R-Vision Security Information and Event Management

Централизованное управление, анализ и корреляция событий ИБ

R-Vision

R-Vision Security information and event management (SIEM) – система для обеспечения централизованного управления потоками событий со всех информационных систем, их анализа и корреляции.

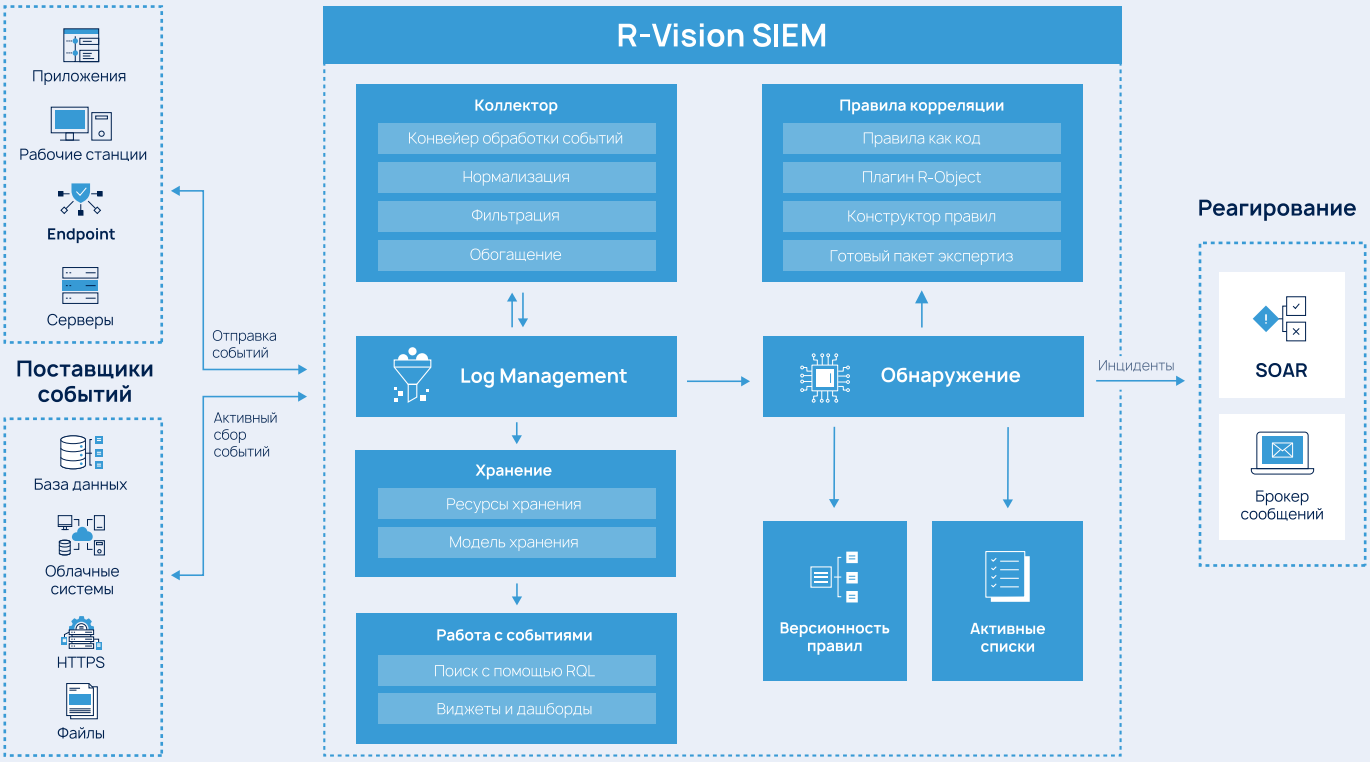
Позволяет бизнесу своевременно выявлять инциденты ИБ и проводить расследования, укрепляя информационную безопасность организации.

