SOAR: AUTOMATING INFORMATION SECURITY INCIDENTS

Article · May 2021

CITATION
1

READS
176

3 authors, including:

Valentin Bogdanov
Ural Federal University
2 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Nickolay Domukhovsky
CyberLympha Ltd.
15 PUBLICATIONS **9** CITATIONS
SEE PROFILE

SOAR: автоматизация работы с инцидентами информационной безопасности

В статье обоснована необходимость использования систем класса Security Orchestration, Automation and Response (SOAR), рассмотрены актуальные проблемы, связанные с рациональным и эффективным применением систем защиты информации, масштабированием функций информационной безопасности (ИБ), управлением инцидентами и процессами обеспечения ИБ. Авторы рассмотрели функциональную архитектуру систем класса SOAR и описали состав основных подсистем, реализующих функции оркестровки средств защиты информации и автоматизации реагирования на инциденты ИБ.

Ключевые слова: автоматизация функций ИБ, оркестровка средств защиты информации, реагирование, имплементация политик безопасности, плейбук, функциональная архитектура SOAR

Валентин Викторович Богданов,
кандидат технических наук,
генеральный директор
vbogdanov@ussc.ru

Николай Анатольевич Домуховский,
заместитель генерального директора
ndomukhovsky@ussc.ru

Михаил Валерьевич Савин,
руководитель проекта
msavin@ussc.ru

ООО «Уральский центр систем безопасности»

Введение

Из-за лавинообразного роста числа инцидентов ИБ, серьезности их последствий, напрямую влияющих на возможность функционирования организации, собственники и руководители в полной мере стали осознавать серьезность проблемы защиты информации. Сегодня организации сталкиваются с проблематикой следующего уровня, заключающейся в невозможности рационально и эффективно использовать создаваемые системы защиты информации, масштабировать внедряемые функции ИБ, оперативно и полноценно управлять инцидентами ИБ и процессами обеспечения ИБ, а арсенал существующих подходов недостаточен для ее решения.

Условно, обозначенную проблематику можно разбить на четыре связанных блока:

- нехватка квалифицированного персонала;
- объективная сложность внедрения полноценных процессов эксплуатации средств защиты информации и управления функциями ИБ;
- разрыв между потребностями руководства в части управления и контроля, с одной стороны, и потенциалом существующих на рынке средств защиты информации, с другой;
- изменение ландшафта объектов защиты.

Рассмотрим данные блоки более детально.

Нехватка квалифицированного персонала в области ИБ отмечается во многих источниках (например, [1]). При этом данная проблема является многофакторной и заключается не только в отсутствии персо-

En SOAR: Automating Information Security Incidents

V. V. Bogdanov,
PhD (Eng.), CEO
vbogdanov@ussc.ru

N. A. Domukhovsky,
Deputy CEO for Science and Technology
ndomukhovsky@ussc.ru

M. V. Savin,
Project Manager
msavin@ussc.ru

Ural Security Systems Center

The article proofs the need of SOAR-Security Orchestration, Automation and Response, discusses topical issues related to the rational and effective use of information security systems, scaling of information security functions, information security incident management and processes. The authors reviewed the functional architecture of SOAR class systems and described the composition of the main subsystems that implement the functions of orchestration of information security tools and automation of the information security incidents response.

Keywords: SOAR, IRP, playbook, functional architecture, DSL, COPS, SOC

нала должной квалификации, но и в том, что рынок труда соответствующих специалистов «перегрет», а их квалификация зачастую далека от требуемых показателей. Особенно остро данная проблема проявляет себя в регионах, что делает фактически невозможным для крупных распределенных организаций полноценно решать вопросы, связанные с унифицированным и централизованным подходом к защите информации.

Вместе с тем, рост требований, угроз и источников информации о событиях ИБ приводит к неэффективному использованию высококвалифицированного персонала, смещая фокус его усилий на срочные операции, не требующие высокой квалификации, вместо важных системных задач по планированию, развитию и организации деятельности системы управления ИБ. Кроме того, из общих соображений, можно отметить, что выполнение ряда операций человеком неэффективно. Долговременный и непрерывный анализ типового потока структурированной информации и высокая оперативность действий, необходимые при решении задач защиты информации, особенно при анализе событий безопасности и реагировании на инциденты ИБ, очевидно, требуют автоматизации этого процесса.

