

SENSE
SENSE
SENSE
SENSE

SENSE

Аналитическая платформа
кибербезопасности

R-Vision



С чем сталкиваются команды SOC?

1

Избыток алертов от SIEM →
невозможно вовремя обработать
все корреляции, инциденты

Ложные срабатывания →
отбирают время аналитика
пропуск атак

Нехватка персонала →
низкая скорость обработки
и расследования событий

2

**Отсутствует выявление атак
на ранней стадии** →
теряется возможность быстро
остановить или предотвратить атаку

Размытый фокус при аналитике →
несвоевременная обработка
критичных инцидентов

**Недостаток текущих инструментов
анализа инцидентов** →
сложно выявлять и устранять
проблемы в защите

Место R-Vision SENSE в SOC

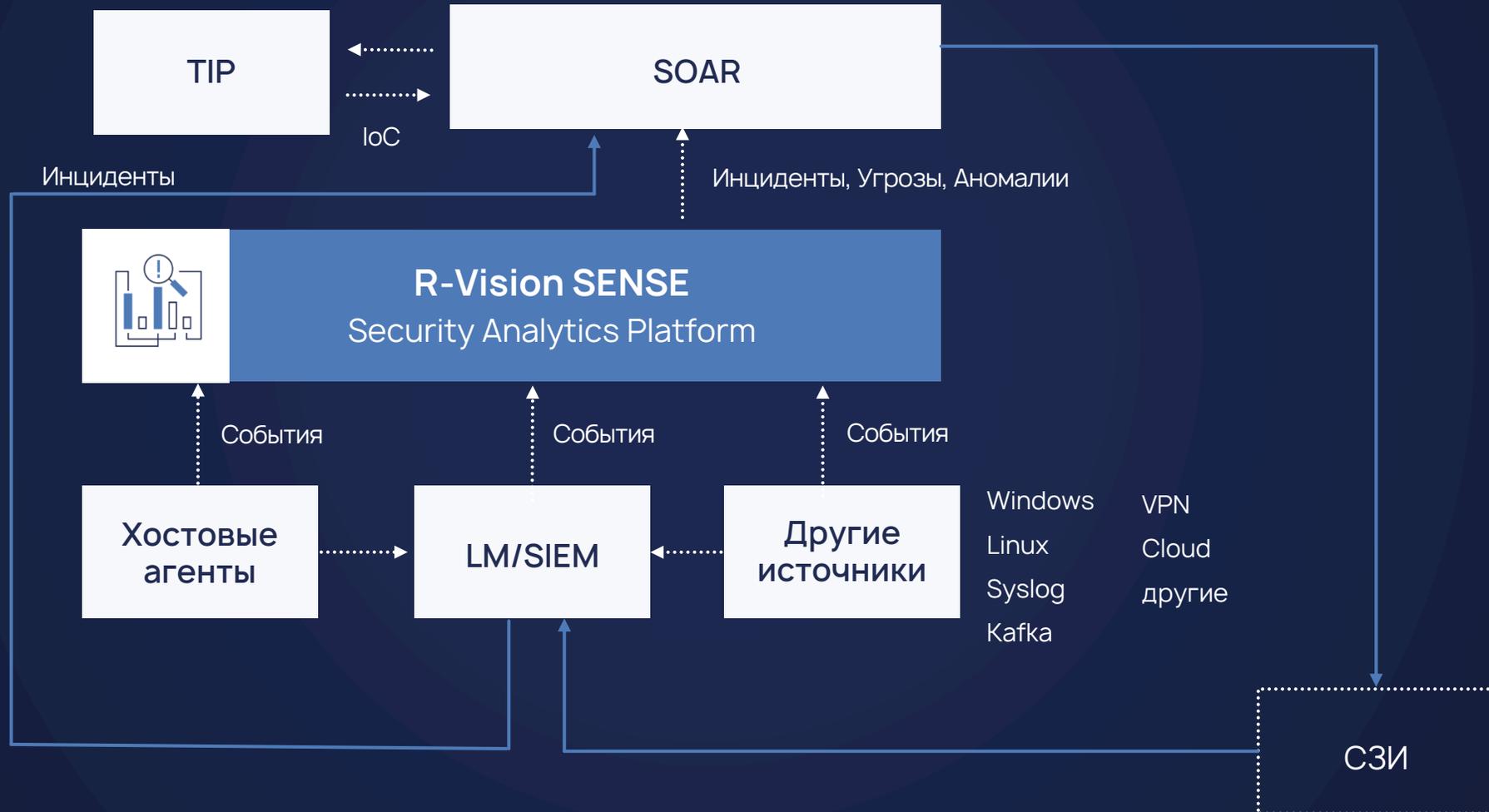


