VB-Trend 2025

АНТИХРУПКОСТЬ БИЗНЕСА

Smart EDR: альянс с BI. ZONE

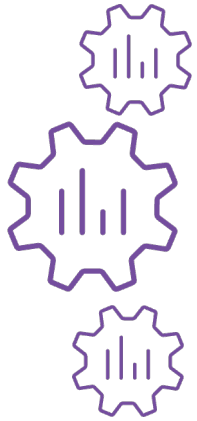
Smart EDR

Силкин Иван
VolgaBlob

Хеирхабаров Теймур
BI.ZONE

BI.ZONE EDR

- Сбор более 200 типов событий мониторинга и инвентаризации
- Обнаружение тактик и техник атакующих
- Расследование и реагирование на конечной точке
- Выявление уязвимостей и недостатков конфигурации
- Мониторинг событий внутри контейнерных сред



Smart Monitor

Smart EDR

- Интеграция с менеджером инцидентов
- Обогащение инвентаризации
- Функциональные дашборды и кейс с анализом покрытия
- Интеграция с модулем Cyber Security и MITRE ATT&CK

Возможности BI.ZONE EDR

Обнаружение

Threat prediction
Автоматизированное выявление недостатков инфраструктуры

IoC
Автоматизированное выявление следов атакующих

Офлайн
Выявление атак без доступа к серверу управления

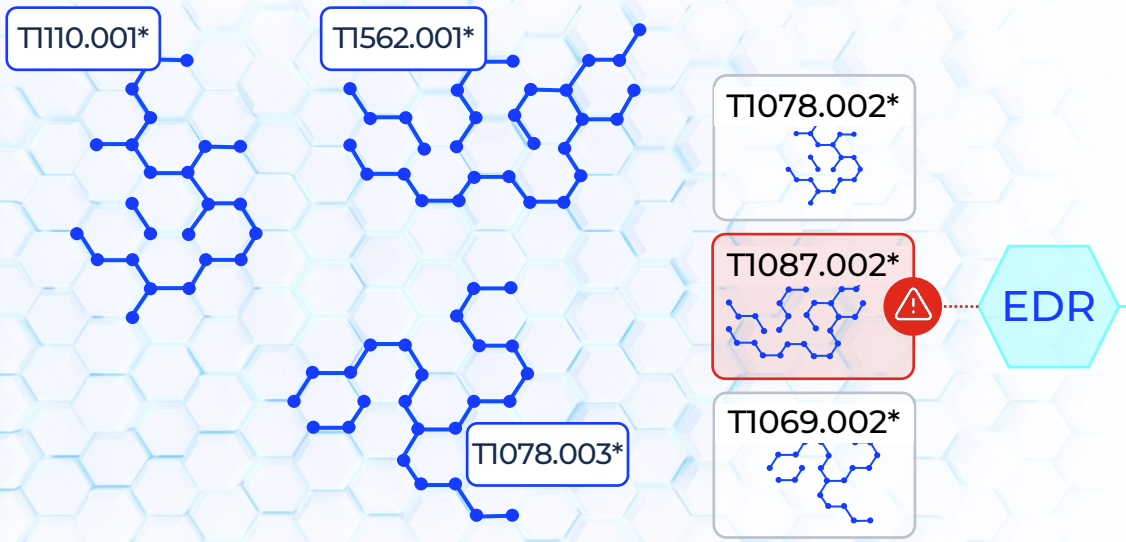
IoA
Автоматизированное выявление TTP атакующих

Deception
Выявление атакующих с помощью хостовых ловушек

Threat hunting
Ручной проактивный поиск следов и TPP атакующих

Мониторинг (сбор телеметрии)

- Процессы
- Файловая система
- Реестр
- Сетевая активность
- Память
- Учетные записи
- Входы, сессии
- Именованные каналы
- WMI
- Контейнеры
- Скрипты (PS, AMSI)



Расследование и реагирование

- Скачивание и загрузка файлов
- Завершение процесса
- Удаление файлов
- Сбор данных
- Изоляция хоста
- Интерактивная консоль
- Запуск процессов и скриптов
- Автоматическое реагирование

