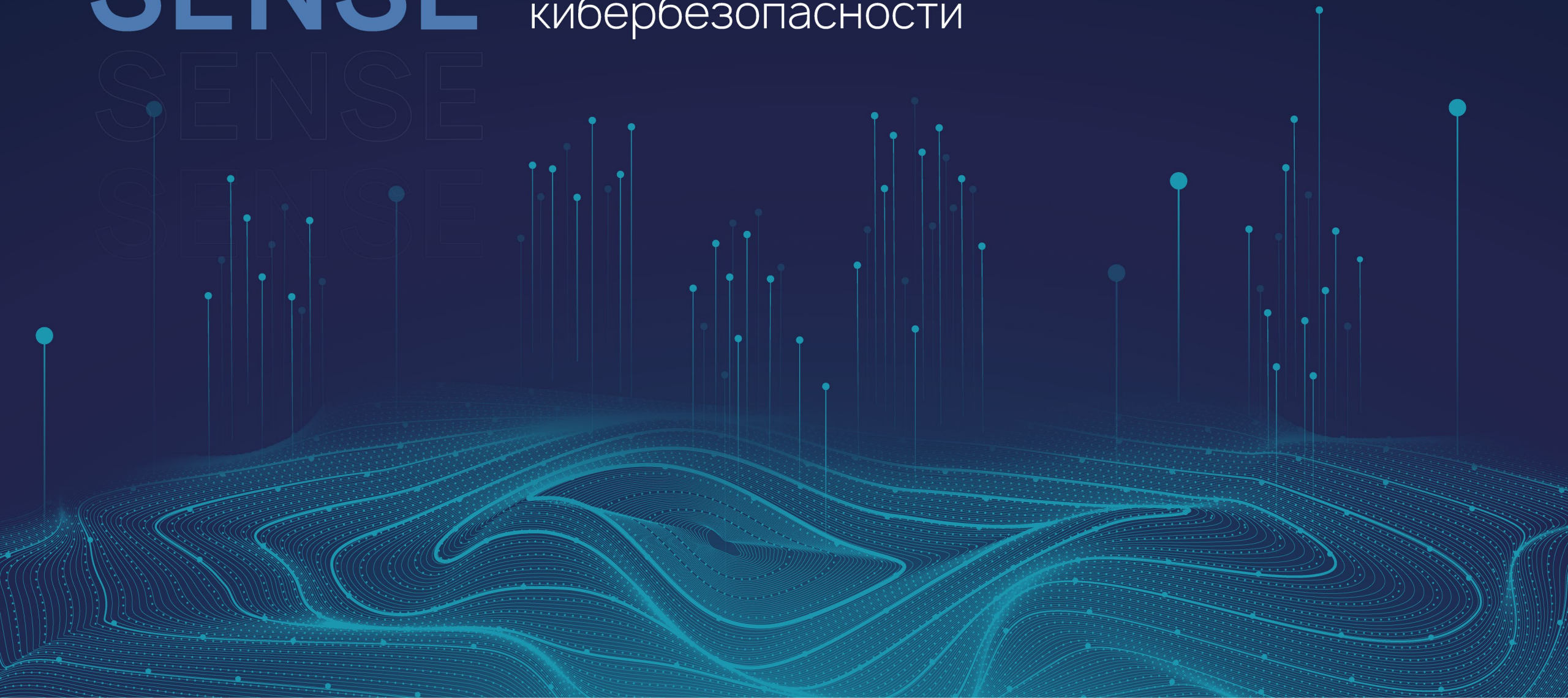
R-Vision

SENSE

Аналитическая платформа кибербезопасности



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

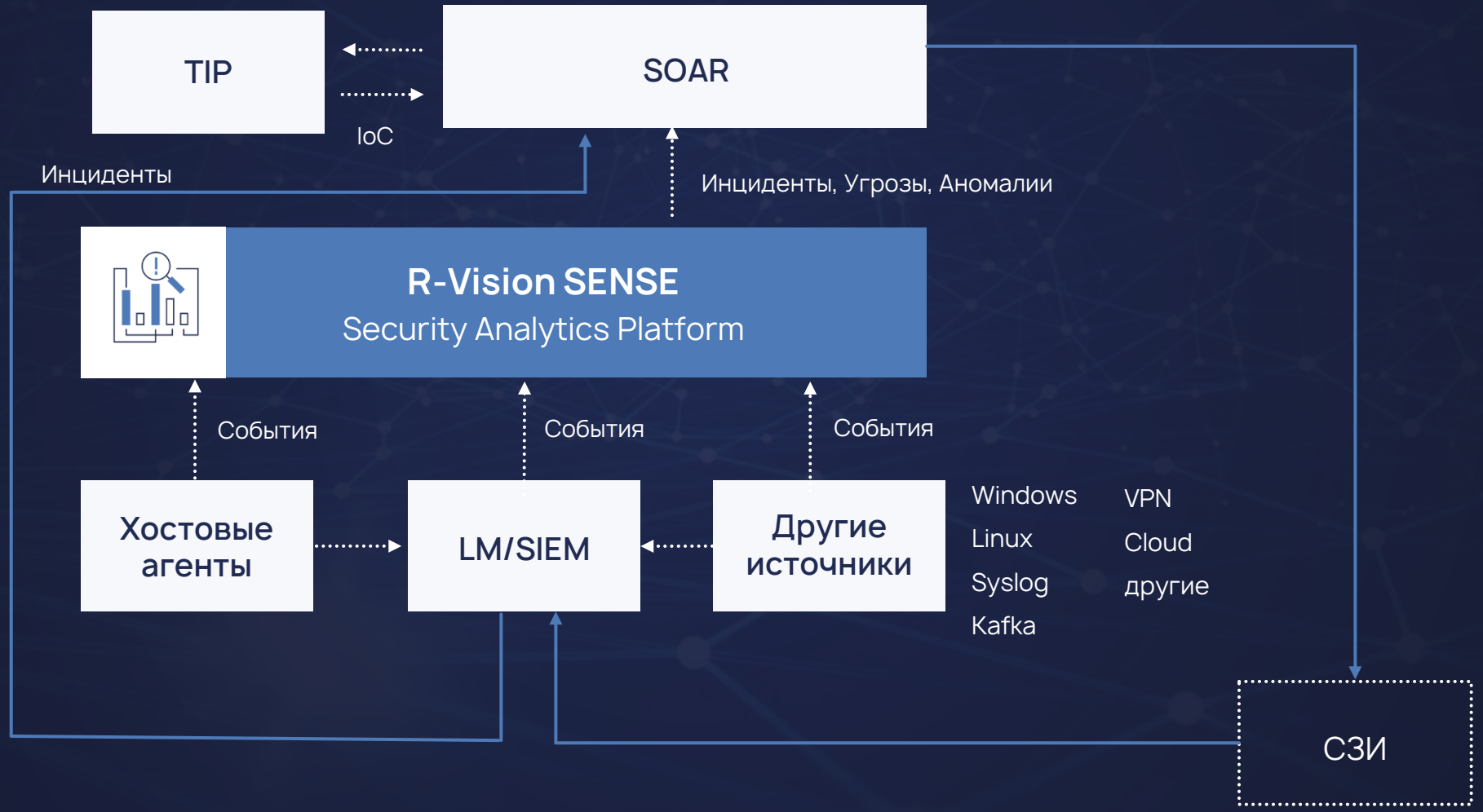
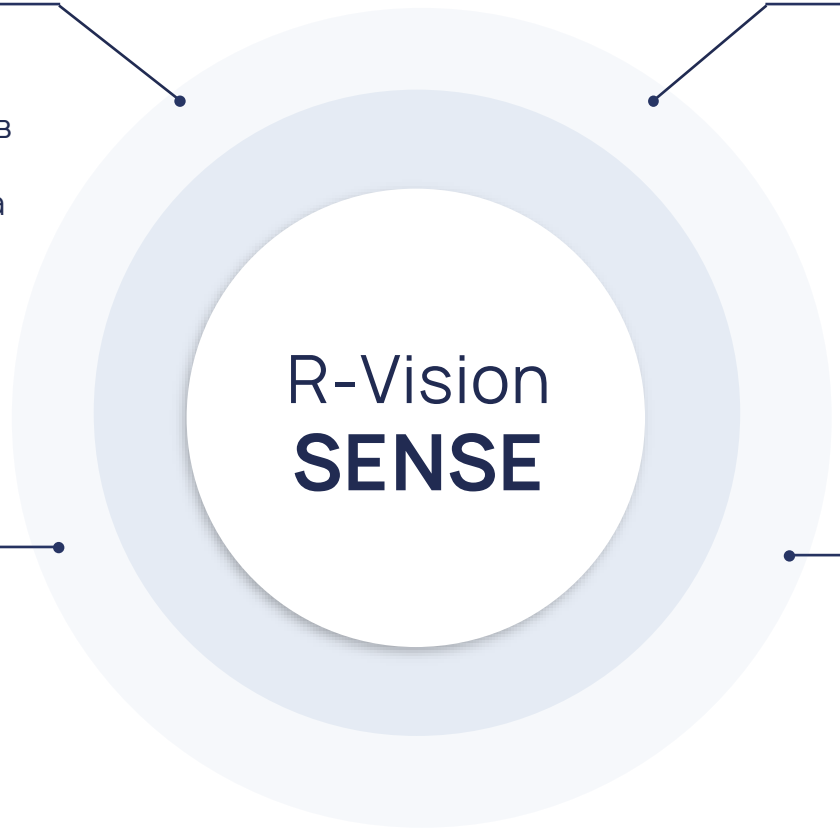


Схема работы

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



Динамическая оценка

- Контроль рейтинга объектов
- Предупреждение аналитика о возникновении угрозы
- Динамика изменений в реальном времени

Продвинутая аналитика

- Многоуровневая система программных экспертов
- Простые правила
- Адаптивная корреляция на основе машинного обучения

Детектирование угроз и аномалий

- Неочевидные, сложные, ранее неизвестные угрозы
- Атаки на ранних этапах
- Внутренние нарушители
- Компрометация учетных записей

