

AlertX AI

SECURITY OPERATIONS PLATFORM

Техническая спецификация продукта

Корпоративная SIEM-платформа с AI-анализом алертов, SOAR-автоматизацией, UEBA, NDR и мультитенантной изоляцией организаций.

SIEM	SOAR	UEBA	NDR	THREAT INTELLIGENCE	MULTI-TENANCY
AI-АНАЛИЗ					

ВЕРСИЯ ДОКУМЕНТА	ДАТА	СТАТУС	КЛАССИФИКАЦИЯ
1.0	17 июля 2026	Актуальная редакция	Внутренний документ

Содержание

1	Работа с системой
1.1	Разделы интерфейса
1.2	Типовой сценарий работы аналитика
2	Архитектура
2.1	Технологический стек
2.2	Поток данных (центральный сервер)
2.3	Удалённые коллекторы
2.4	Мультитенантность
3	Отказоустойчивость
3.1	Кластер OpenSearch
3.2	Буферизация на коллекторе при потере связи
3.3	Прочие механизмы
4	Сетевые порты (справочно)

О документе

Документ описывает три аспекта платформы AlertX AI: как пользоваться системой (разделы интерфейса и сценарии работы), архитектуру решения и механизмы обеспечения отказоустойчивости. Разделы интерфейса проиллюстрированы снимками экрана рабочей системы.

500+

МОНИТОРОВ ДЕТЕКТА

11

КАНАЛОВ
УВЕДОМЛЕНИЙ

40+

ПАЙПЛАЙНОВ
LOGSTASH

3

ЯЗЫКА ИНТЕРФЕЙСА

1 Работа с системой

Вход выполняется через веб-интерфейс (Nginx, HTTPS). Аутентификация — логин/пароль с поддержкой TOTP 2FA, LDAP и SSO. Сессия хранится в HttpOnly-cookie. После 5 неудачных попыток входа аккаунт блокируется на 15 минут. Интерфейс доступен на трёх языках: русский, казахский, английский (переключатель внизу боковой панели).

Роли: `super_admin` видит все организации; `org_admin` и аналитики — только данные своей организации. Каждый объект в системе (алерт, инцидент, индекс) привязан к `org_id`.

1.1 Разделы интерфейса

Боковое меню сгруппировано по блокам. Ниже — все страницы и что на них можно делать.

Обзор

СТРАНИЦА	НАЗНАЧЕНИЕ
Дашборд	Сводная картина: количество алертов по уровням, лента последних событий, состояние системы. Точка входа для дежурной смены.

Алертинг (SIEM)

СТРАНИЦА	НАЗНАЧЕНИЕ
Алерты	Основная рабочая таблица алертов в реальном времени (WebSocket). Фильтры: полнотекстовый поиск, IP источника, хост, уровень критичности, статус, тактика MITRE ATT&CK, организация, категория (Security / DNS / Wazuh / Windows). Быстрые диапазоны времени (15 мин ... 30 дней, всё время). Массовые действия по чекбоксам: смена статуса, эскалация. Клик по алерту — карточка с деталями, обогащением (GeoIP, threat intel) и AI-анализом.
Уведомления	Настройка и тестирование каналов доставки уведомлений: Email, Slack, Telegram, Teams, PagerDuty, OpsGenie, Jira, ServiceNow, TheHive, Google Chat, Webhook — 11 типов. Каждый канал включается/выключается отдельно, есть кнопка «Тест». Здесь же планируются «Технические работы» (уведомление пользователей о плановых окнах).

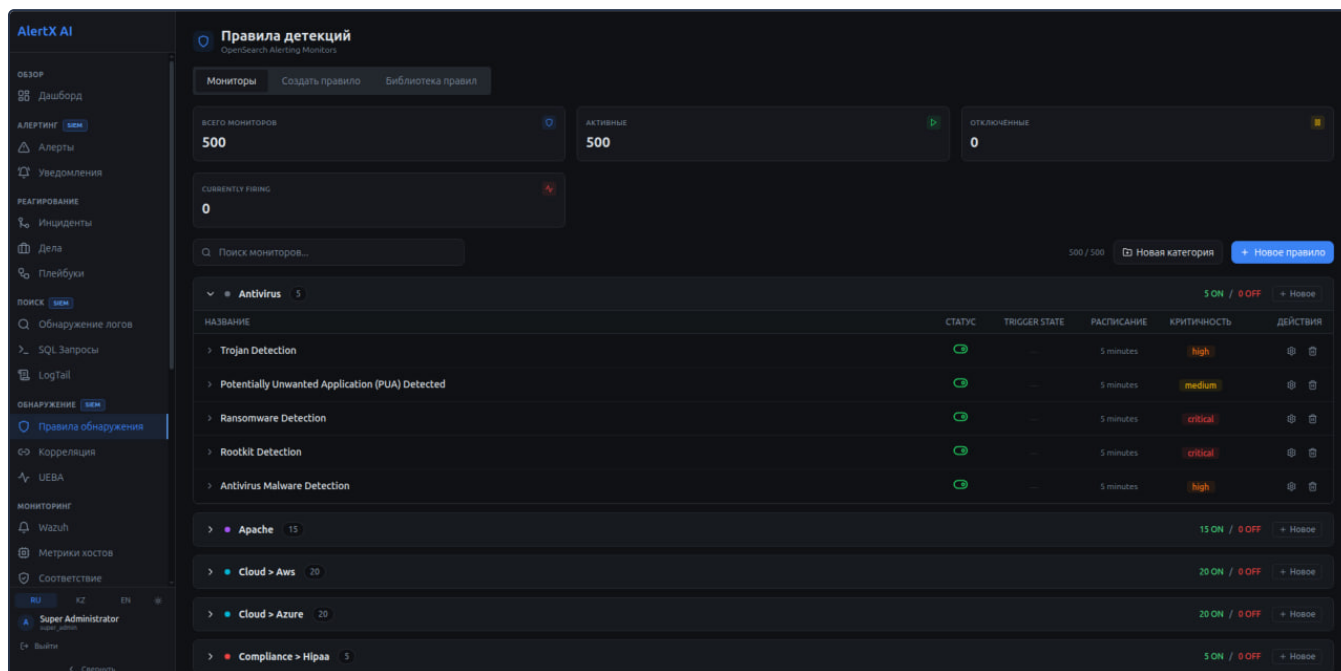


Рис. 1. Страница «Алерты» — рабочая таблица в реальном времени с фильтрами по уровню, статусу, тактике MITRE, организации и категории источника.

