

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.

The screenshot shows the R-Vision SENSE web interface. The top navigation bar includes 'К списку объектов' (To object list), 'Карточка пользователя' (User card), a search bar, and a user profile for 'Николай А.'.

The left sidebar contains navigation links: 'Дашборд' (Dashboard), 'Правила' (Rules), 'Объекты наблюдения' (Monitored objects), and 'Настройки' (Settings).

The main content area features several sections:

- Карточка пользователя:** Displays information for 'Владимир Никифоров' (DEV, Менеджер) with 2 notifications, 32 anomalies, and a rating of 384.
- Тренд по рейтингу:** A line chart showing the trend of ratings over time, with a peak around June 15th.
- Таймлайн:** A timeline view for today, showing an event at 23:12:05: 'Удаленный вход на DB-SRV' (Remote login to DB-SRV) with a rating of +50. This event is detailed in a table below.
- Объяснение:** An explanation section for anomalies, showing a grid of colored bars representing activity times across days of the week.

Имя	Описание	Оповещения	Аномалии	Рейтинг
Владимир Никифоров	DEV, Менеджер	2	32	384

Топ-5 аномалий За всё время	
Новый процесс на хосте	20%
Новый для пользователя процесс	20%
Несколько попыток входа	10%
Нестандартный источник входа	8%
Нестандартное время входа	8%

Тренды по рейтингу За всё время	
09.06	11.06
13.06	15.06
17.06	

Событие	Рейтинг
Удаленный вход на DB-SRV	+50
Первый удаленный вход	+20
Нестандартное время входа	+15

Detailed event table for the remote login event:

Параметр	Значение
Имя источника	80.20.75.144
Уч. запись объекта	vnikiforov
Домен объекта	rvision
Система	windows
Имя целевого хоста	DB-SRV
Тип входа	3 (сетевой)
Ид сессии	0x2438hc4f
Имя процесса авторизации	C:\Windows\System32\winlogon.exe
Имя пакета авторизации	negotiate

Details for the first remote login event:

Параметр	Значение
Тип аномалии	Нестандартный тип входа
Описание	Первый вход с типом входа 3 (Remote) для пользователя vnikiforov
Датчик	Эксперт Login Activity

Details for the unusual login time event:

Параметр	Значение
Тип аномалии	Нестандартное время входа
Описание	Нестандартное время входа пользователя vnikiforov - Вс: 04:02



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.

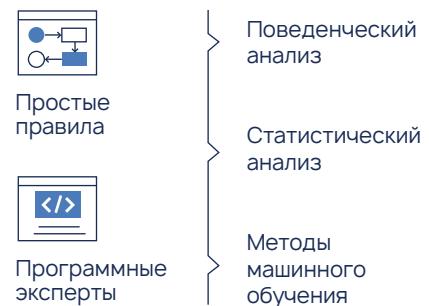
Изучая поведение объектов, R-Vision SENSE формирует профили нормального поведения и фиксирует подозрительную активность в случае отклонений.



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](https://vk.com/rvision_ru)

 [/RVisionPro](https://www.youtube.com/RVisionPro)

