R-Vision
At the root of your security

О компании R-Vision

Компания R-Vision – российский разработчик решений в области информационной безопасности. R-Vision с 2011 года разрабатывает продукты, предназначенные для автоматизации процессов управления информационной безопасностью, мониторинга и реагирования на инциденты и использования данных киберразведки.

Решения R-Vision используются в российских банках, государственных структурах, промышленности, металлургии, компаниях нефтегазовой и других отраслей.

www.rvision.pro

sales@rvision.pro

+7 (499) 322 80 40
8 (800) 350 77 57

121205, г. Москва, Территория инновационного центра «Сколково», ул. Нобеля д.7

Дайджест информационной безопасности: rvision.pro/blog

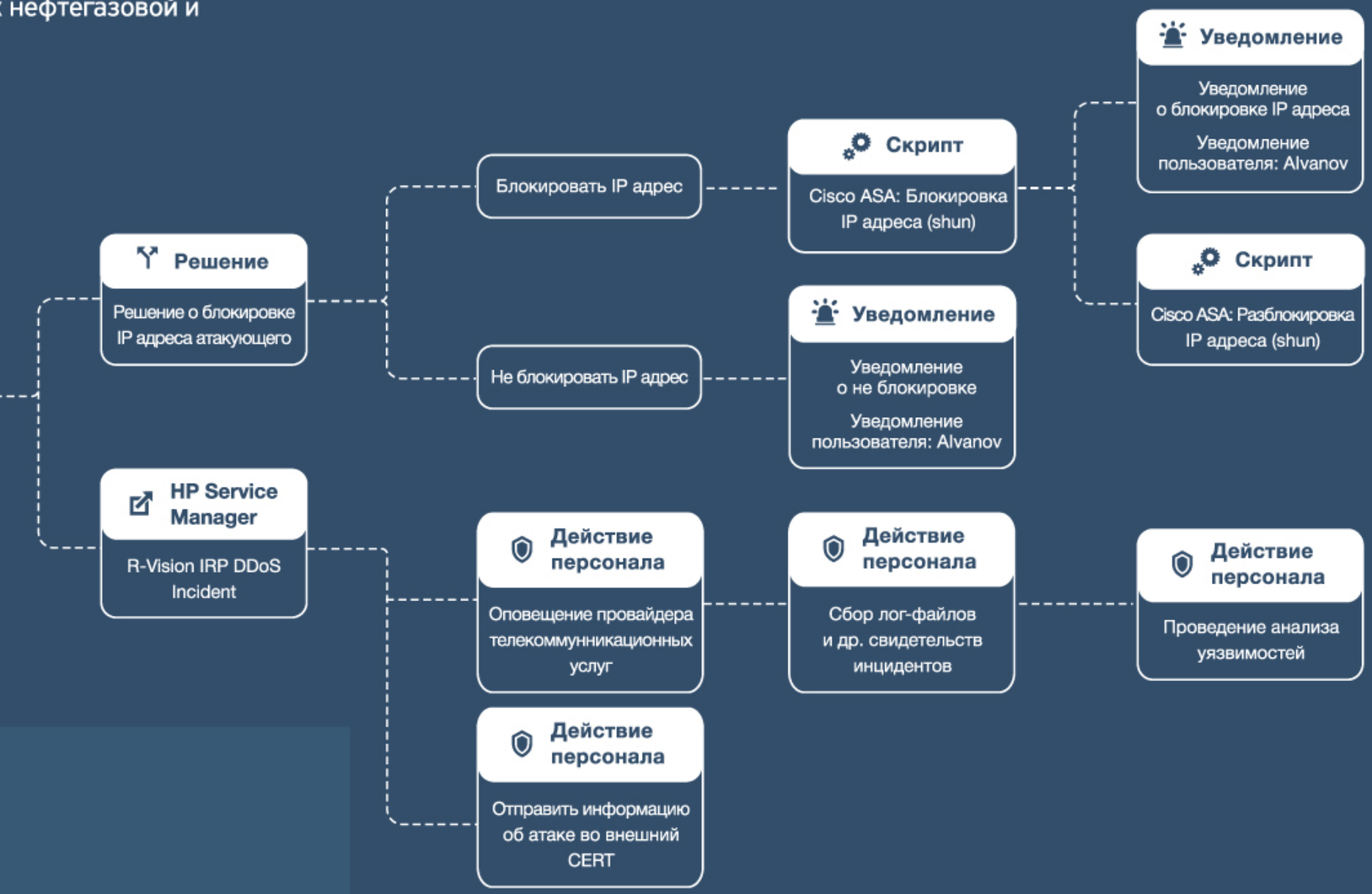
t.me/rvision_pro

/rvision.pro

R-Vision
At the root of your security

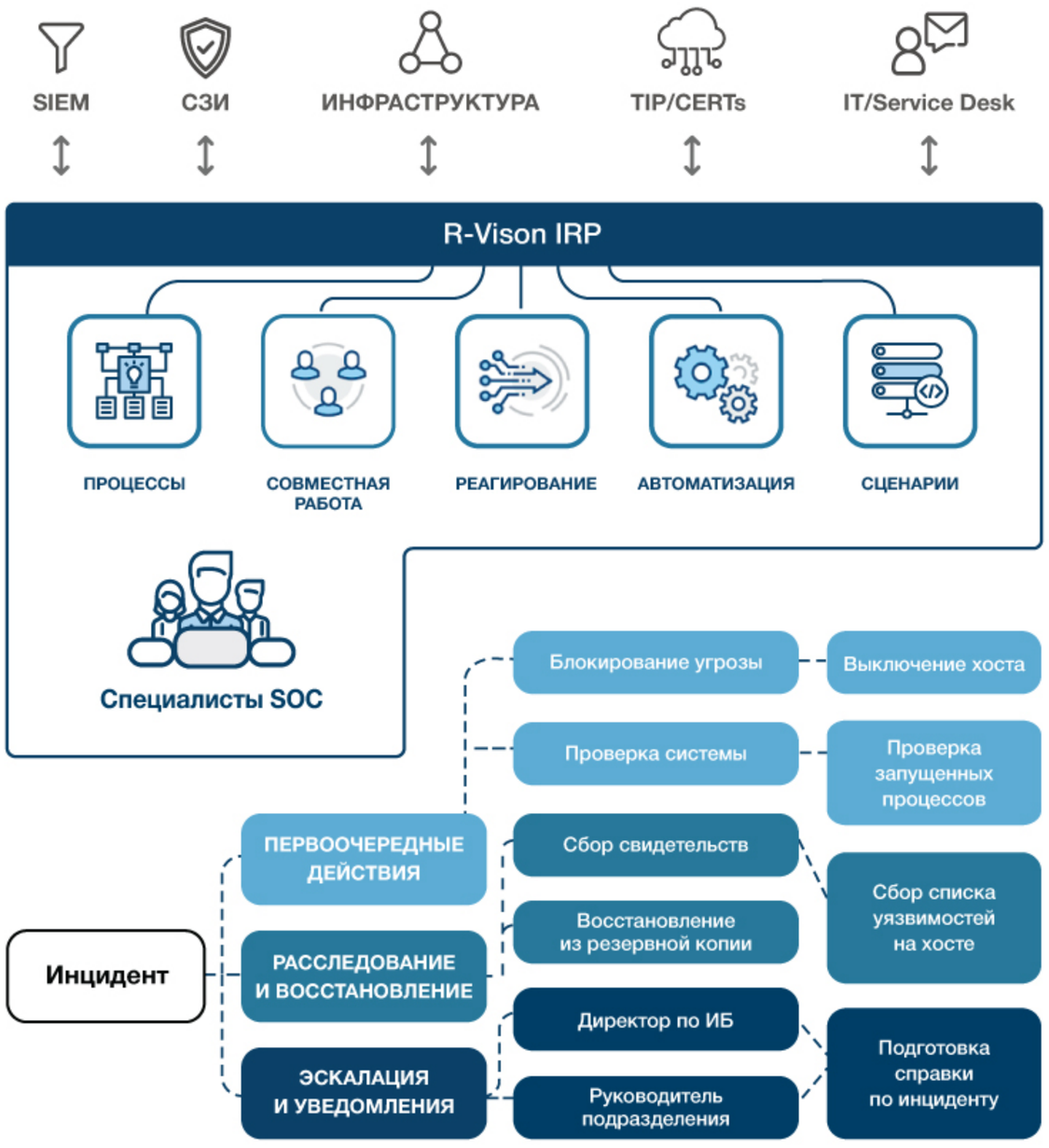
R-Vision Incident Response Platform

Платформа автоматизации мониторинга и реагирования на инциденты информационной безопасности



R-Vision Incident Response Platform представляет собой платформу автоматизации центров мониторинга и реагирования на инциденты информационной безопасности (Security Operation Center).

Продукт позволяет выявлять киберугрозы и инциденты в режиме реального времени, собирая информацию из множества источников, и осуществлять оперативное реагирование с применением автоматизированных алгоритмов. Высокая скорость реакции и слаженность действий команды реагирования позволяют свести к минимуму возможные последствия от кибератак.