Из вышесказанного вытекает и следующий блок проблем: полноценное внедрение систем управления ИБ требует централизации в рамках единой концепции, но отсутствие персонала и адекватных средств делают эту задачу нерешаемой. Во многих организациях нередко можно увидеть следующую картину: налицо большое количество уже внедренных средств защиты информации, которые, однако, невозможно полноценно использовать из-за низкой степени интеграции, а также сложности регулярного управления политиками безопасности. Применение современных средств организации информационной инфраструктуры, таких как SDN (*Software-Defined Networking* – программно-определяемая сеть) или виртуализированные сервисы, многократно усиливает негативный эффект данной проблемы. Зачастую использование человеческого ресурса просто нерационально при наличии сложной, многофункциональной инфраструктуры с множеством внутренних зависимостей и уровней управления.

Между тем, руководство, рассматривая проблему ИБ как бизнес-проблему, требует внедрения управляемой и измеряемой системы обеспечения ИБ, интегрированной в прочие бизнес-процессы организации. При отсутствии адекватного инструмента управления сложной инфраструктурой ИБ решение данной задачи нередко сводится к использованию только формальных методов управления. Это провоцирует создание феномена так называемой «бумажной безопасности»: с точки зрения менеджмента система управления ИБ есть, но де-факто она представляет собой набор оторванных от практики непроверяемых и непрозрачных алгоритмов и регламентов. Такой подход приводит не только к обесцениванию системы обеспечения ИБ как элемента интегрированной системы менеджмента организации, но и к росту финансовых затрат.

Нельзя не учитывать и тот факт, что современные информационные системы подвергаются постоянным радикальным изменениям. Такие технологии, как удаленный мобильный доступ, граничные или периферийные вычисления [2] (*edge computing*) и SDS (Software-Defined Storage – программно-определяемая система хранения) привносят не только новые требования к компетенциям обслуживающего персонала, но и серьезно увеличивают потребность в инструментах имплементации политик безопасности и контроля их исполнения.

Частично решая обозначенные проблемы, многие бизнес-структуры переходят к использованию организационно-технических элементов – SOC (*Security Operations Center* – центр обеспечения безопасности), консолидируя наиболее действенные силы и средства для последующего их использования там, где это будет необходимо. Однако для полного решения указанных задач таким центрам требуется дополнительное оснащение в виде решений класса SOAR [3].

Понятие SOAR

SOAR-системы (*Security Orchestration, Automation and Response*) представляют собой инструментарий, позволяющий автоматизировать процесс сведения данных об угрозах безопасности для последующего анализа. Они решают следующие задачи:

- интеллектуальный сбор в режиме реального времени ИБ-данных из нескольких источников с необходимым обогащением и агрегацией информации, поступающей с разнородных средств защиты информации;
- автоматизация типовых цепочек задач, связанных с инцидентами ИБ и выявлением отклонений от установленных политик и требований безопасности;
- применение политик безопасности в средствах защиты информации как в проактивном, так и в реактивном режимах;
- автоматизация всего перечня организационно-технических задач и процедур обеспечения ИБ в рамках реагирования на инцидент ИБ и выявление отклонений от установленных политик безопасности, в том числе информирования, назначения ответственных лиц и организация их совместной работы;
- ретроспективный анализ состояний, условий, предпринятых действий и результатов реагирования на инциденты ИБ для повышения эффективности практик, обучения и дальнейших расследований;
- формирование и оперативное представление состояния ИБ организации, его оценки с возможностью ретроспективного и предиктивного анализа.

Понятие SOAR возникло относительно недавно. Выделяют три группы функций SOAR: интеграция (integration), автоматизация (automation) и оркестровка[1] (orchestration).

[1] *В связи с неустоявшейся терминологией в ряде источников для этой же функции может использоваться термин «оркестрация».*

Интеграция – это унификация различных технологий, процессов, ресурсов и интерфейсов, позволяющая вести эффективную совместную работу средств защиты информации, направленную на обеспечение ИБ. *Автоматизация* минимизирует участие персонала в решении задач с сохранением, а зачастую и с повышением качества и согласованности. *Оркестровка* направлена на построение сценариев реагирования, имплементацию политик безопасности, выполнение необходимых задач при реагировании и расследовании инцидентов ИБ.

В исследовании [4] авторы дают следующее обобщенное понятие: «Оркестровка безопасности – это средство, решающее комплекс задач по планированию, интеграции, кооперации и координации активностей, функций средств защиты информации и экспертов, для реализации и автоматизации необходимых действий, направленных на реагирование на инцидент ИБ в рамках разнородных технологических парадигм».

