анализа, такие как синтаксический и семантический для идентификации потенциально вредных элементов в сообщении электронной почты. Эти механизмы позволяют выявлять подозрительные ссылки, вложения и другие типичные признаки попыток фишинга. Система также может использовать публичные или частные списки угроз и базы данных, содержащие информацию об известных попытках атак, что позволяет сравнивать содержимое сообщения с этими угрозами.

Если SOAR определяет потенциальную угрозу в сообщении электронной почты, он автоматически квалифицирует инцидент как потенциальную фишинговую атаку. Затем система может выполнить серию автоматизированных действий, чтобы минимизировать риск. Возможные действия могут включать блокировку отправителя сообщения и его IP-адреса и пересылку подозрительного сообщения в специализированную группу анализа безопасности инцидентов.

При обнаружении фишинговой атаки SOAR также может известить соответствующих лиц или команды в организации: команду безопасности, CSIRT или другие подразделения информационной безопасности. Эти уведомления позволяют быстро реагировать на потенциальные угрозы.

Одной из ключевых особенностей SOAR является возможность проводить дальнейший анализ инцидентов. Команда безопасности или CSIRT может тщательно проанализировать ситуацию, выявить потенциальные угрозы и принять необходимые меры для уменьшения ущерба, причиненного атакой.

Варианты использования

Автоматическая блокировка хостов / IP

Это один из важнейших use cases, особенно в контексте защиты от атак вредоносного ПО и взлома сети. Ниже приведен пример того, как SOAR можно использовать в этом конкретном случае.

Процесс начинается с обнаружения потенциальной угрозы. SOAR, интегрированный с различными инструментами безопасности (системы обнаружения и предотвращения вторжений (IDS/IPS), системы защиты от вредоносных программ или инструменты анализа журналов), способен идентифицировать неизвестные или подозрительные IP-адреса, которые пытаются получить доступ к сети. Также SOAR может обнаруживать хосты, создающие подозрительный сетевой трафик.

После обнаружения угрозы SOAR начинает анализ. При этом используются такие методы, как анализ поведения, анализ тенденций и сравнение с внешними источниками информации об угрозах, чтобы оценить, действительно ли выявленная активность представляет угрозу. Инцидент классифицируется как угроза только после того, как SOAR подтверждает злонамеренность действия. Информация об этом инциденте хранится в системе для дальнейшего анализа.

После классификации инцидента SOAR выполняет автоматические действия, чтобы заблокировать вредоносный IP-адрес или хост. Это может включать настройки сетевых брандмауэров для блокировки трафика, поступающего от определенного источника угрозы, или блокировки IP-адреса на уровне управления сетью.

После блокировки вредоносного IP-адреса или хоста SOAR автоматически извещает соответствующих лиц об инциденте. Уведомления можно передавать группе безопасности, CSIRT, IT-менеджерам или другим соответствующим сторонам. Сообщение содержит всю соответствующую информацию об инциденте, включая подробности предпринятых действий.

Получив сообщение, служба безопасности может провести дальнейший анализ ситуации: например, принять дополнительные меры, такие как отслеживание источника атаки, усиление мер безопасности сети или обучение сотрудников, чтобы предотвратить подобные инциденты в будущем.

Наконец, после закрытия инцидента, информация о нем хранится в SOAR для отчетности и улучшения. Эту информацию можно использовать для анализа тенденций, выявления пробелов в безопасности, а также обучения команды.

Варианты использования

Слежение за тенденциями анализа угроз

Energy SOAR не только предлагает организациям эффективное управление инцидентами безопасности, но и позволяет исследовать индикаторы компрометации (IoC) и использует текущие тенденции атак, чтобы определить, имели ли они место в компании.

Пример 1

При обнаружении кампании вредоносного программного обеспечения, которая использует определенный домен для связи HTTP, пользователь SOAR может легко провести анализ журнала DNS. Это помогает проверить, была ли связь с этим доменом в системе. Если обнаружено, что конечная точка установила такую связь, есть подозрение на инфицирование. Для минимизации риска дальнейшего распространения угрозы в SOAR можно принять меры, такие как карантин хоста или его полная изоляция от сети.

