R-Vision

Экосистема продуктов R-Vision

www.rvision.ru

R-Vision. Факты и цифры

>100
клиентов

11 лет
опыта ИБ-проектов различного масштаба

>60
авторизованных партнеров

>60%
сотрудников - это команда R&D

>30
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

Сертификат ФСТЭК России по 4 уровню доверия
на R-Vision SOAR и R-Vision SGRC

Продукты зарегистрированы в Реестре Отечественного ПО

Компания состоит в АРПП «Отечественный софт»

Экосистема

SOAR

Автоматизация мониторинга
и реагирования на инциденты

SENSE

Продвинутая аналитика для
выявления угроз и аномалий

TIP

Платформа анализа
информации об угрозах

TDP

Автоматизированное
обнаружение атак с помощью
имитации ИТ-инфраструктуры

КИИ

Автоматизация категорирования
объектов КИИ и процесса обеспечения
соответствия 187-ФЗ

SGRC

Управление ИБ, оценка рисков
и комплаенс-контроль

CERS

Построение центра реагирования на угрозы и уязвимости

Экосистема R-Vision

- База TI
- Обнаружение IoC в инфраструктуре – инциденты
- Превентивная защита
- Формирование и распространение собственной аналитики

- Обнаружение злоумышленника – инциденты
- Замедление атаки
- Сбор IoC и атрибутов атакующего
- Учесть слабые места защиты – в инфраструктуре, аудитах, рисках

- Сбор событий
- Обнаружение аномального поведения в реальном времени – инциденты
- Таймлайн событий

- Вся картина по ИБ
- Инвентаризация (активы) для ИБ
- Аудиты с ретроспективой
- Риски с учётом инцидентов
- Уязвимости с приоритизацией

- Агрегация всех инцидентов ИБ
- Автоматизация реагирования на инциденты
- Оркестрация
- Обмен с ФинЦЕРТ и ГосСОПКА

SOAR – работа с инцидентами

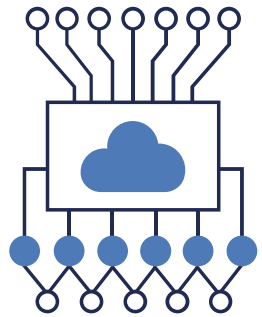
Основные функции R-Vision SOAR

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)

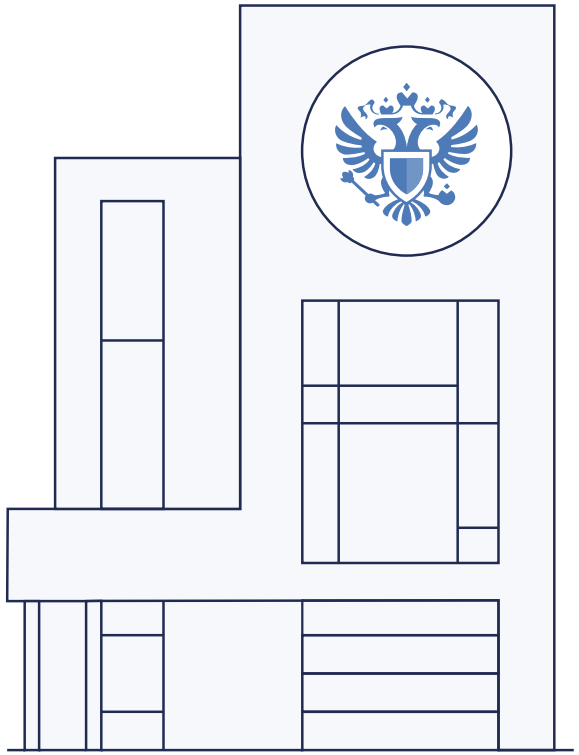
Реагирование

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

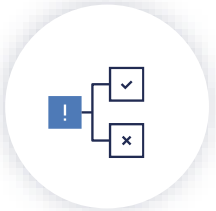
Схема работы R-Vision SOAR

Взаимодействие с НКЦКИ

- Разделение доступа пользователей к взаимодействию с ГосСОПКА
- Автозаполнение карточки, маппинг полей
- Двусторонний обмен с ГосСОПКА по инцидентам и комментариям
- Настройка периодичности обновления данных из ГосСОПКА
- Уведомление пользователя о новых комментариях от ГосСОПКА
- Получение из ГосСОПКА информации о новых инцидентах, атаках и уязвимостях



