R-Vision

Разработчик систем кибер-безопасности

www.rvision.pro

Кто мы?

R-Vision работает с 2011 года
и специализируется на решениях,
автоматизирующих ключевые процессы в ИБ:

- ✓ **Управление ИТ-активами**
- ✓ **Мониторинг и реагирование на инциденты**
- ✓ **Риск-менеджмент**
- ✓ **Контроль соответствия требованиям (аудиты)**
- ✓ **Использование данных киберразведки**

Наша миссия

Мы верим в то, что для успешного развития любого бизнеса и государства важна безопасность, а кибератаки – одна из главных угроз безопасности в современном мире.

Поэтому разрабатываем передовые решения и сервисы, которые дают нашим клиентам необходимый технологический уровень, чтобы уверенно противостоять угрозам и действовать быстрее, чем киберпреступники.

Факты и цифры

>100
клиентов

9 лет
опыта ИБ-проектов различного масштаба

>25
авторизованных партнеров

40%
сотрудников - это команда R&D

>20
SOC в России используют технологии R-Vision

География заказчиков:
Россия, Беларусь, Казахстан и другие страны СНГ

Лицензии ФСТЭК:

- На деятельность по технической защите конфиденциальной информации № 3280 от 26 мая 2017 года
- На деятельность по разработке и производству средств защиты конфиденциальной информации № 1750 от 26 мая 2017 года

Продукты зарегистрированы в Реестре Отечественного ПО

Компания состоит в Ассоциации разработчиков программных продуктов «Отечественный Софт»

Нам доверяют крупные компании

Газпром нефть

ЮНИПРО

СИСТЕМНЫЙ ОПЕРАТОР ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ

ФЕДЕРАЛЬНАЯ НАЛОГОВАЯ СЛУЖБА

ПЕНСИОННЫЙ ФОНД РОССИЙСКОЙ ФЕДЕРАЦИИ

СИБУР

segezha group

РЖД

МАГНИТОГОРСКИЙ МЕТАЛЛУРГИЧЕСКИЙ КОМБИНАТ

АРХАНГЕЛЬСКИЙ ЦЕЛЛЮЛОЗНО-БУМАЖНЫЙ КОМБИНАТ

Ростелеком

media

РИА НОВОСТИ

Нам доверяют крупные компании

ВТБ

ГАЗПРОМБАНК

МТС БАНК

Альфа-Банк

БАНК САНКТ-ПЕТЕРБУРГ

РоссельхозБанк

НАЦИОНАЛЬНЫЙ КЛИРИНГОВЫЙ ЦЕНТР
ГРУППА МОСКОВСКАЯ БИРЖА

СКБ-БАНК

БАНК СОЮЗ

белагропромбанк

Transtelecom

КЫРГЫЗ БАНКЫ

Белгазпромбанк
Энергия твоего будущего!

ҚАЗАҚСТАН ТЕМІР ЖОЛЫ

НАЦЫЯНАЛЬНЫ БАНК РЭСПУБЛІКІ БЕЛАРУСЬ

Технологические партнеры

КОД БЕЗОПАСНОСТИ

kaspersky

INFOWATCH®

GROUP IB

POSITIVE TECHNOLOGIES

Антифишинг

VULNERS.COM

ОКБ АПР

SOLAR SECURITY software&services

attack + killer

PROFESSIONAL Postgres

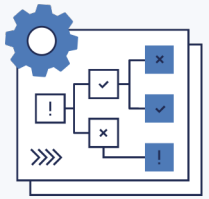
Qualys.