Контроль и анализ

- Профилирование объектов
- Выявление аномалий
- Таймлайн событий

Особенности R-Vision SENSE

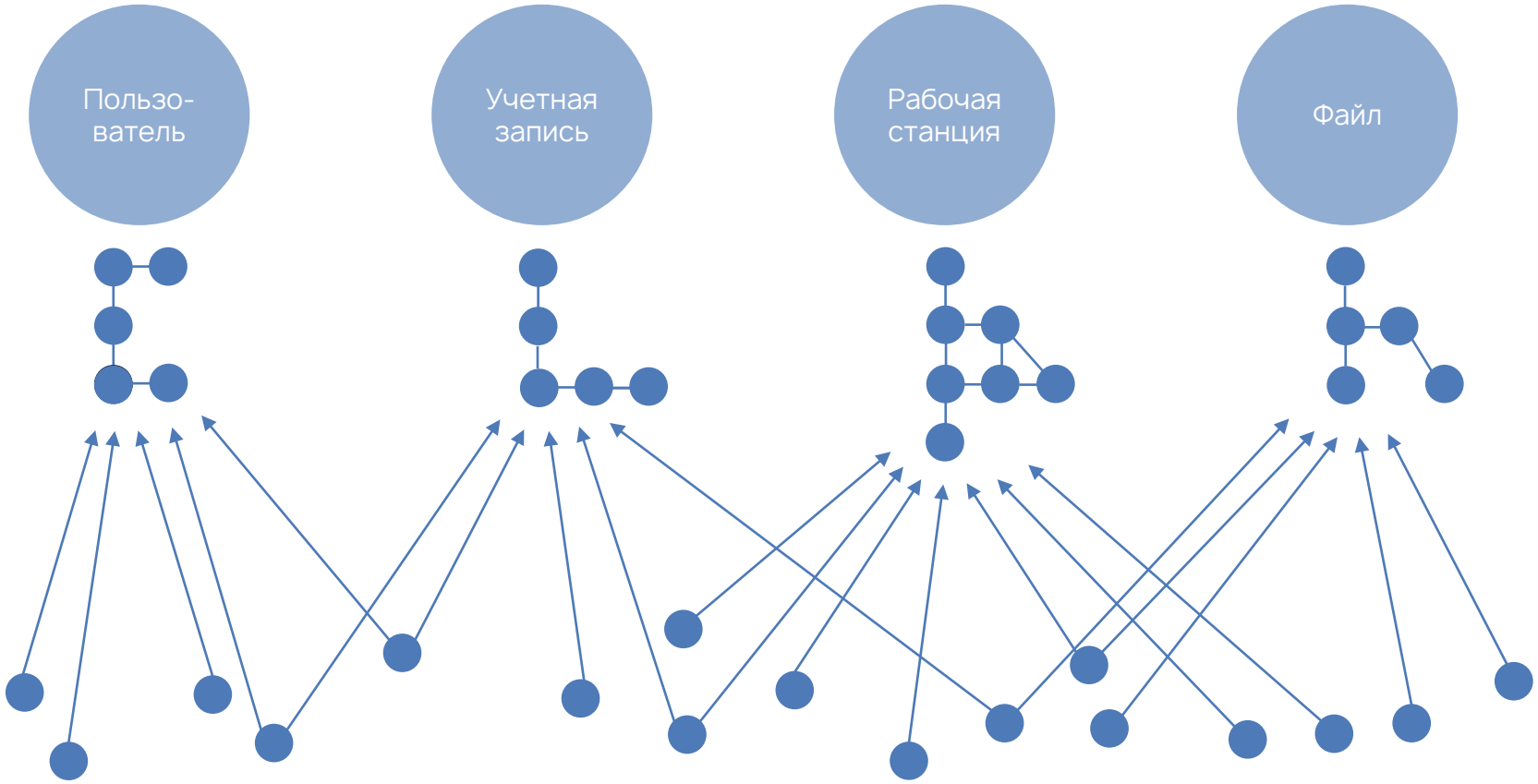
Объектно-центричный подход к мониторингу состояния безопасности

