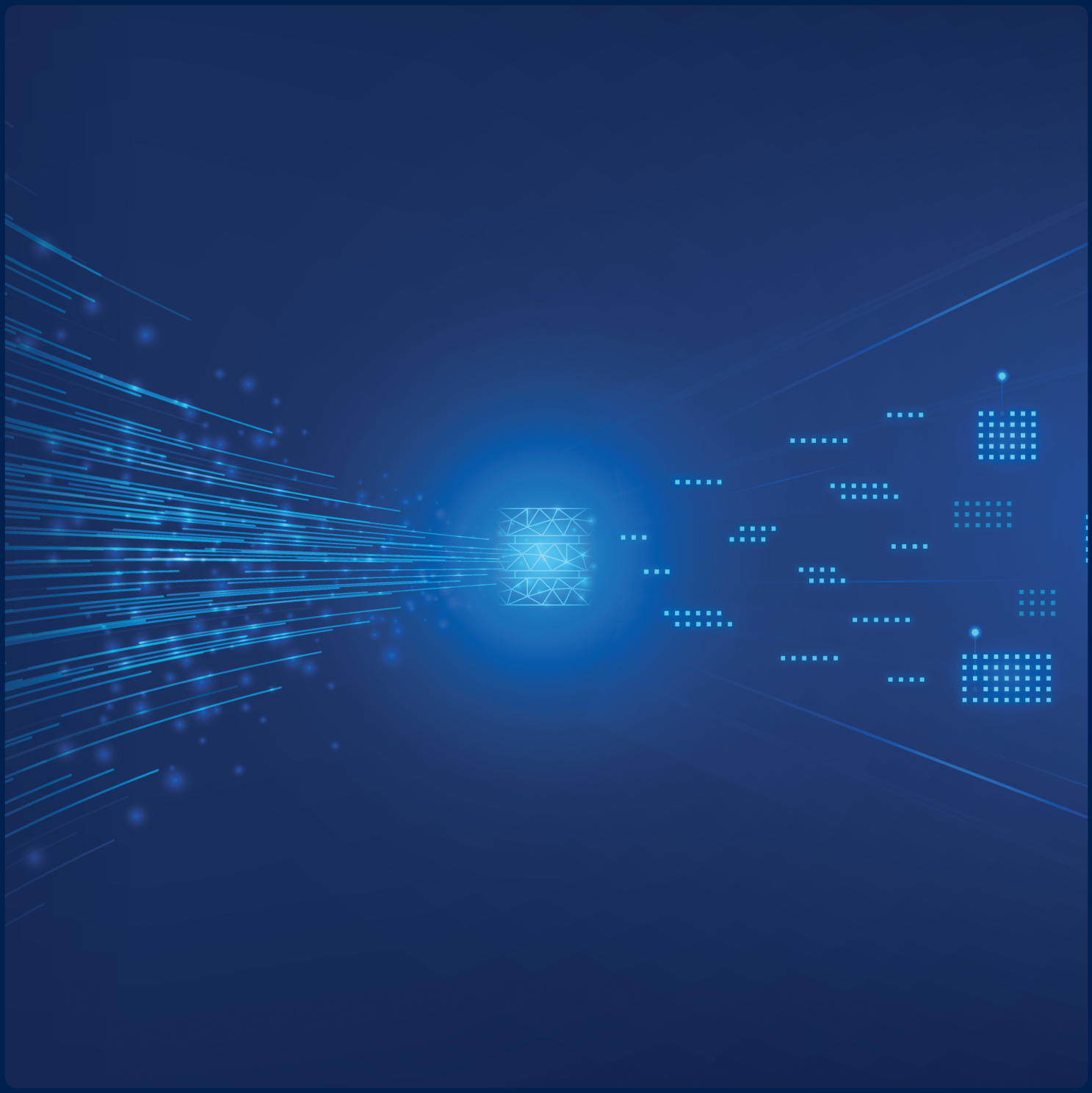
R-Vision SIEM

Современная SIEM для динамично развивающихся инфраструктур



R-Vision Security Information and Event Management

R-Vision SIEM (Security Information and Event Management) – один из ключевых компонентов системы информационной безопасности в организации, отвечающий за мониторинг инфраструктуры, своевременное выявление инцидентов и киберугроз, их расследование и реагирование. R-Vision SIEM спроектирована для бесперебойной работы в сложных, быстро развивающихся и высоконагруженных инфраструктурах.

