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

«Инфосистемы Джет» — одна из крупнейших ИТ-компаний в России. С 1991 года работает на рынке системной интеграции, реализуя сложные проекты в масштабах всей страны. Штат — более 1800 сотрудников.

Центр мониторинга и реагирования на инциденты ИБ Jet CSIRT предоставляет услуги традиционного коммерческого SOC (Security Operation Center) по мониторингу и детектированию инцидентов ИБ, а также экспертные сервисы реагирования на инциденты ИБ, эксплуатации средств защиты информации, тестирования на проникновение и другие.

Каждый коммерческий SOC и MSSP-провайдер выстраивает свои внутренние процессы таким образом, чтобы обеспечивать необходимый уровень качества обработки инцидентов заказчиков, предусмотреть возможности по масштабированию, предлагать новые востребованные сервисы, оптимизируя при этом собственные затраты на технические средства и ресурсы своих специалистов. Один из ключевых моментов – это выбор платформы, с помощью которой будет автоматизирован весь процесс по обработке инцидентов заказчиков.

Почему R-Vision IRP?

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, позволяющих поставить процессы Incident Response на 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

Карточка проекта

Заказчик

Инфосистемы Джет

Задачи

Автоматизация внутренних процессов по обработке инцидентов заказчиков

Выстраивание экспертных сервисов по управлению инцидентами и реагированию

Решение

Платформа реагирования на инциденты R-Vision IRP

Результаты

Единый удобный инструмент для обработки инцидентов из любых SIEM заказчика с единой системой отчетности

Повышение скорости обработки инцидентов в 3 раза

Повышение эффективности 1-й линии в 4 раза

Контроль SLA, полнота статистики

Команда Jet CSIRT отобрала 6 решений класса IRP/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 IRP.

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 IRP-системы, апробирование в ней этих процессов.

Основная техническая реализация, в ходе которой была проведена определенная доработка возможностей продукта под задачи MSSP, настроены необходимые отчеты 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 помощью платформы R-Vision IRP процесс по обработке и реагированию на инциденты заказчиков. Весь цикл по внедрению решения с учетом перестройки внутренних процессов Jet CSIRT занял около 9 месяцев.

Внутренняя кухня

В Jet CSIRT мониторинг инцидентов осуществляют 3 линии аналитиков в режиме 24/7. Отдельно выделены группа реагирования и группа эксплуатации, а также эксперты по форензике, threat hunting и другие более узкие специалисты. Вся команда Jet CSIRT работает в рамках единого комплексного воркфлоу, который регламентирует процесс обработки инцидента и подключение специалистов на каждом этапе.

Алексей МАЛЬНЕВ,
руководитель Центра мониторинга и реагирования на инциденты ИБ Jet CSIRT компании «Инфосистемы Джет»:

Платформа R-Vision IRP — 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 IRP удовлетворила нашим ключевым требованиям.

Этот воркфлоу автоматизирован с помощью платформы R-Vision IRP и преобразуется в 140 сценариев реагирования (или по-другому плейбуков). Каждый плейбук построен под определенный сценарий выявления угроз, которых в Jet CSIRT применяется более 100. При выявлении нового инцидента средствами мониторинга в R-Vision IRP включается предусмотренный сценарий реагирования, в котором четко прописан алгоритм действий на каждом этапе обработки. Операции по сбору первичных данных и обогащению инцидента, уведомлению и ряд технических мер реагирования осуществляются автоматически с помощью имеющихся в R-Vision IRP инструментов и интеграций с используемыми в Jet CSIRT средствами защиты информации, сервисами и решениями, позволяя экономить время специалистов на выполнении ручных операций.

В Jet CSIRT используется 2 модели подключения заказчиков. Первый вариант предполагает подключение заказчика к облачным средствам защиты и SIEM, предоставляемым «Инфосистемы Джет» по подписке. Модель on-premise предполагает осуществление мониторинга и реагирования на инциденты на базе SIEM и средств защиты, развернутых в инфраструктуре заказчика, а это может быть совершенно разный набор продуктов. R-Vision IRP интегрирована со всеми типами SIEM, с которыми работает Jet CSIRT, и выступает своего рода интеграционной платформой, обеспечивая обработку всех инцидентов заказчиков по обеим схемам взаимодействия.

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

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 IRP 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 IRP контролирует SLA на каждом этапе, позволяя Jet CSIRT четко соблюдать строгие обязательства перед заказчиками: для высоко-критичных инцидентов время реакции на инцидент составляет 25 минут, 45 минут предусмотрено на базовый анализ и информирование заказчика, 60 минут – на техническое реагирование.

Использование IRP\SOAR от R-Vision также позволяет Jet CSIRT оказывать заказчиками набор дополнительных экспертных сервисов по мониторингу и реагированию на инциденты ИБ. В отдельный сервис была выделена услуга по управлению киберинцидентами по модели MSSP, т.е. у заказчика появилась возможность использовать технологии R-Vision по подписке.