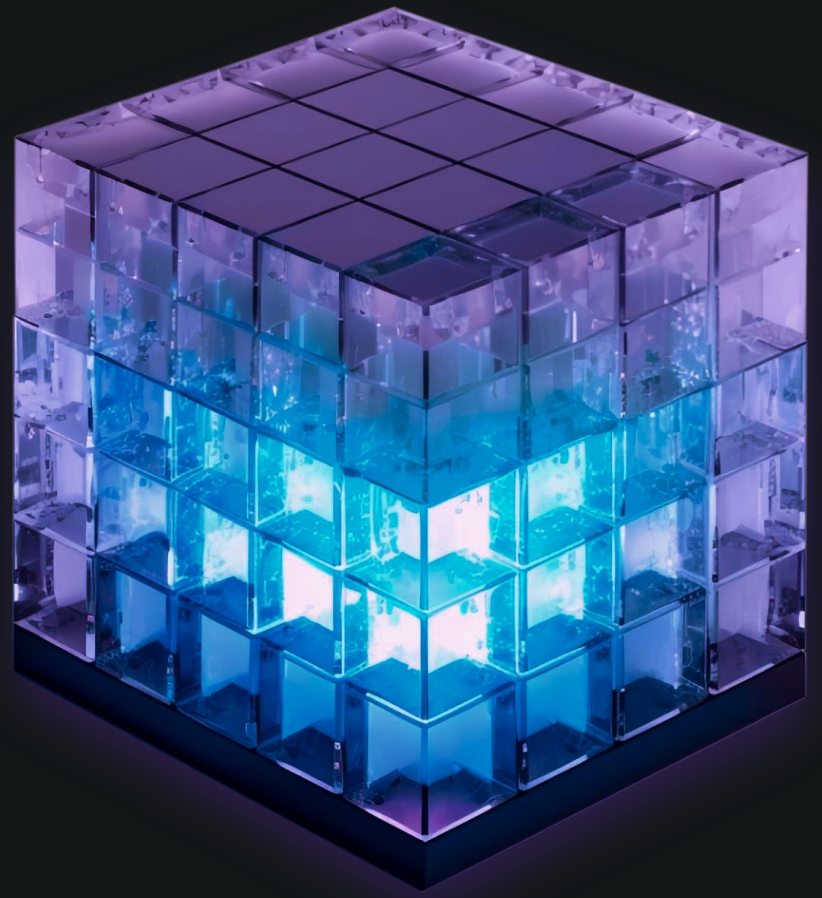
ИндексЛог

ИндексЛог

Универсальная платформа для работы с данными.
Поиск, мониторинг, кибербезопасность.



ИндексЛог

ИндексЛог – это распределенная платформа, которая объединяет в себе функционал корпоративного поиска, единого окна мониторинга ИТ-инфраструктуры и приложений, а также управления информационной безопасностью.

Единое решение для:

поиска

мониторинга

безопасности

ПЕРЕЙТИ В РЕЕСТР

ТЕКУЩИЕ ПРОБЛЕМЫ	РЕШЕНИЕ ИНДЕКСЛОГ
Разрозненные инструменты мониторинга плохо связаны друг с другом и никак не интегрируются	Единое окно для различных данных мониторинга и безопасности
У отдельных инструментов разные возможности автоматизации и алертинга, разные способы экспорта данных	Универсальные механизмы автоматизации и алертинга, вывод алертов и кейсов через интеграции с популярными системами сервис-деска + вебхуки
Отдельное лицензирование используемых решений, трудности при масштабировании системы	Единый механизм лицензирования по общему количеству данных, открывающий все возможности решения, простое масштабирование
Неточные результаты поиска по данным и долгое время выполнения запросов	Быстрый и гибкий поиск по любым данным, хранящимся в ИндексЛог

Готовые решения

Создайте собственные

Мониторинг

Логирование, APM, инфраструктурный и синтетический мониторинг

Безопасность

SIEM, SOC, защита конечных точек EDR

Поиск

Встраиваемый поиск, поиск на рабочем месте, настройка релевантности

ПЛАТФОРМА ИНДЕКСЛОГ

Загрузка и безопасное хранение

- Сбор данных через агенты, прием по протоколу UDP, TCP, инструментирование приложений
- Предварительная обработка данных и индексация
- Интеллектуальное хранение
- Безопасность и управление данными