Задачи SOAR в SOC



SOAR

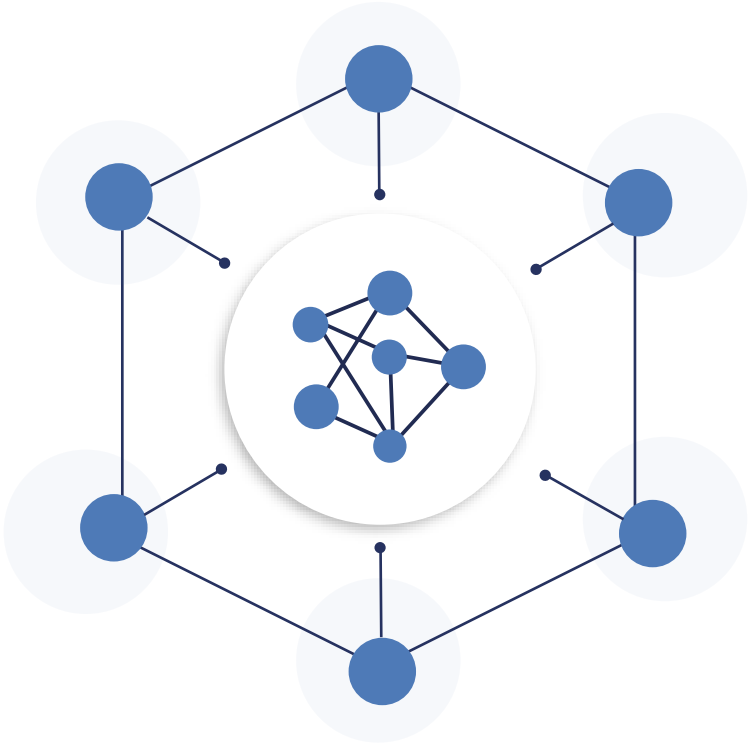
- Основа SOC – workflow
- Агрегация инцидентов
- Автоматизация реагирования
- ИТ-ландшафт по инцидентам
- Оркестрация
- Уязвимости
- Обмен с ГосСОПКА, CERT, MSSP

TIP – анализ информации об угрозах

Основные функции R-Vision TIP

Сбор
индикаторов из разных источников

Автоматизация
повторяющихся операций
и сценариев использования
индикаторов



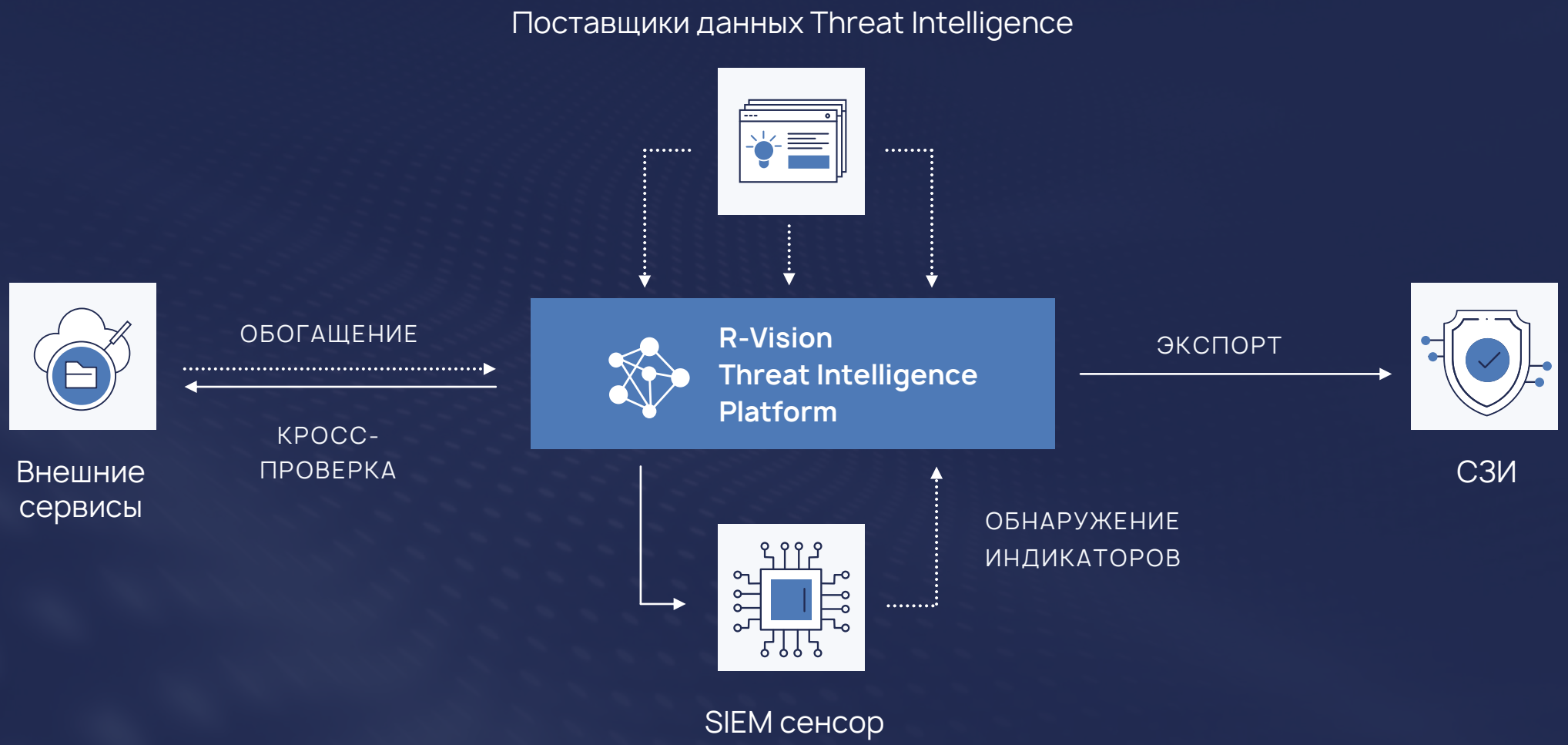
Обработка и обогащение
данных информацией
из внешних систем,
нормализация