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

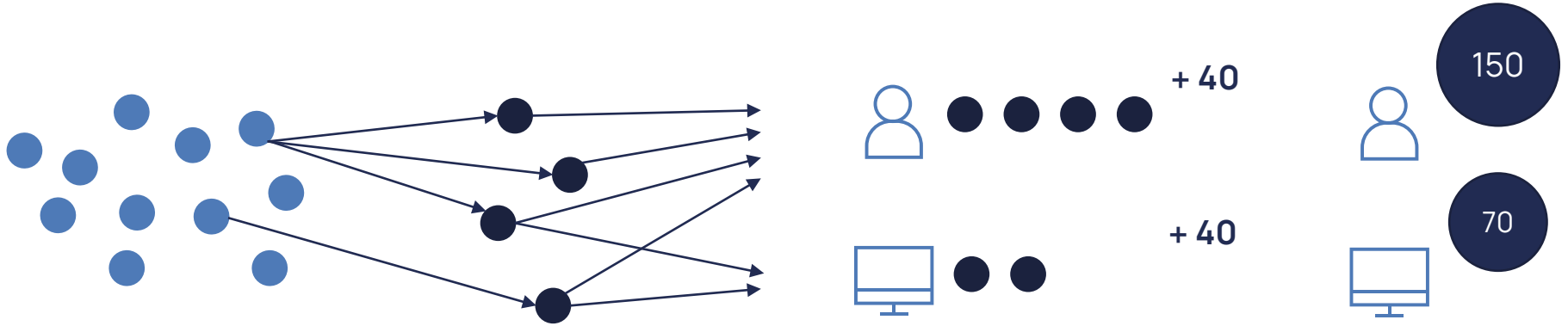
Объектно-центричная система



Типы объектов

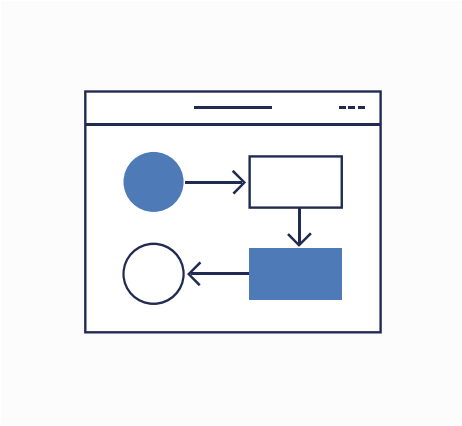
1. Пользователь
2. Учетная запись
3. Оборудование
4. Файл
5. Сервис
6. Другие объекты