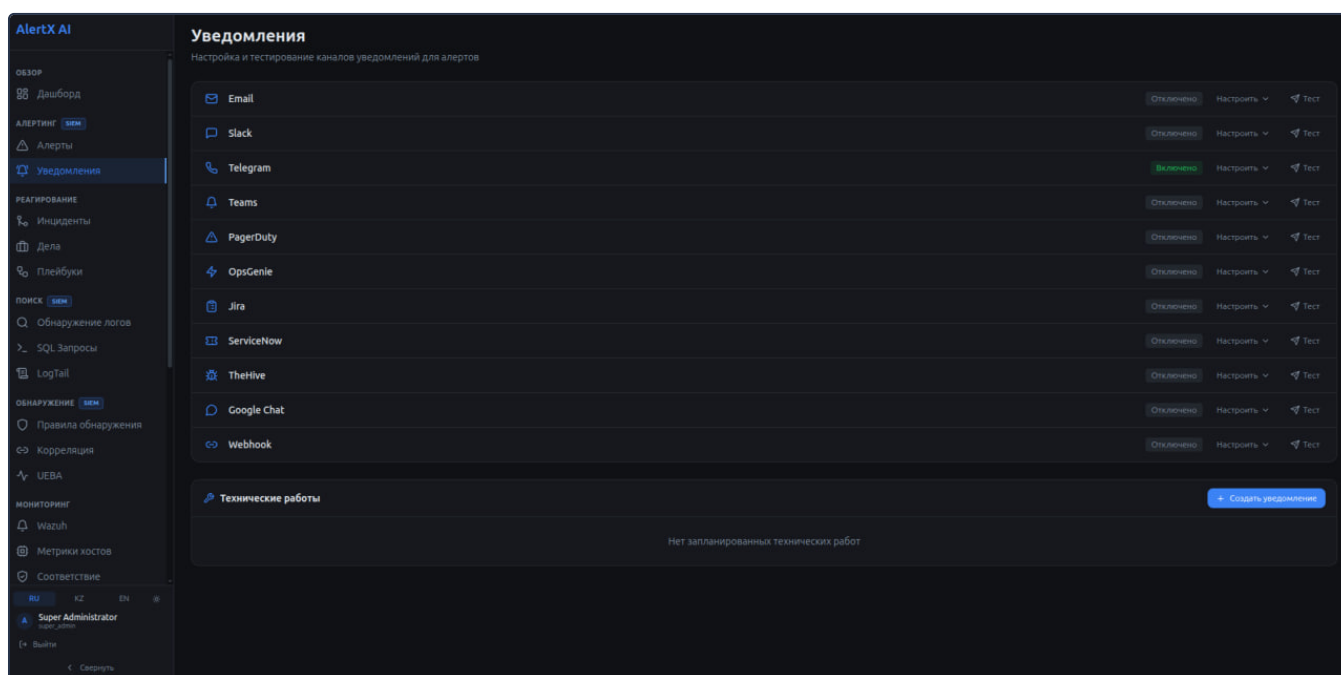


Рис. 2. Страница «Уведомления» — 11 каналов доставки с индивидуальным включением и кнопкой «Тест»; ниже — блок планирования технических работ.

Реагирование

СТРАНИЦА	НАЗНАЧЕНИЕ
Инциденты	Управление инцидентами ИБ. Счётчики: всего / открытые / в работе / критические. Инциденты создаются вручную («Создать инцидент»), автоматически из критических алертов ($\text{severity} \geq 8$) или плейбуками. Фильтры по статусу, уровню, аналитику, датам. У инцидента: статус, назначенный аналитик, связанные алерты.
Дела	Кейс-менеджмент: объединение инцидентов и артефактов расследования в дела с историей работы.
Плейбуки	SOAR-сценарии автоматического реагирования. Примеры штатных: <i>Auto-block C2 IP</i> (блокировка IP источника при C2-активности, $\text{severity} \geq 8$), <i>Enrich IOC + Notify</i> (обогащение индикаторов из Threat Intelligence и уведомление дежурного), <i>Escalate High Severity</i> (эскалация критических алертов на L2/L3 с созданием инцидента и мультиканальным уведомлением). Плейбук можно включать/выключать, запускать вручную, редактировать шаги; есть библиотека стандартных плейбуков и история запусков.

