R-Vision

Автоматизация реагирования на инциденты ИБ: опыт внедрения R-Vision SOAR в «СберАналитике» компанией УЦСБ

История успеха

Отрасль

Информационные технологии

Проект в цифрах

на 90%
повышение скорости реакции

1 минута
время реагирования на часто повторяющиеся типы инцидентов

на 30%
уменьшение среднего времени на обработку инцидентов

Задачи

Перед командой кибербезопасности компании «СберАналитика» стояла задача повысить эффективность процессов по реагированию на инциденты, где наблюдались следующие проблемы:

- Аналитики вынуждены отслеживать оповещения в нескольких системах защиты;
- Обработка алертов вручную приводила к затратам времени на рутинные операции;
- Из-за отсутствия информации об активах приходилось тратить дополнительное время на локализацию инцидента;
- Переключение между консолями СЗИ увеличивало время реагирования.

Чтобы преодолеть эти препятствия, в компании было принято решение автоматизировать процессы по реагированию на инциденты и внедрить систему класса SOAR. Такая система обеспечит команде кибербезопасности единое окно по обработке инцидентов, а также облегчит взаимодействие с внутренней командой ИТ и Центром мониторинга событий кибербезопасности (SOC). СберАналитика выбрала R-Vision SOAR и компанию УЦСБ для внедрения решения.

Ход проекта

Перед командой направления автоматизации ИБ УЦСБ стояла задача — развернуть платформу R-Vision SOAR и настроить её так, чтобы существующие в «СберАналитике» процессы реагирования на инциденты ИБ и координация действий пользователей при отработке мероприятий по выявлению, анализу и реагированию на инцидент реализовывались с помощью данной системы.

Для этого была запланирована интеграция платформы R-Vision SOAR с действующим в компании Центром мониторинга событий кибербезопасности (SOC) и другими смежными системами, участвующими в управлении инцидентами ИБ и восстановлении объектов защиты.

История успеха

Карточка проекта

Заказчик

Компания-разработчик аналитических решений на основе Big Data. На рынке данных с 2018 года, входит в экосистему Сбера

Задачи

Повысить эффективность процессов по реагированию на инциденты: объединить оповещения из разных систем защиты, сократить ручную обработку алертов, обеспечить доступ к информации об активах и минимизировать переключение между консолями СЗИ

Решение

Внедрение компанией УЦСБ решения R-Vision SOAR, системы оркестрации, автоматизации ИБ и реагирования на инциденты

Результат

Внедрение R-Vision SOAR в «СберАналитике» повысило эффективность и скорость реагирования на инциденты, снизило нагрузку на специалистов ИБ и обеспечило централизованный контроль над угрозами за счёт автоматизации и оркестрации процессов

Ключевые этапы проекта

Анализ текущей инфраструктуры. Инженеры УЦСБ изучили работу SOC, DLP-систем и ручных процессов реагирования, чтобы определить зоны для автоматизации и спланировать интеграцию с R-Vision SOAR.

Разработка проектной документации. Команда разработала проектную и эксплуатационную документацию по ГОСТ, учитывая архитектуру системы и требования заказчика, чтобы обеспечить соответствие ожиданиям ещё до внедрения.

Внедрение R-Vision SOAR. Специалисты УЦСБ развернули R-Vision SOAR, выполнили инвентаризацию активов компании, настроили интеграции, автоматизировали обработку инцидентов и разработали кастомный коннектор для полного цикла управления инцидентами через SOC.

Результат

Повышение эффективности защиты от киберугроз. Благодаря инвентаризации активов и оркестрации средств защиты информации специалисты ИБ «СберАналитики» получили единое окно для обзора ИТ-инфраструктуры. Автоматизированная приоритизация и обработка инцидентов позволяют предотвращать серьёзные потери, быстро и точно действовать по заданному сценарию, снижая риск ошибок и повышая надёжность системы.

Ускорение реагирования. Время реакции на типовые инциденты сократилось на 90% — с 10 до 1 минуты благодаря автоматическим уведомлениям и предварительному обогащению карточек инцидентов. Рост скорости реакции минимизировал потенциальный ущерб от атак и дал дополнительное время на принятие решений по устранению последствий.

Снижение нагрузки на ИБ-специалистов. Благодаря автоматизации удалось выстроить слаженное взаимодействие между отделами ОТ, ИТ и внешним SOC. Трудозатраты на рутинные операции снизились: в среднем время обработки инцидентов сократилось на 30%.

R-Vision

История Успеха

R-Vision - разработчик систем цифровизации и кибербезопасности.

С 2011 года компания создаёт технологии, которые помогают организациям эффективно противостоять киберугрозам, поддерживать надёжность ИТ-инфраструктуры и обеспечивать цифровую трансформацию.

Технологии R-Vision используются в крупнейших банках,государственных организациях, нефтегазовой отрасли, энергетике, металлургии, промышленности и компаниях других отраслей.

sales@rvision.ru
+7 (499) 755 55 70

t.me/rvision_pro
vk.ru/rvision_ru

О проекте из первых уст

С компанией УЦСБ работаем не впервые. Коллеги зарекомендовали себя как надёжный и профессиональный интегратор, качественно выполняющий проекты. Все вопросы, возникающие в ходе реализации проекта и внедрения R-Vision SOAR, решались в рабочем порядке.

Цели достигнуты: в компании повысилась эффективность мер защиты, значительно упростились процессы управления инцидентами ИБ, а также налажен более качественный обмен данными между системами и сотрудниками отдела ИБ.

СБЕР АНАЛИТИКА

Марат Шамсутдинов,
CISO «СберАналитика»

Важно подчеркнуть, что чёткое понимание бизнес-процессов и задач со стороны «СберАналитики» значительно ускорило процесс интеграции и автоматизации действий персонала, позволив качественно внедрить технические решения в запланированные сроки. Наша команда представила варианты реализации требований Заказчика с учетом специфики рассматриваемых систем и поставляемого ПО. Благодаря слаженной совместной работе нам удалось создать эффективную автоматизированную систему реагирования на инциденты ИБ.

УЦСБ

Анастасия Федоренко,
руководитель направления автоматизации ИБ, УЦСБ