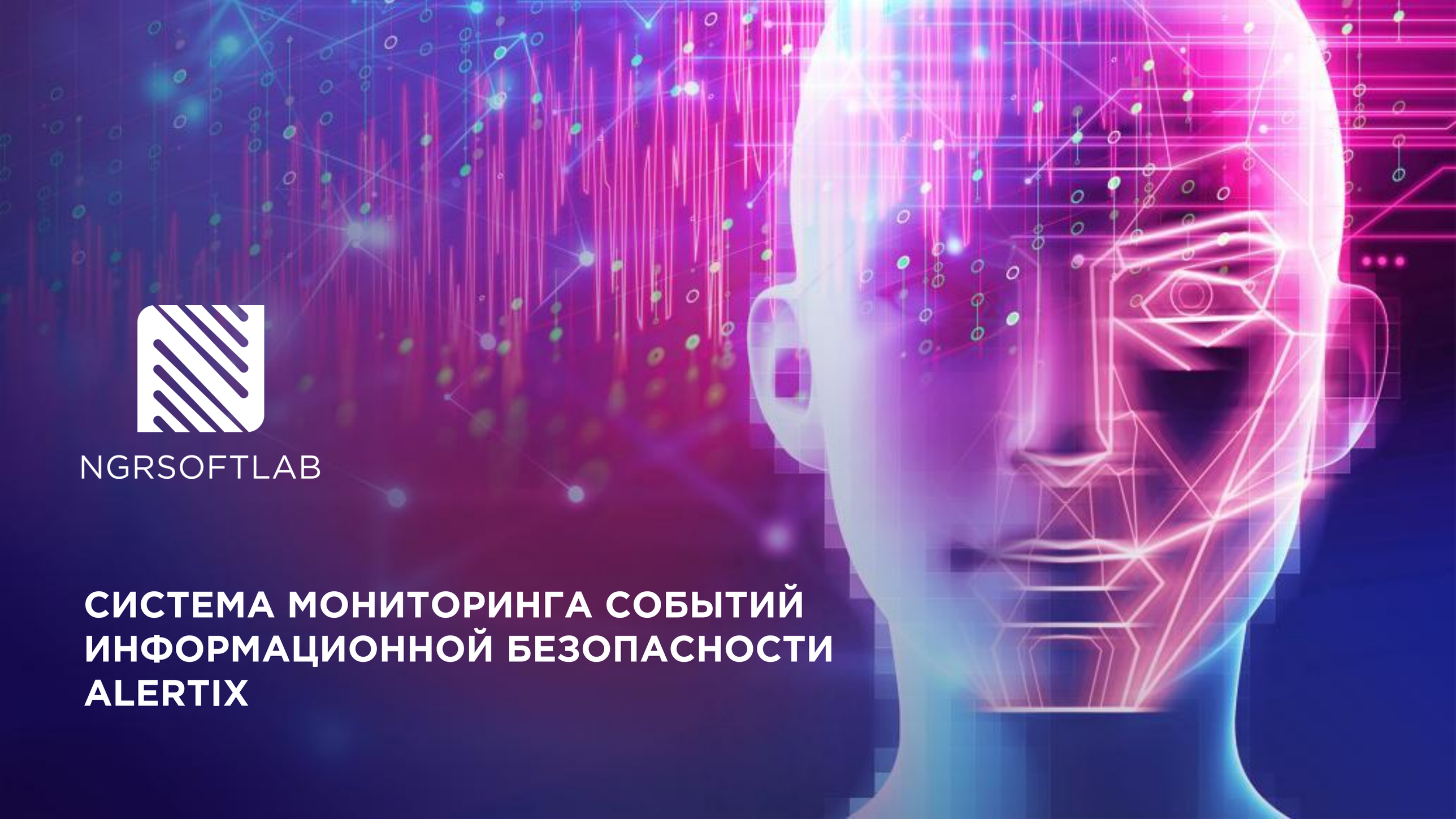


NGRSOFTLAB

СИСТЕМА МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ALERTIX

О компании

NGR Softlab — российский разработчик средств обработки и анализа данных, роботизации бизнес-процессов и решений в области информационной безопасности.

- Нацелена на создание современных и технологичных продуктов.
- R&D и производство расположены в России и ориентированы на российского потребителя.

ЭКОСИСТЕМА ПРОДУКТОВ NGR SOFTLAB
Синергия и расширение функционала

Alertix – максимально сбалансированный по соотношению польза/стоимость владения инструмент, обеспечивающий действительно быстрый поиск для осуществления расследования.

Alertix может использоваться как отдельный инструмент, так и в составе экосистемы продуктов NGR Softlab:

- Аналитическая платформа Dataplan
- Комплексная система управления привилегированным доступом Infrascope

ALERTIX ИСТОРИЯ РАЗВИТИЯ
Инструмент, созданный для аналитиков

ДЛЯ ЧЕГО СЕЙЧАС НУЖЕН SIEM

SIEM - ядро процесса мониторинга, для полноценного обеспечения которого необходима масса дополнительных средств: IRP\SOAR системы, ITAM\CMDB средства, сканеры уязвимостей и модули подключения к регуляторам.

