Автоматизация реагирования на инциденты информационной безопасности: плюсы, особенности, решения

Екатерина Черун, *коммерческий директор Security Vision*
Виктор Сердюк, *генеральный директор АО "ДиалогНаука"*

Количество инцидентов информационной безопасности, особенно в крупных организациях, велико и с каждым годом продолжает расти. При реагировании на них счет идет буквально на минуты, а позволить себе нанять большое количество высококлассных ИБ-специалистов могут далеко не все. Поэтому вопрос о том, как помочь аналитикам ИБ при реагировании на инциденты и снять с них рутинную нагрузку по выполнению однотипных операций, стоит достаточно остро.

IRP – платформа реагирования на инциденты кибербезопасности, используемая для систематизации данных об инцидентах ИБ, а также автоматизации действий оператора, специалиста ИБ, выполняемых при реагировании на инциденты кибербезопасности.

IRP-системы

Системы IRP (Incident Response Platform) помогают выполнить ряд рутинных операций по сбору дополнительной информации, осуществить неотложные действия по сдерживанию и устранению угрозы, восстановить атакованную систему, оповестить заинтересованных лиц, а также собрать и структурировать данные о расследованных инцидентах информационной безопасности.

Системы IRP реализуют меры противодействия угрозам ИБ в соответствии с заранее заданными сценариями реагирования (так называемые playbooks или runbooks). Такие сценарии представляют собой набор автоматизированных задач по детектированию угроз и аномалий в защищаемой инфраструктуре, а также реагированию на угрозы в режиме реального времени. Сценарии реагирования действуют на основании настраиваемых правил и типов инцидентов, выполняя те или иные действия в зависимости от данных, поступающих со средств защиты или от информационных систем. По окончании реагирования на инцидент IRP-платформа поможет создать отчет об инциденте и предпринятых действиях по его устранению.

Security Orchestration, Automation and Response (SOAR)

Можно подумать, что работа аналитиков по кибербезопасности уже в достаточной мере автоматизирована, а применение разнообразных средств защиты (IRP/SGRC/SIEM) позволяет значительно упростить работу сотрудникам SOC-центров. Но зачастую для обеспечения кибербезопасности используются настолько разные системы и средства защиты, а при обработке киберинцидентов нужно решать столько разнородных задач, что реагирование на инциденты ИБ требует еще большей степени автоматизации процессов. Причем речь даже не столько про непосредственно активное противодействие угрозам (с этим справляются IRP-решения), сколько про интеграцию систем обработки данных кибербезопасности, обогащение полученных данных, коммуникации по инцидентам, применение методов машинного обучения и анализа больших данных (Big Data).

При необходимости автоматизировать большое количество смежных процессов реагирования на инциденты применяются системы класса SOAR (Security Orchestration, Automation and Response), платформы оркестрации, автоматизации и реагирования на инциденты ИБ. Данные продукты являются эволюцией платформ реагирования на киберинциденты и предоставляют расширенные функции автоматизации процессов обработки инцидентов информационной безопасности. Платформы SOAR сочетают в себе следующий функционал:

- оркестрация – объединение и централизованное управление ИТ-/ИБ-системами, использующимися при обработке инцидентов ИБ;
- автоматизация – подразумевает алгоритмизацию процессов обработки инцидентов ИБ путем реализации бизнес-логики регламентов реагирования на инциденты в плейбуках;
- реагирование – обеспечивает сбор информации об угрозе и активное противодействие (локализацию и устранение), а также совместную работу аналитиков над инцидентами ИБ в виде удобной платформы коммуникации и обмена информацией.

Дополнительно в решения класса SOAR могут быть включены модули управления данными киберразведки (Threat Intelligence), управления конфигурациями (Configuration Management), обновлениями (Patch Management) и уязвимостями (Vulnerability Management) программного обеспечения, модули аналитики и визуализации информации (дашборды, отчеты, метрики), а также функции машинного обучения и анализа Big Data.

Основные возможности систем SOAR:

- выполнение действий по реагированию благодаря централизованному управлению (оркестрации) ИТ-/ИБ-системами (ОС, ПО, СЗИ);
- наличие механизмов визуализации, отчетности, аналитики, логирования выполненных действий по реагированию, ведения базы знаний;
- кейс-менеджмент для совместной работы группы аналитиков над инцидентами;
- возможности по обработке данных киберразведки благодаря интеграции с поставщиками данных киберразведки (индикаторов компрометации, TI-фидов и др.);
- возможности по обработке Big Data, механизмы машинного обучения для автоматизации действий и помощи в принятии решений при реагировании на инциденты ИБ.

Платформа для индивидуальной автоматизации действий по управлению процессами кибербезопасности – Security Vision IRP/SOAR

На сегодняшний день одним из наиболее эффективных продуктов класса IRP/SOAR является система Security Vision IRP/SOAR – российский программный продукт для автоматизации и роботизации действий по реагированию на инциденты кибербезопасности. Security Vision IRP/SOAR позволяет автоматизировать широкий спектр процессов и охватывает полный цикл работы с инцидентами, включая:

- подготовку к отражению инцидента;
- обнаружение и анализ инцидента;
- сдерживание;
- устранение и восстановление после инцидента;
- выполнение действий после реагирования (Post-Incident Activity) с анализом "выученного урока";
- корректировку планов реагирования и настройку СЗИ.