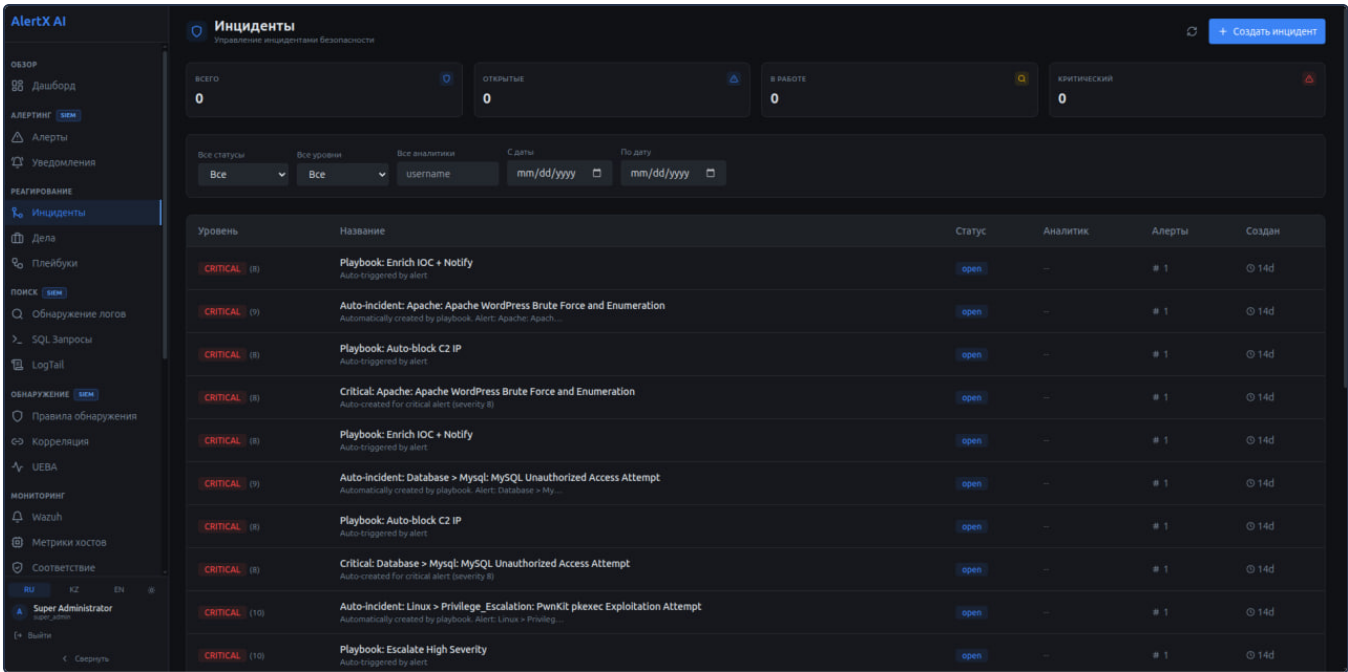


Рис. 3. Страница «Инциденты» — счётчики и лента инцидентов; видно, что часть записей создана автоматически (*Auto-triggered by alert*, *Auto-created for critical alert*).

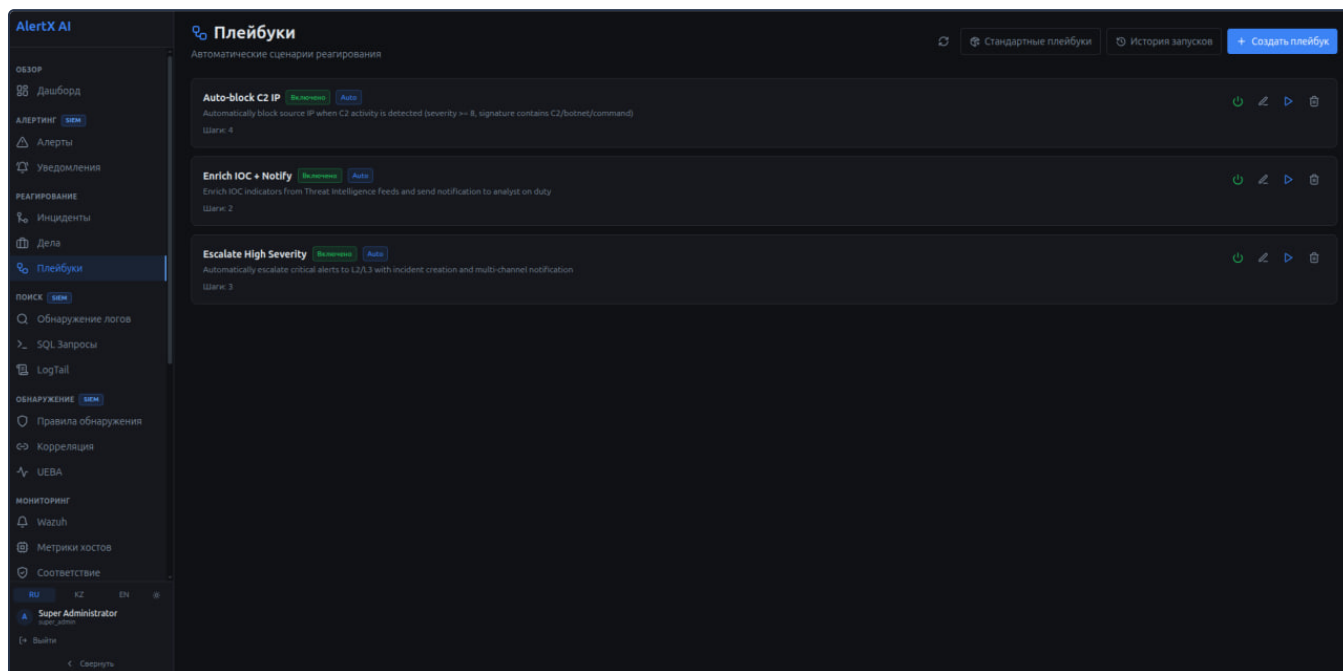


Рис. 4. Страница «Плейбуки» — три штатных SOAR-сценария в режиме Auto с указанием числа шагов, управлением состоянием и историей запусков.

Поиск (SIEM)

СТРАНИЦА	НАЗНАЧЕНИЕ
Обнаружение логов (Discover)	Полнотекстовый поиск по сырым логам с синтаксисом Lucene (пример: <code>host.name:dc01 AND event.code:4625</code>). Выбор индекс-паттерна, гистограмма событий по времени, панель полей слева (<code>agent.type</code> , <code>event.category</code> , <code>host.name</code> ...), раскрытие документа целиком, настройка колонок, экспорт CSV/JSON, автообновление.
SQL Запросы	Консоль SQL/PPL-запросов к OpenSearch для аналитиков, предпочитающих табличный доступ.
LogTail	Живой «хвост» потока логов (аналог <code>tail -f</code>) для контроля поступления данных.