ГосСОПКА
187-ФЗ,
ФинЦЕРТ,
ГОСТ 57580

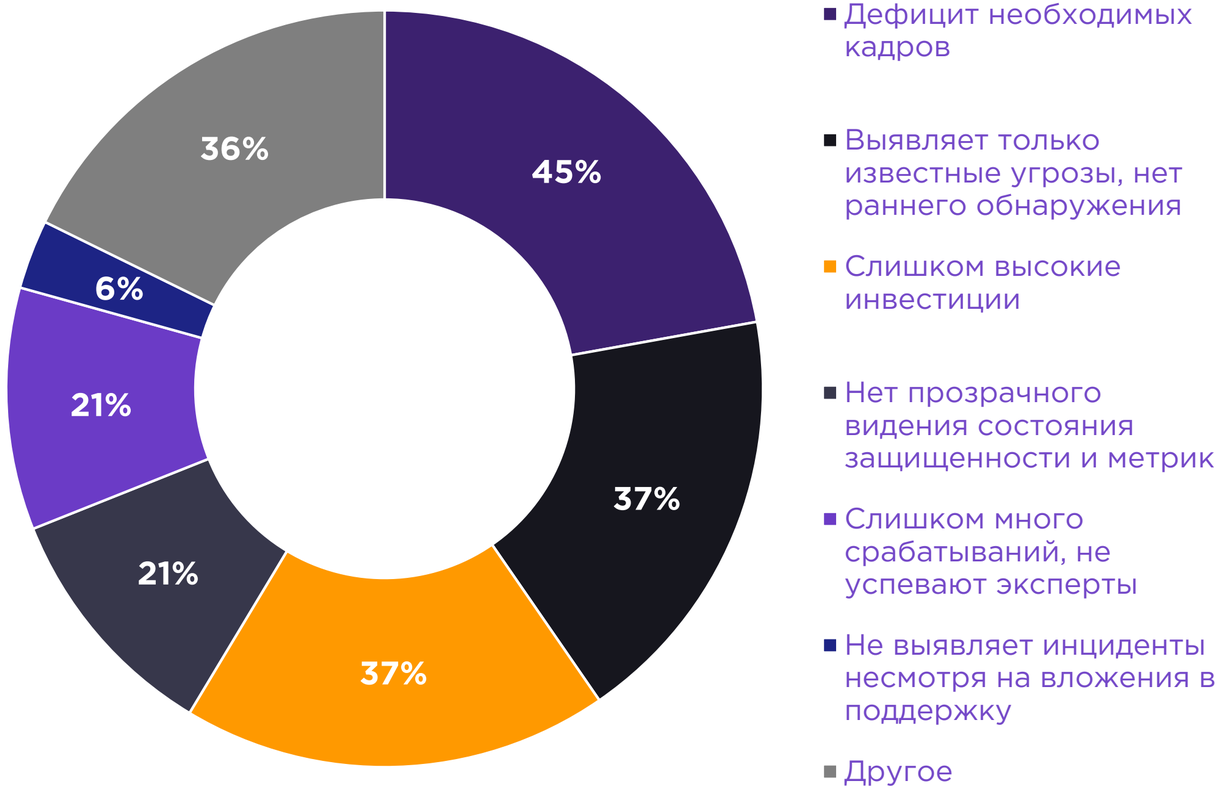
500 EPS
это **1,5 Тб**
данных в
месяц

Более **20%**
угроз не
могут быть
выявлены
сигнатурами

60%
времени
аналитика –
поиск
информации

ПРОБЛЕМАТИКА ЭКСПЛУАТАЦИИ SIEM

SIEM стал стандартным инструментом для компаний, достигших зрелости в понимании значимости ИБ. Вместе с тем, его эффективность не всегда оправдывает вложения. По данным исследования IDC, основными причинами недовольства используемой SIEM в России являлись:



Дополнительно отмечались:

- Недостаточно быстрая реакция SIEM
- Трудности настройки системы
- Нехватка функциональности и негибкость вендора при запросах на изменения

Решаемые проблемы

- Уведомление регуляторов об инцидентах
- Выполнение требований законодательства в области КИИ
- Выполнение требований стандартов для финансовых организации

Соответствие требованиям регуляторов

- Учет инвентаризационной информации об информационных активах
- Учет и управление жизненным циклом атак и инцидентов ИБ

