R-Vision

R-Vision SOAR – один из ключевых элементов сервиса Jet CSIRT

История успеха

Заказчик

ИТ-компания
«Инфосистемы Джет»

Отрасль

MSSP

Проект в цифрах

9 месяцев
срок внедрения решения

25 минут
время реакции
на высококритичный инцидент

140
плейбуков автоматизируют
воркфлоу

в 3 раза
увеличилась скорость
реакции на инцидент

Задачи

Перед центром мониторинга и реагирования на инциденты ИБ Jet CSIRT компании «Инфосистемы Джет» стояла задача по выбору решения класса SOAR для автоматизации внутренних процессов по обработке инцидентов.

При отборе и сравнении решений учитывалось множество критериев, определяющими были следующие:

- Наличие набора функций для реализации сервисной модели, позволяющий выстроить процессы реагирования на инциденты как единый конвейер
- Качество и стабильная работа решения
- Минимизация собственных ресурсов на поддержку решения
- Зрелая команда разработки, оперативная техподдержка, возможность тесного сотрудничества в процессе адаптации решения под задачи Jet CSIRT и возможных доработок

Команда Jet CSIRT отобрала 6 решений класса SOAR для первичного сравнения, 4 из них были протестированы в ходе пилотных проектов. По результатам сравнительного анализа и тестирования выбор был сделан в пользу платформы R-Vision SOAR.

Ход проекта

Первое время команда Jet CSIRT осуществляла планирование и проектирование своих внутренних процессов, формирование логики обработки инцидентов и сценариев реагирования в соответствии с принятыми регламентами центра. Параллельно осуществлялось тестирование и настройка SOAR-системы, апробирование в ней этих процессов.

Основная техническая реализация, в ходе которой была проведена определенная доработка возможностей продукта под задачи MSSP, настроены необходимые отчёты и метрики, интеграции с другими решениями, заняла три месяца. В этот период команды R-Vision и Jet CSIRT находились в очень тесном взаимодействии, что позволило в сжатые сроки решить все технические вопросы.

В итоге Jet CSIRT автоматизировал и поставил на конвейер с по-

Карточка проекта

Заказчик

ИТ-компания
«Инфосистемы Джет»

Задачи

Автоматизация внутренних процессов по обработке инцидентов заказчиков

Выстраивание экспертных сервисов по управлению инцидентами и реагированию

Решение

Система оркестрации, автоматизации и реагирования на инциденты ИБ R-Vision SOAR

Результаты

Удобный инструмент для обработки инцидентов из любых SIEM заказчиков с единой системой отчётности

Повышение скорости обработки инцидентов в 3 раза

Повышение эффективности 1-й линии в 4 раза

Контроль SLA, полнота статистики

мощью платформы R-Vision SOAR процесс по обработке и реагированию на инциденты заказчиков. Весь цикл по внедрению решения с учетом перестройки внутренних процессов занял около 9 месяцев.

Результат

В результате проекта команда Jet CSIRT реализовала эффективно выстроенный процесс потоковой обработки инцидентов, учитывающий индивидуальную процессную модель и экспертизу «Инфосистемы Джет» по детектированию, мониторингу и реагированию. Благодаря автоматизации внутренних процессов на базе платформы R-Vision SOAR процесс обработки инцидентов существенно ускорился — по оценке Jet CSIRT, скорость увеличилась в 3 раза.

Эффективность работы 1-й линии повысилась в 4 раза за счет применения автоматизированного подхода к сбору данных, приоритизации и маршрутизации инцидентов: на 1-й линии мониторинга осуществляется экспресс-оценка критичности и сложности инцидента, базовая аналитика, сбор данных и обогащение, и далее инцидент передается на следующий этап обработки.

Обработка инцидентов из разных SIEM от разных заказчиков осуществляется в одном интерфейсе с единой системой отчётности. R-Vision SOAR контролирует SLA на каждом этапе, позволяя Jet CSIRT четко соблюдать строгие обязательства перед заказчиками: для высококритичных инцидентов время реакции на инцидент составляет 25 минут, 45 минут предусмотрено на базовый анализ и информирование заказчика, 60 минут — на техническое реагирование.

Использование R-Vision SOAR также позволяет Jet CSIRT предоставлять заказчикам набор дополнительных экспертных сервисов по мониторингу и реагированию на инциденты ИБ. В отдельный сервис была выделена услуга по управлению киберинцидентами по модели MSSP, то есть у заказчика появилась возможность использовать технологии R-Vision по подписке.

R-Vision

История успеха

Карточка проекта

Заказчик

ИТ-компания
«Инфосистемы Джет»

Задачи

Автоматизация внутренних процессов по обработке инцидентов заказчиков

Выстраивание экспертных сервисов по управлению инцидентами и реагированию

Решение

Система оркестрации, автоматизации и реагирования на инциденты ИБ R-Vision SOAR

Результаты

Удобный инструмент для обработки инцидентов из любых SIEM заказчиков с единой системой отчётности

Повышение скорости обработки инцидентов в 3 раза

Повышение эффективности 1-й линии в 4 раза

Контроль SLA, полнота статистики

О проекте из первых уст

Платформа R-Vision SOAR — это один из ключевых элементов всего сервиса Jet CSIRT.

Она преобразовывает инциденты в единый формат и обогащает их дополнительными сведениями на этапе обработки. В итоге мы получили конвейер, на котором обрабатываем в одном интерфейсе инциденты из разных SIEM от разных заказчиков.

Мы искали качественное и стабильное решение, уделяли большое внимание зрелости команды разработчиков, и R-Vision SOAR удовлетворила наши ключевые требования.

Представитель компании
«Инфосистемы Джет»

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