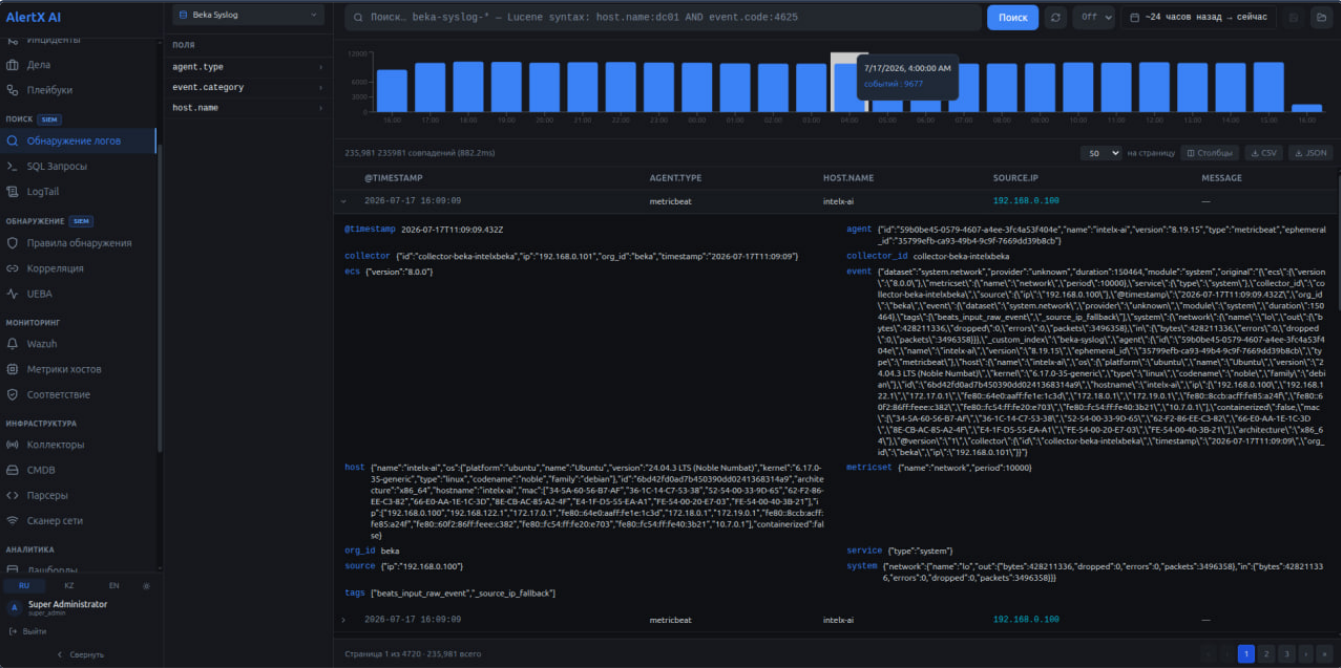


Рис. 5. «Обнаружение логов» — Lucene-запрос по индекс-паттерну, гистограмма событий, панель полей и раскрытый документ целиком с экспортом в CSV/JSON.

Обнаружение (SIEM)

СТРАНИЦА	НАЗНАЧЕНИЕ
Правила обнаружения	Управление мониторами OpenSearch Alerting — основным движком детектирования. Вкладки: Мониторы / Создать правило / Библиотека правил. Правила сгруппированы по категориям (Antivirus, Apache, Cloud > AWS, Cloud > Azure, Compliance > HIPAA и др. — суммарно 500+ мониторов). У каждого правила: статус (вкл/выкл), состояние срабатывания, расписание проверки (например, каждые 5 минут), уровень критичности. Поддерживаются SIGMA-правила (YAML) и конструктор правил в GUI, компилируемый в OpenSearch DSL.
Корреляция	Корреляционные правила, связывающие цепочки событий из разных источников в один алерт.
UEBA	Поведенческая аналитика пользователей и сущностей. Счётчики риска (критический / высокий / средний / низкий), рейтинг пользователей по риск-баллу, тепловая карта активности по часам суток, лента аномалий. Пример детекта: «Вход вне рабочих часов» с учётом рабочего графика (09:00–18:00, таймзона организации) и контекстом действий за ближайшие 2 часа.

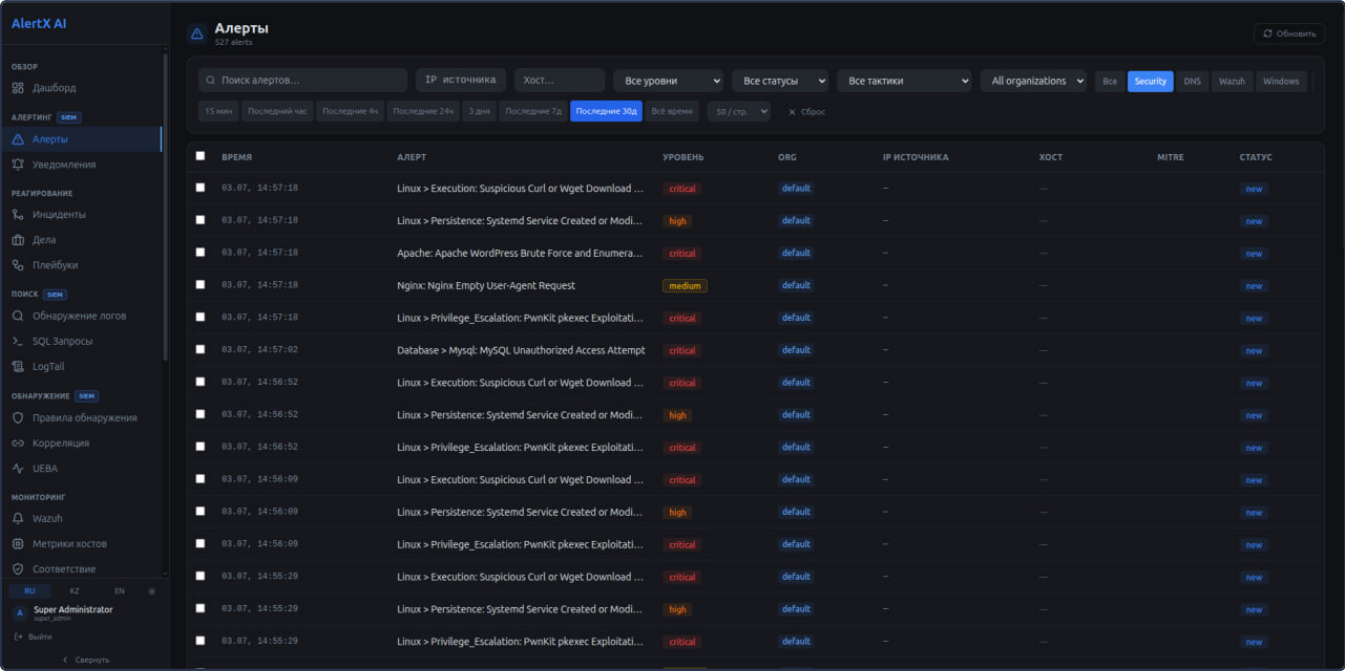


Рис. 6. «Правила детекций» — 500 мониторов OpenSearch Alerting, сгруппированных по категориям, с расписанием проверки и уровнем критичности.