Учет ИТ активов и инцидентов

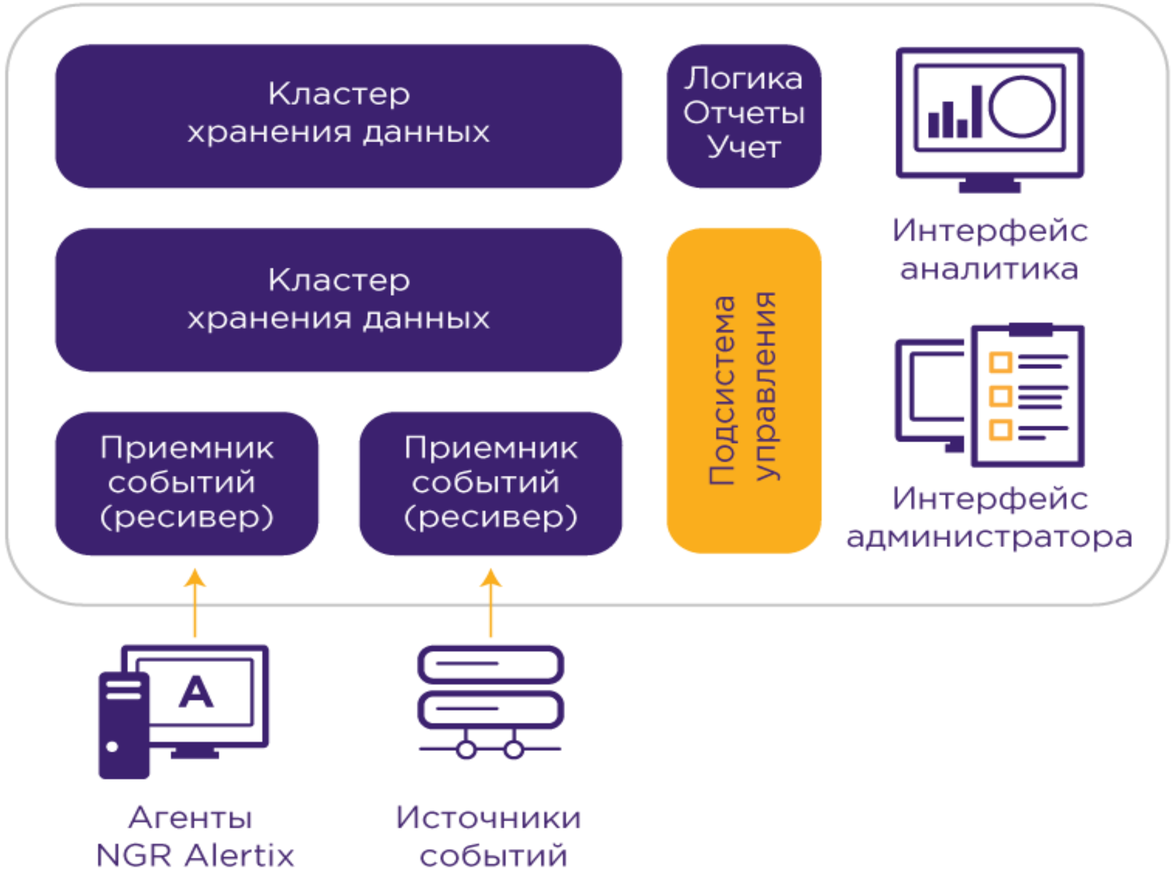
Сбор, обработка и хранение событий

- Разбор (парсинг) значимых полей
- Хранение с использованием сжатия
- Обогащение и нормализация событий

Автоматическое выявление и расследо-вания

- Быстрый полнотекстовый поиск
- Настраиваемая визуализация
- Риск-скоринг и настраиваемая приоритезация

Архитектура решения



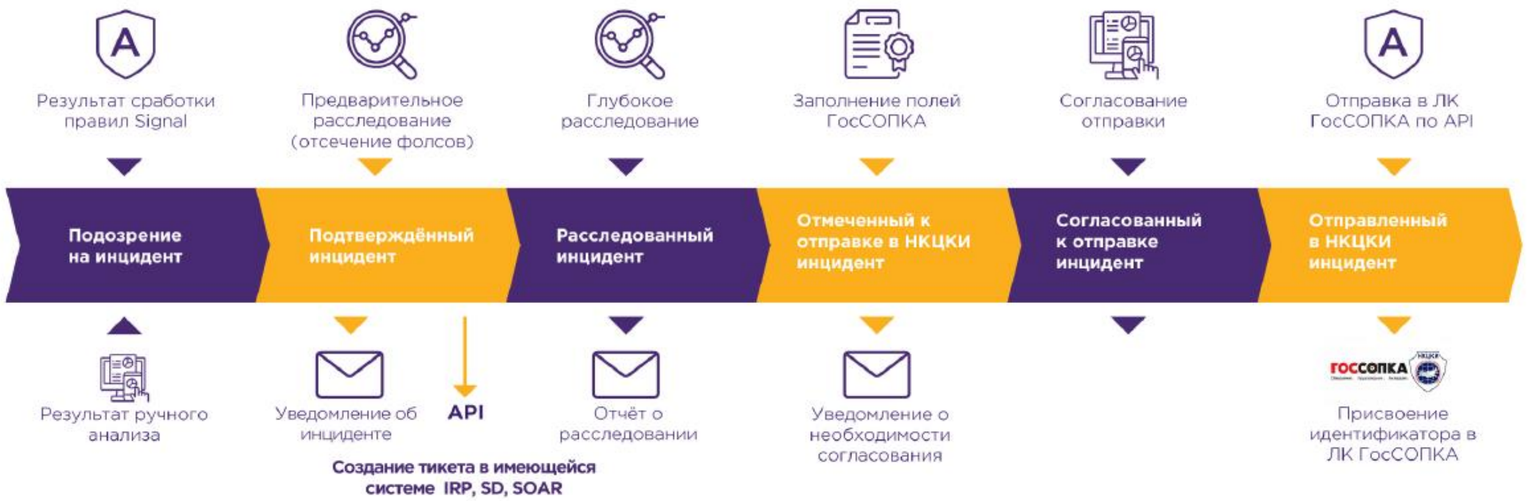
ALERTIX
SECURITY EVENT PLATFORM

- Не требует приобретения лицензии ОС, СУБД
- Функционирует в среде Linux, в том числе сертифицированных ОС
- Децентрализованная схема обеспечивает высокую отказоустойчивость
- Использование контейнеризации обеспечивает простоту и скорость устранения сбоев и обновлений