АЛТЭКС СОФТ

Линейка решений R-Vision

SENSE

Продвинутая аналитика для выявления угроз и аномалий



IRP

Автоматизация мониторинга и реагирования на инциденты

TIP

Платформа управления данными киберразведки

SGRC

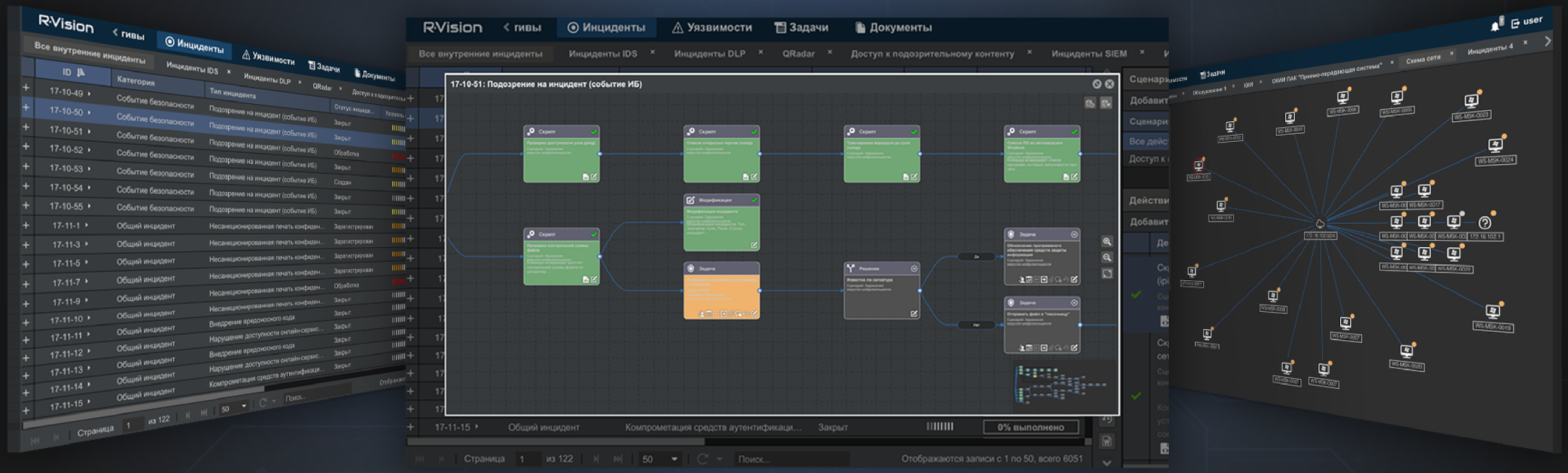
Управление ИБ, оценка рисков и комплаенс-контроль

Пакет расширения 187

Автоматизация категорирования объектов КИИ и формирования отчетности, учет и управление объектами КИИ, обеспечение соответствия 187-ФЗ

01

R-Vision IRP



Автоматизированный центр мониторинга, обработки
и реагирования на инциденты информационной безопасности (SOC)

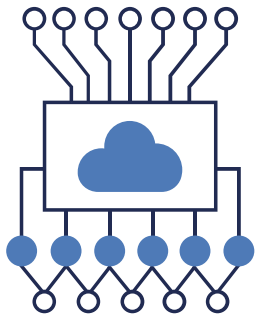
Основные функции

Агрегация

- ✓ Все инциденты в едином окне
- ✓ Детали и контекст

Оркестрация

- ✓ Контроль всех средств защиты и внешних источников
- ✓ Управление командой реагирования



Автоматизация

- ✓ Скрипты автоматизации
- ✓ Конструктор коннекторов
- ✓ Приоритезация, уведомление, эскалация
- ✓ Обмен данными (ФинЦЕРТ, ГосСОПКА, внешние CERT и SOC)

Реагирование

- ✓ Контроль активов
- ✓ Динамические плейбуки
- ✓ Визуализация цикла обработки инцидента (workflow)
- ✓ Статус обработки, SLA, сроки реагирования
- ✓ Отчетность и визуализация

Схема работы

SIEM

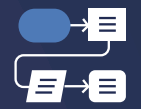
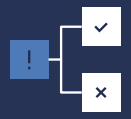
СЗИ