Скоринговая оценка

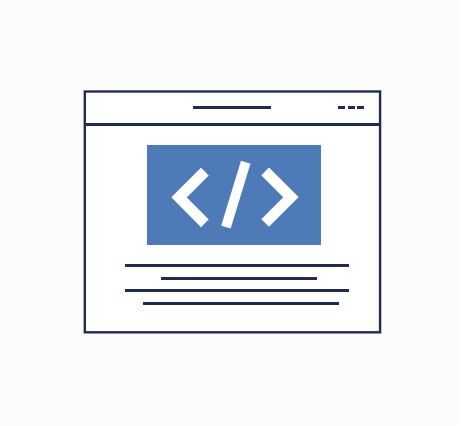


События **Аномалии** **Объекты** **Итоговый показатель**

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

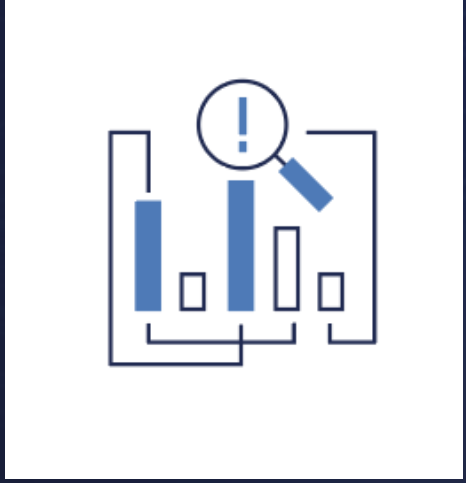
Определение DGA и look-a-like доменов

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

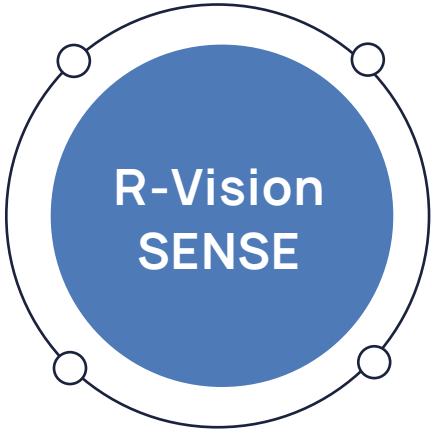
Преимущества R-Vision SENSE

Фокусировка на важном