Встроенные подсистемы

Набор инструментов быстрого старта мониторинга ИБ:

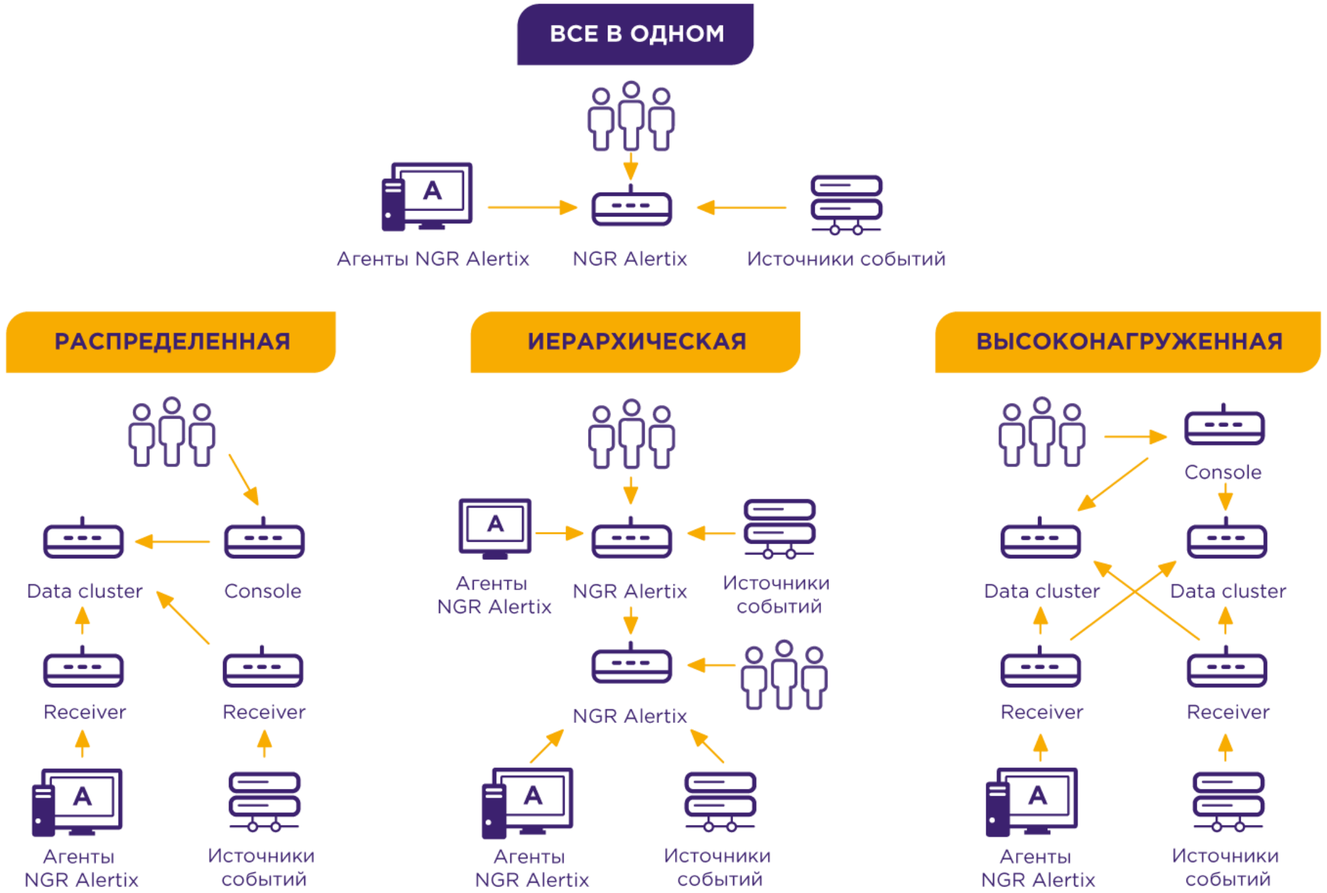
- Управления конфигурацией агентов
- Формирования отчетов
- Учета подозрений и инцидентов
- Учета сведений об ИТ-активах
- Отправки сведений в НКЦКИ



- Выстройте процесс выявления и расследования инцидентов с учетом критичности ИТ-активов
- Контролируйте эффективность, используя отчетность
- Экономьте на вычислительных ресурсах, отключая неиспользуемые компоненты
- Управляйте покрытием и конфигурацией агентов