AI/ML и поиск

- Полнотекстовый поиск
- Машинное обучение
- Корреляция данных
- Аналитика и агрегация
- Объединенный поиск и запросы

Визуализация и автоматизация

- Обмен и совместная работа с данными
- Исследование данных
- Визуализация данных
- Настраиваемые панели управления
- Интеграция со сторонними системами
- Автоматизация рабочих процессов

ПРИНЦИП РАБОТЫ

01 СБОР ДАННЫХ

- Автономные сборщики с открытым исходным кодом
- Унифицированный агент с готовыми интеграциями
- Кастомная обработка данных с помощью Logstash
- Прием данных по UDP/TCP

02 ОБРАБОТКА И ХРАНЕНИЕ

- Настройка пайплайнов для обработки данных перед индексацией
- Обогащение данными из других источников
- Гибкая настройка циклов хранения

03 АНАЛИЗ И АВТОМАТИЗАЦИЯ

- Пороговый алертинг
- Обнаружение аномалий машинным обучением
- Категоризация логов
- Встроенная система кейсов
- Экспорт кейсов и алертов во внешние системы

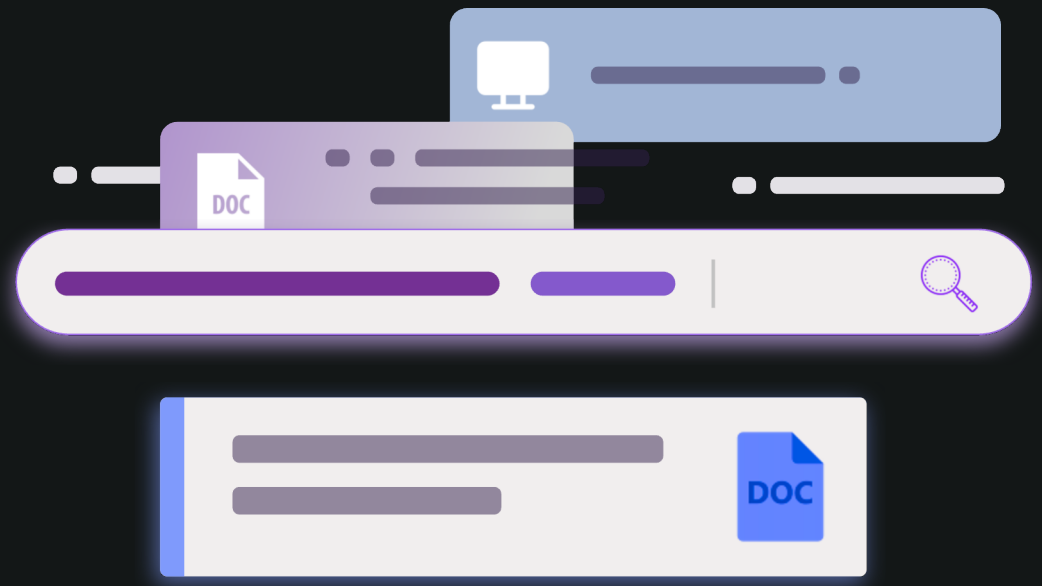
ПРЕИМУЩЦСТВА ИНДЕКСЛОГ

- Агрегация любых данных из различных источников
- Безопасное и масштабируемое хранилище
- Встроенное машинное обучение
- Единый интерфейс для поиска, анализа и управления
- Визуализация и отчетность
- Автоматизация рабочих процессов

ИндексЛог

Индекслог - платформа для построения поисковых приложений

- Единый интерфейс для анализа и настройки поискового опыта
- Мониторинг показателей поискового приложения в реальном времени
- Гибкая настройка релевантности результатов с возможностью совместной работы
- Векторный поиск и NLP



Индекслог - платформа для мониторинга

- Единое окно для агрегации данных
- Инфраструктурный мониторинг
- Мониторинг производительности приложений (APM)
- Сбор и анализ логов
- Синтетический мониторинг

ИндексЛог

Индекслог - платформа для безопасности (SIEM, SOC)

- Сбор и обработка событий информационной безопасности
- Управление правилами SIEM и их выполнение
- Анализ автоматически созданных сигналов
- Совместное расследование инцидентов
- Экспорт алертов и инцидентов во внешние системы

ИндексЛог - полный набор инструментов для работы с вашими данными

Различные механизмы сбора данных

Любой источник данных подключается через готовую интеграцию, либо через пользовательскую обработку данных.