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

Адаптивная аналитика,

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

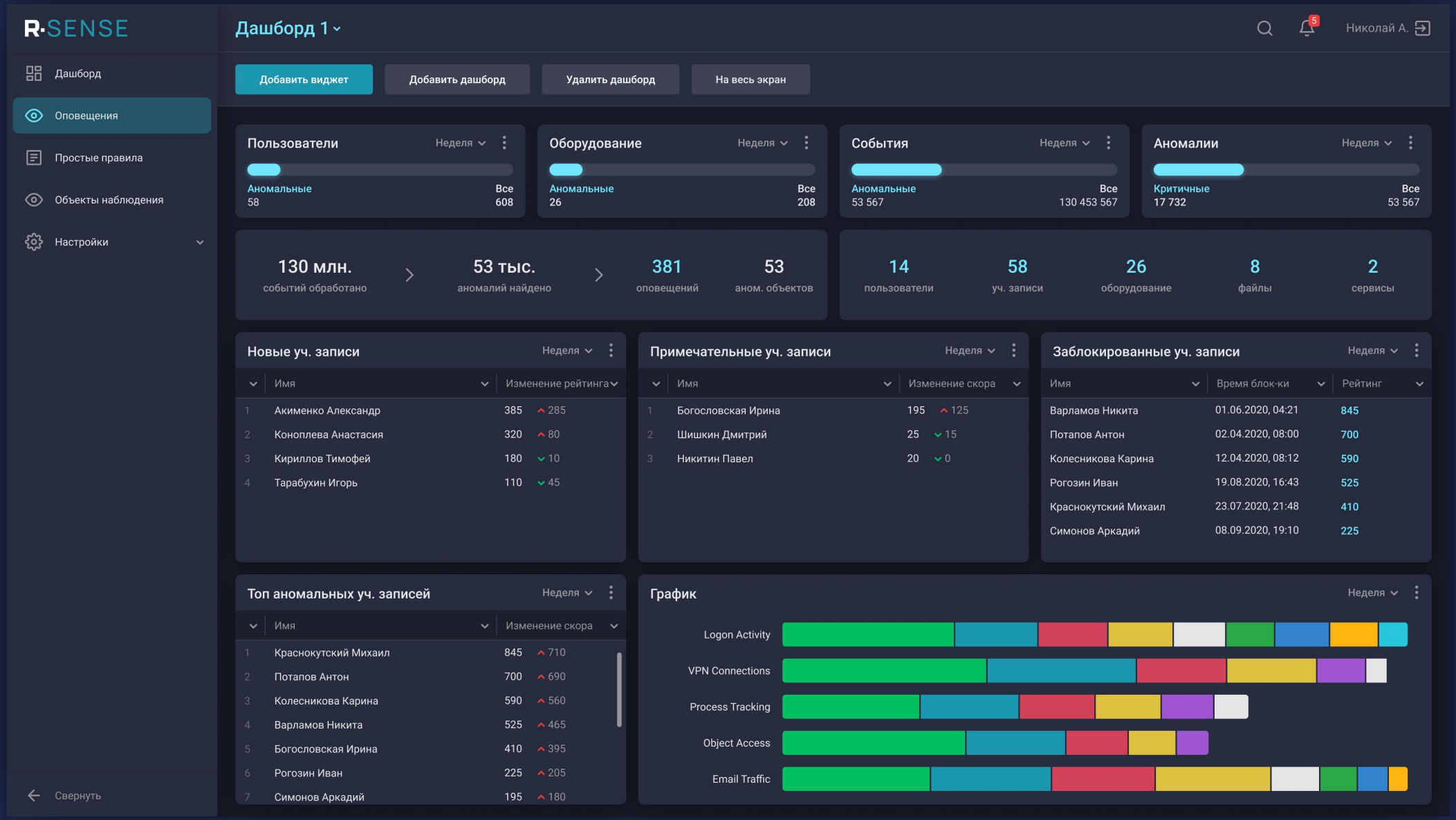


Автоматическая адаптация новых источников

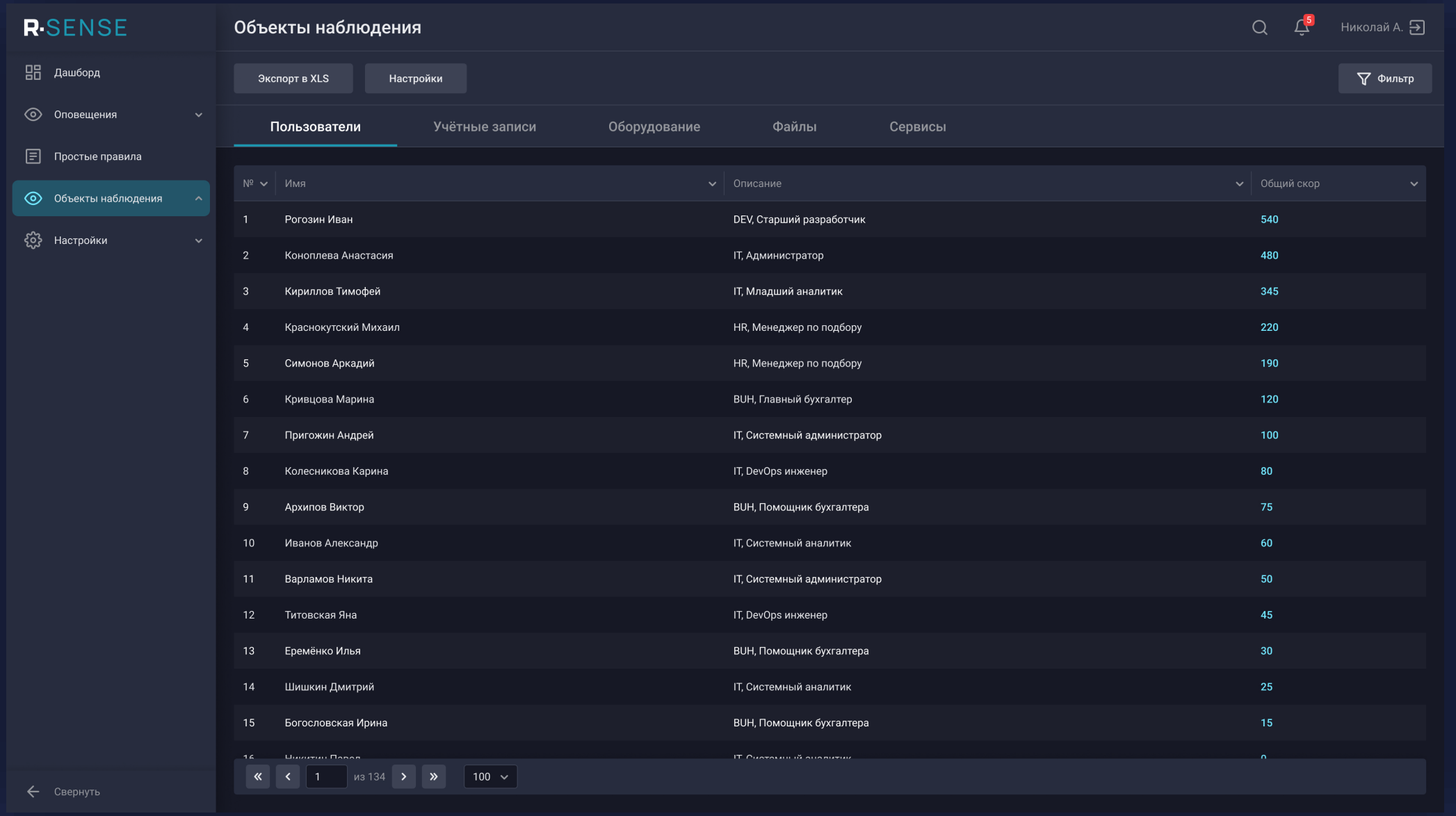
SENSE использует универсальный формат данных для анализа, что позволяет создавать набор правил корреляции, которые сами адаптируются и не зависят от источника данных

