R-Vision

Разработчик систем кибербезопасности

Содержание

О компании

R-Vision – разработчик систем кибербезопасности. Компания 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.

Направления деятельности

Автоматизация ИБ и реагирование на инциденты

Использование данных о киберугрозах

Выявление и предупреждение кибератак

Управление ИТ-активами и уязвимостями

Контроль соответствия требованиям (аудиты ИБ)

Автоматизация оценки ИБ-рисков

>100
клиентов

>60
технологических и авторизованных партнеров

>30
SOC в России используют технологии R-Vision

11 лет
опыта ИБ-проектов различного масштаба

>200
сотрудников, из них 60% – это команда R&D

География заказчиков:

Россия, Беларусь, Казахстан и другие страны СНГ

Линейка продуктов

SOAR

Оркестрация, автоматизация ИБ
и реагирование на инциденты

TIP

Анализ
информации
об угрозах

SENSE

Продвинутая
аналитика для
выявления угроз
и аномалий

КИИ

Автоматизация
категорирования
и соответствия
187-ФЗ

TDP

Имитация ИТ-
инфраструктуры
для обнаружения
кибератак

CERS

Построение центра
реагирования на
угрозы и уязвимости

SGRC

Управление ИБ,
оценка рисков и
комплаенс-контроль

R-Vision SOAR

R-Vision Orchestration, Automation and Response (SOAR) — ключевой инструмент для повышения эффективности SOC. Система агрегирует данные по инцидентам из множества источников, автоматизирует процессы обогащения, реагирования и внедрения 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.

Возможности

- ✓ Агрегация и обогащение инцидентов из произвольных источников
- ✓ Автоматизация ИБ и реагирования с использованием гибко настраиваемых сценариев
- ✓ Оркестрация внешних систем, low-code/no-code конструктор коннекторов
- ✓ Инвентаризация и контроль ИТ-активов, управление уязвимостями
- ✓ Интеграции с ведущими ИБ- и IT-решениями, работа с системой через REST API
- ✓ Готовые шаблоны и конструктор графиков, дашбордов и отчетов

Результат

- Повышение скорости реагирования и внедрения защитных мер
- Снижение нагрузки на команду SOC за счет автоматизации рутинных задач и оркестрации внешних систем
- Прозрачность работы SOC, отчетность и метрики для оценки эффективности
- Полная видимость ИТ-активов и инфраструктуры для служб ИБ
- Автоматизация взаимодействия с ГосСОПКА, ФинЦЕРТ и MSS-провайдерами

R-Vision SGRC

R-Vision Security Governance, Risk Management and Compliance (SGRC) – платформа для централизованного управления информационной безопасностью. R-Vision SGRC облегчает контроль за соблюдением внешних и внутренних нормативных требований, обеспечивает своевременное выявление рисков, автоматизирует процесс управления уязвимостями.

Платформа R-Vision служит единым рабочим пространством для совместной работы специалистов по информационной безопасности.

Возможности

- ✓ Контроль и управление информационными активами
- ✓ Оценка соответствия требованиям информационной безопасности
- ✓ Управление рисками
- ✓ Моделирование угроз
- ✓ Ведение внутренней и внешней нормативной документации
- ✓ Мониторинг состояния информационной безопасности

Результат

Своевременная оценка ИБ-рисков, выявление потенциальных нарушителей, оценка вероятности реализации угроз ИБ и возможного ущерба

Обеспечение соответствия требованиям регуляторов с минимальными трудозатратами за счет автоматизации процесса

Подбор оптимальных мер защиты и обоснованный подход к бюджетированию за счет выстроенного процесса риск-менеджмента

Визуализация и прозрачность информации о состоянии и эффективности системы ИБ

R-Vision TIP

R-Vision Threat Intelligence Platform (TIP) представляет собой платформу анализа информации об угрозах. Продукт обеспечивает автоматический сбор, нормализацию и обогащение индикаторов компрометации, передачу обработанных данных напрямую на внутренние средства защиты, а также поиск и обнаружение индикаторов в инфраструктуре организации с помощью сенсоров к SIEM-системам.