Там же приводится сопоставление работы служб реагирования на инциденты ИБ без использования SOAR и с таковой (рис. 1). В первом случае эксперты должны заниматься всем множеством задач, связанных с расследованием инцидента ИБ и реагированием на него, включая настройку, имплементацию политик и анализ средств защиты информации, мониторинг в части расследования инцидента ИБ и использование механизмов реагирования с получением дополнительной информации из TI (*Threat Intelligence* – платформы и сервисы киберразведки), применение блокировок и временных политик. Отдельно рассматривается блок задач, связанных с планированием и, в общем случае, управлением ИБ, а также совершенствованием системы управления ИБ.

Во втором случае, SOAR позволяет экспертам сфокусироваться на решении задач управления, планирования и совершенствования системы управления ИБ, используя SOAR в качестве единого интерфейса доступа к функциям управления и необходимым данным.

Платформа SOAR и ее компоненты

В качестве типовой архитектуры SOAR авторы статьи предлагают следующую функциональную схему, сформированную в результате анализа имеющихся на рынке решений, представленных как отечественными, так и зарубежными производителями: Cortex XSOAR, Splunk Phantom, Siemplify, Swimlane, FortiSOAR, R-Vision IRP и ePlat4m (рис. 2).

Как следует из определения, основные функции SOAR реализуются в подсистеме оркестровки и ав-

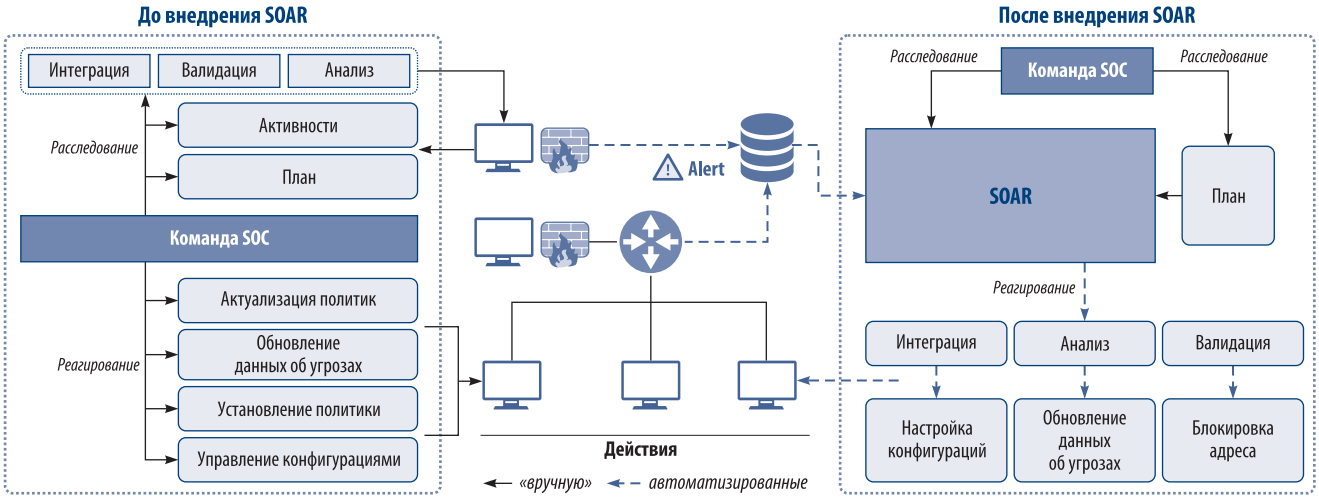

Рис. 1. ***Процессы организации до и после внедрения SOAR***

Рис. 2. ***Схема функциональной структуры SOAR***

томатизации, предназначенной для интеграции программно-технических средств ИБ, в том числе обогащения контекста события или инцидента ИБ, определения стартовой точки для вмешательства персонала и эксперта информационной безопасности, автоматизации процесса реагирования.

В свою очередь, эту подсистема состоит из двух модулей:

- модуля оркестровки, который обеспечивает централизованную обработку событий и инцидентов, информация о которых поступает от СрЗИ/SIEM, а также сбор информации об угрозах ИБ из различных внешних источников (этот модуль представлен набором коннекторов к различным системам защиты, а также механизмом управления этими коннекторами, в том числе управления полномочиями и необходимыми учетными данными);
- модуля автоматизации, который обеспечивает этап реагирования на событие или инцидент ИБ, используя механизм плейбуков.

