R-Vision Security Information and Event Management

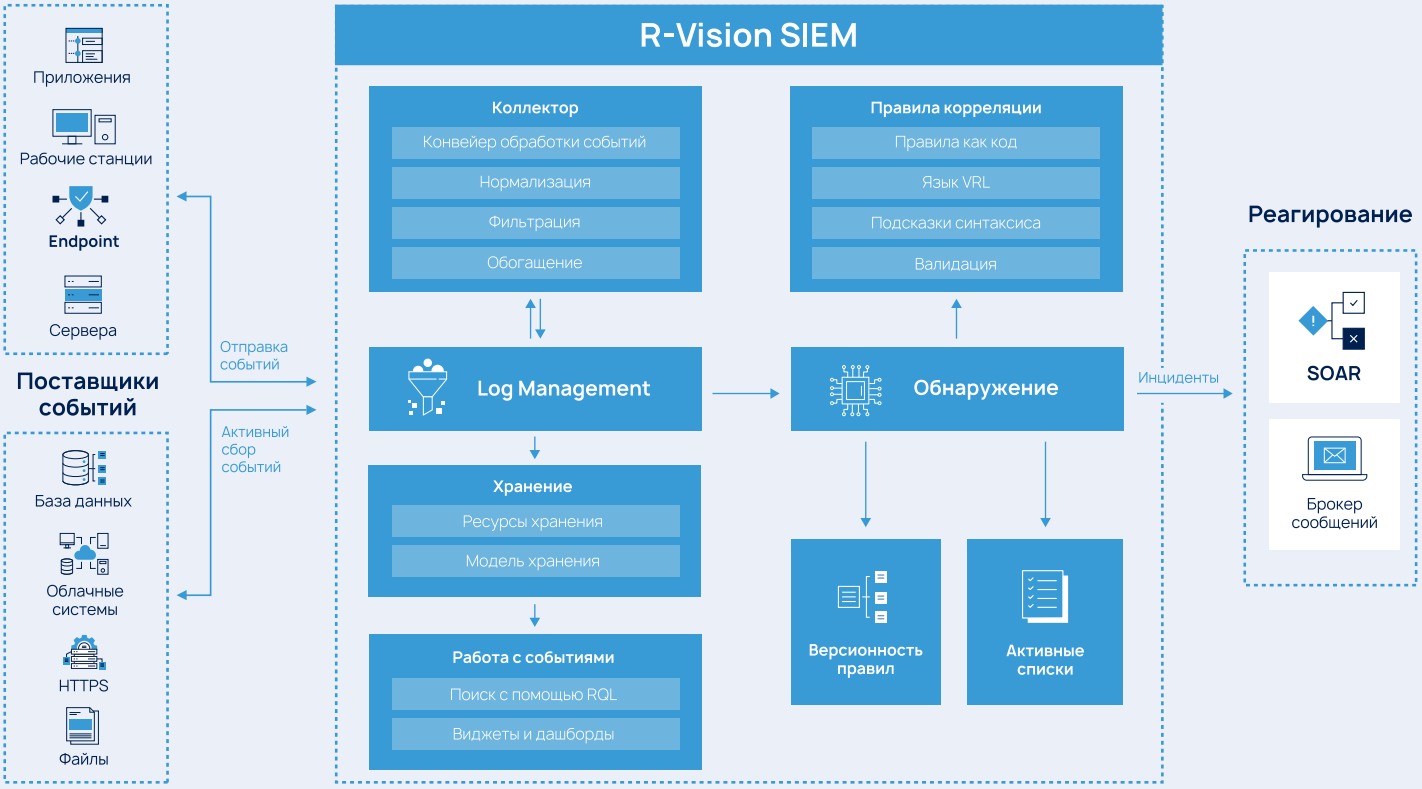
Централизованное управление событиями ИБ

R-Vision

R-Vision Security information and event management (SIEM) – основной компонент для построения центра кибербезопасности. Обеспечивает централизованное управление потоками событий со всех информационных систем, помогает своевременно выявлять инциденты и сохранять целостность бизнеса.

В R-Vision SIEM реализован комплексный подход к обработке событий, который охватывает все этапы работы с данными, при этом помогает оптимизировать ресурсы компании.

