R-Vision

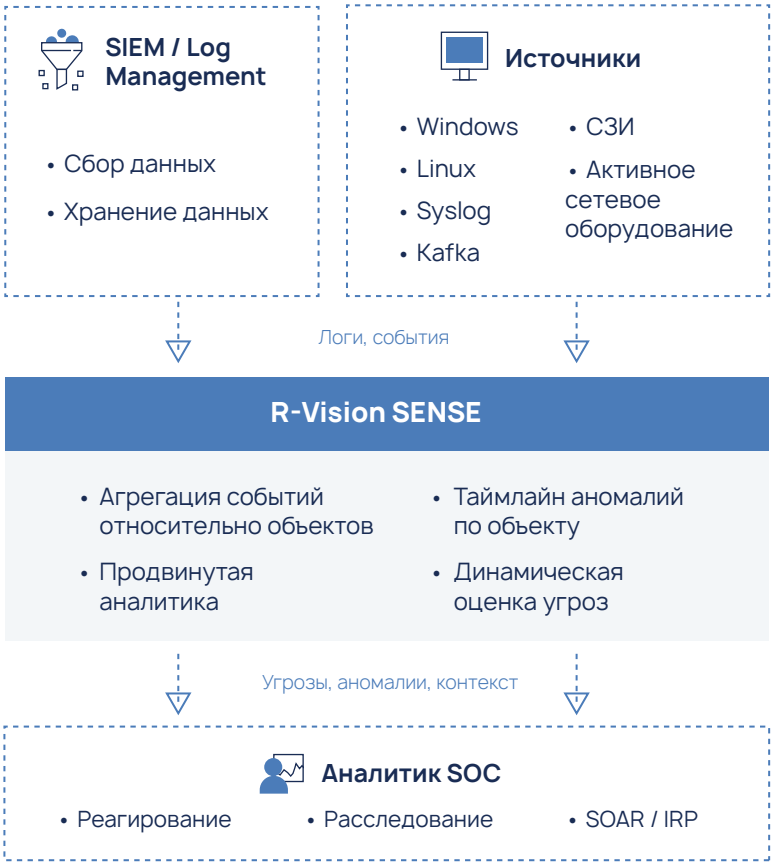
# SENSE

Аналитическая платформа кибербезопасности

R·Vision

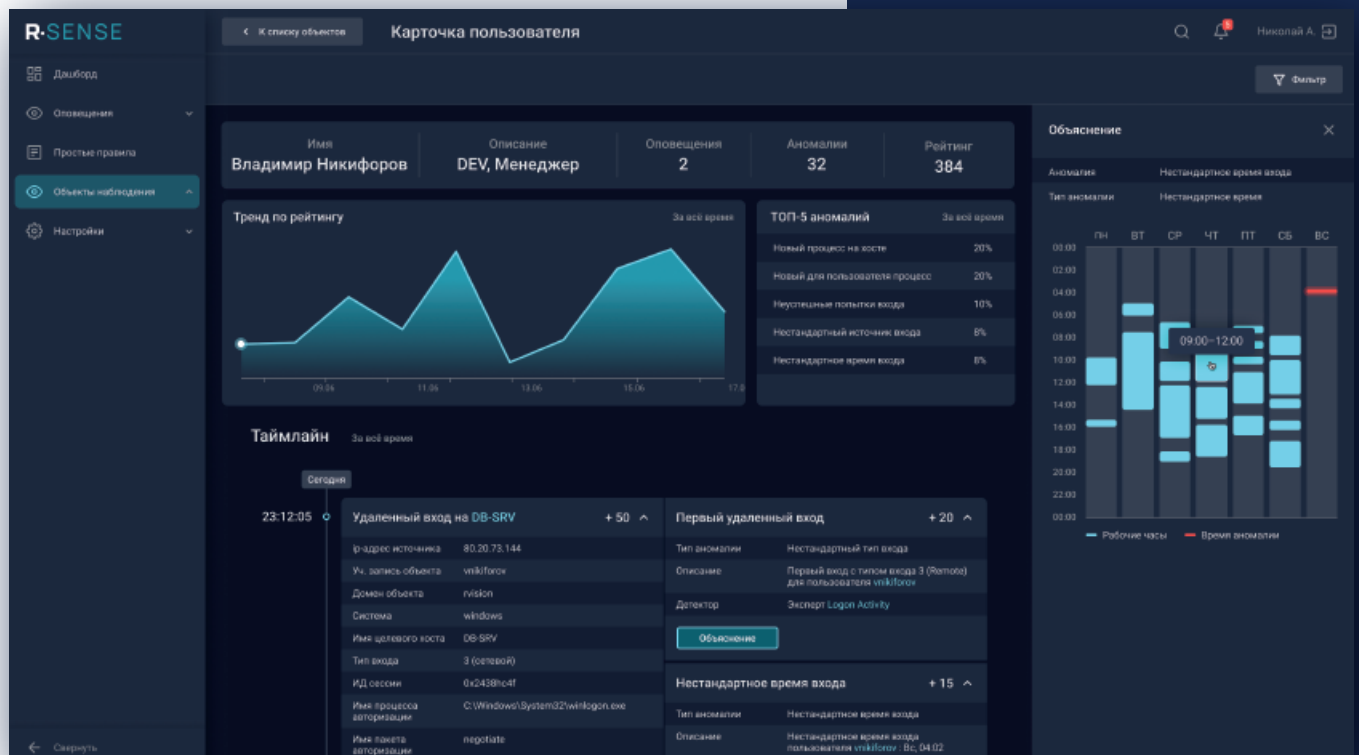
**R-Vision SENSE** представляет собой аналитическую платформу кибербезопасности, которая детектирует нарушения в состоянии систем, подозрительную активность объектов и осуществляет динамическую оценку угроз и аномалий.

