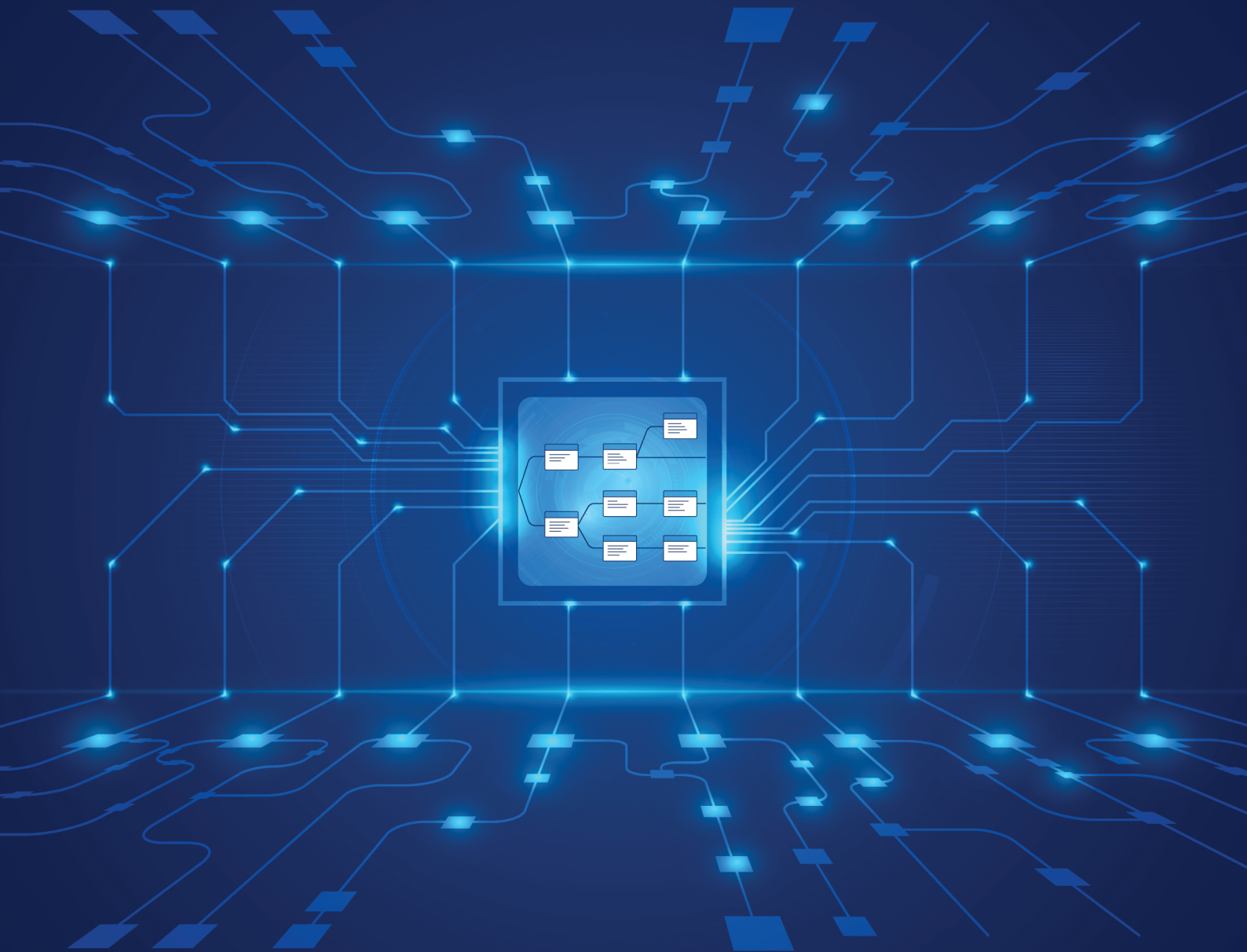


# R-Vision Security Orchestration, Automation and Response

Система оркестрации ИБ и автоматизации  
реагирования на киберинциденты



**R-Vision**

**R-Vision Security Orchestration, Automation and Response (SOAR)** — ключевой инструмент для повышения эффективности SOC. Система агрегирует данные по инцидентам из множества источников, автоматизирует обогащение, реагирование и внедрение защитных мер, обеспечивает единое пространство для совместной работы ИБ-специалистов. В результате использования повышает эффективность SOC за счет увеличения скорости реагирования и систематизации ИБ-процессов, а также дает полную картину о состоянии ИБ.