Для сбора можно использовать:

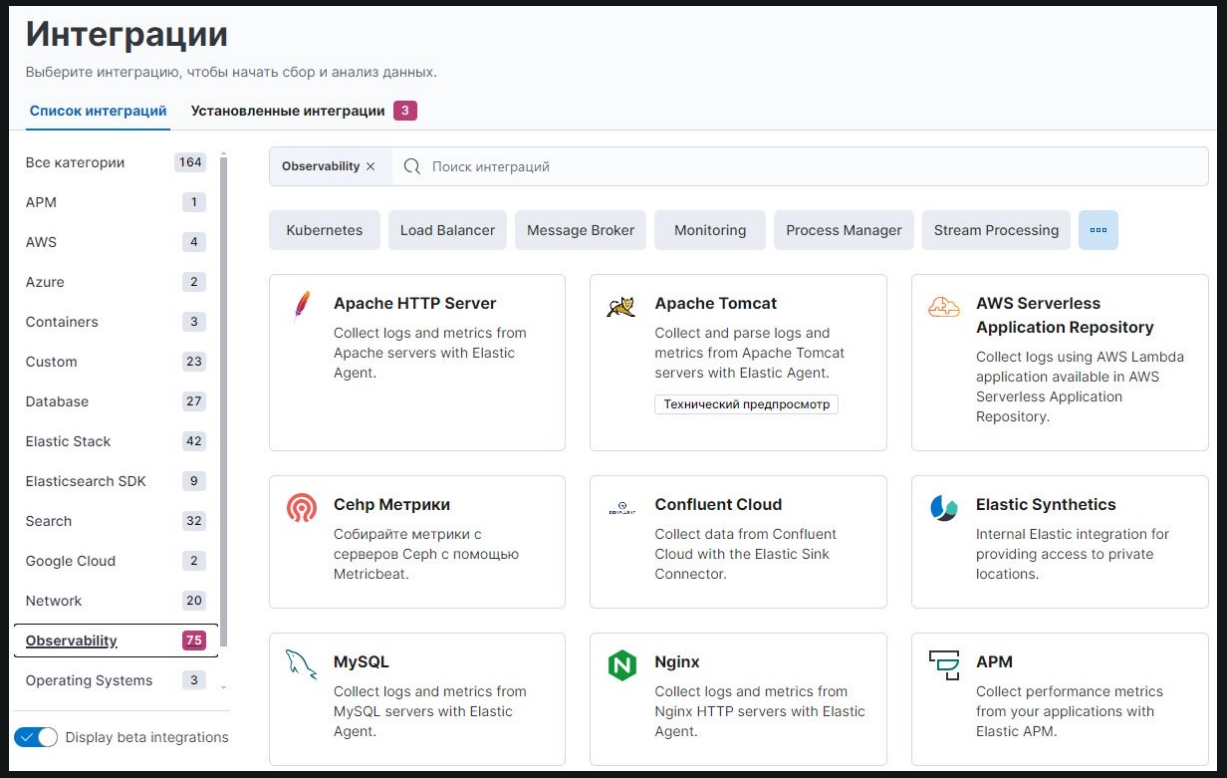
Специализированные агенты Beats

- конфигурируются индивидуально

Универсальный агент с интеграциями

- управляются централизованно с помощью политик
- возможно автономное развертывание централизованного управления в закрытых средах

