# Компания «Полюс» повысила эффективность процессов управления ИБ с помощью технологий российского разработчика R-Vision


ПОЛЮС

**«Полюс»** — крупнейший производитель золота в России и одна из 5 ведущих глобальных золотодобывающих компаний, себестоимость производства на предприятиях которой является одной из самых низких в мире.

## Задачи

Основной задачей, которая стояла перед компанией «Полюс», было повышение эффективности процесса управления инцидентами ИБ в масштабах всей организации за счет автоматизации действующих регламентов и процессов обработки инцидентов.

Вместе с этим также был ряд сопутствующих задач такие как сокращение времени реагирования на инциденты, снижение количества рутинных операций и оптимизация трудозатрат Департамента ИБ. Сотрудникам подразделения требовался удобный инструмент для формирования целостной картины по выявленным и устраненным инцидентам, а также автоматического предоставления детализированной отчетности и визуализации статистический данных.

В результате для решения всего пула задач был выбран продукта R-Vision SOAR, который полностью отвечал всем потребностям организации.

## Ход проекта

Проект затронул всю инфраструктуру организации, а это более 20 000 единиц различных активов.

На первом этапе было проведено предпроектное обследование с дельным сбором информации обо всех объектах автоматизации, по результатам которого была определена полная картина по текущему состоянию, описаны все существующие процессы реагирования на инциденты ИБ в организации, а также сформирована целевая картина.

На следующем этапе были произведены работы по установке, настройке и подключению R-Vision SOAR к системам

## Карточка проекта

### Заказчик

Золотодобывающая компания «Полюс»

### Задачи

Автоматизация и повышения эффективности процесса управления инцидентами ИБ

Сокращение времени реагирования на инциденты и оптимизация трудозатрат сотрудников

### Решение

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

### Результаты

Сокращение времени реагирования на инциденты ИБ в 2 раза

Высвобождение ресурсов сотрудников за счет автоматизации процессов

Повышение эффективности и прозрачности ИБ-процессов

Предоставлен единый инструмент для совместной работы по инцидентам для территориально распределенной команды

Заказчика: осуществлена интеграция с почтовым сервером, контроллером домена, системой сбора и корреляции инцидентов ИБ и другими источниками данных. Кроме того, для обогащения инцидентов ИБ дополнительным контекстом произведен ряд интеграций R-Vision SOAR был со службами анализа подозрительных файлов и веб-ссылок на наличие вредоносного ПО VirusTotal, контроля и анализа доменных имен WhoIS, а также с системой управления IP-адресами заказчика. В результате интеграций продукта со всеми этими системами удалось организовать единый унифицированный процесс, который контролируется из интерфейса одного решения – R-Vision SOAR.

Далее, на базе уже существующих регламентов и процессов управления инцидентами ИБ, были разработаны и внедрены 26 уникальных сценариев реагирования (плейбуков), отвечающих всем потребностям «Полюс» и соответствующих лучшим мировым практикам. Также были сформированы четкие SLA для процессов реагирования и расследования инцидентов.

Заключительным этапом реализации проекта стало проведение комплексного обучения 16-специалистов Заказчика работе с R-Vision SOAR. Программа обучения состояла из 1-го теоретического и 6-ти практических блоков, раскрывающих весь функционал и возможности внедренного продукта, а также предоставляющих исчерпывающие знание пользователя о том, как работать с продуктом с учетом специфики Заказчика и реализованных бизнес-процессов.

## Проект в цифрах

**20 000+**
активов оборудования обрабатывается

**в 2 раза**
сокращено время реагирования на инциденты

**26**
уникальных плейбуков разработаны и внедрены

**16**
специалистов заказчика обучены работе с продуктом

**Андрей Тихонин,**
начальник управления информационной безопасности «Полюс»

Текущие реалии доказывают необходимость автоматизации процессов информационной безопасности и важность выбора российских решений. Внедренный нами продукт R-Vision SOAR уже неоднократно продемонстрировал свою эффективность в систематизации ИБ-процессов и повышении их эффективности».

## Результат

Гибкость внедряемого продукта R-Vision SOAR позволила, не нарушая существующий процесс управления инцидентами ИБ, перенести его в инструмент автоматизации и реализовать 26 уникальных плейбуков.

В результате чего компания «Полюс» в 2 раза сократила время реагирования на инциденты ИБ, а также высвободила ресурсы сотрудников департамента ИБ за счет автоматизации рутинных процессов и задач. Кроме того, для сотрудников департамента ИБ, находящихся в 5 регионах РФ, было предоставлено единое пространство для совместной работы и удобный инструмент для автоматического представления статистики, аналитики и управленческой отчетности.

Все это повысило общий уровень кибербезопасности «Полюс», а также обеспечило прозрачность работы департамента ИБ.

## Планы по развитию проекта

Все новые регламенты и процессы в департаменте ИБ «Полюс» теперь разрабатываются с учетом использования R-Vision SOAR. К платформе подключаются все больше источников данных и средств защиты, число которых в дальнейшем будет только возрастать.