Плейбук – это сценарий реагирования на инцидент, который позволяет задать для конкретного типа инцидента ИБ алгоритм действий по реагированию и в автоматическом режиме реализовать его при срабатывании определенного правила. Аналогичный инструмент может использоваться для проактивного и реактивного применения оперативных и долгосрочных политик безопасности, в том числе для реализации установленных требований и контроля отклонений от них.

Каждый плейбук может быть представлен в виде детерминированного конечного автомата – алгоритма, имеющего один вход, один выход и в каждый момент времени находящегося в одном состоянии. Модель конечного автомата может быть реализована как на определенном языке программирования (например, Python), так и с помощью предметно-ориентированного языка (*Domain-specific language*, DSL): например, COPS (*Collaborative Open Playbook Standard*), разработанного компанией Demisto [5]. В этом случае на предметно-ориентированном языке описывается логика сценария, а для получения данных или выполнения команд управления средствами защиты информации из сценария осуществляются вызовы скриптов, написанных на различных языках программирования (Python, PowerShell, Linux script, Node.js и др.). Таким образом, плейбук может состоять из полностью автоматических шагов выполнения, полностью ручных шагов выполнения или сочетания и тех и других.

В своем описании плейбук должен поддерживать определенный уровень абстракции, но с возможностью реализации конкретных действий и применения политик при выполнении.

Опишем следующий пример работы SOAR. Пусть заданное средство обнаружения компьютерных атак зафиксировало некоторую активность, потенциально свидетельствующую о возможности реализации инцидента ИБ (например, взаимодействие с C&C-сервером бот-сети), однако для локализации и подтверждения инцидента ИБ этого недостаточно. Полученная информация обрабатывается модулем оркестровки, и соответствующий плейбук SOAR инициирует временное повышение уровня оперативного журналирования на активном сетевом оборудовании и серверах, потенциально связанных с источниками инцидента ИБ, а также сверку актуальных конфигураций сетевых узлов с эталонными версиями. В случае выявления отклонений от ранее определенной политики безопасности модуль автоматизации инициирует меры, связанные с автоматическим активным противодействием инциденту ИБ, вовлекая в процесс дополнительные средства защиты информации, такие как межсетевые экраны, средства ограничения доступа и, безусловно, информируя персонал.

В отчете об инциденте, сгенерированном средствами SOAR, должна содержаться структурированная информация, достаточная для оперативного расследования и ликвидации последствий инцидента ИБ. В приведенном примере важно представить анализ конфигурационных уязвимостей, наличие которых привело к возможности реализации инцидента ИБ. Эта информация предназначена как для внесения корректировок в политики безопасности с целью исключения подобных инцидентов в дальнейшем, так и для обеспечения возможности автоматического контроля аналогичных проблем в других элементах информационной инфраструктуры.

Таким образом, благодаря описанным выше функциям и возможностям, концепция SOAR позволяет эффективно решить обозначенные во введении проблемы.

Нехватка квалифицированного персонала компенсируется фокусировкой сотрудников на задачах управления и планирования. Типовые и рутинные задачи по применению политик безопасности, реагированию на инциденты ИБ решаются в автоматическом или полуавтоматическом режимах. Работа может вестись в кооперативном режиме, с использованием единой, точно подобранной информации и подходов на основе предиктивного анализа.

Высокоэффективная эксплуатация средств защиты информации и управление функциями ИБ обеспечиваются автоматизацией функций защиты, настройки и применения политик. При этом достигается снижение количества ошибок конфигурирования, повышается оперативность реагирования на инциденты ИБ и качество этих операций.

Разрыв между потребностями руководства в части управления и потенциалом существующих на рынке средств защиты информации нивелируется за счет наличия плейбуков различного уровня с возможностью автоматической настройки и использования средств и функций защиты информации, интерфейсов единого централизованного управления, имплементации политик и прозрачного получения обратной связи в рамках процесса управления с учетом минимизации зависимости от знаний и умений конкретных специалистов. Внедрение SOAR способствует повышению эффективности управления ИБ, качества работы персонала, оптимизации затрат, необходимых для поддержания и развития инфраструктуры ИБ.

Использование групп функций автоматизации и оркестровки SOAR

позволяет масштабировать и унифицировать функции управления ИБ-инфраструктурой вне зависимости от ее масштаба, архитектуры и типа отдельных элементов.