Прием данных напрямую по UDP, TCP с помощью Filebeat и Logstash

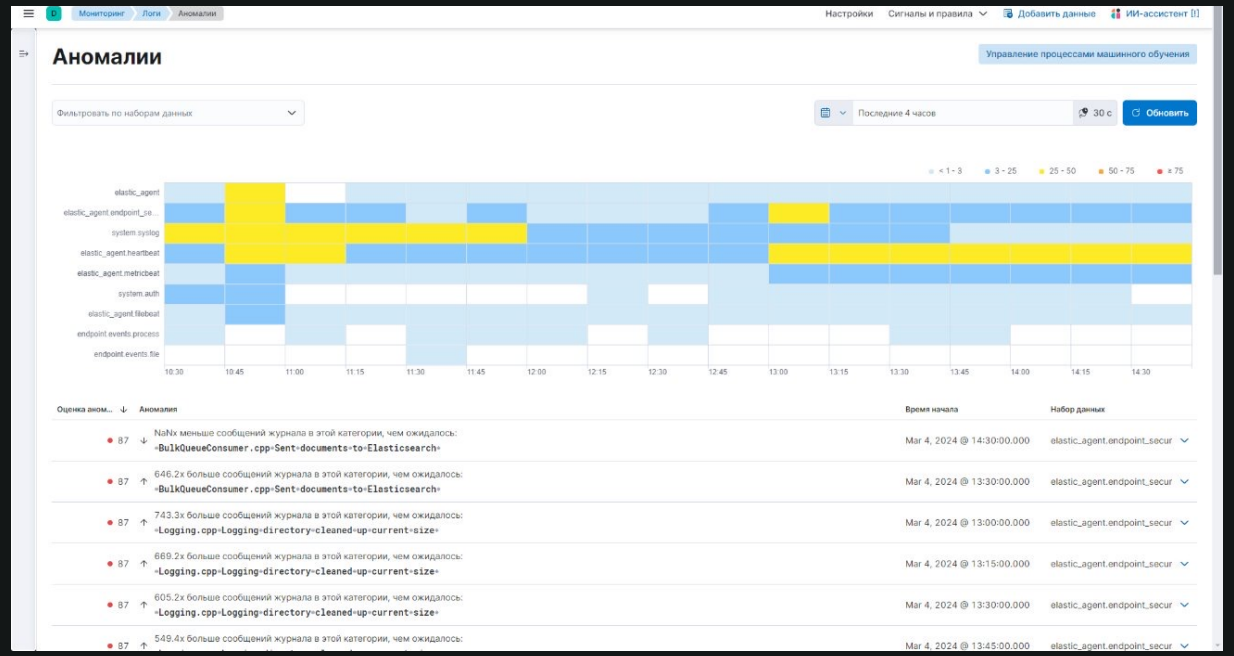


Автоматизированная обработка и анализ данных

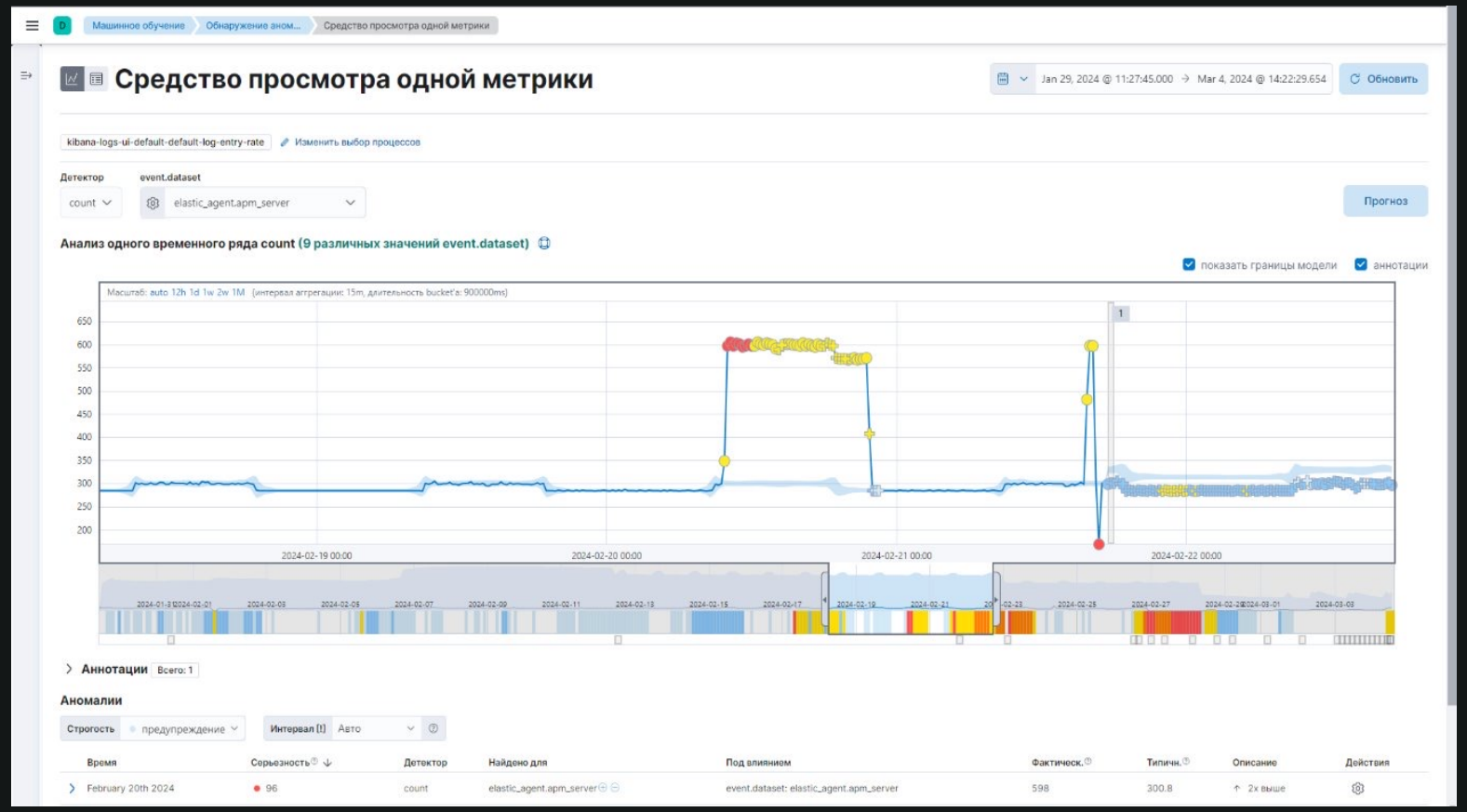
Цель работы с ИндексЛог – централизовать и автоматизировать обработку больших объемов данных мониторинга и инфраструктуры.

Для этого:

- Настраиваются правила машинного обучения (обнаружение аномалий, классификация)
- Проводится анализ правилами SIEM
- Данные визуализируются на дашбордах