Инфраструктура

TIP / CERTs

IT / Service Desk

R-Vision IRP/ SOAR

- Процессы 
- Совместная работа 
- Реагирование 
- Автоматизация 
- Сценарии 

- Уведомление
- Локализация
- Внедрение мер
- Восстановление
- Расследование
- Отчетность

Результат

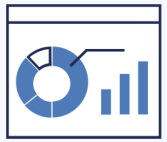
Повышение **скорости реагирования** на инциденты

Минимизация **потенциального ущерба** и простоя бизнеса

Компенсация **нехватки персонала** в условиях роста числа инцидентов

Повышение эффективности работы корпоративного SOC

Контроль ИТ-инфраструктуры и защищенности ресурсов



Полная картина о состоянии ИБ, отчетность и метрики для принятия решений

Кейсы использования R-Vision IRP

Автоматизация SOC крупной нефтегазовой компании, осуществляющего мониторинг и реагирование на инциденты для более 100 дочерних предприятий в 30 регионах страны

Автоматизация управления жизненным циклом инцидентов в крупной промышленной компании с объемом инфраструктуры в 10 тыс. хостов и множеством дочерних предприятий

Автоматизация реагирования на инциденты и обмена данными с ФинЦЕРТ в ряде крупнейших российских банков

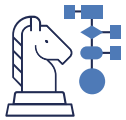
Автоматизация workflow в коммерческих SOC и возможность предоставления дополнительных услуг по модели MSSP

02

R-Vision SGRC

Автоматизация управления рисками, моделирования угроз
и оценки соответствия требованиям ИБ

Основные функции



Автоматизация управления ИБ

Стратегическое планирование,
единая база документации,
учет и контроль мер защиты

Автоматизация управления рисками ИБ

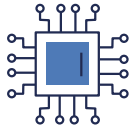
Оценка и обработка рисков ИБ,
моделирование угроз

Автоматизация аудитов и оценки соответствия требованиям ИБ

Контроль соответствия законодательным
требованиям и стандартам

Управление уязвимостями

Агрегация информации
по уязвимостям, автоматизация
задач по их устранению



Контроль ИТ-активов

Контроль ИТ-инфраструктуры,
управление информационными
и физическими активами

Центр управления ИБ

Инфраструктура

СЗИ

Сканеры уязвимостей

Пользователи

Регуляторы

R-Vision SGRC

Информация, бизнес-процесс Информационные системы Физические активы (пользователи, ПО, оборудование, орг.структура)	Агрегированный список уязвимостей Анализ, приоритизация Контроль статуса устранения	Схемы оценки рисков (ISO, NIST, OCTAVE, пользовательская) Анализ рисков, прогнозирование, план обработки Оценка бюджета и эффективности	ISO 27001, NIST, PCI DSS и другие проверки Заполнение форм аудита Список замечаний по аудиту	Чек-листы, планы, база документации Управление задачами, контроль исполнения, совместная работа Визуализация данных, отчетность
Asset Management	Vulnerability Management	Risk Management	Compliance Control	Security Management

Результат

Своевременное выявление угроз,

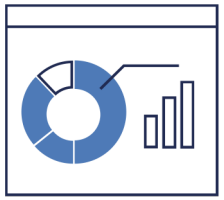
потенциальных нарушителей, оценка ИБ-рисков, прогнозирование

Подбор оптимальных мер защиты,

исходя из оценки ИБ-рисков, текущего состояния системы защиты и доступного бюджета

Обеспечение соответствия требованиям

регуляторов с минимальными издержками



Контроль состояния и эффективности

системы ИБ, защищенности инфраструктуры, отчетность для принятия решений

Доп. модуль: Пакет 187

- ✓ **Учет субъектов КИИ**, сводная информация по субъектам КИИ, перечень критических процессов и объектов КИИ
- ✓ **Учет объектов КИИ**, автоматический сбор данных о составе компонентов объекта КИИ, инвентаризация оборудования и ПО
- ✓ **Обеспечение** работы комиссии по категорированию
- ✓ **Автоматическое выставление** категории значимости объекта КИИ
- ✓ **Моделирование угроз** для объектов КИИ по требованиям ФСТЭК
- ✓ **Проведение аудита** на соответствие требованиям Приказа ФСТЭК №239
- ✓ **Автоматический учет** примененных и необходимых мер защиты в отношении объекта КИИ