Телеметрия
Передача собранных событий

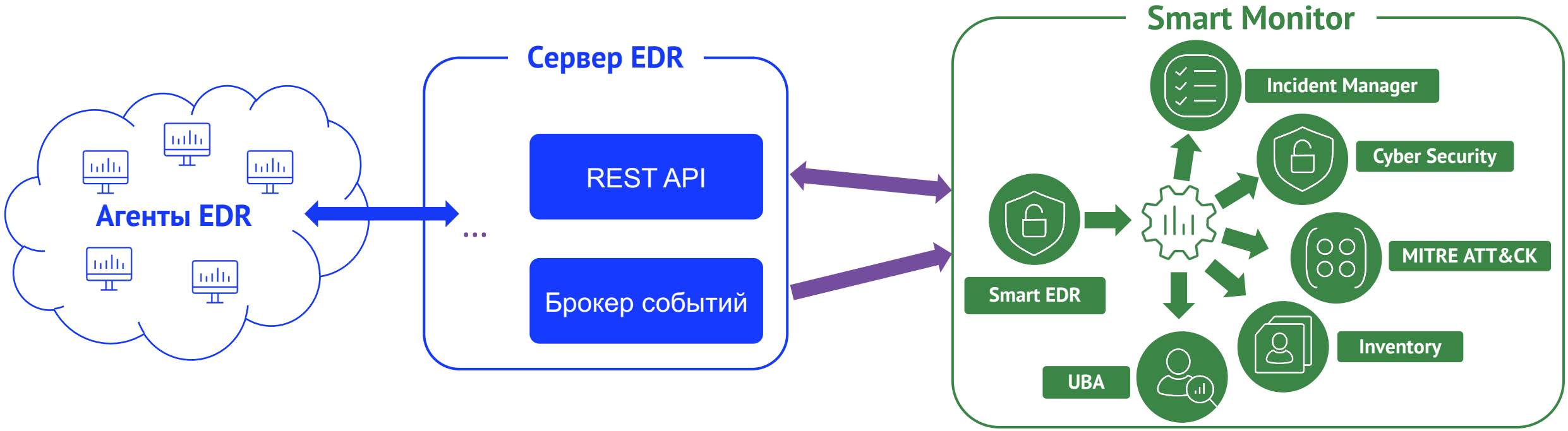
Обнаружение
Передача обнаружений по внутренним правила

Реагирование
Возможность запуска задач реагирования извне

Интеграции с внешними системами

VolgaBlob

Схема интеграции



REST API

- **задачи** расследования и реагирования
- результаты задач
- **агенты** и **инвентаризация**
- метаданные **инцидентов**
- **триггеры**

Забираем из брокера

- алерты правил **выявления угроз**
- алерты правил **превентивного выявления угроз**
- **телеметрия хоста** (создание процессов, вход, общее состояние системы и агента EDR и т.д.)

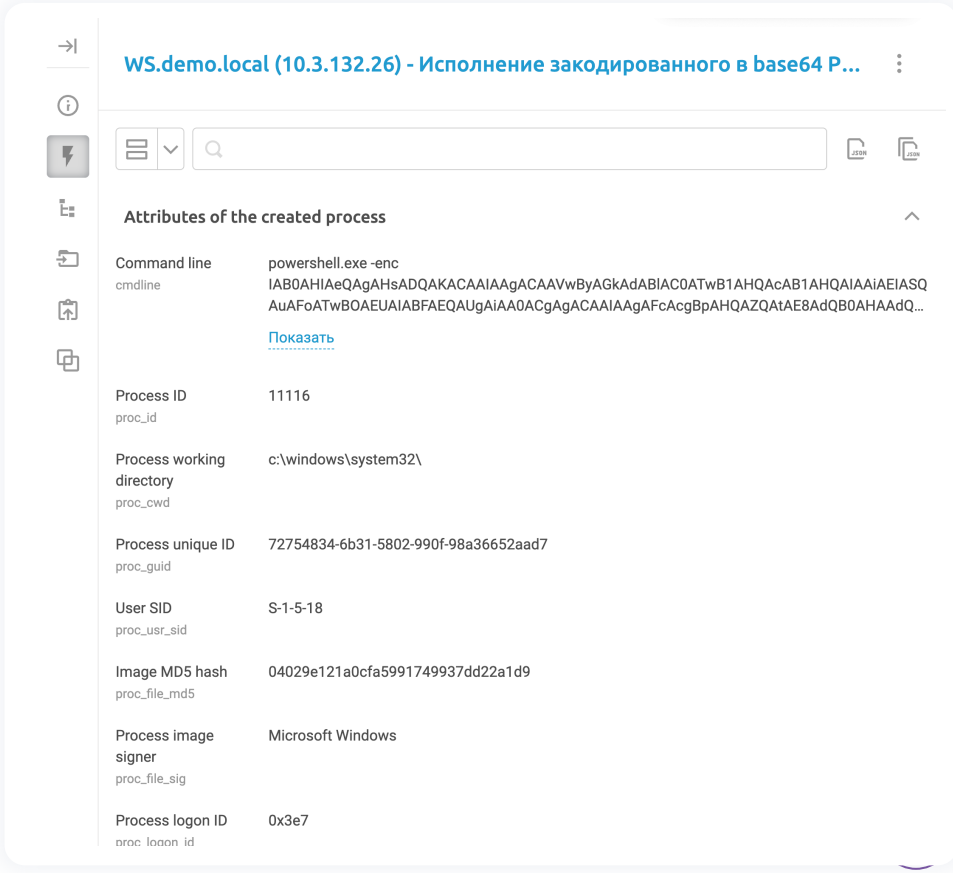
VolgaBlob

Обнаружения с помощью BI.ZONE EDR

- Различные технологии обнаружения: IoC, YARA, IoA
- Пользовательские правила и исключения
- Офлайн-детектирование без общения с сервером
- Встроенный модуль Deception, хостовые приманки