Обнаружение аномалий с помощью машинного обучения



ИндексЛог

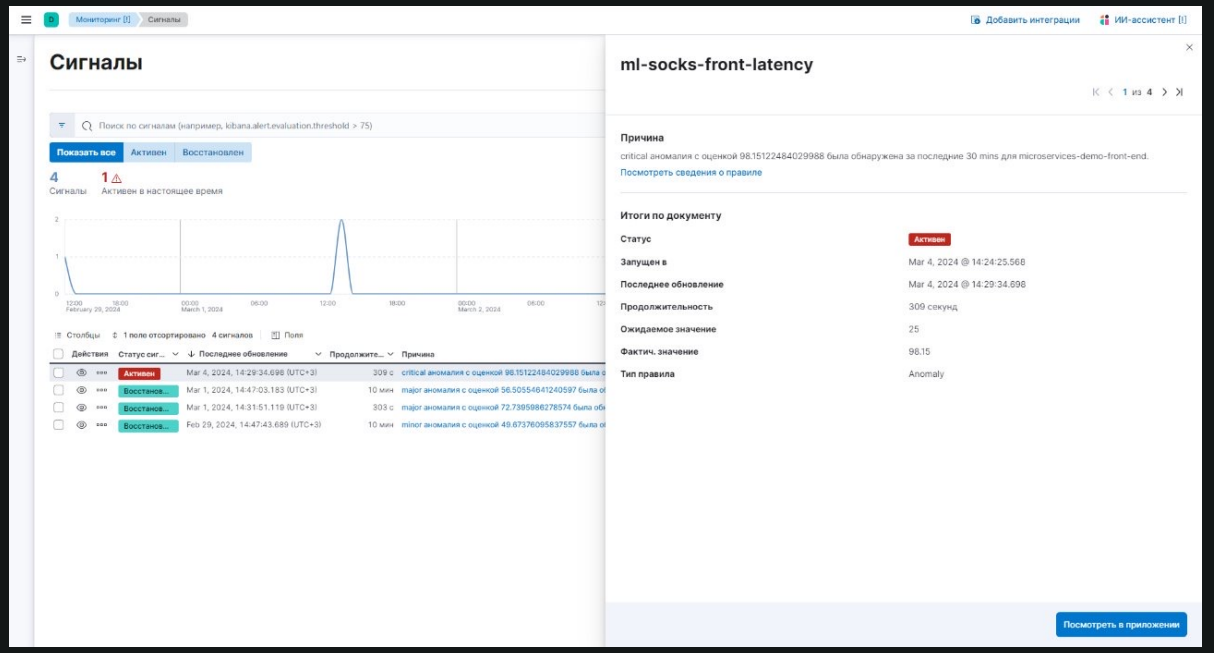
Алертинг и экспорт

Чтобы обнаруживать проблемы в работе приложений и инфраструктуры:

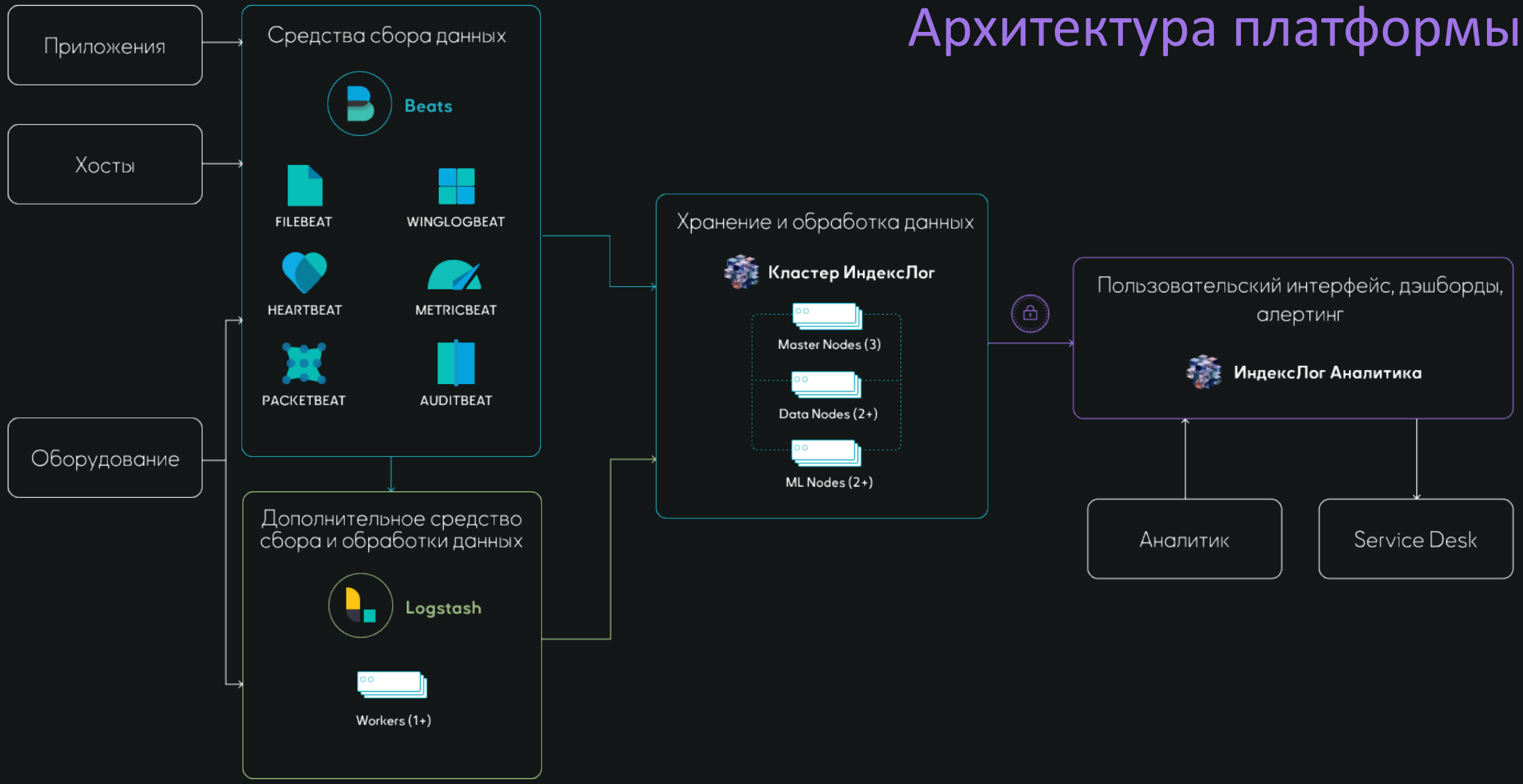
01 Создайте пороговое правило, правило SIEM или задайте минимальное отклонение от ожидаемых значений для создания алерта