Задачи	Решение
Построить центр обнаружения инцидентов	Расширенный функционал сбора событий и правил корреляции, помогают своевременно обнаружить инциденты
Собирать и хранить уникальные данные организации	Гибкие настройки конвейеров обработки событий и моделей событий обеспечивают сбор всех необходимых данных
Сократить время на подключение новых источников событий	Наличие базовых шаблонов и большого перечня коннекторов дает возможность в кратчайшие сроки подключать любые источники событий



Преимущества использования R-Vision SIEM

- **Своевременное обнаружение угроз** за счет обработки событий и детектирования инцидентов в режиме реального времени
- **Выявление критичных инцидентов** с расширенным функционалом правил корреляции
- **Управление потоками данных** с помощью инструментов визуализации
- **Рациональное использование ресурсов** благодаря гибким настройкам хранения
- **Сбор необходимых событий** используя настраиваемые модели данных
- **Легкое масштабирование** за счет архитектурных возможностей

Любые источники для сбора событий

Сбор данных в R-Vision SIEM организован с помощью конвейера обработки событий, который в удобном формате помогает определять источники для сбора информации и параметры подключения.

Для подключения источников событий можно использовать как предустановленные шаблоны коннекторов, так и создавать собственные и в дальнейшем тиражировать их в системе R-Vision SIEM.

Единый центр управления событиями

Для дальнейшей работы с собранными данными разработан графический конструктор, который позволяет централизованно настроить:

- Прием
- Нормализацию
- Обогащение
- Фильтрацию и отправку событий в хранилища или в систему для последующего анализа

Полнофункциональные правила корреляции

Правильно написанные правила корреляции позволяют выявлять широкий спектр инцидентов. В R-Vision SIEM правила детектирования реализованы вокруг концепции «detection as code» без ограничений в логике для обнаружения инцидентов различного типа.

Оптимизировать процесс подготовки правил детектирования помогают подсказки и тестирование доступные из интерфейса. В дальнейшем версионирование позволяет контролировать состояние создаваемого контента.

Гибкое хранение

Чтобы учесть важные события и нетипичные потребности по хранению информации, в системе R-Vision SIEM разработаны:

Универсальная модель данных, которая содержит большое количество преднастроенных полей	Инструмент создания собственных моделей событий, которые можно расширить без ущерба для хранимых данных	Функционал для гибкой донастройки полей в собственных моделях событий

Система метрик хранения позволяет отслеживать загрузку хранилищ и баз данных, задавать временные интервалы для различных типов хранения и оптимизировать использование аппаратных ресурсов.

Быстрый поиск событий

Функционал поиска дает возможность анализировать большие объемы собранных данных:

- При обращении к событиям можно создавать запросы любого уровня сложности, используя математические и логические условия
- Для формирования более точной выборки доступна многоуровневая фильтрация результатов поиска, гибкое управление настройками фильтров и возможность добавлять значения в фильтры прямо из просматриваемого события
- Выявить наиболее часто встречающиеся значения помогает статистика по полям событий
- Все созданные запросы можно сохранять, что минимизирует трудозатраты аналитикам при работе с данными

Построение комплексной защиты вместе с технологиями R-Vision

Сбор	Обогащение			Реагирование
Endpoint	TDP	UEBA	TIP	SOAR
✓ События ✓ Телеметрия	✓ Данные с ловушек и приманок ✓ Идентификаторы приманок (УЗ)	✓ Поведение объектов ✓ Аномалии	✓ Индикаторы компрометации	✓ Предотвращение инцидента

R-Vision

О компании

R-Vision – разработчик систем кибербезопасности. Компания с 2011 года создает технологии, которые помогают бизнесу и государственным организациям по всему миру уверенно противостоять актуальным киберугрозам и обеспечивать надежное управление информационной безопасностью.

Технологии **R-Vision** используются в банках, государственных организациях, нефтегазовой отрасли, энергетике, металлургии, промышленности и компаниях других отраслей.

rvision.ru

sales@rvision.ru

+7 (499) 322 80 40

Дайджест информационной безопасности:
rvision.ru/blog

t.me/rvision_pro

/rvision_ru

/RVisionPro