АВТОМАТИЗАЦИЯ РЕАГИРОВАНИЯ

- Жизненный цикл инцидента
- Динамические сценарии реагирования (плейбуки)
- Графический редактор плейбуков
- Карта рабочего процесса по инциденту
- Действия и технические меры реагирования
- Скрипты автоматизации
- Конструктор коннекторов
- Приоритизация по уровню критичности
- Уведомление и эскалация
- Статус обработки, SLA, сроки реагирования
- Информационный обмен данными по инцидентам (ФинЦЕРТ, ГосСОПКА, внешние CERT и SOC)

Агрегация информации обо всех инцидентах в едином окне оперативного реагирования.

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

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

Интеграция с SIEM, NGFW, IPS/IDS, сканерами уязвимостей, антивирусным ПО, DLP, сервисами TI, ITSM, Service Desk и базами данных, конструктор коннекторов для интеграции с любыми сторонними решениями.

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 ДЛЯ ИБ

- Ускоряет реагирование на инциденты ИБ, тем самым сокращая масштабы потенциального ущерба и негативных последствий
- Повышает эффективность команды реагирования SOC и системы информационной безопасности в организации
- Снижает влияние человеческого фактора и вероятность ошибки
- Обеспечивает визуализацию данных для оперативного принятия решений по обработке инцидентов и контроля эффективности системы ИБ