Инструментарий SOAR не ограничивается традиционными средствами автоматизации и интерфейсами. Эффективное решение задач, стоящих перед SOAR, возможно при привлечении средств онтологического представления для унификации функций управления и представления политик безопасности. Например, политики межсетевого экранирования должны быть инвариантны к интерфейсам настройки и моделям управления конкретного производителя.

Заключение

SOAR можно рассматривать как средство защиты информации, направленное на решение проблем управления ИБ, связанных не непосредственно с защитой от угроз, а с повышением эффективности и качества данного процесса в условиях ограничений, обусловленных персоналом и технологиями.

Использование SOAR позволит устранить разрыв между бизнес-целями и применяемыми мерами ИБ, а также поспособствует обеспечению необходимого уровня защиты информации и эффективному достижению целей организации с использованием информационных технологий в целом.

В следующей статье мы приведем классификацию и дадим краткую характеристику имеющихся на рынке продуктов класса SOAR. Рассмотрим критерии принятия решений при выборе систем оркестровки и автоматического реагирования на события безопасности. Расскажем о направлениях развития SOAR-систем в сторону их большей интеллектуализации, в том числе использования методов машинного обучения и графов знаний в области кибербезопасности. ■

ЛИТЕРАТУРА

1. *Обзор отчета SANS по Security Operations Center [Электронный ресурс]. – Режим доступа: https://bis-expert.ru/blog/660/59079/ (дата обращения: 12.02.2021).*
2. *Облачные и граничные вычисления: в чем разница? [Электронный ресурс]. – Режим доступа: https://market.cnews.ru/articles/2019-12-24_oblachnye_i_granichnye_vychisleniya/ (дата обращения: 14.02.2021).*
3. *Zimmerman C. Ten Strategies of a World-Class Cyber Security Operations Center [Электронный ресурс]. – Режим доступа: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf (дата обращения: 12.02.2021).*
4. *C. Islam, M. Ali Babar, S. Nepal: A Multi-Vocal Review of Security Orchestration, 2019, [Электронный ресурс]. – Режим доступа: https://DOI:10.1145/3305268/ (дата обращения: 11.02.2021).*
5. *COPS – Collaborative Open Playbook Standard [Электронный ресурс]. – Режим доступа: https://github.com/demisto/COPS/ (дата обращения: 05.02.2021).*

НОВОСТИ

Российская инициатива позитивно воспринята в мире

Предложение России создать международную систему хранения ключей шифрования от мобильных приложений позитивно воспринято зарубежными партнерами.

Об этом сообщил в интервью РИА Новости замглавы МИД РФ Олег Сыромолотов. «Хотел бы обратить внимание на контртеррористическую инициативу ФСБ России по созданию универсальной системы доверенного хранения (депонирования) ключей шифрования от мобильных приложений для оперативного доступа правоохранительных органов к зашифрованной информации», – сказал он. – «Не буду углубляться в детали. Скажу только, что это предложение в целом воспринято позитивно зарубежными партнерами».

Спецслужбы должны иметь ключи к шифрованным приложениям в Интернете. Такую точку зрения выразил в свое время директор ФСБ России Александр Бортников. «Считаем, что серьезным технологическим препятствием для эффективного противодействия вторжению террористов в информационное пространство является отсутствие доступа спецслужб к шифрованной переписке террористов, использующих специальные приложения мобильной связи», – отметил глава ведомства, предложив создать «доверенную и прозрачную для контроля систему депонирования ключей шифрования, генерируемых мобильными приложениями». По его мнению, выработать единые правила обращения с ключами шифрования и доступа к ним можно только при тесном сотрудничестве спецслужб, операторов связи и телекоммуникационных компаний.

«Что касается вопроса о вредоносной активности, то, по данным Национального координационного центра по компьютерным инцидентам, большинство кибератак на Россию в 2020 году осуществлялось из адресного пространства США, Германии и Нидерландов», – продолжил беседу Олег Сыромолотов. Он отметил, что вредоносному вмешательству подвергались объекты финансового сектора, военно-промышленного комплекса и государственного управления. Кроме того, атаки были направлены на компании, связанные с наукой, образованием, разработкой вакцин и здравоохранения.

Далее Олег Сыромолотов обратил внимание на ситуацию с соцсетями. «Что касается социальных сетей, то мы неоднократно наблюдали примеры использования этих инструментов для целевого воздействия на отдельные социальные группы, прежде всего молодежь, дестабилизации обстановки в странах и регионах мира», – заключил дипломат.