Возможности

- ✓ Автоматическая агрегация данных об угрозах из различных источников
- ✓ Обработка и обогащение данных информацией из внешних систем, нормализация
- ✓ Анализ взаимосвязей индикаторов между собой, с отчетами, уязвимостями, вредоносным ПО
- ✓ Обнаружение индикаторов компрометации внутри инфраструктуры, ретроспективный и проактивный поиск в SIEM
- ✓ Экспорт на средства защиты для мониторинга и блокировки
- ✓ Создание собственных бюллетеней данных об угрозах и рекомендациях по их обработке

Результат

Упрощает работу с данными TI, осуществляя непрерывный сбор, нормализацию и хранение данных из различных источников в единой базе

Облегчает выявление скрытых угроз, обеспечивая автоматический мониторинг релевантных индикаторов в SIEM с помощью сенсоров

Ускоряет расследование за счет быстрого поиска информации в доступных источниках и автоматизации ключевых рабочих процессов

Позволяет вовремя блокировать угрозы и минимизировать возможный ущерб, благодаря автоматической выгрузке обработанных данных напрямую на СЗИ

R-Vision SENSE

R-Vision SENSE – это аналитическая платформа кибербезопасности, которая детектирует нарушения в состоянии систем и подозрительную активность объектов, осуществляет динамическую оценку угроз и аномалий. Продвинутые аналитические возможности платформы повышают эффективность служб ИБ, позволяя своевременно выявлять признаки начинающейся атаки и приоритизировать угрозы для реагирования среди всего потока событий информационной безопасности.

Возможности

- ✓ Контроль состояния безопасности объектов
- ✓ Многоуровневая система программных экспертов
- ✓ Технология адаптивной корреляции событий
- ✓ Динамическая оценка угроз и аномалий
- ✓ Визуализация последовательности событий

Результат

Обеспечение непрерывности бизнеса за счет обнаружения угроз на ранних этапах

Снижение количества ложных срабатываний за счет продвинутых аналитических инструментов

Приоритизация угроз и аномалий по критичности, фокусировка на объектах и непрерывный контроль их изменений

Упрощение анализа инцидентов, восстановление последовательности событий

R-Vision TDP

R-Vision Threat Deception Platform (TDP) – это комплекс технологий цифровой имитации элементов ИТ-инфраструктуры для обнаружения злоумышленников, проникших в корпоративную сеть, замедления их продвижения внутри сети и предотвращения кибератак на ранних этапах.

Возможности

- ✓ Обнаружение злоумышленника с помощью сети ловушек и приманок, эмулирующих реальную инфраструктуру
- ✓ Автоматическая генерация и расстановка сети ловушек и приманок в инфраструктуре
- ✓ Сбор данных и атрибутов атакующего для анализа, определение стадии атаки и целей злоумышленника
- ✓ Оповещение об обнаружениях, передача данных во внешние системы

Результат

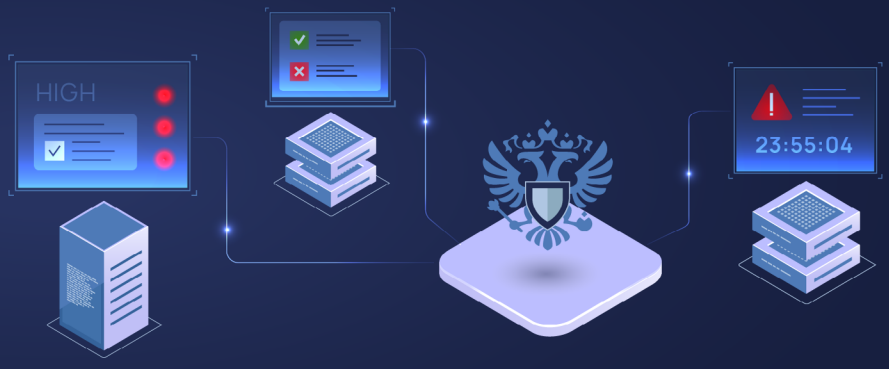
Обнаружение атак, которые невозможно детектировать другими средствами (APT, 0-day и другие угрозы)

Выявление слабых мест в защите, понимание инструментов и действий атакующего в отношении инфраструктуры организации

Снижение скорости горизонтального перемещения злоумышленника внутри сети за счет создания дополнительного слоя из эмулированных элементов

Возможность предотвратить атаки до нанесения значительного ущерба

R-Vision КИИ



R-Vision КИИ позволяет субъектам КИИ с минимальными трудозатратами выстроить процесс обеспечения соответствия требованиям федерального закона 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ.