Сценарии развертывания

- Распределяйте, масштабируйте каждый компонент, как этого требует инфраструктура и каналы
- Ответственные на местах могут работать с инцидентами, ЦО, контролировать эффективность и формировать отчеты
- Распределенное хранение повышает отказоустойчивость и производительность



100 агентов используют всего **1Mbit/s** полосы

10Mbit/s необходимо в пиковые часы при среднем потоке **500 EPS**

Поток **500 EPS** генерирует **1,5 ТБ** данных в месяц

Поток от Receiver в **2 раза** ниже входящего потока

Модульный управляемый агент

Подсистема управления

Конфигурацией
агентов Windows

Конфигурация
Управление составом
Обновления

Состояние
События
Телеметрия

Конфигурация
Управление составом
Обновления

Агент для Windows

- Beats (filebeat/winlogbeat/и др.)
- Sysmon
- Config manager and updater

Подсистема управления

Агентами
Linux и MacOS

Агент для Linux

- Wazuh Agent
- Modules manager

Правила автоматического обнаружения

Реально работающие правила

- Нарушение заданных политик ИБ
- Эксплуатация уязвимостей
- Ошибки конфигурации и потенциальные угрозы
- Цепочки событий и вложенная корреляция
- Обнаружение атак на различных стадиях: заражение, закрепление и др.

Ключевые особенности

- Используйте степень критичности ИТ-актива, чтобы снижать FR rate (false positive rate)
- Вносите любое количество исключений
- Настраивайте параметры расчета риска, добиваясь максимума эффективности
- Будьте уверены в актуальности правил за счет их использования в услугах SOC

Более 50% правил применимо сразу после установки и подключения источников

За счет услуг SOC состав правил Alertix максимально эффективен по соотношению точность выявления/трудоемкость расследования

Около **60%** из более чем **300** используемых правил, срабатывают в течение недели у клиентов, приобретающих услуги SOC, остальные 40% - в течение 3 месяцев

Ключевые особенности

Сценарии применения

Внедрение единого решения мониторинга

Alertix позволяет без приобретения и внедрения дополнительных средств обеспечить базовый процесс выявления, расследования, учета инцидентов и уведомления регуляторов.

Фильтрация входящего потока событий

Alertix может быть использован, дополняя внедренное SIEM решение, снижая его лицензируемые параметры.

Импортозамещение иностранного SIEM

Готовность Alertix и NGR Softlab к развитию позволяет уже сейчас добиваться функциональности, сравнимой с иностранными решениями.

Замена «мертвого» SIEM

Alertix спроектирован и разработан для эффективного оказания услуг. Это легко демонстрируется на пилоте и не требует длительного внедрения.

По данным опроса IDC, проведенного среди 102 организаций РФ,
34% рассматривают возможность замены системы SIEM, причем большинство
из них - 60% - планирует это сделать из-за политики импортозамещения

Интерфейс и администрирование

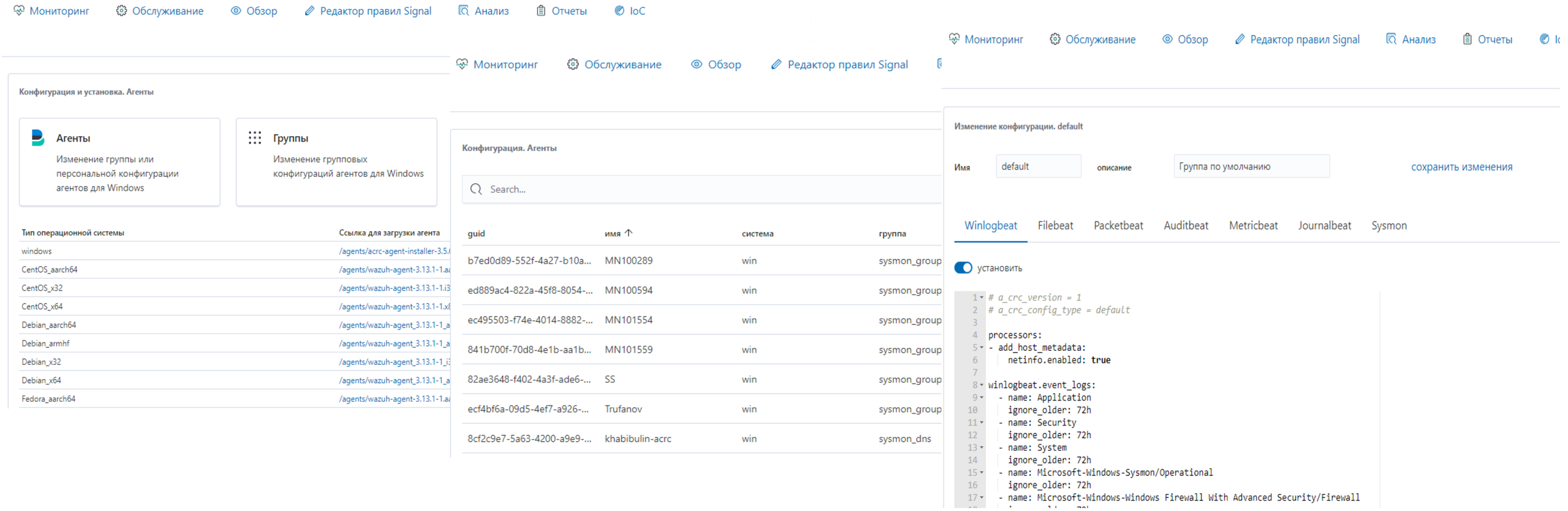
Поддержание жизненного цикла с минимум усилий:

- Защита от ошибочных действий и настроек на этапе попытки их применения
- Встроенная проверка синтаксиса (файлов конфигурации, правил выявления, запросов)
- Понятный мониторинг состояния (утилизация, ошибки, очереди, поток событий и др.)
- Простое и быстрое обновление «в два клика»: замена контейнера компонента целиком

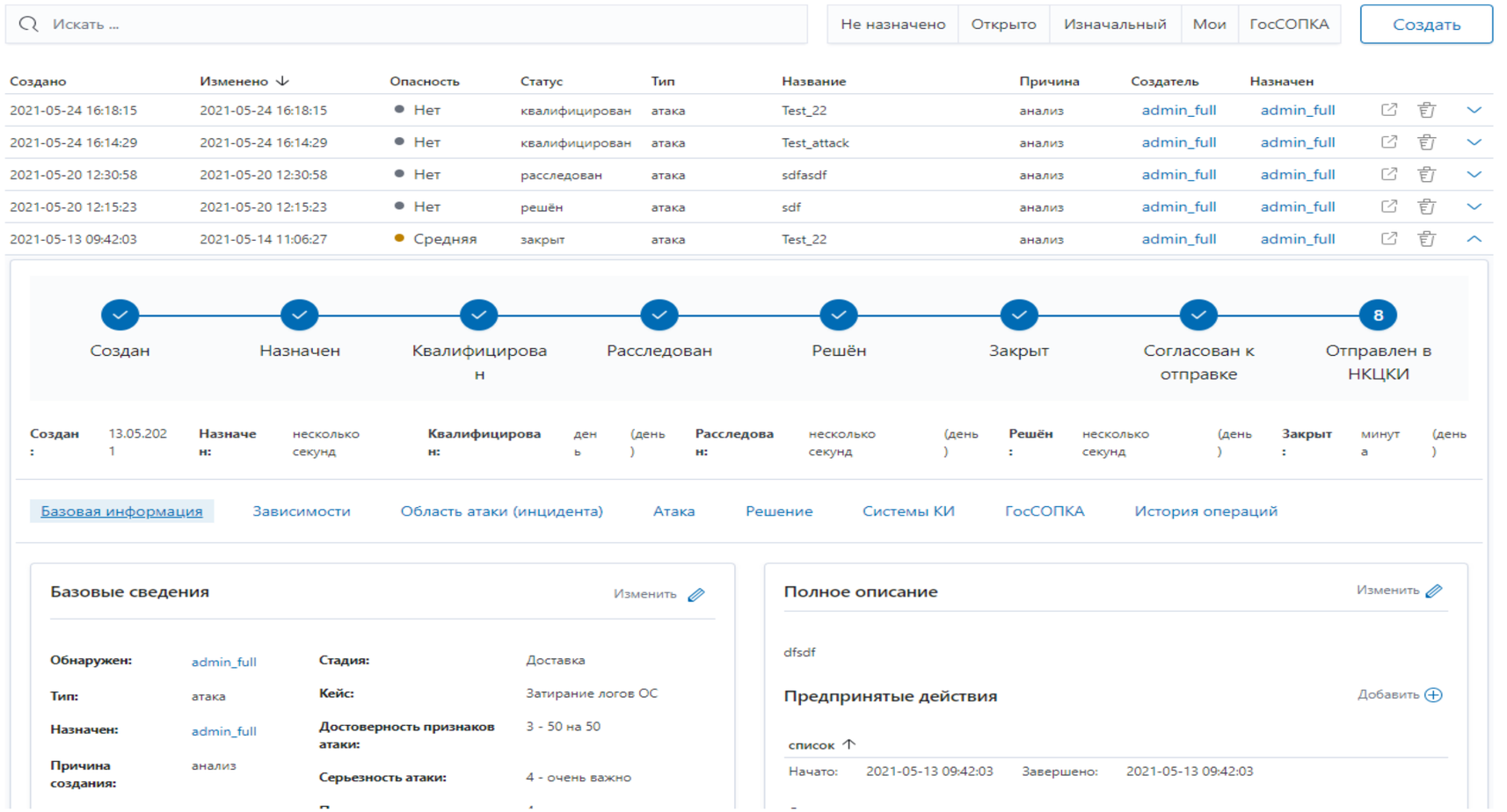
Высокая степень отказоустойчивости и обеспечение резервирования:

- Резервирование на уровне данных без использования зеркалирования
- Подробное журналирование действий пользователей и работы компонентов
- Резервное копирование конфигурации всех компонентов
- Разграничение «локального» и «глобального» контента: правила выявления, коннекторы, шаблоны отчетов