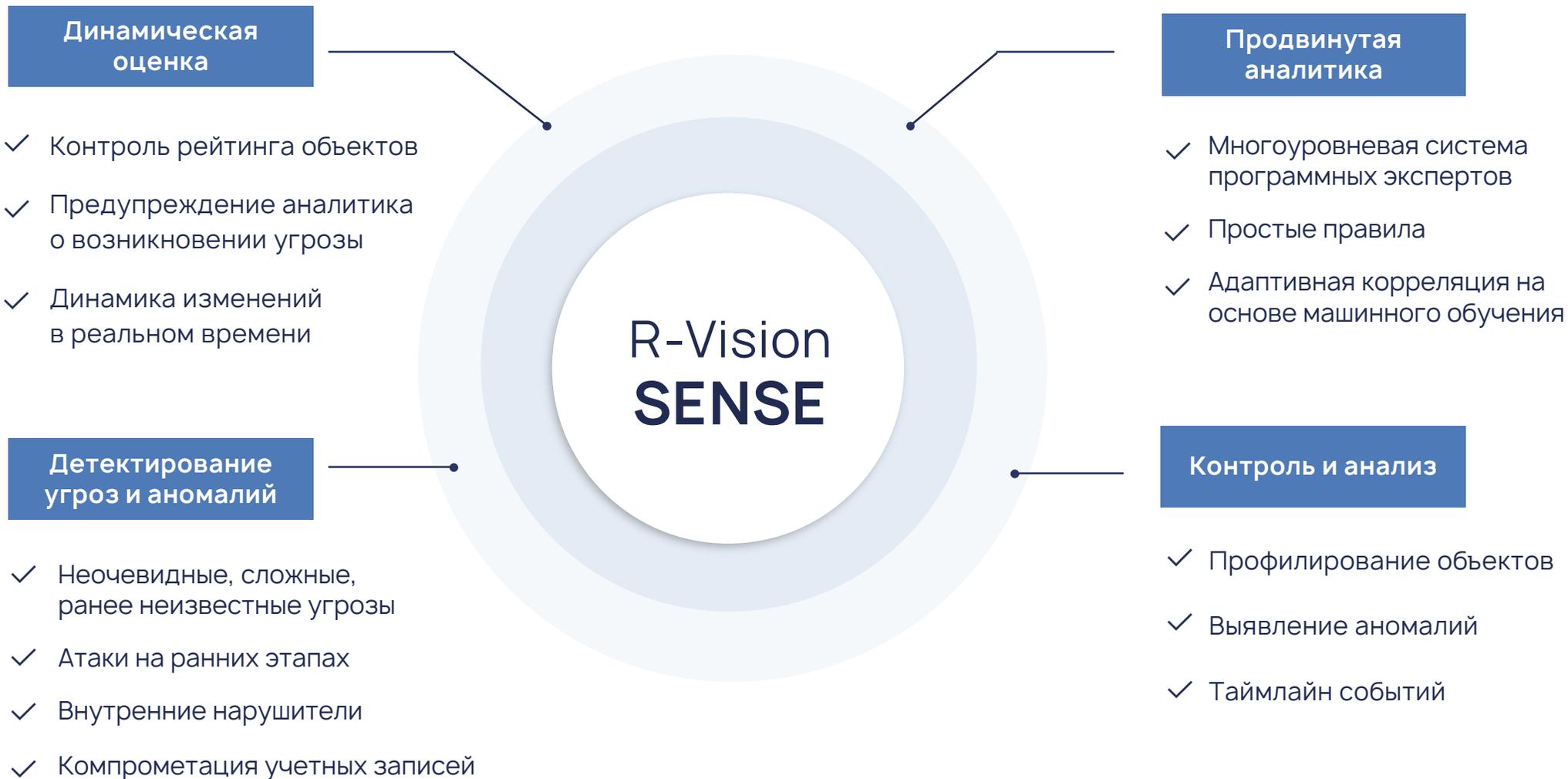
Схема работы



SENSE vs SIEM vs UEBA

	Решаемые задачи	SIEM	SENSE	UEBA
Сбор, хранение	Сбор сырых событий, логов	✓	✓	
	Хранение сырых событий	✓		
	Предобработка и выборка данных для хранения		✓	
	Универсальный формат представления данных	✓	✓	✓
	Обогащение контекстом, сбор данных из сторонних систем	✓	✓	✓
Инструменты анализа	Объектно-центричный анализ данных		✓	
	Детектирование на основе правил	✓	✓	✓
	Поведенческий анализ пользователей и объектов		✓	✓
	Адаптивная корреляция, самообучение инструментов анализа		✓	✓
	Скоринговая оценка аномалий, приоритизация угроз		✓	✓
	Визуализация хронологии всех событий по объекту на таймлайне			✓
	Отображение контекстного обогащения и изменений в динамике			✓