Продвинутые аналитические возможности R-Vision SENSE повышают эффективность работы SOC, позволяя своевременно выявлять признаки начинающейся атаки и приоритизировать угрозы для реагирования среди всего потока подозрительных событий и инцидентов.




## Преимущества от использования

- **Непрерывный контроль и выявление изменений в состоянии безопасности**, раннее предупреждение об угрозах.
- **Обнаружение скрытых и неочевидных угроз**, детектирование ранее неизвестных атак.
- **Приоритизация критичности угроз и аномалий**, фокус внимания на объектах с высоким рейтингом опасности.
- **Снижение количества инцидентов и ложных срабатываний** за счет продвинутых аналитических алгоритмов, самообучающихся в процессе работы.
- **Упрощение анализа инцидентов** и восстановления последовательности событий с помощью таймлайна.



## Контроль состояния безопасности объектов

R-Vision SENSE осуществляет непрерывный мониторинг событий безопасности, анализируя данные из различных источников, включая системы лог-менеджмента, SIEM и другие. В основу работы платформы заложен объектно-центричный подход, согласно которому все события анализируются в отношении конкретных объектов: пользователей, рабочих станций, файлов, учетных записей, сервисов и т.д.

Изучая поведение объектов, R-Vision SENSE формирует профили нормального поведения и фиксирует подозрительную активность в случае отклонений.

## Многоуровневая система программных экспертов

С помощью многоуровневой системы программных экспертов платформа постоянно контролирует

- ✓ запуск процессов и приложений,
- ✓ запросы аутентификации,
- ✓ доступ процессов к файлам,
- ✓ подключения VPN,
- ✓ определение DGA и look-a-like доменов
- ✓ почтовый трафик и другие параметры.


## Технология адаптивной корреляции событий

R-Vision SENSE автоматически совершенствует встроенную аналитику по выявлению аномалий. При появлении новых источников и моделей данных простые правила и программные эксперты адаптируются в автоматическом режиме и не требуют донастройки.

R-Vision SENSE использует универсальный формат данных для анализа, что обеспечивает гибкость в работе аналитических инструментов.

## Динамическая оценка угроз и аномалий

Система динамической оценки угроз и аномалий рассчитывает рейтинг опасности контролируемых объектов. При обнаружении подозрительной активности рейтинг объекта увеличивается, и в случае превышения допустимого уровня аналитик получит оповещение. Это позволяет приоритизировать угрозы и своевременно реагировать на значимые отклонения.

## Визуализация последовательности событий в таймлайне

Подробная информация о подозрительной активности объектов сохраняется в виде таймлайна – временной шкалы, на которой отмечаются аномалии, выстраивается последовательность событий и контекст.

Таймлайн значительно упрощает анализ инцидентов и выявление проблем в защите для устранения.

R-Vision

## О компании

**R-Vision** – разработчик систем кибербезопасности. Компания с 2011 года R-Vision создает решения и сервисы, 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 структурах, 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