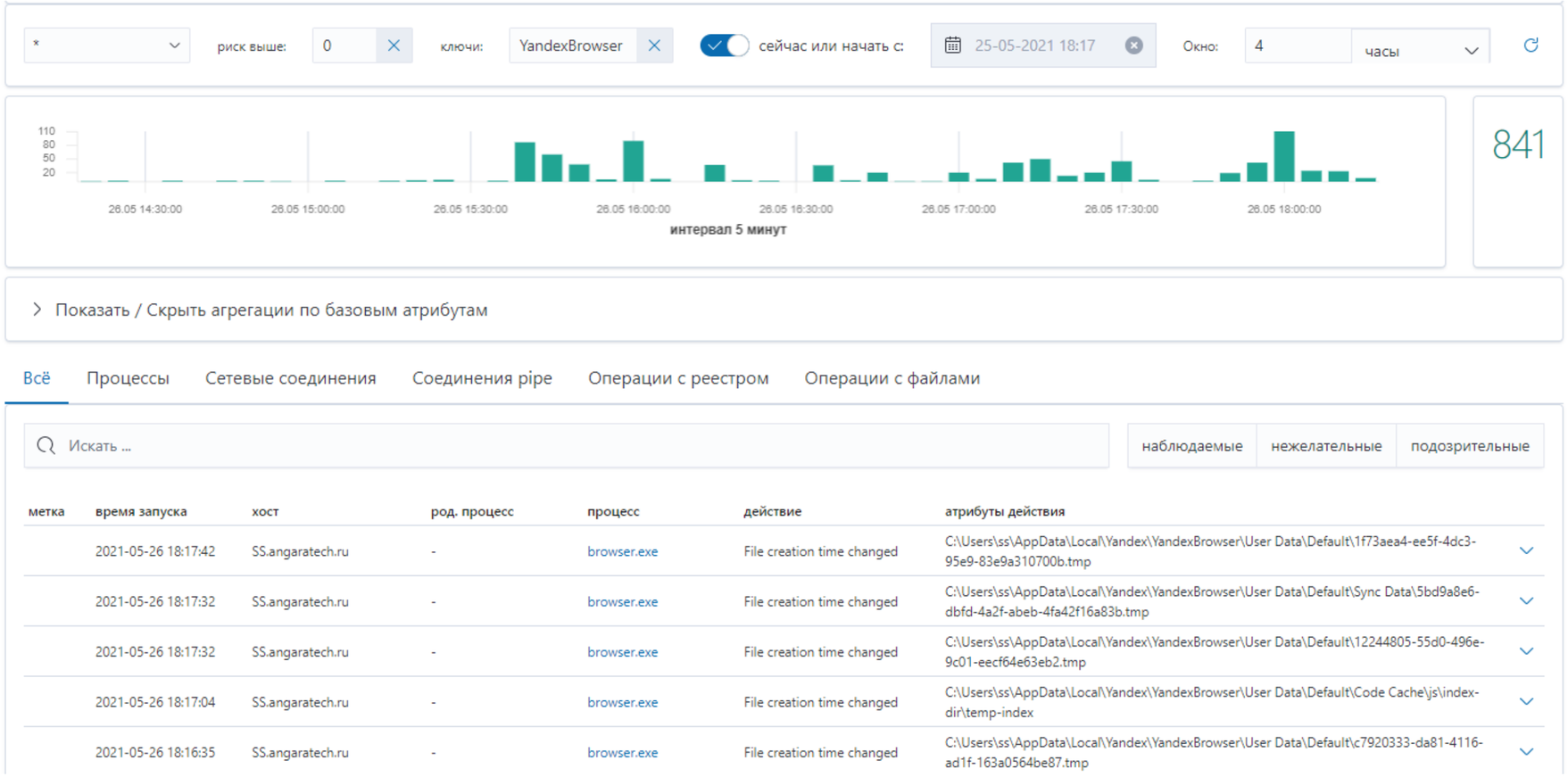
Интерфейс.
Управление групповой конфигурацией агентов