Решаемые задачи

Централизованный сбор и управление потоками событий (Log Management)

Выявление инцидентов и киберугроз в режиме реального времени

Непрерывный мониторинг инфраструктуры и контроль изменений

Получение контекста, расследование и реагирование

Преимущества

500k EPS

Держим высокую нагрузку

Распределённая корреляция

Для инфраструктур уровня Enterprise

Выносной коллектор

Multitenancy

Контроль использования ресурсов из интерфейса

Инструменты для профессионалов

600+ правил «из коробки»

78% покрытие MITRE ATT&CK

Конструктор правил

Экспертиза «Как код» (as Code)

200+ источников

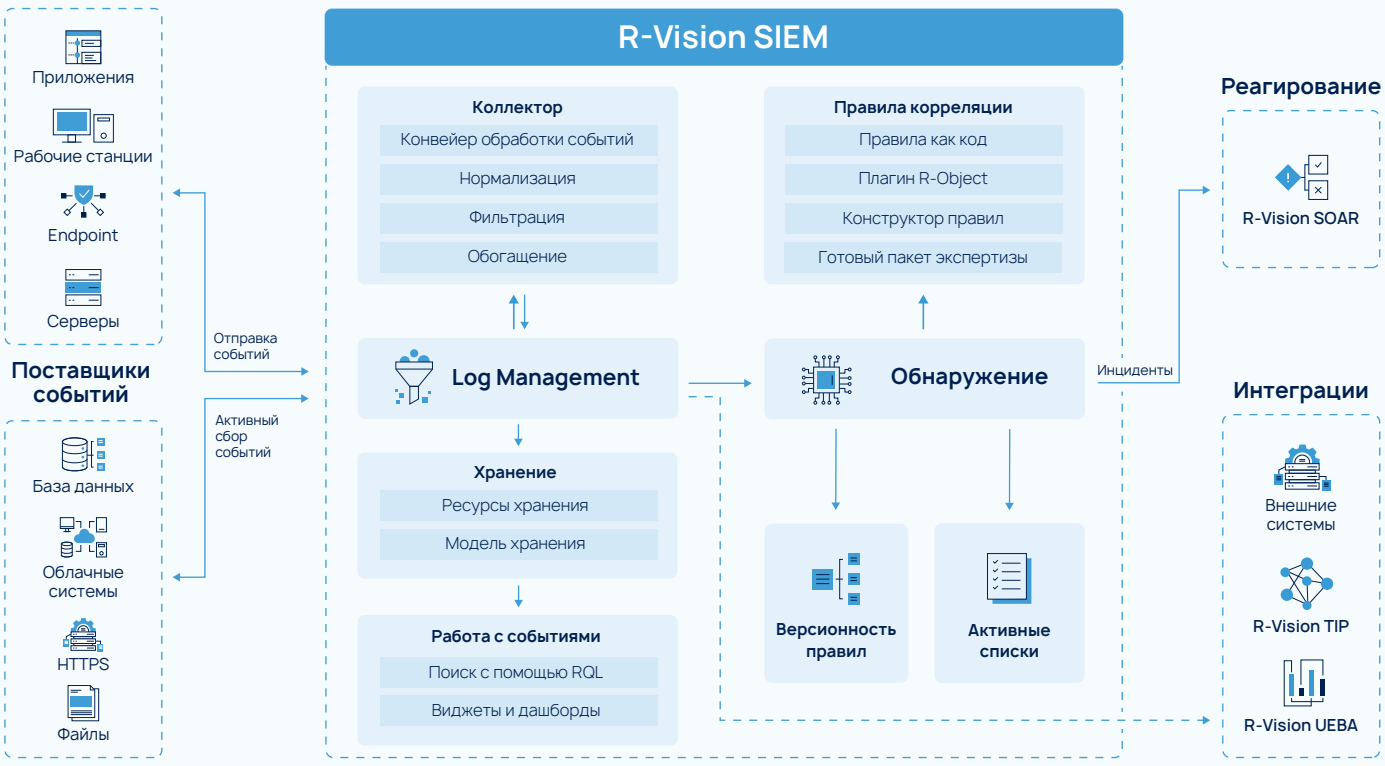
Поддерживает большинство известных источников