Формирование пакета документов:

Акт категорирования

Сведения о присвоении объекту КИИ одной из категорий значимости

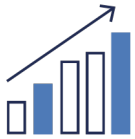
Акт проверки объекта КИИ

Перечень объектов КИИ

Перечень критических процессов

Преимущества для субъектов КИИ

Упрощение и ускорение процесса категорирования
объектов КИИ, подготовки отчетных документов



Повышение эффективности работы ИБ-подразделения,
компенсация дефицита кадров в условиях дополнительной нагрузки в рамках обеспечения соответствия 187-ФЗ

Выполнение требований 187-ФЗ
с минимальными дополнительными расходами

Соблюдение Приказов ФСТЭК
по обеспечению безопасности значимых объектов КИИ

Кейсы использования R-Vision SGRC

Централизованное управление ИБ, автоматизация контроля соответствия и формирования отчетов по требованиям ЦБ РФ для ряда крупнейших банков из Топ-20

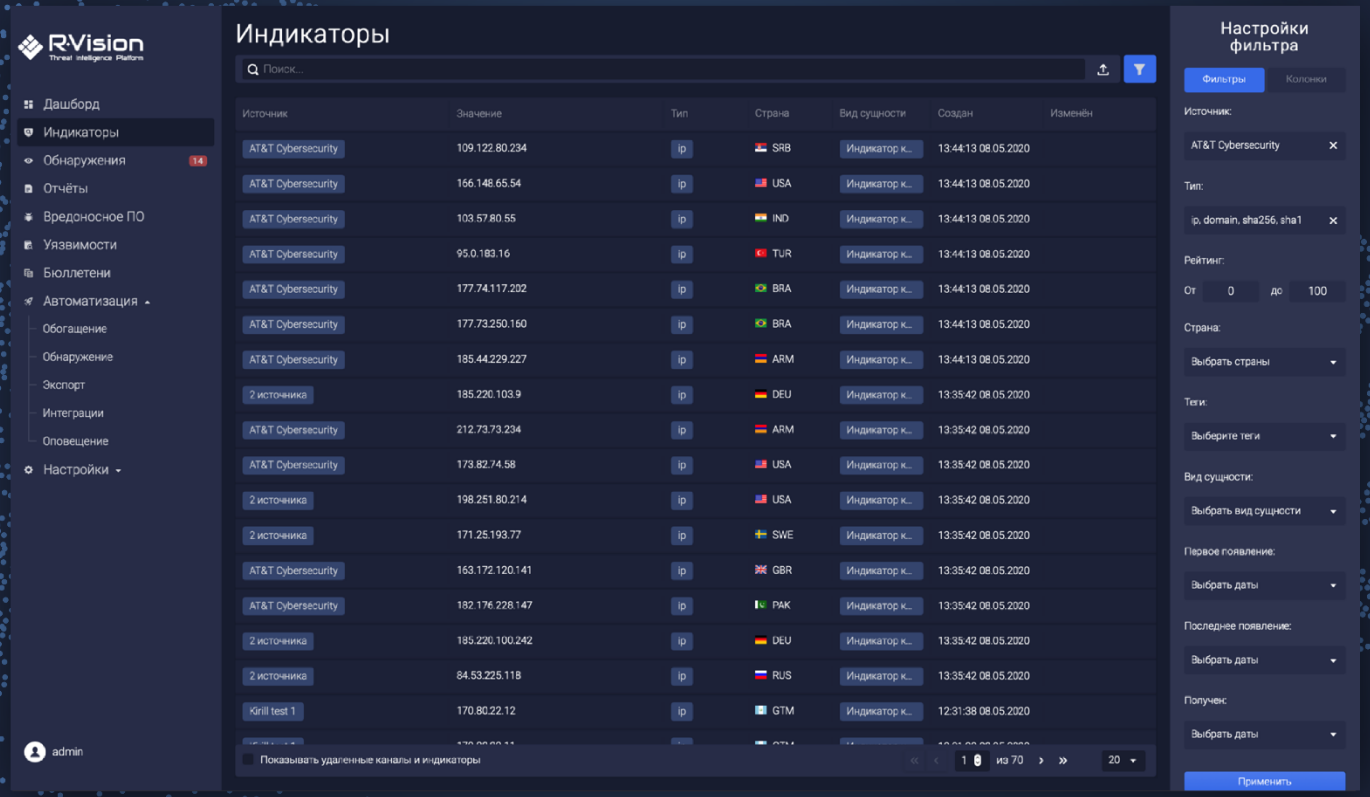
Автоматизация аудитов с помощью мобильного АРМ для одной из крупнейших промышленных компаний с территориально-распределенной инфраструктурой на 100 тыс. хостов