Возможности

- ✓ Учет субъектов и объектов КИИ, автоматический сбор данных о составе компонентов, обеспечение работы комиссии по категорированию
- ✓ Автоматический расчет категории значимости объекта КИИ
- ✓ Автоматический учет примененных и необходимых мер защиты в отношении объекта КИИ
- ✓ Моделирование угроз по требованиям ФСТЭК
- ✓ Проведение аудита на соответствие требованиям Приказа ФСТЭК №239
- ✓ Учет инцидентов и двусторонний обмен данными с ГосСОПКА по выбранным инцидентам
- ✓ Автоматический импорт данных, собранных вручную, формирование полного пакета документов

Результат

- В разы упрощает и ускоряет процесс категорирования объектов КИИ и подготовки отчетных документов
- Обеспечивает полностью контролируемый и прозрачный процесс и понимание выполненных и оставшихся этапов
- Снижение человеческого фактора, вероятности ошибок и утери данных, возможность быстро найти и устранить недочеты
- Упрощение процедуры пересмотра категории значимости вне зависимости от интервала между процедурами
- Обеспечение соответствия проведенных мероприятий требованиям регуляторов, соблюдение требований законодательства (187-ФЗ, Приказы ФСТЭК)

R-Vision CERS

R-Vision Computer Emergency Response System (CERS) – программный комплекс, позволяющий создать на базе конкретной организации ведомственный, региональный или корпоративный центр мониторинга и реагирования на компьютерные инциденты – CERT (Computer Emergency Response Team). Оператор CERT получает удобный инструмент взаимодействия с подключенными организациями для выстраивания процессов по мониторингу кибератак, обмену сообщениями по инцидентам и уведомлениями об угрозах и уязвимостях.

Возможности

- ✓ Аккумуляция всей информации об угрозах и уязвимостях
- ✓ Создание личного кабинета подключенной организации для оперативного обмена данными
- ✓ Передача сведений об ИТ-активах подключённой организации оператору CERT
- ✓ Автоматизация реагирования на сообщения об инцидентах
- ✓ Формирование и рассылка бюллетеней об угрозах и уязвимостях
- ✓ Выстраивание двустороннего взаимодействия с внешними CERT/SCIRT/SOC
- ✓ Предоставление статистических данных и отчетности

Результат

- Упрощение создания государственного или корпоративного центра мониторинга
- Выстроенные процессы и обмен информацией по инцидентам, угрозам и уязвимостям внутри отрасли или ряда организаций
- Удобный инструмент для обработки больших объемов данных по участникам CERT
- Распространение собственной экспертизы на группу компаний, отрасль, регион
- Повышение уровня защищенности подключенных организаций за счет осведомленности об актуальных угрозах

Лицензии, партнеры и награды

Лицензии

- Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации № 3280 от 26 мая 2017 года
- Лицензия ФСТЭК на деятельность по разработке и производству средств защиты конфиденциальной информации № 1750 от 26 мая 2017 года
- Сертификат ФСТЭК России по 4 уровню доверия на R-Vision SOAR и R-Vision SGRC
- Продукты компании зарегистрированы в Реестре Отечественного ПО

Партнеры

>50 авторизованных партнеров

осуществляют поставку и интеграцию продуктов R-Vision

>15 технологических партнеров

обеспечивают глубокую интеграцию продуктов R-Vision

3 MSSP партнера

оказывают услуги на основе технологий R-Vision

Награды

Контакты

rvision.ru

sales@rvision.ru

+7 (499) 322 80 40

t.me/rvision_pro

/rvision_ru

/RVisionPro

Дайджест информационной безопасности:
rvision.ru/blog

R-Vision