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 R-Vision TIP



Задачи TIP в SOC

TIP

- База знаний TI
- Источник инцидентов – поиск в инфраструктуре
- Превентивная защита – экспорт на СЗИ
- Формирование собственной аналитики и распространение аналитики, бюллетеней

SENSE – анализ аномалий

Возможности R-Vision SENSE

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 R-Vision SENSE

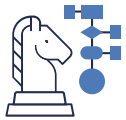
Задачи SENSE в SOC

SENSE

- Сбор событий
- Обнаружение аномального поведения, выявление инцидентов
- Динамический рейтинг опасности объектов наблюдения
- Таймлайн событий по каждому объекту

SGRC – стратегическое управление ИБ + КИИ

Основные функции R-Vision SGRC



Автоматизация управления ИБ

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

Автоматизация управления рисками ИБ

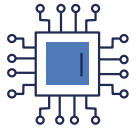
Оценка и обработка рисков ИБ,
моделирование угроз

Автоматизация аудитов и оценки соответствия требованиям ИБ

Контроль соответствия законодательным
требованиям и стандартам

Управление уязвимостями

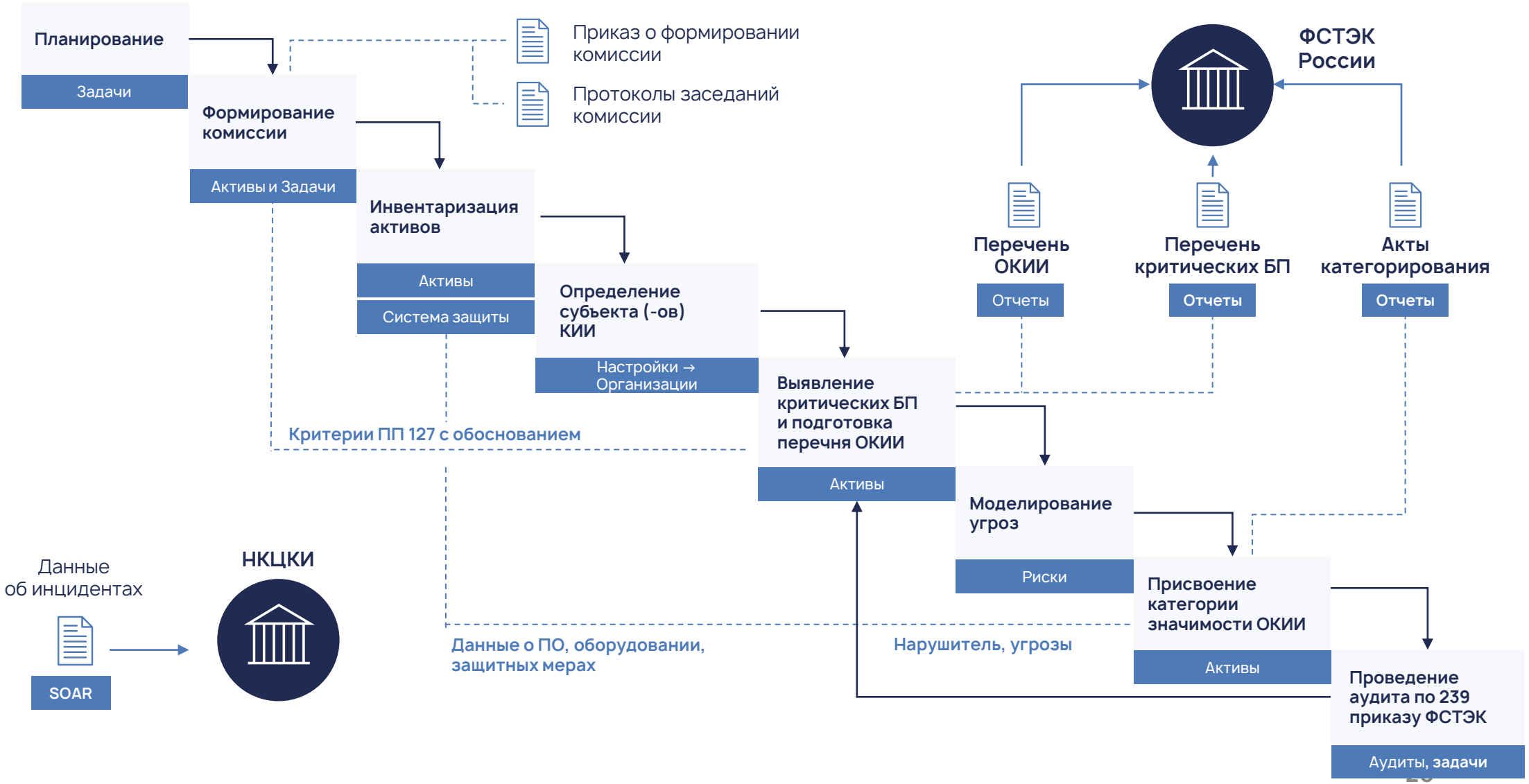
Агрегация информации
по уязвимостям, автоматизация
задач по их устранению