## Задачи



Повысить эффективность работы SOC



Автоматизация рутинных задач в R-Vision SOAR позволяет снизить нагрузку на команду SOC, повысить скорость реагирования и внедрения защитных мер



Выстроить процесс реагирования на инциденты «с нуля»



Конструктор интеграций R-Vision SOAR оркестрирует взаимодействие с внешними системами, а функционал гибко настраиваемых сценариев обеспечивает автоматизацию ИБ и реагирования на инциденты



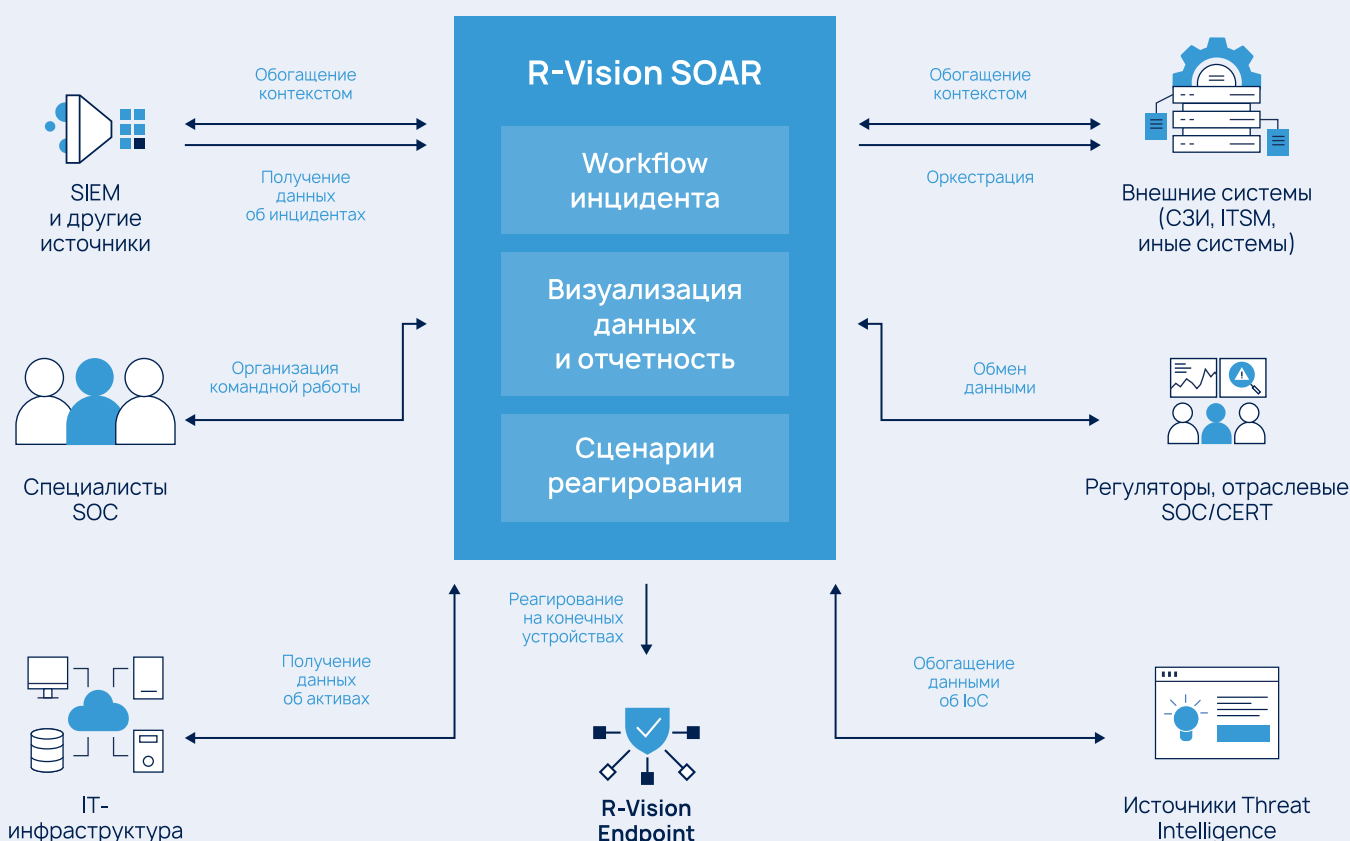
Обеспечить взаимодействие с регуляторами и MSS-провайдерами