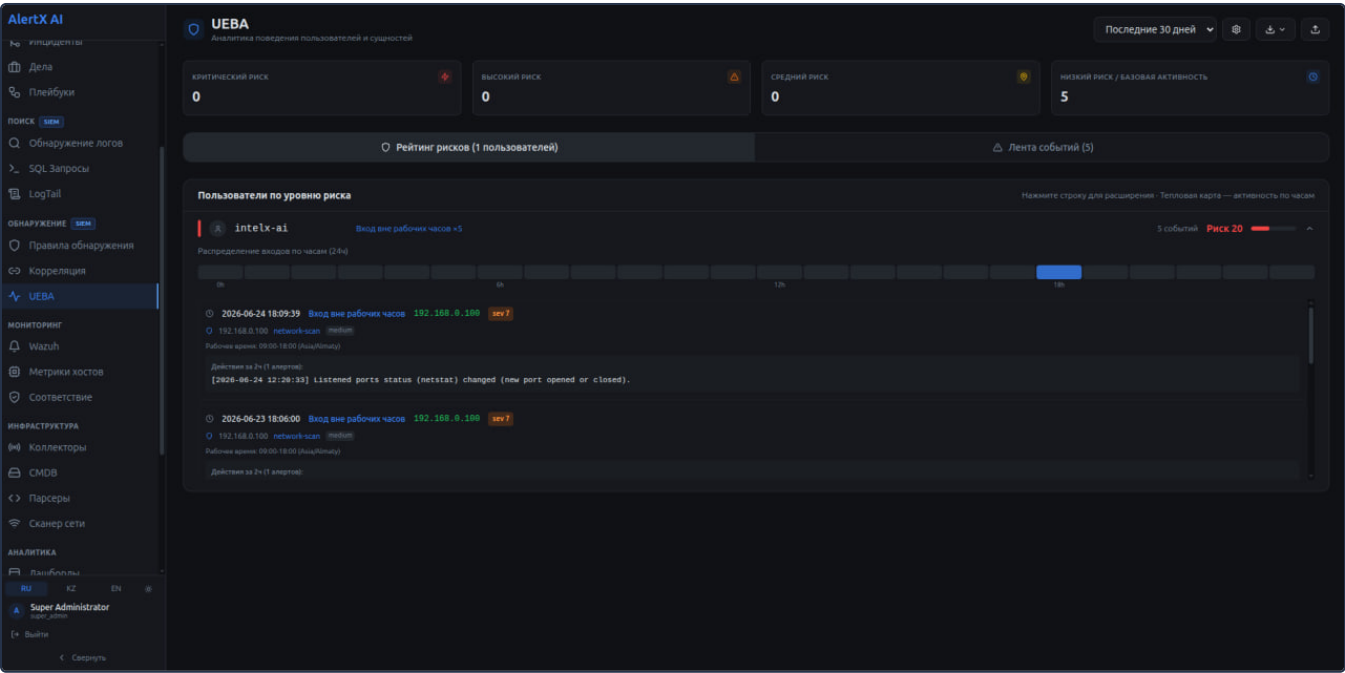


Рис. 7. UEBA — рейтинг пользователей по риск-баллу, распределение входов по часам суток и лента аномалий с контекстом действий за ближайшие 2 часа.

Мониторинг

СТРАНИЦА	НАЗНАЧЕНИЕ
Wazuh	Интеграция с Wazuh (HIDS): агенты, события, правила для вредоносных файлов.
Метрики хостов	Метрики наблюдаемых хостов (CPU, память, сеть — данные Metricbeat).
Соответствие	Комплаенс-контроли и отчётность по стандартам.

