R-Vision SOAR

Система оркестрации, автоматизации
и реагирования на инциденты ИБ

R-Vision Security Orchestration, Automation, Response

R-Vision SOAR (Security Orchestration, Automation and Response) – ключевой инструмент для повышения эффективности SOC. Система агрегирует данные по инцидентам из множества источников, автоматизирует обогащение, реагирование и внедрение ответных мер, обеспечивает единое пространство для совместной работы команды SOC.

Сценарии использования

Автоматизация деятельности SOC: повышение эффективности процессов SOC и разгрузка аналитиков за счёт автоматизации операций

Построение процесса обработки с нуля: вся функциональность и экспертиза вендора «из коробки», легко настраиваемые интеграции с СЗИ и инструменты no-code для быстрого старта

Координация с MSSP провайдерами: R-Vision SOAR – удобный инструмент для взаимодействия по выявленным инцидентам и осуществления технического реагирования

Создание многоуровневого SOC: организация работы SOC в несколько линий для предоставления сервисов мониторинга и реагирования дочерним организациям или заказчикам

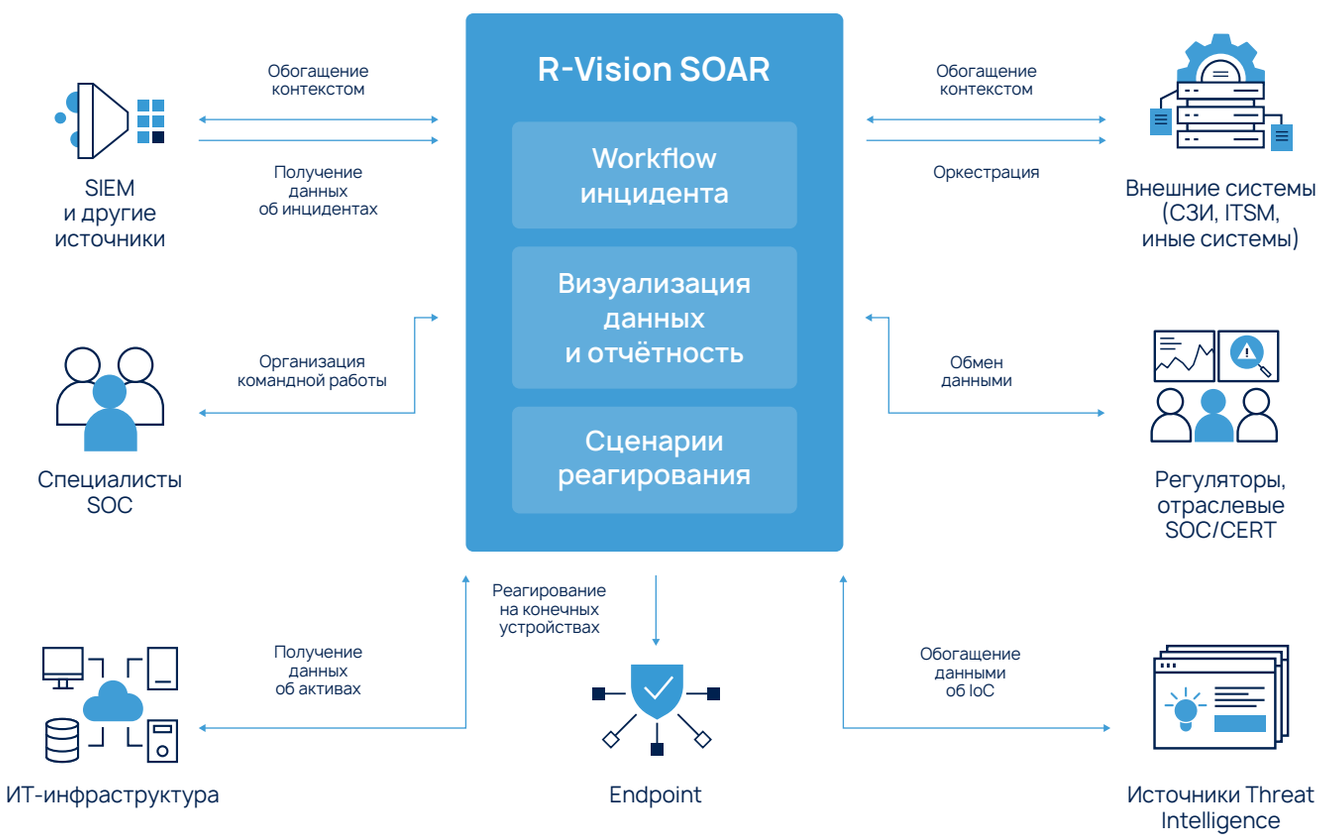
Результат

Автоматизация до 90% рутинных операций

Ускорение реагирования в 2–7 раз по типу инцидента

Снижение нагрузки на персонал SOC и требований к компетенциям

Соблюдение SLA, контроль метрик, наглядная отчётность



Контроль ИТ-инфраструктуры

- Инвентаризация и учёт активов, установленного ПО
- Создание ресурсно-сервисной модели
- Создание инцидентов из уязвимостей
- Карта влияния инцидента на бизнес-процессы

Агрегация данных по инцидентам

- Поддержка множества источников
- Нормализация данных
- Поиск инцидентов по заданным правилам
- Объединение инцидентов в группы

Выполнение требований регуляторов

- Встроенный сервис ГосСОПКА
