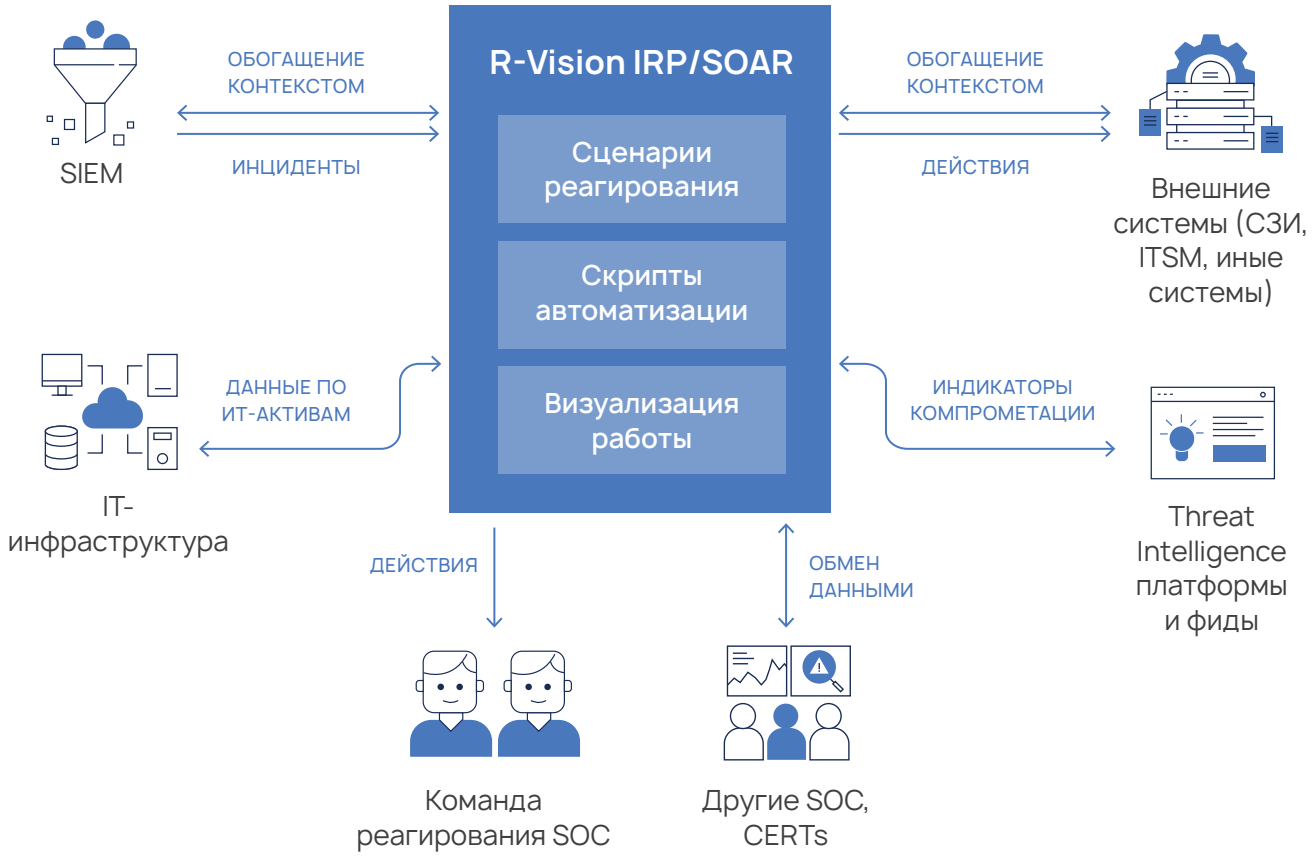
R-Vision Incident Response Platform

Платформа автоматизации мониторинга
и реагирования на киберинциденты

R-Vision

R-Vision Incident Response Platform (IRP) представляет собой решение класса SOAR, которое агрегирует данные об инцидентах из множества источников, обогащает дополнительным контекстом, автоматизирует рутинные процессы по обработке инцидентов, процедуры реагирования и координацию действий команды центра мониторинга и реагирования на инциденты ИБ (SOC), повышая его эффективность и скорость реакции на киберугрозы.

R-Vision IRP – единая консоль работы аналитика SOC



Результаты для аналитика SOC

- Работа в едином интерфейсе с отслеживанием состояния системы ИБ
- Повышение эффективности и оперативности работы команды реагирования SOC
- Автоматизация рутинных задач в процессе обработки инцидентов
- Выстроенное взаимодействие между ИБ и ИТ-подразделениями

Результаты для CISO

- Контроль ИТ-инфраструктуры и уровня ее защищенности
- Автоматизация процессов управления инцидентами и уязвимостями
- Снижение вероятности негативных событий и сокращение масштабов потенциального ущерба
- Полная картина о состоянии ИБ, отчетность и метрики для принятия решений

Основные функциональные возможности

Агрегация информации обо всех инцидентах в едином окне оперативного реагирования.

Автоматизация процесса реагирования на инциденты за счет запуска предустановленных алгоритмов и сценариев; возможность настроить сценарий реагирования под свои процессы; полный цикл обработки инцидентов.

Управление командой реагирования и процессами, распределение ролей, координация действий, уведомление, эскалация, планирование и контроль задач в едином рабочем пространстве.

Инвентаризация и контроль ИТ-активов, управление уязвимостями, контроль установленного ПО; обнаружение несанкционированного ПО, оборудования и внешних подключений; консолидация сведений о состоянии безопасности инфраструктуры.

Возможность работы в рамках единой инсталляции в режиме мультиарендности: распространение действия сценариев реагирования и коннекторов, получение обратной связи; возможность многократного запуска сценариев реагирования.

Интеграция с SIEM, NGFW, IPS/IDS, сканерами уязвимостей, антивирусным ПО, DLP, сервисами TI, системой Skybox, ITSM, Service Desk и базами данных.

Взаимодействие с любыми внешними системами с помощью конструктора коннекторов, получение данных по активам за счет скриптов на Python.

Оркестрация подключенных систем, координация их взаимодействия в рамках сценария реагирования, управление запуском плейбуков и обработкой инцидента.

Визуализация информации на разных уровнях представления, набор метрик по реагированию, шаблоны и конструктор графиков, набор предустановленных отчетов и конструктор отчетов, формирование и рассылка отчетности в автоматическом режиме по расписанию, экспорт в различные форматы.

Преимущества системы

- Гибкая адаптация под текущую ИТ-инфраструктуру и процессы
- Уникальный механизм интеграции с любыми сторонними системами
- Готовые скрипты автоматизации
- Приоритизация инцидентов по уровню критичности
- Динамические сценарии реагирования и удобный графический редактор
- Взаимодействие с внешними центрами реагирования
- Поддержка мультиарендной архитектуры

R-Vision

О компании

Компания R-Vision – разработчик систем кибербезопасности. С 2011 года создает продукты и сервисы, которые помогают бизнесу и государственным организациям по всему миру уверенно противостоять актуальным киберугрозам и обеспечивать надежное управление информационной безопасностью.

Технологии R-Vision используются в банках, государственных организациях, нефтегазовой отрасли, энергетике, металлургии, промышленности и компаниях других отраслей.

www.rvision.pro

sales@rvision.pro

+7 (499) 322 80 40

t.me/rvision_pro

/rvision.pro

/RvisionPro

Дайджест информационной безопасности: rvision.pro/blog

MTE

Партнер в Республике Беларусь: ООО «МультиТек Инжиниринг»

www.mte-cyber.by

info@mte-cyber.by

+375 17 28 28 959