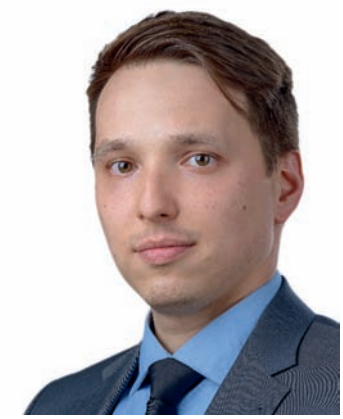
SOAR: автоматизация реагирования

Роман Ванерке, *технический директор АО "ДиалогНаука"*



Хакеры используют для проникновения в корпоративные сети автоматизированные инструменты, которые действуют быстро и точно. В то же время средства защиты могут в автоматическом режиме предотвратить только заранее известные атаки, однако ручная работа с инцидентами — это все равно что сражаться шашкой против танков. "Ручная" защита, даже если и успеет отреагировать, то уже на совершенную атаку. Пока оператор будет разбираться в том, что произошло, хакер может успеть закрепиться в системе и уничтожить следы своего проникновения. Для организации и автоматизации процесса расследования и реагирования используется инструментарий, получивший наименование SOAR (Security Orchestration, Automation and Response).

Активный щит

Само сокращение SOAR определяет набор функций технологии: оркестрация для интеграции со средствами защиты и другими ИТ-системами предприятия, автоматизация за счет заранее описанных шагов расследования (Playbook) выявленных инцидентов и реагирование на них с помощью оркестрации. Не стоит также забывать о системе управления и оценки эффективности работы SOC. Следует отметить, что SOAR является продолжением развития технологии SIEM. Однако последняя ограничена мониторинговыми функциями и подготовкой отчетов, оставляя реагирование на внешние решения. Фактически результатом деятельности SIEM является подробный отчет о инцидентах с возможными рекомендациями по реагированию. В то же время SOAR может не только предлагать рекомендации, но и автоматически реагировать на события. Таким образом, функциональные возможности SOAR следующие:

1. Оркестрация. В рамках расследования для сбора дополнительных данных и контекста аналитику необходимо взаимодействовать с разного рода средствами и системами как ИБ, так и ИТ. Подобный "ручной" труд, с одной стороны, сильно замедляет процесс расследования, с другой – достаточно однотипный и скучный. Эта однотипная работа является одной из причин высокой текучки аналитиков первой линии. Оркестрация позволяет интегрироваться со сторонними системами для сбора данных и управления, сокращая время на переключение между различными консолями и интерфейсами. Например, при обнаружении атаки, когда сработала виртуальная ловушка, запускаются дополнительные процессы проверки показателей компрометации, включаются системы более строгого сегментирования корпоративной сети или поиск вредоносных кодов.

2. Автоматизация. SOAR-решение позволяет описать и автоматизировать выполняемые в рамках расследования действия посредством заранее подготовленных планов реагирования (Playbook). Таким образом, система позволяет автоматизировать однотипные действия, которые ранее аналитики выполняли вручную, тем самым значительно сокращая время на расследование и сбор необходимых данных для принятия решений. Стоит также отметить, что не все операции можно автоматизировать полностью и система должна позволять останавливать процесс и ожидать дальнейших действий от оператора. Например, после автоматического сбора данных о заражении аналитик проводит анализ достаточности доказательств и принимает решение о блокировке учетной записи или переносе узла сети в изолированный сегмент. План реагирования должен позволять строить сложные конструкции с разными путями развития и ветвлениями (в зависимости от результата анализа).

3. Реагирование. За счет оркестрации SOAR-решение имеет возможность автоматического реагирования на выявленные инциденты. Естественно, что не всегда возможно в автоматическом режиме решить проблему, но это позволяет сделать перевод средств защиты в более "жесткие" режимы работы, выполнить сбор более подробной статистики и ограничить потенциально опасные операции. После заражений шифровальщиком WannaCry актуальной функциональностью стало оперативное реагирование на заражения, чтобы минимизировать распространение вредоносных кодов, – от скорости реакции на агрессивные заражения может сильно зависеть полученный ущерб. Когда автоматические сценарии с помощью показателей компрометации выявили зараженные устройства, средства реагирования отключают их от основной сети, чтобы блокировать дальнейшее распространение вредоносного кода.

Стоит отметить другие важные функции SOAR: оценку эффективности, управление

инцидентами ИБ, интеграцию с поставщиками Threat Intelligence. Так, например, SOAR-решение может стать единой точкой управления инцидентами ИБ в компании.

Следует отметить, что достаточно большая часть функционала SOAR относится к классу SIEM. Поэтому решения SOAR либо включают в себя модуль SIEM как элемент первичного сбора и обработки сведений об инцидентах, либо интегрируются с внешними SIEM для получения сигналов тревоги, векторов атаки, признаков компрометации и других характеристик вредоносной деятельности.

Решения

В качестве примера продуктов, относящихся к классу SOAR, можно привести разработки компании RSA NetWitness Orchestrator, IBM Resilient и R-Vision. Так, компания RSA выпускает несколько продуктов, которые в целом и составляют SOAR-систему. В частности, компания предлагает платформу Security Orchestration, которая обеспечивает оркестрацию и автоматизацию процессов управления средствами защиты, платформу Incident Management, с помощью которой можно реагировать на инциденты и восстанавливать штатную работу систем после атак, и платформу Interactive Investigation, которая обеспечивает интеллектуальную обработку событий для мониторинга систем информационной безопасности. Все платформы интегрируются между собой и в целом составляют SOAR с максимально функциональной реализацией всех функций.

Компания IBM, купившая одного из первых производителей SOAR-решений Resilient, предлагает платформу Resilient Incident Response Platform, которая обеспечивает выполнение всех задач SOAR, от оркестрации до реагирования на инциденты. Это единая SOAR-платформа, интегрированная с другими защитными продуктами IBM и одной из популярных SIEM IBM QRadar. Таким образом, для IBM платформа Resilient является хорошим дополнением к другим продуктам, с помощью которых можно построить полноценную SOAR-систему. В этом случае возможно использовать связку качественной SIEM QRadar и автоматизации обработки инцидентов на Resilient Incident Response Platform.

Российская компания R-Vision предлагает продукт R-Vision Incident Response Platform (IRP), это программная платформа для оперативной организации и автоматизации деятельности по мониторингу, регистрации и реагированию на инциденты информационной безопасности. Система позволяет создать единую точку консолидации информации обо всех инцидентах информационной безопасности (корпоративный SOC), а также платформу для совместной работы группы реагирования на инциденты ИБ с возможностью сбора, анализа и хранения сведений, относящихся к инцидентам ИБ. R-Vision IRP обеспечивает координацию деятельности сотрудников компании, распределение задач и учет выполненных мероприятий по реагированию на инциденты ИБ. Однако это, скорее, координатор для ручной обработки инцидентов, который со временем может развиться в полноценную SOAR.

Заключение

Рынок SOAR достаточно молодой: аналитики сформировали потребность в подобного класса продуктах только в последние два года. Игроков на нем пока немного, хотя уже появляются и российские решения. Тем не менее уже сейчас очевидно, что для эффективного реагирования на инциденты информационной безопасности будут требоваться инструменты для автоматизации этих процессов. В этой связи востребованность SOAR-решений в долгосрочной перспективе будет только расти.

NM
АДРЕСА И ТЕЛЕФОНЫ АО "ДИАЛОГНАУКА" см. стр. 56