- Коннектор к ФинЦЕРТ

Интеграции

- SIEM, NGFW, IPS/IDS, DLP, сканеры уязвимостей, антивирусы, Theat Intelligence, ITSM, CMDB, Service Desk, базы данных, российские MSSP и др. источники
- REST API
- Сервисы обогащения IoC

Для SOC уровня Enterprise

- Поддержка мультиарендности
- Отказоустойчивость и масштабирование
- Поддержка контейнеризации и работы в кластере

Автоматизация реагирования

- Интерактивные плейбуки для 1-й линии
- Динамические no-code сценарии реагирования
- Настройка карточки и жизненного цикла инцидента
- Контроль SLA в самой карточке инцидента

Командная работа

- Гибкое разграничение доступа
- Распределение нагрузки между операторами системы
- Организация совместной работы нескольких линий SOC
- Настраиваемые механизмы уведомлений и эскалации
- Встроенный чат и e-mail переписка из интерфейса
- Поддержка Telegram

Оркестрация внешних систем

- Выполнение технических мер реагирования
- Low-code конструктор коннекторов и запросов для взаимодействия с любыми системами

Визуализация и отчётность

- Предустановленные дашборды и шаблоны
- Конструктор отчётов и графиков
- Автоматическое формирование и рассылка отчётов

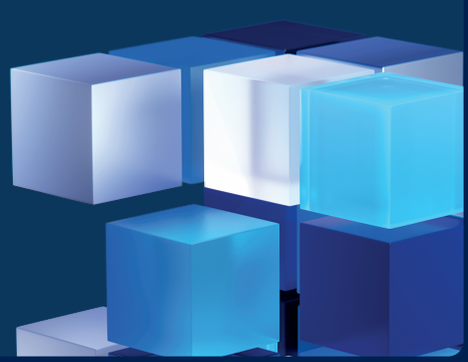
R-Vision

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.

R-Vision SOAR зарегистрирован в Реестре отечественного ПО и сертифицирован ФСТЭК России по 4 уровню доверия.

Единая платформа R-Vision EVO

Продукты R-Vision разработаны на основе единой платформы. Общая технологическая база обеспечивает бесшовную интеграцию ИБ и ИТ-продуктов, позволяя выстраивать процессы, при которых автоматизация бизнеса и кибербезопасность работают как единое целое.



rvision.ru
sales@rvision.ru
+7 (499) 322 80 40
t.me/rvision_pro
vk.ru/rvision_ru
youtube.com/@rvision_ru

rvision.ru