Контроль ИТ-активов

Контроль ИТ-инфраструктуры,
управление информационными
и физическими активами

Процесс категорирования ОКИИ в R-Vision



Управление уязвимостями

- Единая база уязвимостей, агрегированных из разных источников
- Учет устранения, контроль SLA
- Приоритизация, отсев нерелевантных уязвимостей
- Оперативное обновление статусов уязвимостей
- Централизованная постановка задач ИТ-персоналу
- Полная отчетность для служб ИТ и ИБ

Задачи SGRC в SOC

SGRC

- Агрегация всей картины по ИБ
- Инвентаризация глазами ИБ
- Аудиты с ретроспективой
- Риски с учётом инцидентов
- Уязвимости с приоритизацией
- Категорирование ОКИИ

TDP – имитация ИТ-инфраструктуры для раннего выявления угроз

Приманки и ловушки

Приманки

Информация, представляющая интерес для злоумышленника, которая ведет в ловушку.

- Учетные записи
- Файлы данных
- История браузера
- Ключи
- И т. д.

Ловушки

Ложные узлы сети, позволяющие обнаружить злоумышленника и отвлечь его от реальных узлов.

- Рабочие станции
- Устройства
- Сетевое оборудование
- Серверы
- И т. д.

Функции R-Vision TDP

1. Сбор данных об инфраструктуре (в т. ч. из AD) для создания идеальной сети ловушек и приманок
2. Автоматическая генерация ловушек и приманок из шаблонов
3. Имитация любых систем, в том числе специфических: АРМ КБР, АБС, финансовые системы, CRM, промышленные контроллеры и других.
4. Автоматическая расстановка взаимосвязанных ловушек и приманок в инфраструктуре
5. Обнаружение злоумышленника, создание инцидентов и отправка оповещений
6. Сбор данных и атрибутов атакующего для анализа