Пример 2

Злоумышленники часто используют домены, похожие на популярные компании, такие как microsoft.com (например, mlcrosoft.com). В этом случае информация о текущих кампаниях может появиться в списках Threat Intelligence. С помощью SOAR можно проанализировать журналы, чтобы проверить, нет ли подключения к этому подозрительному домену. Если такие соединения обнаружены, можно принять соответствующие меры по защите организации от фишинга — например, заблокировать доступ к этому домену или предупредить пользователей о потенциальной угрозе.

Таким образом, благодаря использованию возможностей SOAR для интеграции со списками разведки об угрозах и анализе текущих тенденций атак решение Energy SOAR позволяет организациям быстро реагировать на потенциальные угрозы.

Выявление неавторизованных входов администраторов в нерабочее время с помощью SMS-подтверждения

Рассмотрим пример компании XYZ, которой нужно было оградить свою систему от несанкционированного входа администратора в нерабочее время. Цель заключалась в том, чтобы реализовать механизм проверки входа посредством SMS-сообщения с уникальной ссылкой, которую администратор должен был подтвердить в течение определенного времени. В противном случае аккаунт администратора будет автоматически заблокирован.

Процесс реализации:

Выявление неавторизованных попыток входа:

Energy SOAR был сконфигурирован для мониторинга системных журналов и событий, связанных с входом. При обнаружении несанкционированной попытки входа администратора в нерабочее время система начинает процедуру проверки.

Генерация SMS-сообщения:

SOAR автоматически генерирует SMS-сообщение, содержащее уникальную ссылку для подтверждения входа. Каждая попытка входа ограничена по времени (например, 30 минут).

Отправка SMS-сообщения:

SOAR отправляет сгенерированное SMS-сообщение со ссылкой для подтверждения входа на зарегистрированное мобильное устройство, связанное с учетной записью администратора.

Подтверждение входа:

Администратор получает SMS-сообщение, содержащее ссылку для подтверждения входа на мобильное устройство. Для подтверждения входа ему необходимо перейти по предоставленной ссылке.

Действия после подтверждения входа:

После нажатия ссылки SOAR получает подтверждение администратора. Если подтверждение получено в течение указанного времени (например, 30 минут), вход считается авторизованным.

Блокировка учетной записи в случае неподтверждения:

Если администратор не сможет подтвердить вход в течение определенного периода времени, SOAR автоматически блокирует аккаунт администратора, минимизируя риск несанкционированного доступа и действий в системе.

Вывод

Благодаря процедуре проверки входа администратора во внерабочее время с помощью Energy SOAR, компания XYZ получила дополнительный уровень защиты от неавторизованных входов.

Процесс проверки входа посредством SMS обеспечивает дополнительный уровень безопасности, минимизируя риск несанкционированного доступа. Реализация описанной процедуры может существенно повысить кибербезопасность организации, защищая данные и инфраструктуру от возможных атак.

Energy SOAR — это одно из наиболее инновационных решений SOAR, доступных на рынке. Оно представляет собой интегрированную платформу с IT-системами компании, предназначенную для повышения скорости и эффективности реагирования на инциденты безопасности. Energy SOAR является комплексным решением для управления инцидентами безопасности в организациях, которое собирает всю информацию об обнаруженных угрозах.

BAKOTECH® — международная компания, которая занимает передовые позиции в сфере фокусной Value Added IT-дистрибуции и поставляет решения ведущих мировых IT-производителей. Позиционируя себя как True Value-Added IT-дистрибьютор, BAKOTECH предоставляет профессиональную пред- и постпродажную, маркетинговую, техническую поддержку партнерам и конечным заказчикам.
Географически компания работает в 26 странах на рынках Центральной и Восточной Европы, Балкан, Балтии, Кавказа, Центральной Азии с офисами в Праге, Кракове, Риге, Киеве, Баку и Нурсултане.

Если вам нужна консультация по решению, пожалуйста, свяжитесь с нами: els@bakotech.com

+380 67 100 0068
www.bakotech.com
www.energylogserver.com