Интерфейс. Кейс менеджмент

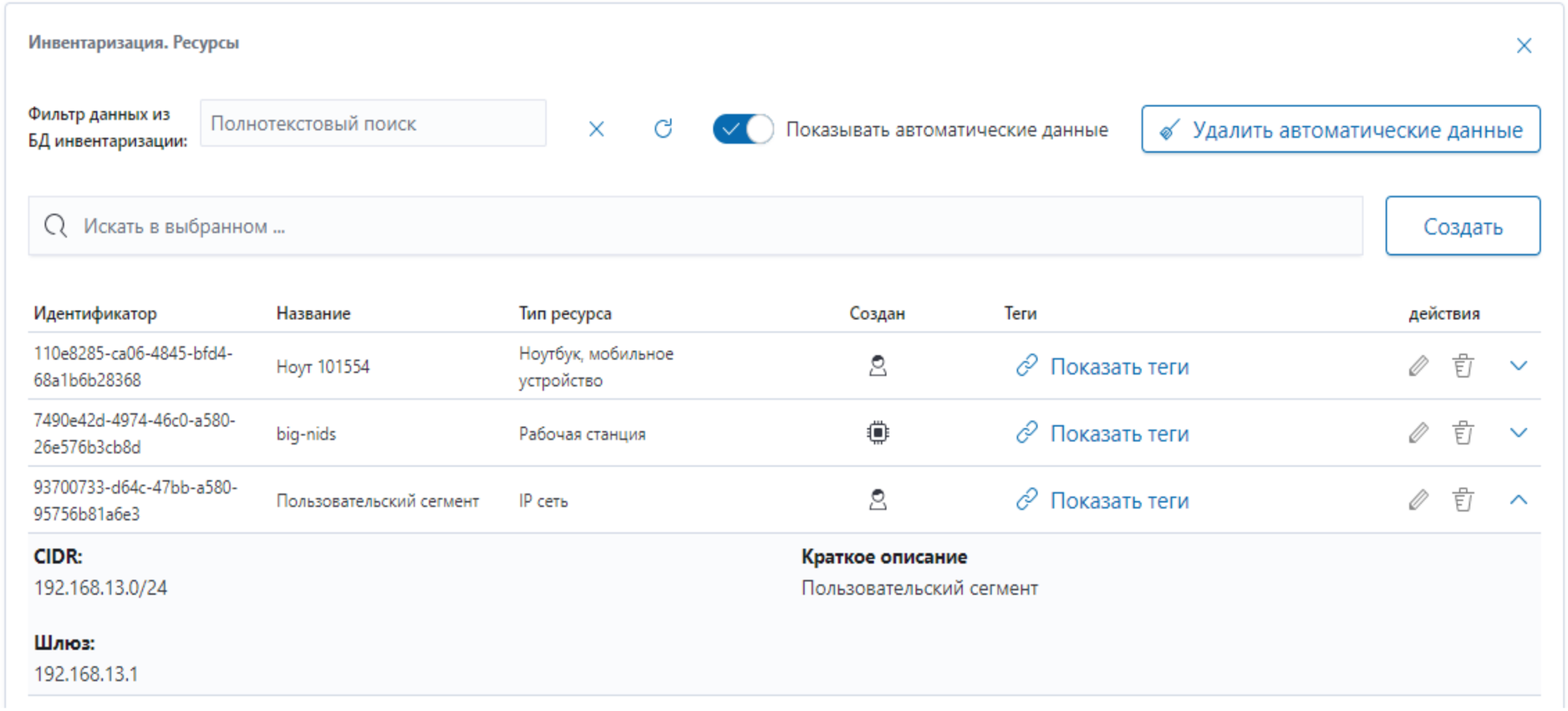


Интерфейс. Threat hunting с поддержкой полнотекстового поиска



метка	время запуска	хост	род. процесс	процесс	действие	атрибуты действия
	2021-05-26 18:17:42	SS.angaratech.ru	-	browser.exe	File creation time changed	C:\Users\ss\AppData\Local\Yandex\YandexBrowser\User Data\Default\1f73aea4-ee5f-4dc3-95e9-83e9a310700b.tmp
	2021-05-26 18:17:32	SS.angaratech.ru	-	browser.exe	File creation time changed	C:\Users\ss\AppData\Local\Yandex\YandexBrowser\User Data\Default\Sync Data\5bd9a8e6-dbfd-4a2f-abeb-4fa42f16a83b.tmp
	2021-05-26 18:17:32	SS.angaratech.ru	-	browser.exe	File creation time changed	C:\Users\ss\AppData\Local\Yandex\YandexBrowser\User Data\Default\12244805-55d0-496e-9c01-eecf64e63eb2.tmp
	2021-05-26 18:17:04	SS.angaratech.ru	-	browser.exe	File creation time changed	C:\Users\ss\AppData\Local\Yandex\YandexBrowser\User Data\Default\Code Cache\js\index-dir\temp-index
	2021-05-26 18:16:35	SS.angaratech.ru	-	browser.exe	File creation time changed	C:\Users\ss\AppData\Local\Yandex\YandexBrowser\User Data\Default\c7920333-da81-4116-ad1f-163a0564be87.tmp

Интерфейс. БД ИТ-активов: автонаполнение и учет критичности, влияющей на расчет риска коррелятором



ALERTIX Преимущества платформы

Комплексность решения: функционал LM, SIEM, учет инцидентов, учет активов

Возможности взаимодействия с НКЦКИ в части регистрации инцидентов в ЛК ГосСОПКА

ALERTIX
SECURITY EVENT PLATFORM

- Встраивается в любую инфраструктуру: высокая гибкость и возможности интеграции
- Непрерывно совершенствуется за счет использования в MSSP-исполнении
- Не требует больших усилий и вложений в персонал для поддержания уровня доступности 99% и выше
- Не зависит от курса доллара, не облагается НДС – российское ПО
- Лицензия является перманентной и включает 1 год поддержки вендора
- Базовая лицензируемая метрика – «чистый» EPS, платите только за те события, которые необходимо хранить

КОНТАКТЫ

121096 г. Москва, ул. Василисы Кожиной,
д. 1, корп. 1, этаж 7

ТЕЛ +7 (495) 269-29-59
ПОЧТА sales@ngrsoftlab.ru
САЙТ ngrsoftlab.ru