Ключевые возможности



Особенности R-Vision SENSE



Объектно-центричный подход к мониторингу состояния безопасности



Динамическая, скоринговая оценка угроз и аномалий для раннего предупреждения

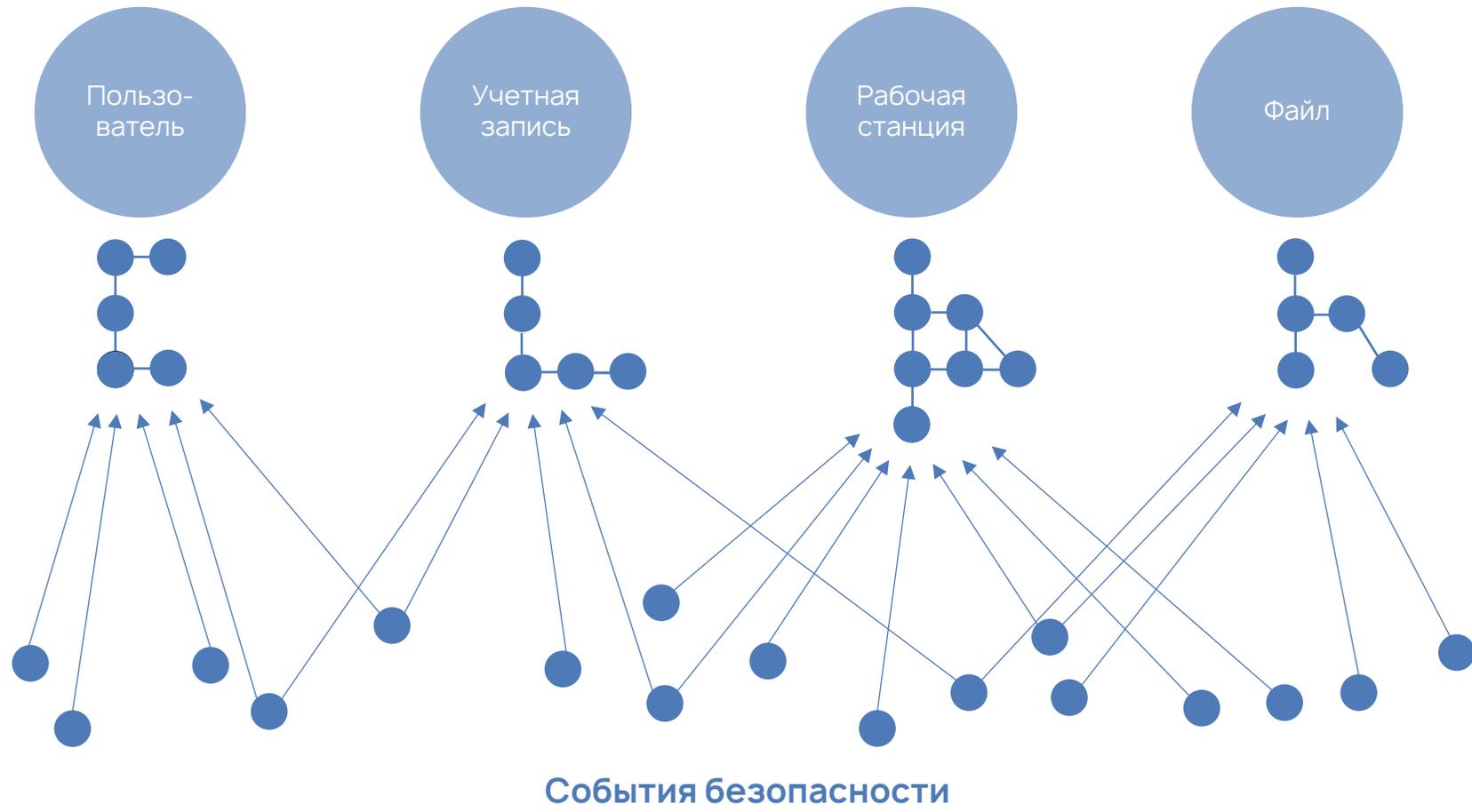