Оптимизация ресурсов при работе с данными

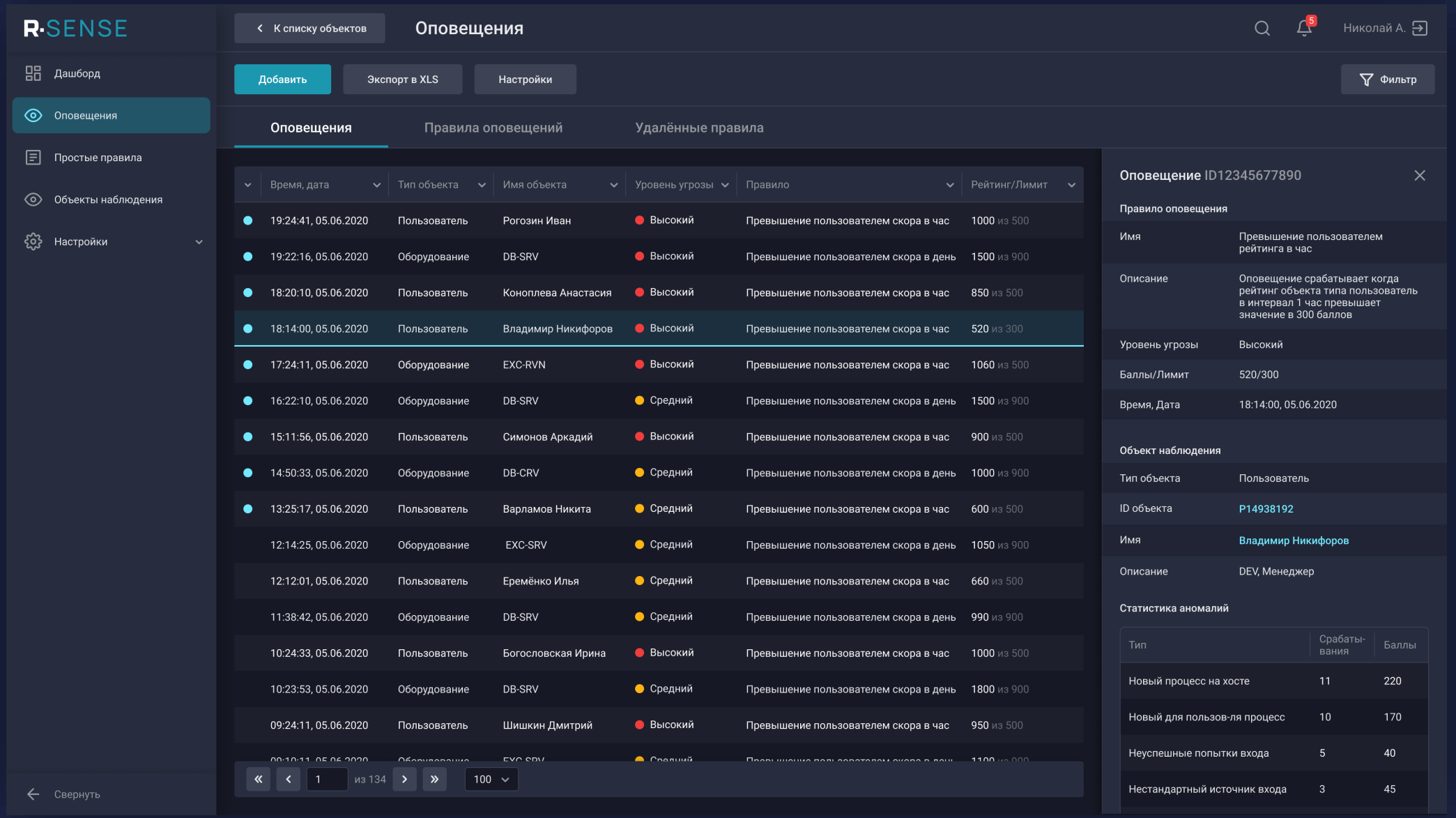
SENSE использует обработанные и структурированные данные на вход, что позволяет в разы увеличивать скорость аналитики


R-SENSE
Дашборд
Оповещения
Простые правила
Объекты наблюдения
Настройки
Свернуть
Дашборд 1
Николай А.
Добавить виджет
Добавить дашборд
Удалить дашборд
На весь экран
Пользователи
Неделя
Аномальные
58
Все
608
Оборудование
Неделя
Аномальные
26
Все
208
События
Неделя
Аномальные
53 567
Все
130 453 567
Аномалии
Неделя
Критичные
17 732
Все
53 567
130 млн.
событий обработано
53 тыс.
аномалий найдено
381
оповещений
53
аном. объектов
14
пользователи
58
уч. записи
26
оборудование
8
файлы
2
сервисы
Новые уч. записи
Неделя
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
Неделя
Имя
Изменение скора
1 Богословская Ирина 195 125
2 Шишкин Дмитрий 25 15
3 Никитин Павел 20 0
Заблокированные уч. записи
Неделя
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
Неделя
Имя
Изменение скора
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
График
Неделя
Logon Activity
VPN Connections
Process Tracking
Object Access
Email Traffic