Низкие аппаратные требования

5000 EPS:
CPU — 16 CPU
RAM — 24 Гб
Storage — 10 Тб
90 дней хранения

Сертификат ФСТЭК России

№ 4888 от 10.12.2024,
срок действия-10.12.2029.
Требования доверия (4), ТУ



Сбор и управление потоками событий

- Конвейер обработки - единая точка доступа к инструментам сбора и обработки событий
- Визуальное управление потоком событий
- Быстрое подключение новых источников информации
- Универсальная модель данных с возможностью быстрого расширения
- Возможность создания пользовательской модели данных

Анализ данных и поиск

- Диспетчер запросов и язык поиска RQL
- Сохранение запросов и настроек таблиц
- Атрибутный контроль доступа к данным с помощью ABAC-политик
- Расширенная статистика и быстрые фильтры для эффективной работы с данными

Выявление инцидентов

- Работа с событиями ИБ в режиме реального времени
- Преднастроенная экспертиза для быстрого старта работы «из коробки»
- Пакеты экспертизы с наборами правил корреляции и нормализации
- Регулярное обновление пакетов экспертизы командой исследователей R-Vision

Гибкий подход к хранению

- Поддержка нескольких вариантов хранилищ
- Управление глубиной хранения событий и экономия ресурсов
- Выполнение требований законодательства
- Контроль нагрузки на инфраструктуру

Детектирование инцидентов любой сложности

- Конструктор правил с интуитивно понятным UI
- Редактор для написания кода
- Подсветка синтаксиса, подсказки, тестирование, версионирование
- Вся экспертиза представлена как код для гибкой настройки

Архитектура R-Vision SIEM

Современная микросервисная архитектура R-Vision SIEM с глубокой интеграцией в Kubernetes позволяет управлять ресурсами и архитектурой системы прямо из интерфейса. Это ускоряет внесение изменений, обеспечивает повторное использование ресурсов, масштабируемость, отказоустойчивость и наблюдаемость.

Визуализация

- Шаблоны дашбордов и виджетов
- Аналитика по активным спискам

Больше, чем SIEM

- **R-Vision UEBA** расширяет возможности R-Vision SIEM, позволяя выявлять неизвестные атаки и скрытые угрозы, включая инсайдеров.
- Использование системы в связке с платформой анализа информации о киберугрозах **R-Vision TIP** позволяет обогащать события данными об индикаторах компрометации.
- Тесная интеграция с **R-Vision SOAR** обеспечивает быстрое реагирование на выявленные инциденты, а также обмен данными об инцидентах с НКЦКИ с помощью встроенного модуля ГосСОПКА.

R-Vision

R-Vision - разработчик систем цифровизации и кибербезопасности. С 2011 года компания создаёт технологии, которые помогают организациям эффективно противостоять киберугрозам, поддерживать надёжность ИТ-инфраструктуры и обеспечивать цифровую трансформацию. Технологии R-Vision используются в крупнейших банках, государственных организациях, нефтегазовой отрасли, энергетике, металлургии, промышленности и компаниях других отраслей.

rvision.ru

rvision.ru

sales@rvision.ru

+7 (499) 322 80 40

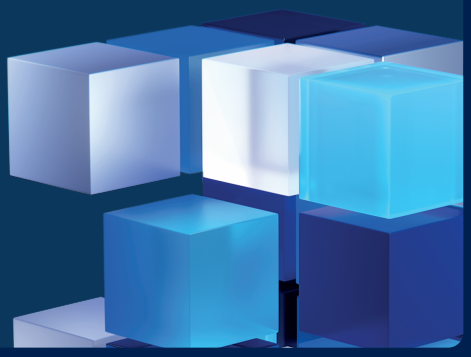
t.me/rvision_pro

vk.ru/rvision_ru

youtube.com/@rvision_ru

Единая платформа R-Vision EVO

Продукты R-Vision разработаны на основе единой платформы. Общая технологическая база обеспечивает бесшовную интеграцию ИБ и ИТ-продуктов, позволяя выстраивать процессы, при которых автоматизация бизнеса и кибербезопасность работают как единое целое.



Сообщество R-Vision SIEM

Подписывайтесь на сообщество R-Vision SIEM в Telegram: здесь мы делимся новостями и полезными материалами, отвечаем на вопросы и разбираем практические кейсы.

t.me/rvision
siem_community