Автоматизация управления активами для государственной организации, инфраструктура которой насчитывает 400 тыс. хостов и более 100 систем

Сертификация по ISO/IEC 27001 и контроль соответствия для крупной телекоммуникационной компании

03

R-Vision TIP

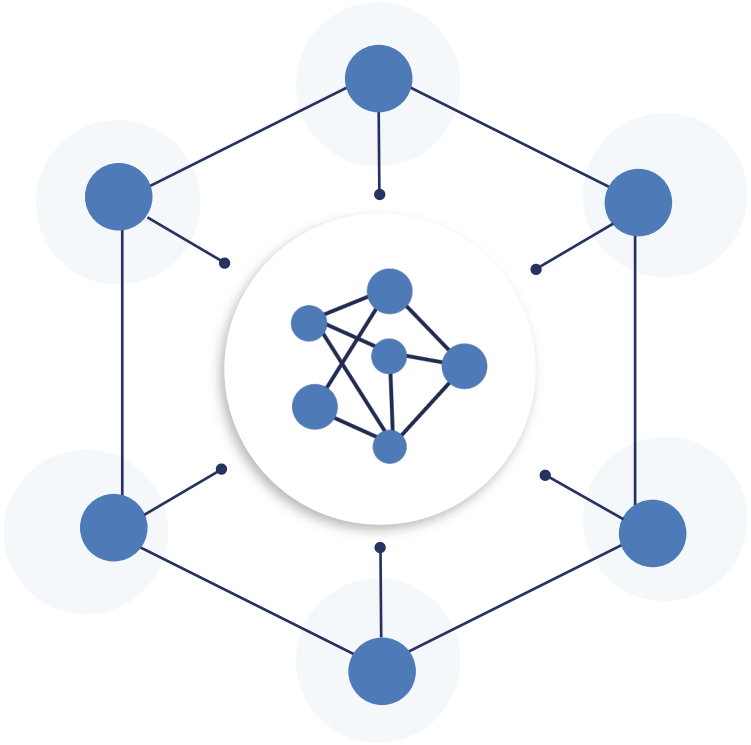


Платформа управления данными киберразведки

Основные функции

Сбор
индикаторов из разных источников

Автоматизация
повторяющихся операций
и сценариев использования
индикаторов



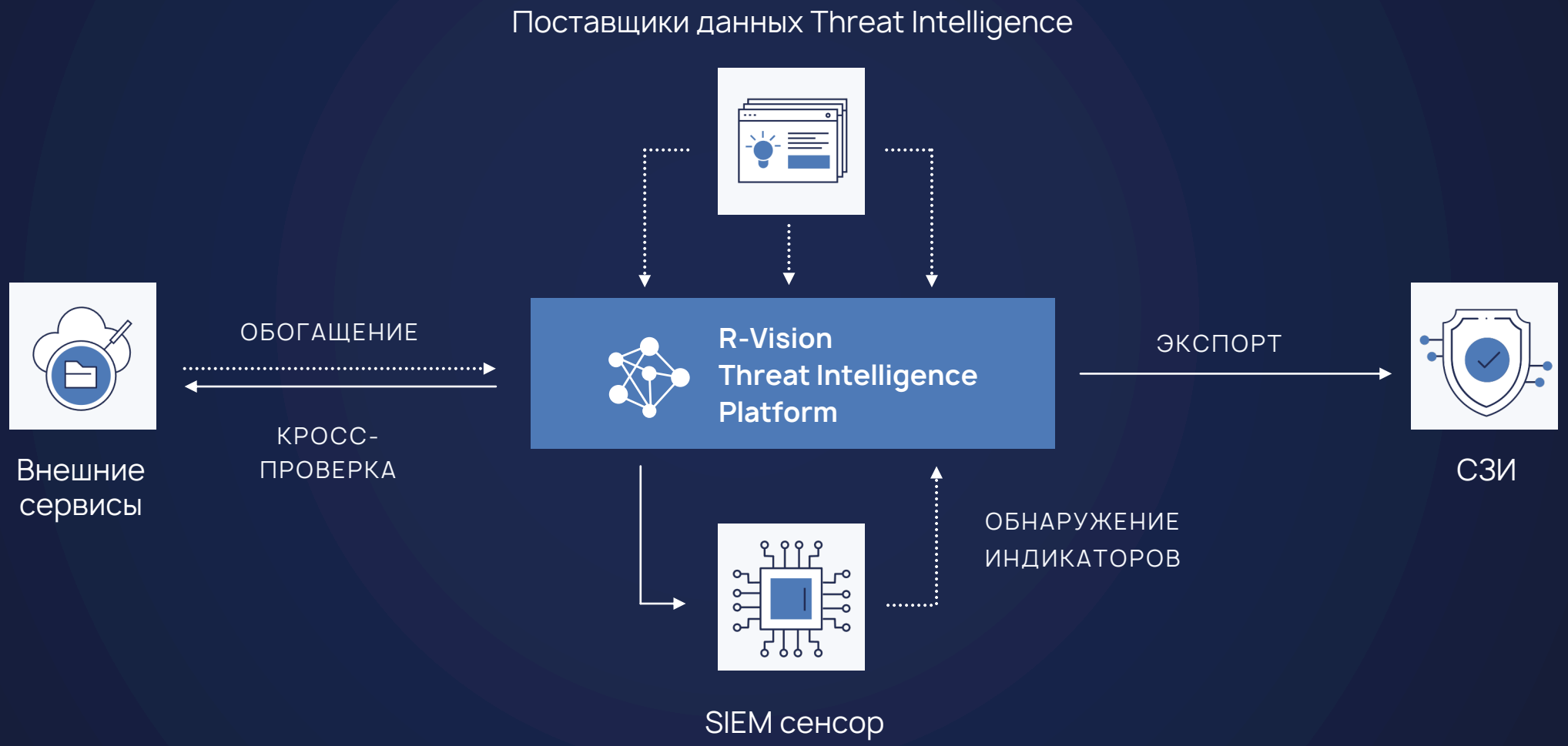
Обработка и обогащение
данных информацией
из внешних систем,
нормализация

Экспорт
на средства защиты для
мониторинга и блокировки

Анализ взаимосвязей
индикаторов между собой, с отчетами,
уязвимостями, вредоносным ПО

Обнаружение
индикаторов компрометации внутри инфраструктуры

Схема работы



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

Позволяет вовремя блокировать угрозы

и минимизировать возможный ущерб, благодаря автоматической выгрузке обработанных данных напрямую на СЗИ