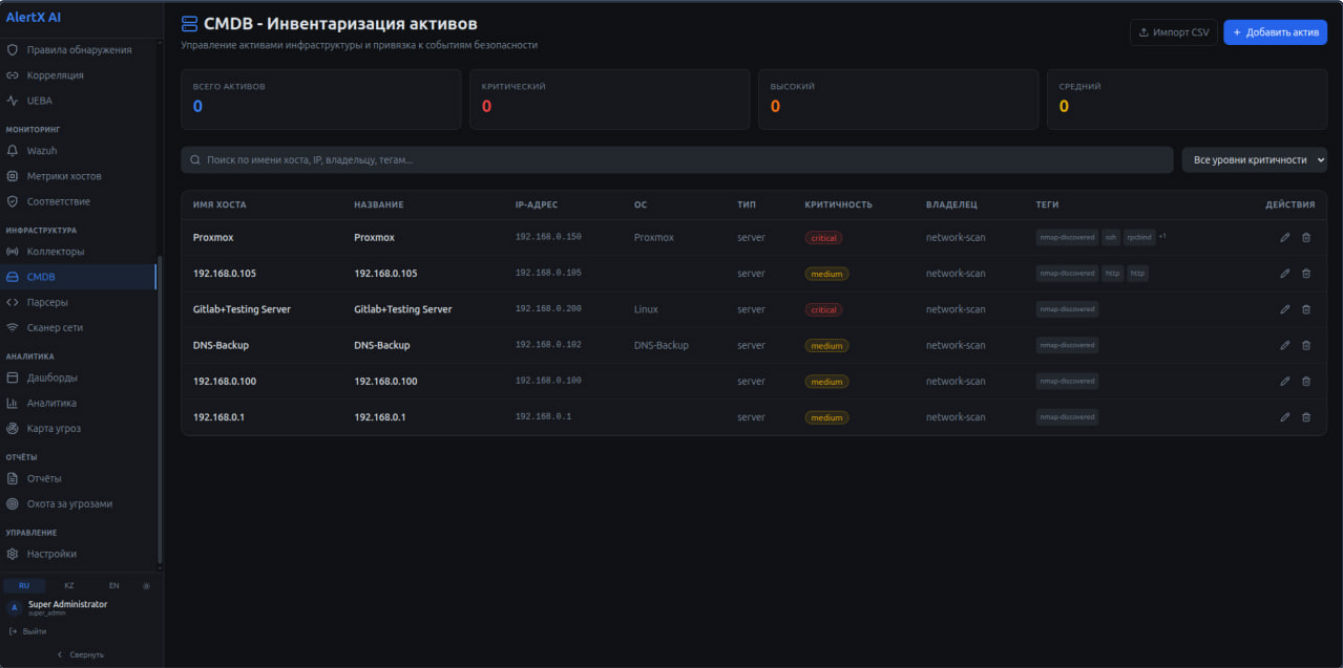


Рис. 9. C MDB — инвентаризация активов с уровнем критичности, владельцем и тегами; записи с тегом `ntmap-discovered` получены автоматически из сканера сети.

Аналитика

СТРАНИЦА	НАЗНАЧЕНИЕ
Дашборды	Пользовательские дашборды (конструктор виджетов).
Аналитика	Статистика, риск-скоринг, ML-инсайты.
Карта угроз	Геокарта атак по GeolP-данным источников.

Отчёты

СТРАНИЦА	НАЗНАЧЕНИЕ
Отчёты	Вкладки: Шаблоны / Сгенерированные / Расписания. «Мастер отчёта» (3 шага): выбор шаблона и периода, предпросмотр, скачивание или сохранение в архив. Форматы: PDF и HTML. Отчёты бывают разовыми (one-off) и по расписанию.
Охота за угрозами	Threat hunting: проактивный поиск по гипотезам.

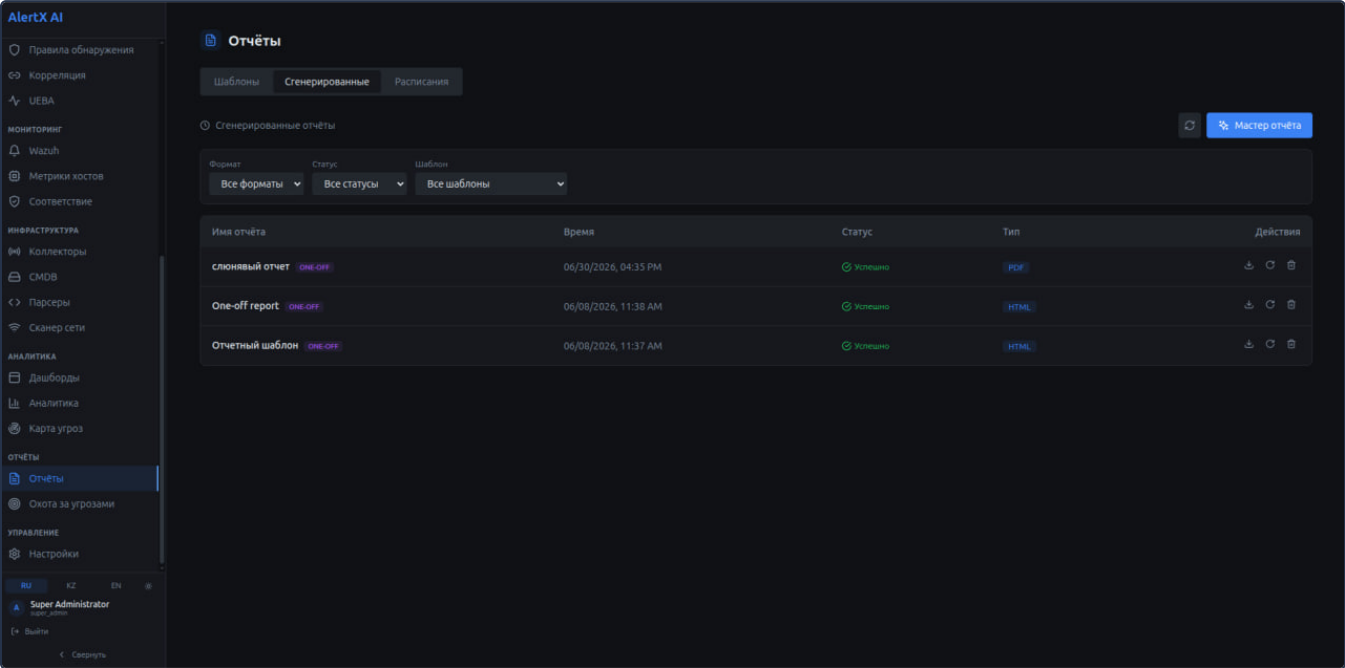


Рис. 10. «Отчёты», вкладка «Сгенерированные» — архив отчётов с фильтрами по формату, статусу и шаблону; действия: скачать, регенерировать, удалить.