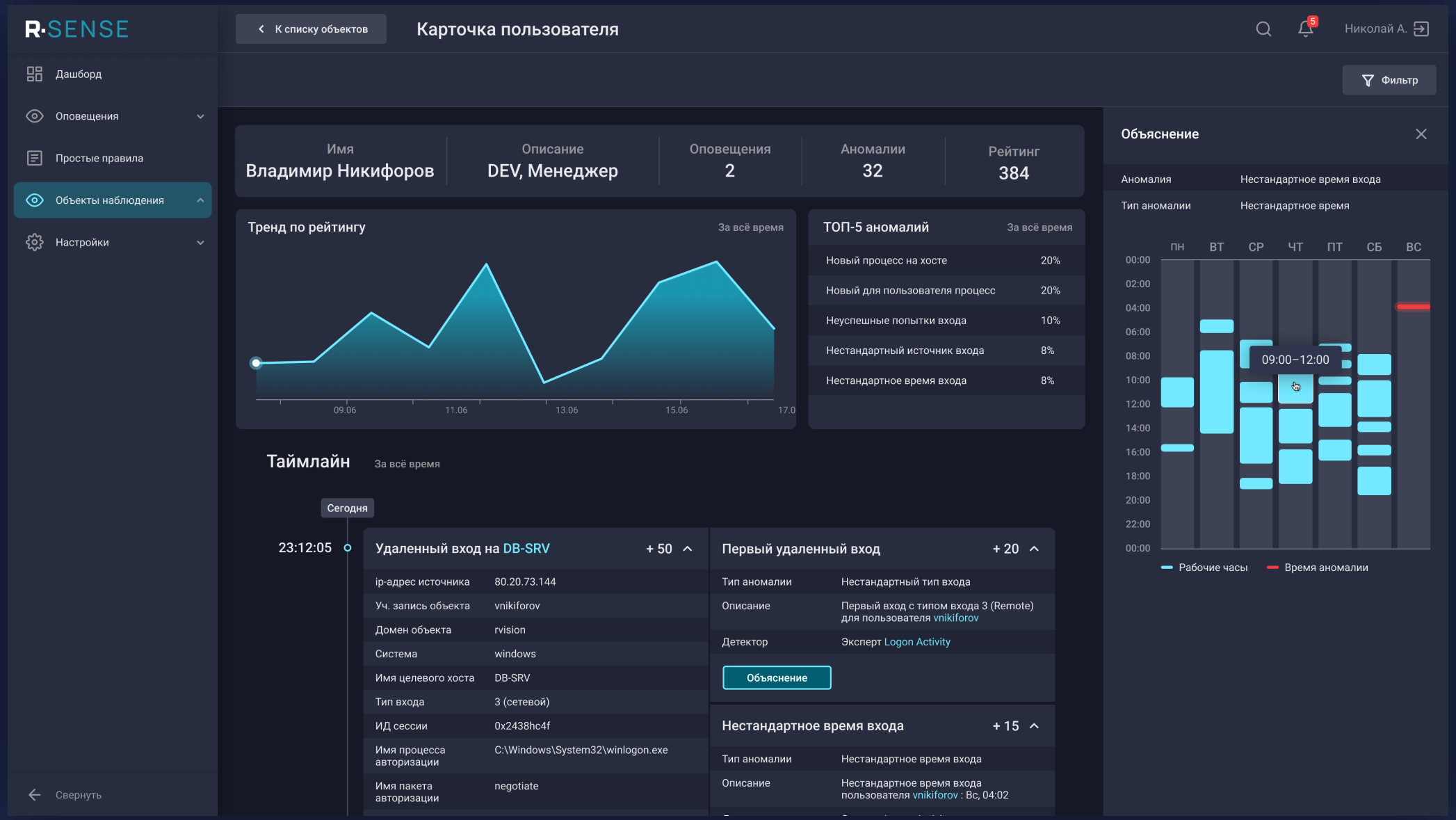
Дашборд



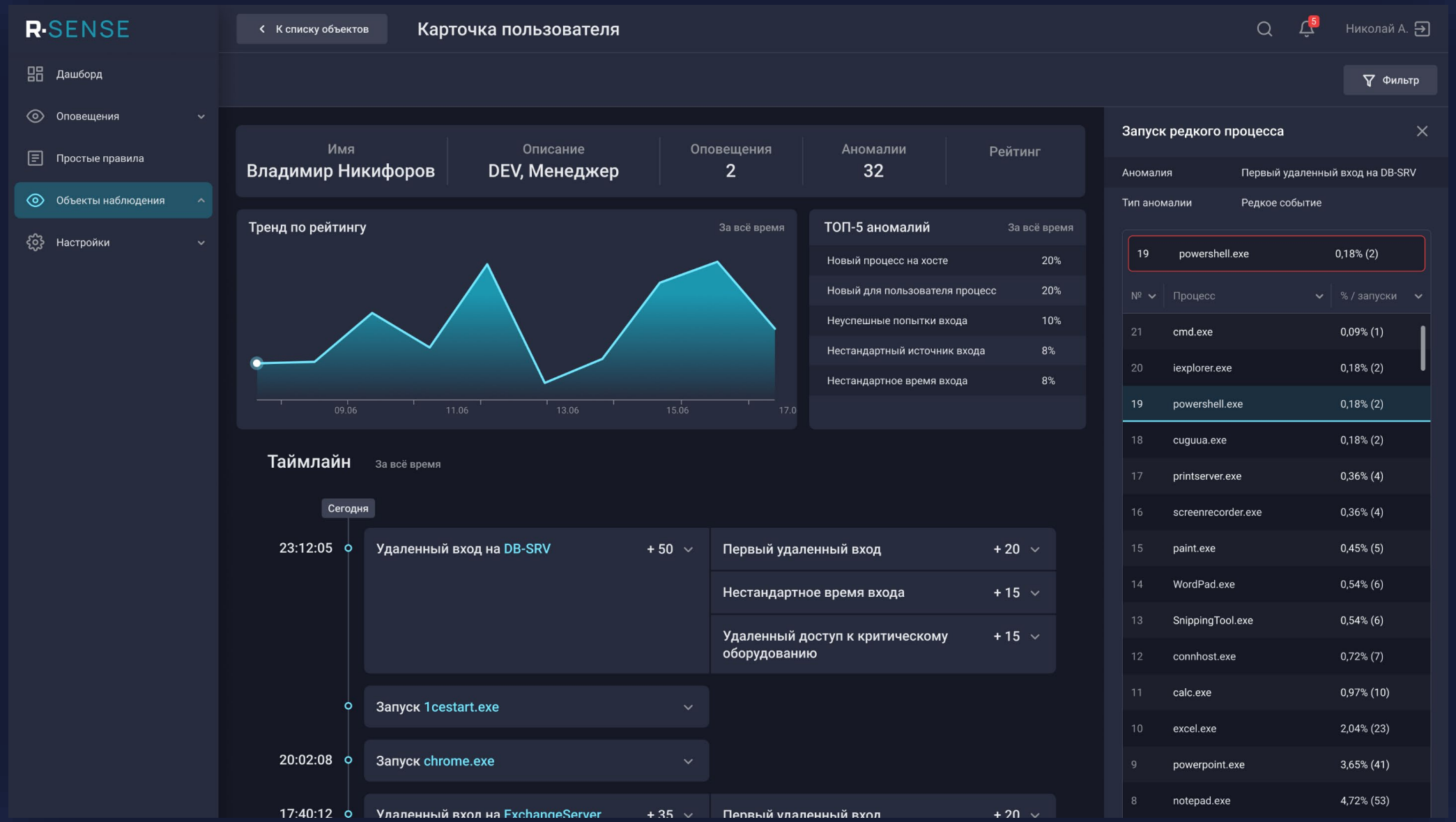
Объекты наблюдения


R·SENSE
Дашборд
Оповещения
Простые правила
Объекты наблюдения
Настройки
Свернуть
К списку объектов
Оповещения
Николай А.
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 скора в час 1000 из 500
19:22:16, 05.06.2020 Оборудование DB-SRV Высокий Превышение пользователем скора в день 1500 из 900
18:20:10, 05.06.2020 Пользователь Коноплева Анастасия Высокий Превышение пользователем скора в час 850 из 500
18:14:00, 05.06.2020 Пользователь Владимир Никифоров Высокий Превышение пользователем скора в час 520 из 300
17:24:11, 05.06.2020 Оборудование EXC-RVN Высокий Превышение пользователем скора в час 1060 из 500
16:22:10, 05.06.2020 Оборудование DB-SRV Средний Превышение пользователем скора в день 1500 из 900
15:11:56, 05.06.2020 Пользователь Симонов Аркадий Высокий Превышение пользователем скора в час 900 из 500
14:50:33, 05.06.2020 Оборудование DB-CRV Средний Превышение пользователем скора в день 1000 из 900
13:25:17, 05.06.2020 Пользователь Варламов Никита Средний Превышение пользователем скора в час 600 из 500
12:14:25, 05.06.2020 Оборудование EXC-SRV Средний Превышение пользователем скора в день 1050 из 900
12:12:01, 05.06.2020 Пользователь Еремёнко Илья Средний Превышение пользователем скора в час 660 из 500
11:38:42, 05.06.2020 Оборудование DB-SRV Средний Превышение пользователем скора в день 990 из 900
10:24:33, 05.06.2020 Пользователь Богословская Ирина Высокий Превышение пользователем скора в час 1000 из 500
10:23:53, 05.06.2020 Оборудование DB-SRV Средний Превышение пользователем скора в день 1800 из 900
09:24:11, 05.06.2020 Пользователь Шишкин Дмитрий Высокий Превышение пользователем скора в час 950 из 500
1 из 134
100
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
Срабаты-вания
Баллы
Новый процесс на хосте 11 220
Новый для пользов-ля процесс 10 170
Неуспешные попытки входа 5 40
Нестандартный источник входа 3 45

Оповещения



Карточка объекта



Карточка объекта

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

R-Vision

+ 7 (499) 322 80 40

sales@rvision.ru

www.rvision.ru

Подписывайтесь на наш дайджест ИБ: **rvision.ru/blog**