Ускоряет процессы ИБ

за счет быстрого поиска контекста в доступных источниках, анализу связанной информации и автоматизации ключевых сценариев

Кейсы использования

Threat Hunting,
выявление и предотвращение APT-атак на ранних этапах в крупной компании нефтегазового сектора

Автоматическое обнаружение вредоносной активности,
связанной с ИТ-активами организаций, которые обслуживаются внешним SOC

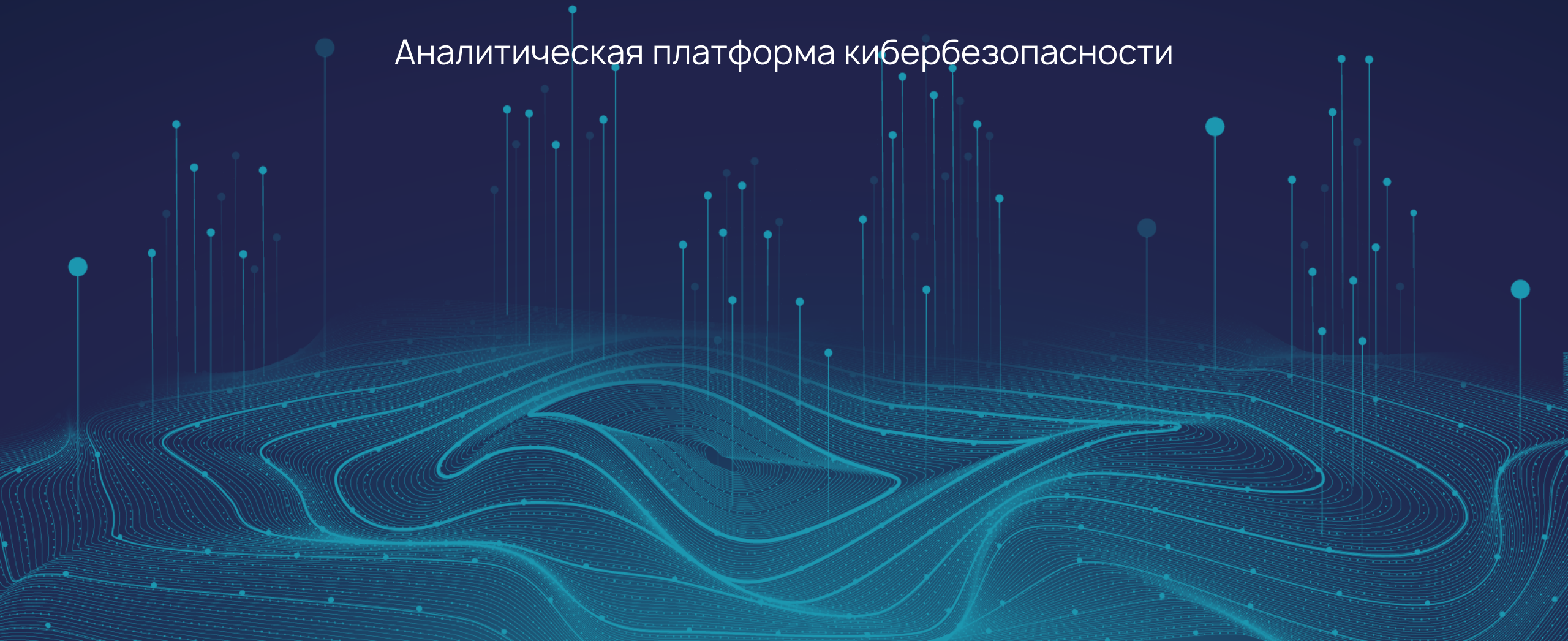
Формирование собственных бюллетеней угроз и уязвимостей
в ряде крупных российских банков для информирования дочерних структур

Анализ данных об угрозах
для повышения эффективности управления уязвимостями, рисками и стратегического планирования в компании промышленного сектора