Задачи

- Сбор данных со всех ключевых источников
- Непрерывный мониторинг бизнес-инфраструктуры
- Детектирование в режиме реального времени
- Выявление критичных инцидентов
- Проведение расследований по выявленным инцидентам

Преимущества

- Выдерживает высокую нагрузку
- Обеспечивает непрерывную работу за счет обновления без остановки системы
- Обладает гибкой лицензионной политикой, учитывающей потребности организации
- Имеет полный набор функционала для выявления инцидентов: подготовленная экспертиза, конструктор правил, as Code для детектирования угроз любой сложности
- Располагает низкими системными требованиями, распределенными хранилищами и контролем ресурсов из интерфейса
- Дает возможность снизить требования к аппаратному обеспечению, без потери качества, скорости и надежности за счет распределенной корреляции



Сбор и работа с событиями

Сбор событий осуществляется за счет **конвейера обработки событий**, который позволяет в удобном графическом формате определить источники сбора информации и параметры подключения.

Анализ событий продуктивен благодаря созданному набору инструментов:

RQL

- Язык запросов для работы с базой данных
- Возможность сохранять запросы и настройки таблиц
- Весь функционал для анализа событий

Фильтры

- Возможность добавлять значения в фильтры из просматриваемого события
- Помощь в быстром получении необходимой выборки событий
- Гибкое управление настройками

Статистика

- Получение информации по полям в пару кликов
- Просмотр статистики по нескольким полям одновременно
- Сортировка выборки

Хранение данных в R-Vision SIEM реализовано через единый интерфейс, который позволяет управлять:

- Политикой ротации
- Мониторингом использования ресурсов
- Конфигурацией томов

Выявление инцидентов

Для выявления инцидентов в R-vision SIEM есть все необходимое:

Преднастроенная экспертиза позволяет сразу после установки приступить к детектированию угроз. Предустановленные правила проходят проверки и апробацию в реальных инфраструктурах, что обеспечивает их эффективность.

400+ правил

76% MITRE ATT&CK

Detection as Code дает возможность создавать правила без ограничений в логике для обнаружения инцидентов различного типа. В интерфейсе правил доступны подсказки и тестирование, помогающие оптимизировать процесс их разработки. Обеспечивает профессиональный подход к созданию контента и его контролю.

Конструктор правил предоставляет аналитикам удобный инструмент для выявления инцидентов. Благодаря интуитивно понятному интерфейсу и наглядной визуализации процесса, аналитики могут легко создавать необходимые правила.

Архитектура

Масштабирование и отказоустойчивость R-Vision SIEM разработаны с использованием современных и надёжных технологий. В системе применяется гибкий **микросервисный подход и технология Kubernetes**, что обеспечивает высокую отказоустойчивость и легкую масштабируемость системы.

Тесная интеграция с **Kubernetes** позволяет управлять ресурсами и архитектурой прямо из интерфейса R-Vision SIEM.

Распределенная корреляция обеспечивает горизонтальное масштабирование и повышает отказоустойчивость системы. Это позволяет снизить требования к аппаратному обеспечению без ущерба для качества, скорости и надежности работы системы.

Все для построения SOC

Сбор	Обогащение			Реагирование
Endpoint	VM	UEBA	TIP	SOAR

R-Vision

О компании

R-Vision – российский разработчик систем кибербезопасности. Компания с 2011 года создает технологии, которые помогают организациям эффективно противостоять актуальным киберугрозам и обеспечивать надежное управление информационной безопасностью.

Технологии R-Vision применяются в государственных учреждениях, финансовой сфере, телекоммуникациях, а также в нефтегазовой, энергетической и металлургической отраслях промышленности в России и странах СНГ.

rvision.ru

sales@rvision.ru

+7 (499) 322 80 40

t.me/rvision_pro

vk.ru/rvision_ru

youtube.com/@rvision_ru

t.me/rvision
siem_community

rvision.ru