Технология адаптивной корреляции событий, требующая минимального участия со стороны пользователя



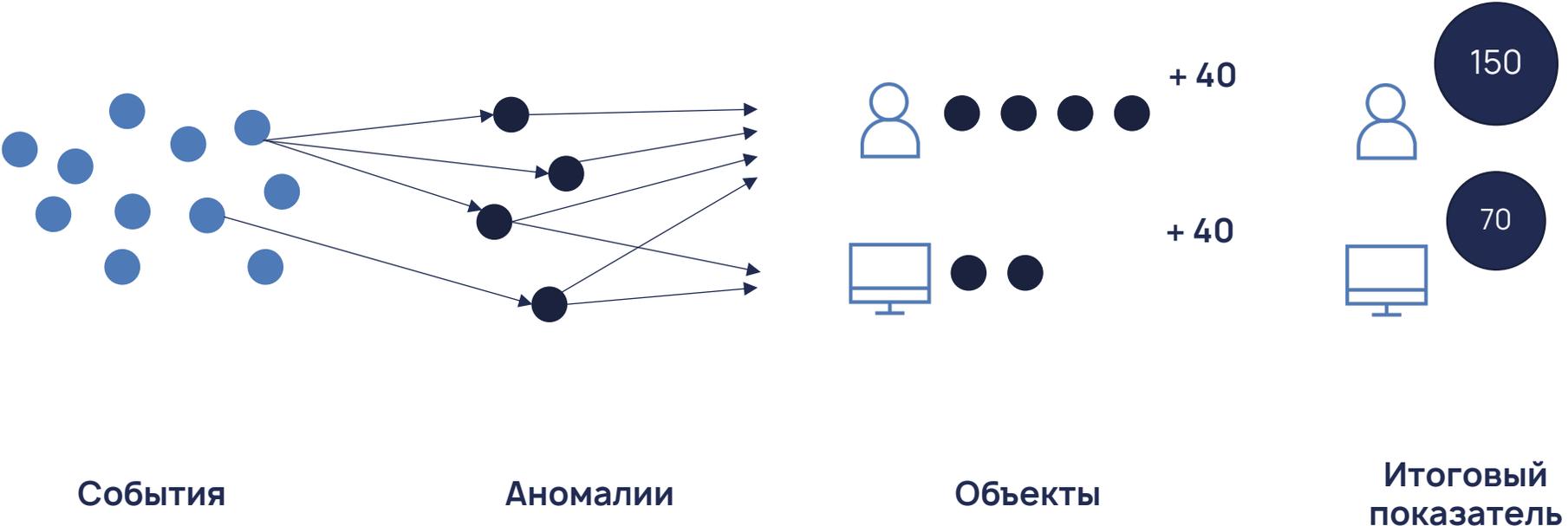
Многоуровневая система программных экспертов с возможностью тонкой настройки под специфические задачи