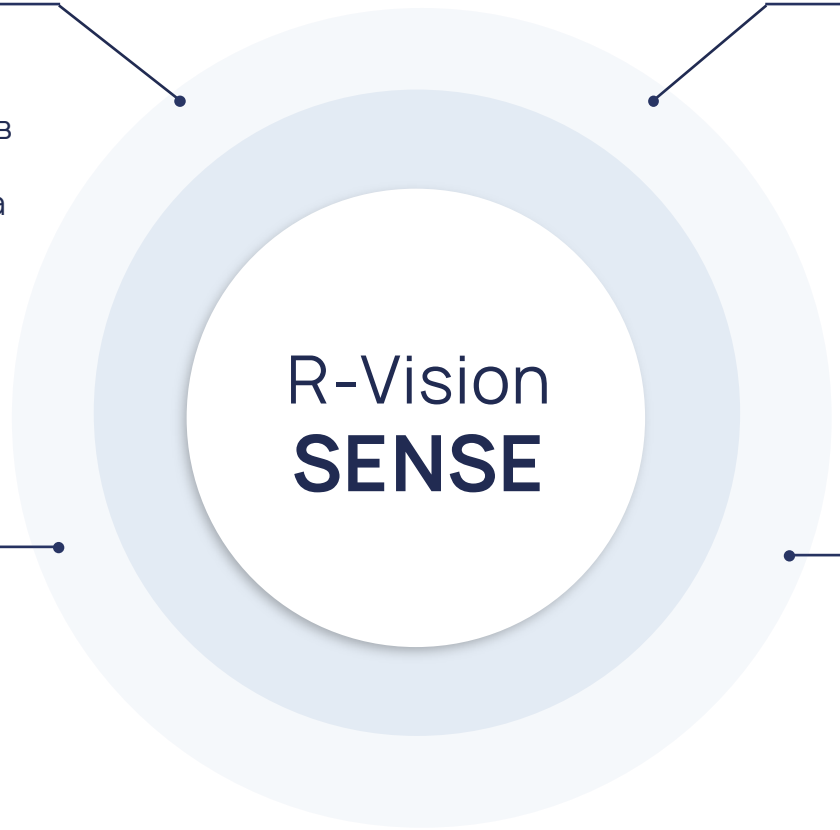
04

R-Vision SENSE

Аналитическая платформа кибербезопасности



Ключевые возможности



Динамическая оценка

- Контроль рейтинга объектов
- Предупреждение аналитика о возникновении угрозы
- Динамика изменений в реальном времени

Продвинутая аналитика

- Многоуровневая система программных экспертов
- Простые правила
- Адаптивная корреляция на основе машинного обучения

Детектирование угроз и аномалий

- Неочевидные, сложные, ранее неизвестные угрозы
- Атаки на ранних этапах
- Внутренние нарушители
- Компрометация учетных записей

Контроль и анализ

- Профилирование объектов
- Выявление аномалий
- Таймлайн событий

Схема работы

Особенности R-Vision SENSE

Объектно-центричный подход к мониторингу состояния безопасности

Динамическая, скоринговая оценка угроз и аномалий для раннего предупреждения

Технология адаптивной корреляции событий, требующая минимального участия со стороны пользователя

Многоуровневая система программных экспертов с возможностью тонкой настройки под специфические задачи

Результат

Обнаружение угроз на ранних этапах

Выявление отклонений в состоянии безопасности и признаков начинающейся атаки

Приоритизация для реагирования

Фокус на объектах с высоким рейтингом опасности и непрерывный контроль изменений

Снижение ложных срабатываний

И выявление ранее недетектируемых атак за счет продвинутых аналитических инструментов

Упрощение анализа инцидентов

Визуализация аномалий на таймлайне, восстановление последовательности событий

R-Vision

+ 7 (499) 322 80 40

sales@rvision.pro

www.rvision.pro