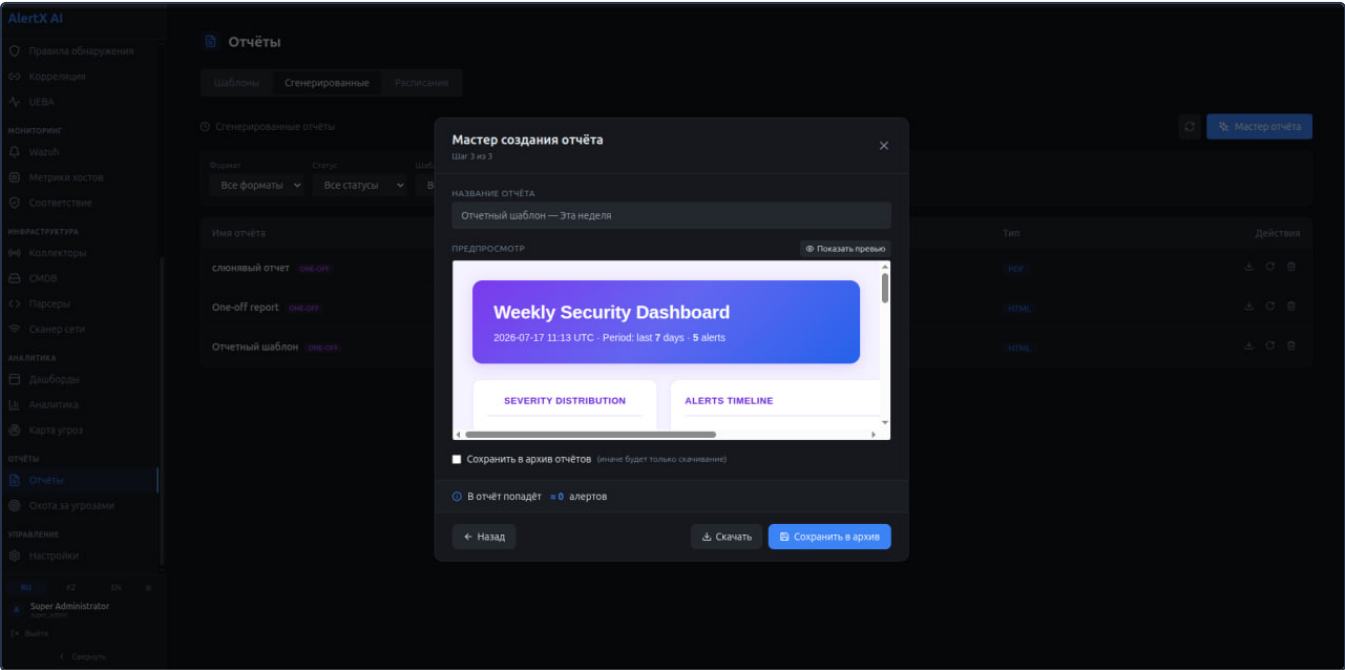


Рис. 11. «Мастер создания отчёта», шаг 3 из 3 — предпросмотр отчёта перед скачиванием или сохранением в архив.

Управление	
СТРАНИЦА	НАЗНАЧЕНИЕ
Настройки	Пользователи, организации, аудит-лог, резервное копирование, здоровье системы, API-ключи, интеграции.

1.2 Типовой сценарий работы аналитика

1. Дежурный следит за страницей **Алерты** (обновление в реальном времени).
2. По новому алерту открывает карточку: обогащение (GeoIP, threat intel, AI-анализ), связанные события.
3. Ложное срабатывание — закрывает алерт; подтверждённая угроза — эскалирует. Критические алерты ($\text{severity} \geq 8$) автоматически становятся инцидентами, срабатывают плейбуки (блокировка IP, обогащение IOC, уведомления в Telegram/Email и др.).
4. Расследование ведёт в **Обнаружении логов** (Lucene-запросы по сырым логам) и **SQL Запросах**.
5. Результаты фиксирует в **Инциденте / Деле**; по итогам периода формирует **Отчёт**.

2 Архитектура

2.1 Технологический стек

КОМПОНЕНТ	ТЕХНОЛОГИЯ
Backend	FastAPI (Python 3.11), Uvicorn, порт 8000
Frontend	React 18 + TypeScript + Vite + Tailwind CSS
Хранилище	OpenSearch 2.18 (кластер до 3 нод), Redis (кэш, сессии, auth)
Шина сообщений	Apache Kafka 3.8 (KRaft, SSL для внешних подключений)
Конвейер логов	Logstash 8.17 (40+ фильтр-пайплайнов), Filebeat на коллекторах
AI	LM Studio (локальная LLM для анализа алертов)
HIDS	Wazuh
Прокси	Nginx (TLS-терминация, порты 80/443)

2.2 Поток данных (центральный сервер)



Схема 1. Поток данных на центральном сервере: от приёма событий на трёх портах до доставки алертов аналитику и в каналы уведомлений.

2.3 Удалённые коллекторы

Коллектор — автономный узел на площадке заказчика, устанавливаемый скриптом `install.sh` (генерирует docker-compose, конфигурации пайплайнов и SSL-сертификаты).