Объектно-центричная система

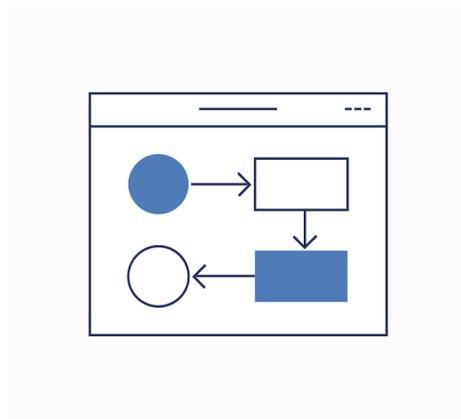


- Типы объектов
- 1. Пользователь
 - 2. Учетная запись
 - 3. Оборудование
 - 4. Файл
 - 5. Сервис
 - 6. Другие объекты

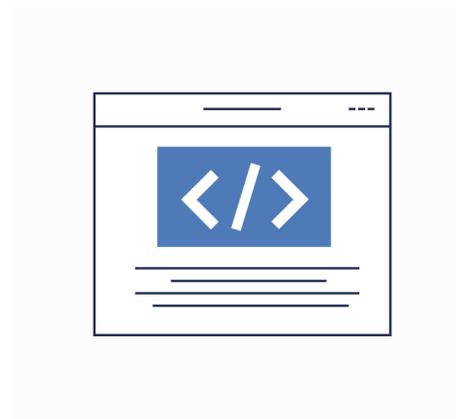
Скоринговая оценка



Инструменты анализа



Простые правила



Программные эксперты



- Поведенческий анализ
- Статистический анализ
- Методы машинного обучения

Программные эксперты



Анализ событий
авторизации



Мониторинг доступа
процессов к файлам



Мониторинг
почтового трафика



Определение DGA
и look-a-like доменов



Мониторинг
запуска процессов



Выявление аномалий
в соединениях VPN

Адаптивная корреляция R-Vision SENSE

заменяет целый набор правил в классических SIEM



- ✓ Универсальные представления
- ✓ Самообучение программных экспертов
- ✓ Поведенческий анализ
- ✓ Простой конструктор правил

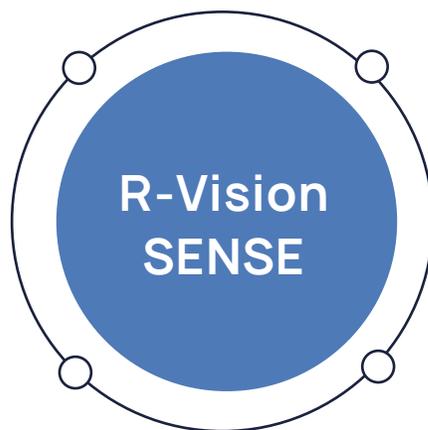
Преимущества R-Vision SENSE

Фокусировка на важном

Скоринговая оценка позволяет ограничить поток алертов в SENSE и отслеживать состояние инфраструктуры исходя из скорингового балла каждого объекта

Автоматическая адаптация новых источников

SENSE использует универсальный формат данных для анализа, что позволяет создавать набор правил корреляции, которые сами адаптируются и не зависят от источника данных



Адаптивная аналитика,

которая использует программных экспертов и простые правила позволяет заменить правила в SIEM и в автоматическом режиме перенастраивать и адаптировать аналитику