Автоматическая передача инцидентов в ГосСОПКА, ФинЦЕРТ и взаимодействие с MSS-провайдерами реализована с использованием API

## При совместном использовании с R-Vision Endpoint позволяет:

- ✓ Осуществлять сетевую изоляцию конечных устройств
- ✓ Останавливать вредоносные процессы
- ✓ Отправлять файлы во внешние системы для анализа
- ✓ Удалять файлы с конечных устройств





**Агрегация** информации об инцидентах из множества источников, нормализация данных к принятому в организации виду, настройка правил и поиск похожих инцидентов, объединение их в группы.



**Автоматизация реагирования** с использованием гибко настраиваемых сценариев. Возможность создания как полностью автоматических сценариев, так и интерактивных, взаимодействующих с оператором системы.



**Оркестрация** внешних систем, выполнение управляющих воздействий в рамках сценариев реагирования. Возможность конструирования собственных коннекторов для взаимодействия с произвольными системами и конечными узлами.



**Командная работа** над инцидентами: гибкое разграничение доступа, распределение нагрузки между операторами системы, организация совместной работы нескольких линий SOC, настраиваемые механизмы для уведомлений и эскалации, встроенный чат.



**Инвентаризация, контроль ИТ-активов** и установленного ПО, обнаружение несанкционированных подключений оборудования, агрегация информации об уязвимостях и управление процессом их устранения.



**Интеграции** с SIEM, NGFW, IDS/IPS, сканерами уязвимостей, антивирусным ПО, DLP, сервисами TI, системами ITSM, Service Desk, базами данных, возможность встраивания R-Vision SOAR в любые инфраструктуры с использованием REST API.



**Визуализация и отчетность** как в виде предустановленных дашбордов и шаблонов, так и с возможностью создавать собственные в режиме графического конструктора. Возможность формирования и рассылки отчетов в автоматическом режиме.



**Взаимодействие с регуляторами** и провайдерами услуг безопасности прямо из карточки инцидента.



**Поддержка режима мультиарендности** — возможность работы внутри системы с несколькими организациями или филиалами с разграничением доступа на уровне данных организационных структур.

## Результаты для CISO

- Прозрачность работы SOC, отчетность и метрики для принятия решений
- Выстроенные и автоматизированные ИБ-процессы
- Контроль ИТ-инфраструктуры и защищенности ресурсов
- Снижение вероятности негативных последствий и потенциального ущерба

## Результаты для аналитика SOC

- Снижение нагрузки за счет автоматизации рутинных задач и оркестрации внешних систем
- Повышение скорости реагирования и внедрения защитных мер
- Необходимый для работы ИБ-специалиста уровень данных по инфраструктуре
- Единое пространство для совместной работы команды SOC

# R-Vision

## О компании


**R-Vision** – российский разработчик систем кибербезопасности. Компания с 2011 года создает технологии, которые помогают организациям эффективно противостоять актуальным киберугрозам и обеспечивать надежное управление информационной безопасностью.

Технологии R-Vision применяются в государственных учреждениях, финансовой сфере, телекоммуникациях, а также в нефтегазовой, энергетической и металлургической отраслях промышленности в России и странах СНГ.

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

 [rvision.ru](http://rvision.ru)

 [sales@rvision.ru](mailto:sales@rvision.ru)

 +7 (499) 322 80 40

 [t.me/rvision\\_pro](https://t.me/rvision_pro)

 [vk.ru/rvision\\_ru](https://vk.ru/rvision_ru)

 [youtube.com/@rvision\\_ru](https://youtube.com/@rvision_ru)