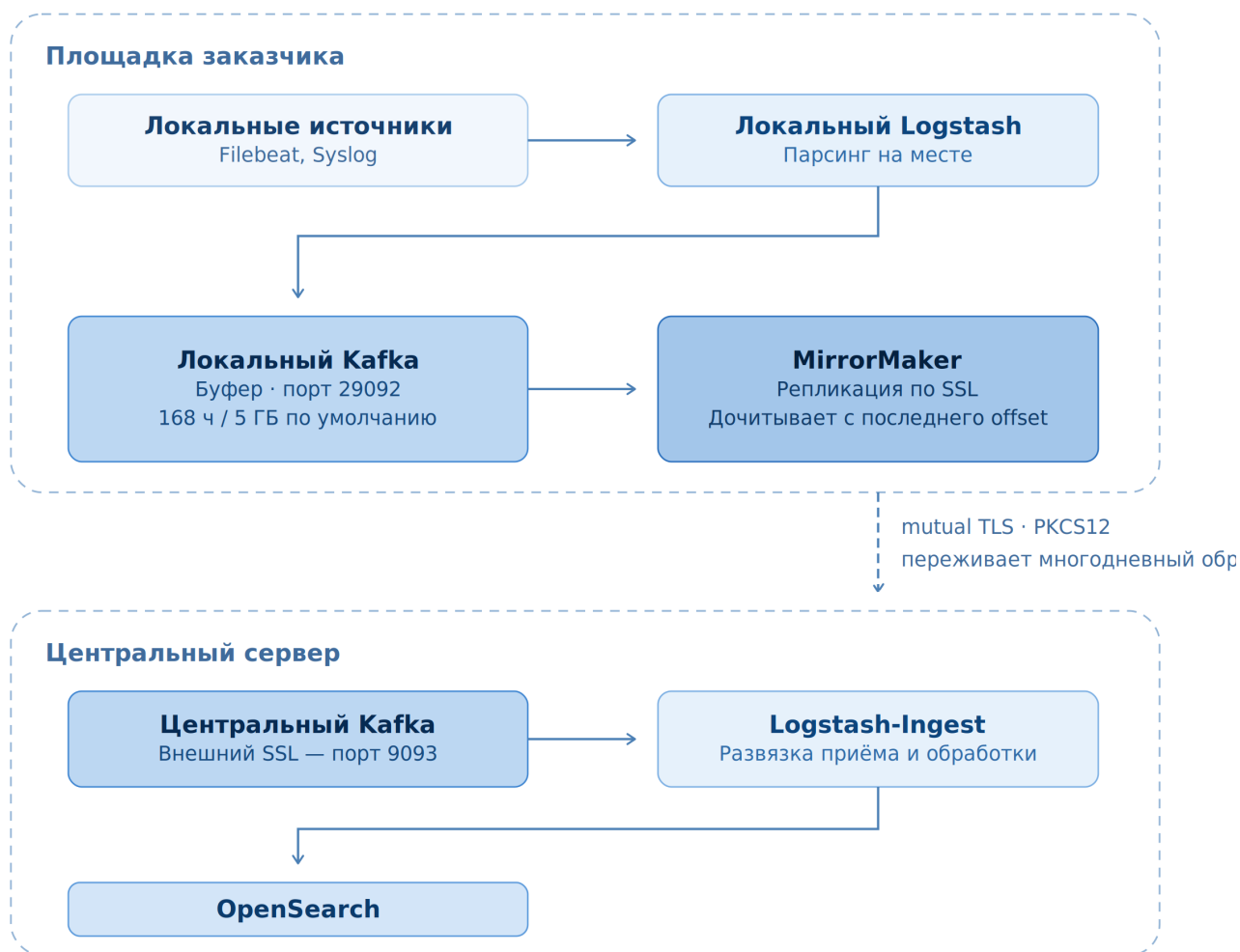


Схема 2. Удалённый коллектор: локальный Kafka принимает события независимо от доступности центра, MirrorMaker реплицирует очередь по mutual TLS и дочитывает её с последнего offset после восстановления связи.

Каналы коллектор → центр защищены mutual TLS: центральный Kafka слушает внешний порт 9093 с SSL-keystore; коллектор получает CA-сертификат в truststore при установке (PKI управляется центральным сервером).

2.4 Мультитенантность

Каждый объект данных содержит `org_id`; все запросы к OpenSearch фильтруются по организации. Индексы именуются `{тип}-{org_id}-{дата}`. Super admin видит все организации, org_admin — только свою.



Изоляция на уровне запроса и на уровне имени индекса

Схема 3. Мультиотенантная изоляция: роль определяет область видимости, фильтр по `org_id` разводит запросы к индексам конкретной организации.

3 Отказоустойчивость

3.1 Кластер OpenSearch

Целевая топология хранилища — **кластер из трёх нод OpenSearch** с репликацией шардов: выход из строя одной ноды не приводит к потере данных и остановке приёма событий — кластер продолжает работать на оставшихся нодах, реплики повышаются до primary. Снапшоты пишутся в общий репозиторий (`opensearch-snapshots`) для резервного копирования.

В dev/single-node конфигурации `docker-compose.yml` активна одна нода (node2/node3 закомментированы); в продакшен-развёртывании включаются все три.

3.2 Буферизация на коллекторе при потере связи

Ключевой механизм устойчивости к обрывам канала «площадка → центр»:

- Локальный Kafka на коллекторе принимает все события от Logstash **независимо от доступности центрального сервера**.
- MirrorMaker непрерывно пытается реплицировать очередь в центральный Kafka; при недоступности центра события просто накапливаются в локальном топике.
- После восстановления связи MirrorMaker дочитывает очередь с последнего зафиксированного offset — **данные доставляются без потерь и без дублей**, порядок сохраняется.
- Глубина буфера задаётся retention-настройками локального Kafka: `KAFKA_RETENTION_HOURS` (по умолчанию **168 часов = 7 суток**) и `KAFKA_RETENTION_BYTES` (по умолчанию 5 ГБ на топик). Значения настраиваются через `.env` коллектора; для буфера в 3 суток задаётся `KAFKA_RETENTION_HOURS=72`.
- Таким образом коллектор переживает многодневный обрыв связи с центральным сервером без потери логов (пока не исчерпан лимит времени/объёма буфера).

3.3 Прочие механизмы

- **Kafka на центральном сервере** развязывает приём (Logstash-Ingest) и обработку: пики нагрузки и рестарты потребителей не теряют события.
- **Redis + OpenSearch для auth-данных**: пользователи хранятся в OpenSearch (персистентно, шифрование через ConfigStore) и кэшируются в Redis (TTL 24 ч) — рестарт Redis не теряет учётные записи, рестарт OpenSearch не рвёт активные сессии.
- **ConfigStore** — шифрованное key-value хранилище (индекс `config-system` в OpenSearch + горячий кэш Redis) для конфигураций, API-ключей и настроек коллекторов.
- **Автовосстановление сервисов**: контейнеры Docker перезапускаются политиками restart; при старте backend гарантированно создаёт администратора (`_ensure_admin_exists()`).
- **Детектирование не зависит от backend**: основной движок — OpenSearch Alerting Plugin, мониторы выполняются внутри кластера OpenSearch по расписанию, поэтому кратковременная недоступность backend не останавливает детект.
- **Nginx** терминирует TLS и является единственной внешней точкой входа; реальный IP клиента берётся из `X-Forwarded-For` только от доверенного прокси.

4 Сетевые порты (справочно)

ПОРТ	НАЗНАЧЕНИЕ
80 / 443	Nginx (веб-интерфейс, HTTPS)
8000	Backend FastAPI (за Nginx)
514/udp	Приём Syslog
5044	Приём Beats
5000	Приём Wazuh
9092	Kafka внутренний (центр)
9093	Kafka внешний SSL (для коллекторов)
29092	Kafka локальный (на коллекторе)
9200	OpenSearch API (внутренний)