Оптимизация ресурсов при работе с данными

SENSE использует обработанные и структурированные данные на вход, что позволяет в разы увеличивать скорость аналитики

Результат

Обнаружение угроз на ранних этапах

Выявление отклонений в состоянии безопасности и признаков начинающейся атаки

Приоритизация для реагирования

Фокус на объектах с высоким рейтингом опасности и непрерывный контроль изменений

Снижение ложных срабатываний

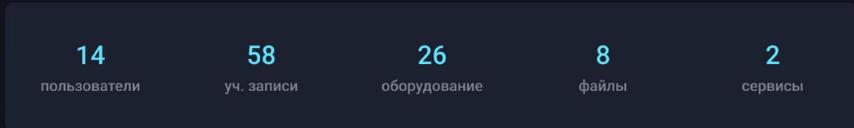
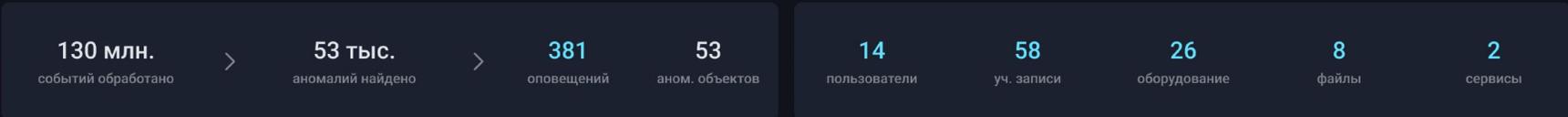
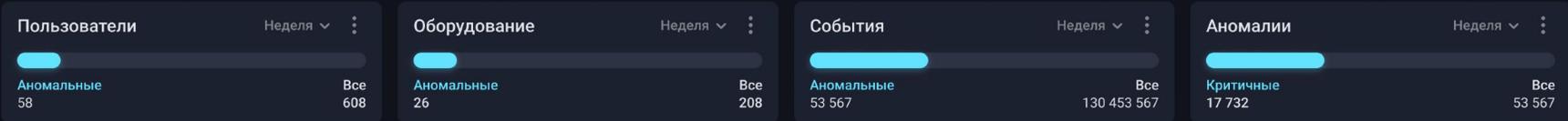
И выявление ранее недетектируемых атак за счет продвинутых аналитических инструментов

Упрощение анализа инцидентов

Визуализация аномалий на таймлайне, восстановление последовательности событий

- 🏠 Дашборд
- 👁️ Оповещения
- ☰ Простые правила
- 👁️ Объекты наблюдения
- ⚙️ Настройки

Добавить виджет | Добавить дашборд | Удалить дашборд | На весь экран



Новые уч. записи

Имя	Изменение рейтинга
1. Акименко Александр	385 ↑ 285
2. Коноплева Анастасия	320 ↑ 80
3. Кириллов Тимофей	180 ↓ 10
4. Тарабухин Игорь	110 ↓ 45

Примечательные уч. записи

Имя	Изменение сгора
1. Богословская Ирина	195 ↑ 125
2. Шишкин Дмитрий	25 ↓ 15
3. Никитин Павел	20 ↓ 0

Заблокированные уч. записи

Имя	Время блок-ки	Рейтинг
Варламов Никита	01.06.2020, 04:21	845
Потапов Антон	02.04.2020, 08:00	700
Колесникова Карина	12.04.2020, 08:12	590
Рогозин Иван	19.08.2020, 16:43	525
Краснокутский Михаил	23.07.2020, 21:48	410
Симонов Аркадий	08.09.2020, 19:10	225

Топ аномальных уч. записей

Имя	Изменение сгора
1. Краснокутский Михаил	845 ↑ 710
2. Потапов Антон	700 ↑ 690
3. Колесникова Карина	590 ↑ 560
4. Варламов Никита	525 ↑ 465
5. Богословская Ирина	410 ↑ 395
6. Рогозин Иван	225 ↑ 205
7. Симонов Аркадий	195 ↑ 180