Обнаружение и реагирование

Остановимся подробнее на двух базовых составляющих управления инцидентами, обнаружении и реагировании – активном действии, направленном на локализацию, сдерживание, устранение угрозы и на возврат информационной системы в состояние "до начала атаки". В рамках обнаружения инцидентов с помощью Security Vision IRP/SOAR автоматизируются следующие процессы:

- поиск и сбор дополнительной информации о затронутом инцидентом активе;
- поиск индикаторов компрометации (IoC – Indicator of Compromise) и данных о тактиках, техниках, процедурах (TTPs – Tactics, Techniques, Procedures) атакующих в платформах киберразведки (TIP – Threat intelligence Platform);
- первичная классификация и анализ инцидентов, а также отсеивание явных ложноположительных срабатываний.

В рамках реагирования на инциденты с помощью Security Vision IRP/SOAR могут быть автоматизированы следующие действия:

- блокировка IP-адреса атакующего на сетевом оборудовании;
- изоляция атакованного хоста от сети;
- завершение подозрительных процессов и остановка служб;
- удаление непрочитанных фишинговых сообщений с почтового сервера;
- восстановление работоспособности СЗИ на атакованных конечных точках.

Результаты применения Security Vision IRP/SOAR

Внедрение системы Security Vision IRP/SOAR позволяет достичь следующих результатов:

- роботизации выполнения дежурных процедур оператора в режиме реального времени и автоматизированной обратной реакции на инциденты. После громких эпидемий вирусов и троянцев-шифровальщиков стало очевидно, что реагирование – это не оповещение, а автоматическое выполнение действий оператора;
- снижения риска человеческого фактора, а именно ошибок сотрудников, привлекаемых для реагирования на инциденты (две трети инцидентов ИБ связаны с человеческим фактором);
- автоматического насыщения и обогащения информацией о событиях со смежных ИТ- и ИБ-систем – двусторонний обмен между ИТ- и ИБ-системами обеспечивает необходимые и достаточные условия отсутствия белых пятен;
- повышения скорости реагирования на инциденты. Как показывает опыт внедрения Security Vision IRP/SOAR, если до использования продукта специалисту нужно было не менее двух часов для проверки 1–2 сложных инцидентов, то сейчас система осуществляет более 200 проверок за несколько секунд;
- систематизации интеграций со средствами защиты и ИТ-системами, такими как: средства обеспечения безопасности электронной почты, средства антивирусной защиты, Service Desk, Active Directory, DNS, CMDB, средства контроля изменений межсетевых экранов, средства контроля целостности данных, межсетевые экраны, средства защиты от фишинговых атак, системы предотвращения вторжений (IPS), "песочницы", системы хранения журналов событий, средства хранения архивов корпоративной электронной почты, FinCert, Gov-CERT, VirusTotal, UrlScan.io, MXTool.box и др.;
- повышения удобства и наглядности реагирования на инциденты ИБ – учет активов в собственной базе CMDB-системы, построение картинки активных инцидентов, построение графических схем инцидентов (взаимосвязь объектов в рамках расследования), интеграция более чем с одной SIEM-системой, зонтичная технология, построение отчетов и дашбордов для разных ролей, оповещение о критичных инцидентах по e-mail, СМС, IM.

Итак, с организационной точки зрения Security Vision IRP/SOAR позволяет существенно упростить решение профильных задач ИБ-аналитикам, снять с них рутинную нагрузку и, как следствие, высвободить их ценное время для решения более важных задач, а значит, уменьшить вероятность профессионального выгорания и текучки кадров.

С точки зрения бизнеса Security Vision IRP/SOAR демонстрирует высокий коэффициент возврата инвестиций ROI (Return On Investment) путем подсчета сэкономленных за счет автоматизации человеко-часов аналитиков, а также сокращения времени обнаружения и реагирования на инциденты, уменьшения расчетного ущерба от реализации киберугрозы, отсутствия штрафных санкций со стороны регуляторов и выполнения временных нормативов реагирования на киберинциденты. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Security Vision IRP/SOAR позволяет не только гибко выстроить обработку инцидентов ИБ, но и интегрироваться с внешними ИТ-системами для автоматизации действий по реагированию.

Security Vision IRP/SOAR позволяет автоматизировать широкий спектр процессов и охватывает полный цикл работы с инцидентами.

Security Vision IRP/SOAR позволяет существенно упростить решение профильных задач ИБ-аналитикам, снять с них рутинную нагрузку и, как следствие, высвободить их ценное время для решения более важных задач.

С технической точки зрения польза от внедрения Security Vision IRP/SOAR заключается в сокращении времени обнаружения инцидентов и реагирования на них, результатом чего является существенное уменьшение прогнозируемого ущерба от кибератак.