02 После генерации алерта проведите расследование и создайте кейс внутри ИндексЛог

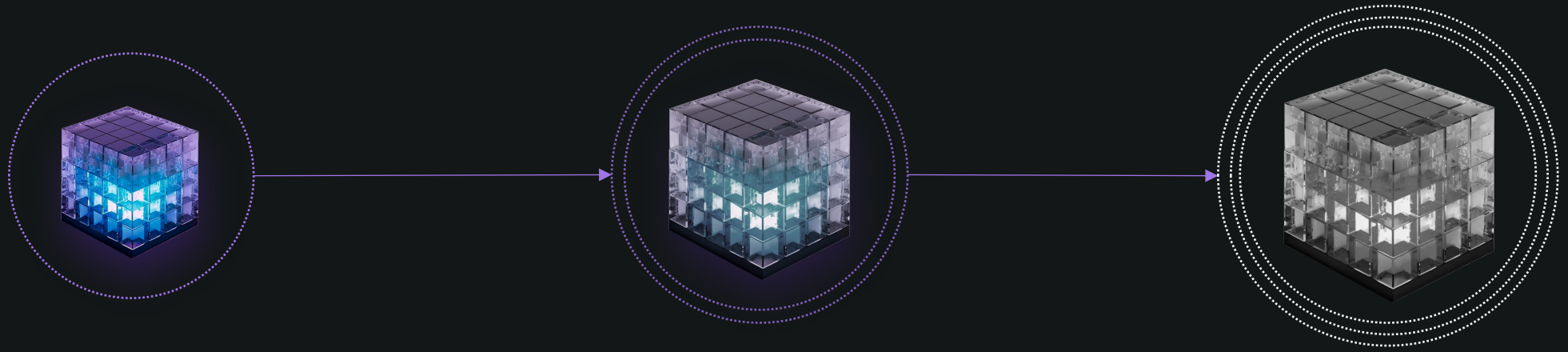
03 Экспортируйте кейс во внешнюю систему управления инцидентами



Архитектура платформы



Цикл хранения данных в ИндексЛог



Горячие данные

Самые свежие данные. Для того, чтобы обеспечить к ним быстрый доступ, мы выделяем больше всего ресурсов

Теплые данные

Эти данные все еще актуальны, но запрашиваются реже. Таких данных мы можем хранить больше на ГБ оперативной памяти, немного жертвуя скоростью поиска

Холодные данные

Исторические данные. Нам все еще нужно их хранить, но быстрый доступ к ним не требуется

ИндексЛог

ЛИЦЕНЗИРОВАНИЕ

Сайзинг по объему данных

Единица лицензирования – «node» (VM на 64Gb RAM)

Лицензируются только «node», хранящие и обрабатывающие данные

Первая покупка от 3х «node»

Подписка на 1, 2 или 3 года

Техническая поддержка 8/5 (прием обращений 24/7)

НАШИ ПАРТНЕРЫ

Вместе с партнерами мы стремимся к обеспечению высокого качества продуктов и сервисов, помогая бизнесу достигать новых высот и успешно адаптироваться к изменяющимся требованиям рынка.

ИНФОСИСТЕМЫ ДЖЕТ
Эксперт

ICL
Эксперт

T1
Реселлер

RONDEM
Эксперт

MAXIMA
Эксперт

Open Solutions
Реселлер

MEPATEX
Дистрибьютор в Беларуси

ИндексЛог

КОНТАКТЫ

Телефон

+7 (495) 231-73-64

Электронная почта

office@rr-th.com

Адрес

Москва, Цветной бульвар
д.26, стр.1, офис 36

Перейти на сайт ИндексЛог