← Свернуть

🏠 Дашборд

👁️ Оповещения

📄 Простые правила

👁️ Объекты наблюдения

⚙️ Настройки

Экспорт в XLS

Настройки

🔽 Фильтр

Пользователи

Учётные записи

Оборудование

Файлы

Сервисы

№	Имя	Описание	Общий скор
1	Рогозин Иван	DEV, Старший разработчик	540
2	Коноплева Анастасия	IT, Администратор	480
3	Кириллов Тимофей	IT, Младший аналитик	345
4	Краснокутский Михаил	HR, Менеджер по подбору	220
5	Симонов Аркадий	HR, Менеджер по подбору	190
6	Кривцова Марина	БУН, Главный бухгалтер	120
7	Пригожин Андрей	IT, Системный администратор	100
8	Колесникова Карина	IT, DevOps инженер	80
9	Архипов Виктор	БУН, Помощник бухгалтера	75
10	Иванов Александр	IT, Системный аналитик	60
11	Варламов Никита	IT, Системный администратор	50
12	Титовская Яна	IT, DevOps инженер	45
13	Еремёнко Илья	БУН, Помощник бухгалтера	30
14	Шишкин Дмитрий	IT, Системный аналитик	25
15	Богословская Ирина	БУН, Помощник бухгалтера	15
16	Чикитин Павел	IT, Системный аналитик	0

« < 1 из 134 > » 100 ▾

← Свернуть

[🏠 Дашборд](#)**[👁 Оповещения](#)**[☰ Простые правила](#)[👁 Объекты наблюдения](#)[⚙ Настройки](#)[Добавить](#)[Экспорт в XLS](#)[Настройки](#)[🔽 Фильтр](#)**Оповещения**[Правила оповещений](#)[Удалённые правила](#)

▼	Время, дата	▼	Тип объекта	▼	Имя объекта	▼	Уровень угрозы	▼	Правило	▼	Рейтинг/Лимит	▼
●	19:24:41, 05.06.2020	Пользователь	Рогозин Иван	●	Высокий	Превышение пользователем сгора в час	1000 из 500					
●	19:22:16, 05.06.2020	Оборудование	DB-SRV	●	Высокий	Превышение пользователем сгора в день	1500 из 900					
●	18:20:10, 05.06.2020	Пользователь	Коноплева Анастасия	●	Высокий	Превышение пользователем сгора в час	850 из 500					
●	18:14:00, 05.06.2020	Пользователь	Владимир Никифоров	●	Высокий	Превышение пользователем сгора в час	520 из 300					
●	17:24:11, 05.06.2020	Оборудование	EXC-RVN	●	Высокий	Превышение пользователем сгора в час	1060 из 500					
●	16:22:10, 05.06.2020	Оборудование	DB-SRV	●	Средний	Превышение пользователем сгора в день	1500 из 900					
●	15:11:56, 05.06.2020	Пользователь	Симонов Аркадий	●	Высокий	Превышение пользователем сгора в час	900 из 500					
●	14:50:33, 05.06.2020	Оборудование	DB-CRV	●	Средний	Превышение пользователем сгора в день	1000 из 900					
●	13:25:17, 05.06.2020	Пользователь	Варламов Никита	●	Средний	Превышение пользователем сгора в час	600 из 500					
	12:14:25, 05.06.2020	Оборудование	EXC-SRV	●	Средний	Превышение пользователем сгора в день	1050 из 900					
	12:12:01, 05.06.2020	Пользователь	Еремёнко Илья	●	Средний	Превышение пользователем сгора в час	660 из 500					
	11:38:42, 05.06.2020	Оборудование	DB-SRV	●	Средний	Превышение пользователем сгора в день	990 из 900					
	10:24:33, 05.06.2020	Пользователь	Богословская Ирина	●	Высокий	Превышение пользователем сгора в час	1000 из 500					
	10:23:53, 05.06.2020	Оборудование	DB-SRV	●	Средний	Превышение пользователем сгора в день	1800 из 900					
	09:24:11, 05.06.2020	Пользователь	Шишкин Дмитрий	●	Высокий	Превышение пользователем сгора в час	950 из 500					
	09:10:11, 05.06.2020	Оборудование	EXC-SRV	●	Средний	Превышение пользователем сгора в день	1100 из 900					