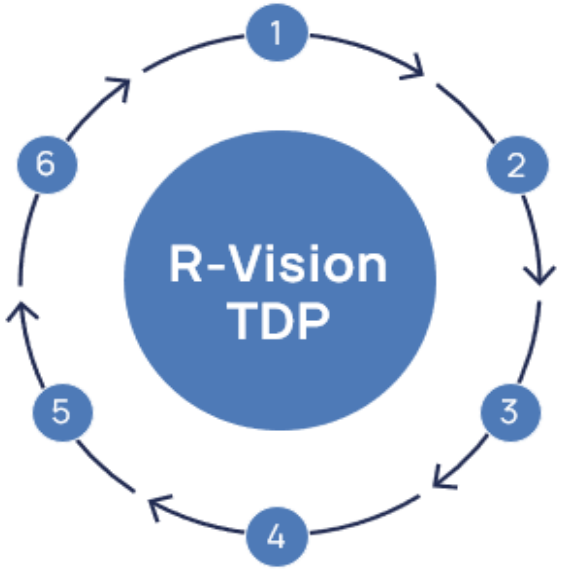
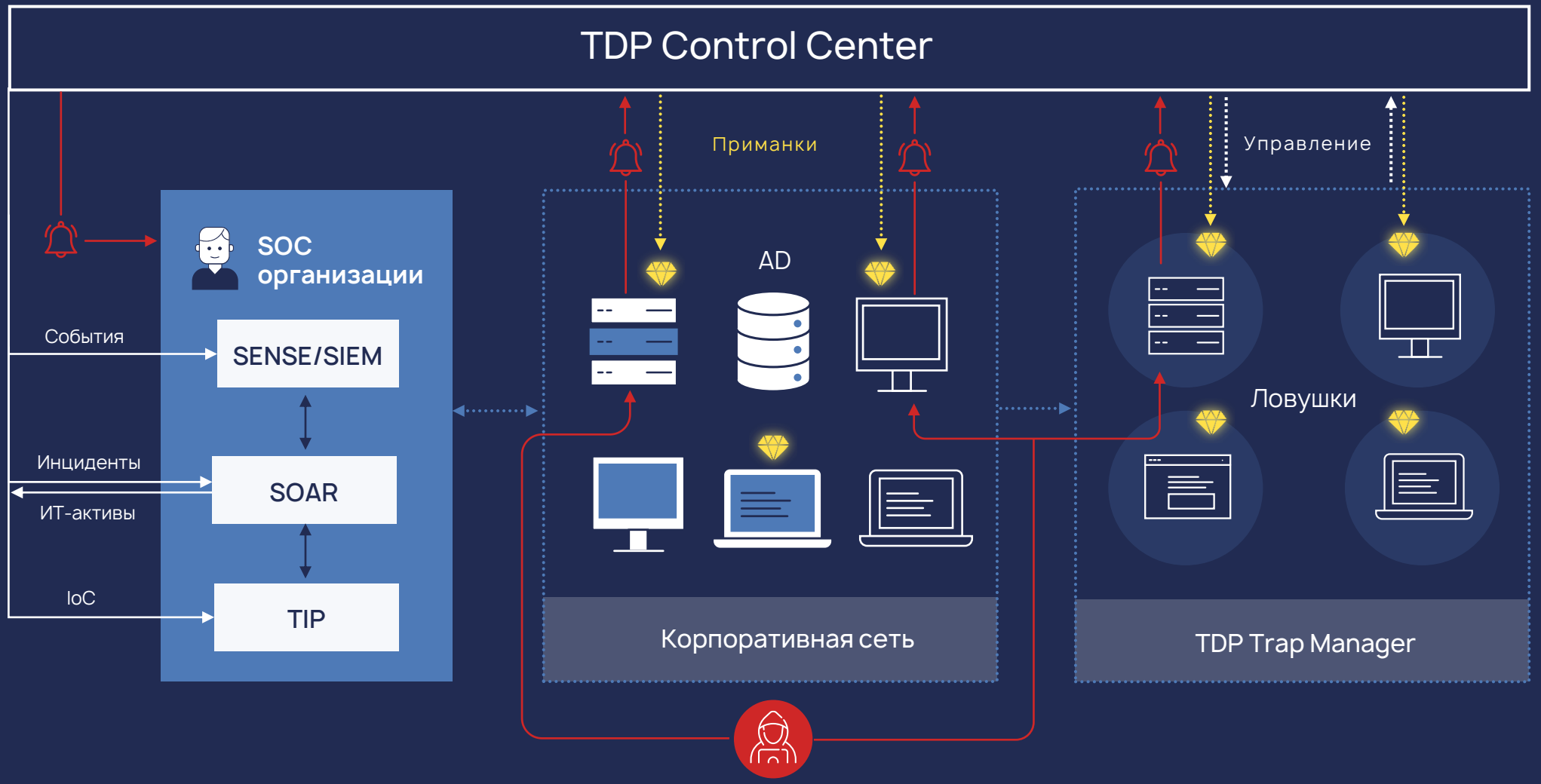


Схема работы R-Vision TDP

Схема работы R-Vision TDP



Задачи TDP в SOC

TDP

- Обнаружить APT, 0-day и сложные ранее неизвестные атаки
- Замедлить продвижение злоумышленника в инфраструктуре
- Собрать информацию по атакующему, его тактиках и методах, IoC
- Как следствие, усилить защиту

Реализация в группах компаний и холдингах

Архитектура экосистемы в ГК

R-Vision

+ 7 (499) 322 80 40

sales@rvision.ru

www.rvision.ru