« < 1 из 134 > » 100 ▼

[← Свернуть](#)**Оповещение ID12345677890** [✕](#)**Правило оповещения****Имя** Превышение пользователем рейтинга в час**Описание** Оповещение срабатывает когда рейтинг объекта типа пользователь в интервал 1 час превышает значение в 300 баллов**Уровень угрозы** Высокий**Баллы/Лимит** 520/300**Время, Дата** 18:14:00, 05.06.2020**Объект наблюдения****Тип объекта** Пользователь**ID объекта** **P14938192****Имя** **Владимир Никифоров****Описание** DEV, Менеджер**Статистика аномалий**

Тип	Срабатывания	Баллы
Новый процесс на хосте	11	220
Новый для пользов-ля процесс	10	170
Неуспешные попытки входа	5	40
Нестандартный источник входа	3	45

🏠 Дашборд

👁️ Оповещения

📄 Простые правила

👁️ Объекты наблюдения

⚙️ Настройки

🔽 Фильтр

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%
Неуспешные попытки входа	10%
Нестандартный источник входа	8%
Нестандартное время входа	8%

Таймлайн За всё время

Сегодня

23:12:05 ○ **Удаленный вход на DB-SRV** + 50 ^

ip-адрес источника	80.20.73.144
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

Первый удаленный вход + 20 ^

Тип аномалии	Нестандартный тип входа
Описание	Первый вход с типом входа 3 (Remote) для пользователя vnikiforov
Детектор	Эксперт Logon Activity

[Объяснение](#)

Нестандартное время входа + 15 ^

Тип аномалии	Нестандартное время входа
Описание	Нестандартное время входа пользователя vnikiforov : Вс, 04:02

Объяснение

Аномалия Нестандартное время входа

Тип аномалии Нестандартное время



← Свернуть

Карточка объекта

🗑️ Дашборд

👁️ Оповещения

📄 Простые правила

👁️ Объекты наблюдения

⚙️ Настройки

🔽 Фильтр

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



ТОП-5 аномалий За всё время

Новый процесс на хосте	20%
Новый для пользователя процесс	20%
Неуспешные попытки входа	10%
Нестандартный источник входа	8%
Нестандартное время входа	8%

Таймлайн За всё время

Сегодня

23:12:05	Удаленный вход на DB-SRV	+ 50	Первый удаленный вход	+ 20
			Нестандартное время входа	+ 15
			Удаленный доступ к критическому оборудованию	+ 15
	Запуск 1cestart.exe			
20:02:08	Запуск chrome.exe			
17:40:12	Удаленный вход на ExchangeServer	+ 35	Первый удаленный вход	+ 20

Запуск редкого процесса

Аномалия Первый удаленный вход на DB-SRVТип аномалии Редкое событие

19	powershell.exe	0,18% (2)
21	cmd.exe	0,09% (1)
20	iexplorer.exe	0,18% (2)
19	powershell.exe	0,18% (2)
18	cuguuu.exe	0,18% (2)
17	printserver.exe	0,36% (4)
16	screenrecorder.exe	0,36% (4)
15	paint.exe	0,45% (5)
14	WordPad.exe	0,54% (6)
13	SnippingTool.exe	0,54% (6)
12	conhost.exe	0,72% (7)
11	calc.exe	0,97% (10)
10	excel.exe	2,04% (23)
9	powerpoint.exe	3,65% (41)
8	notepad.exe	4,72% (53)

Карточка объекта

R-Vision

 + 7 (499) 322 80 40

 sales@rvision.pro

 www.rvision.pro

Подписывайтесь на наш дайджест ИБ:
rvision.pro/blog