700+
IoA-правил

2 500+
YARA-правил



VolgaBlob

Интеграция с менеджером инцидентов

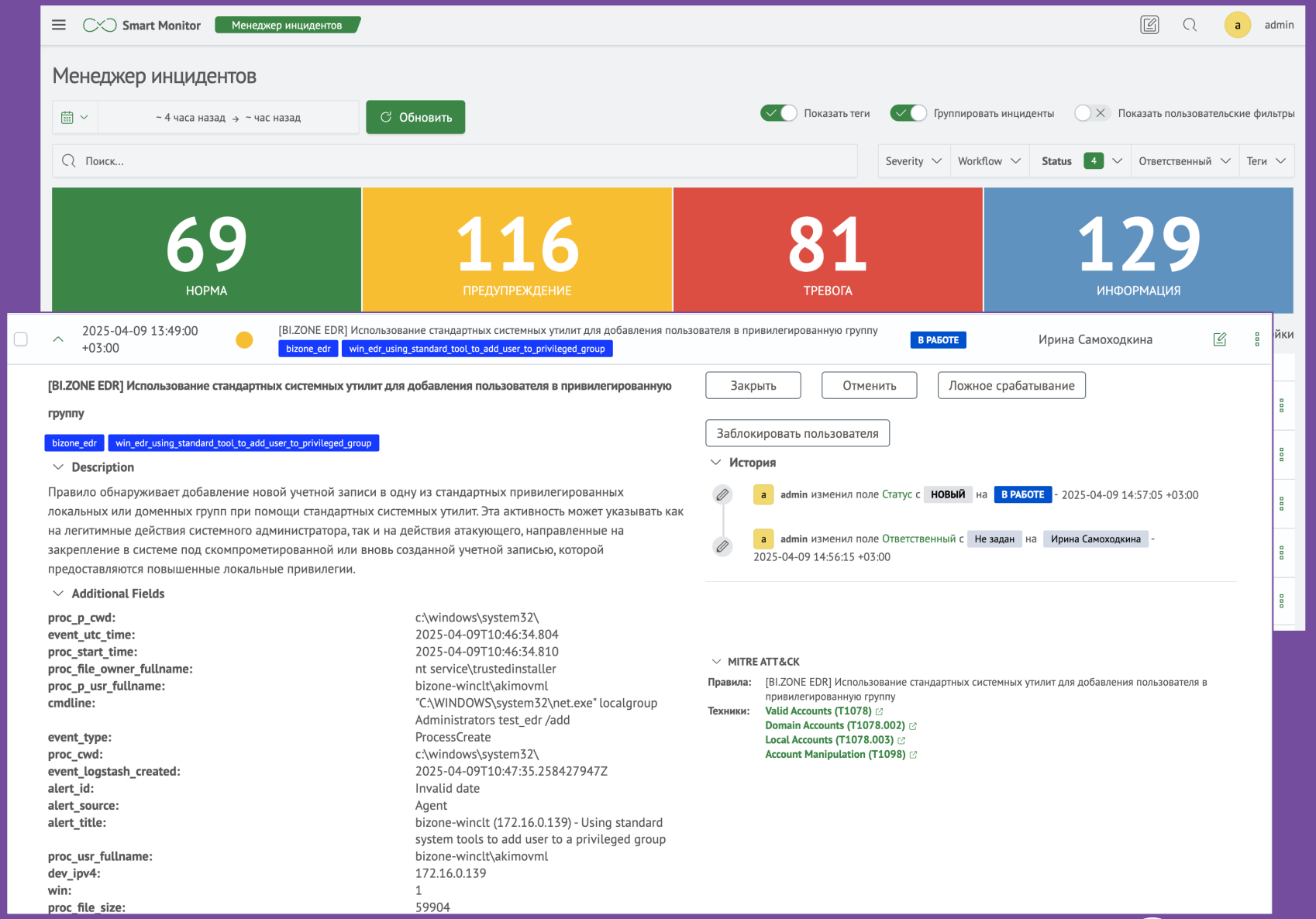
Алерты со всей мета-информацией

Гибкая настройка

Работа с инцидентами и анализ процесса

Реакции по кнопке

Дополнительные данные для расследования



VolgaBlob

Интеграция с менеджером инцидентов

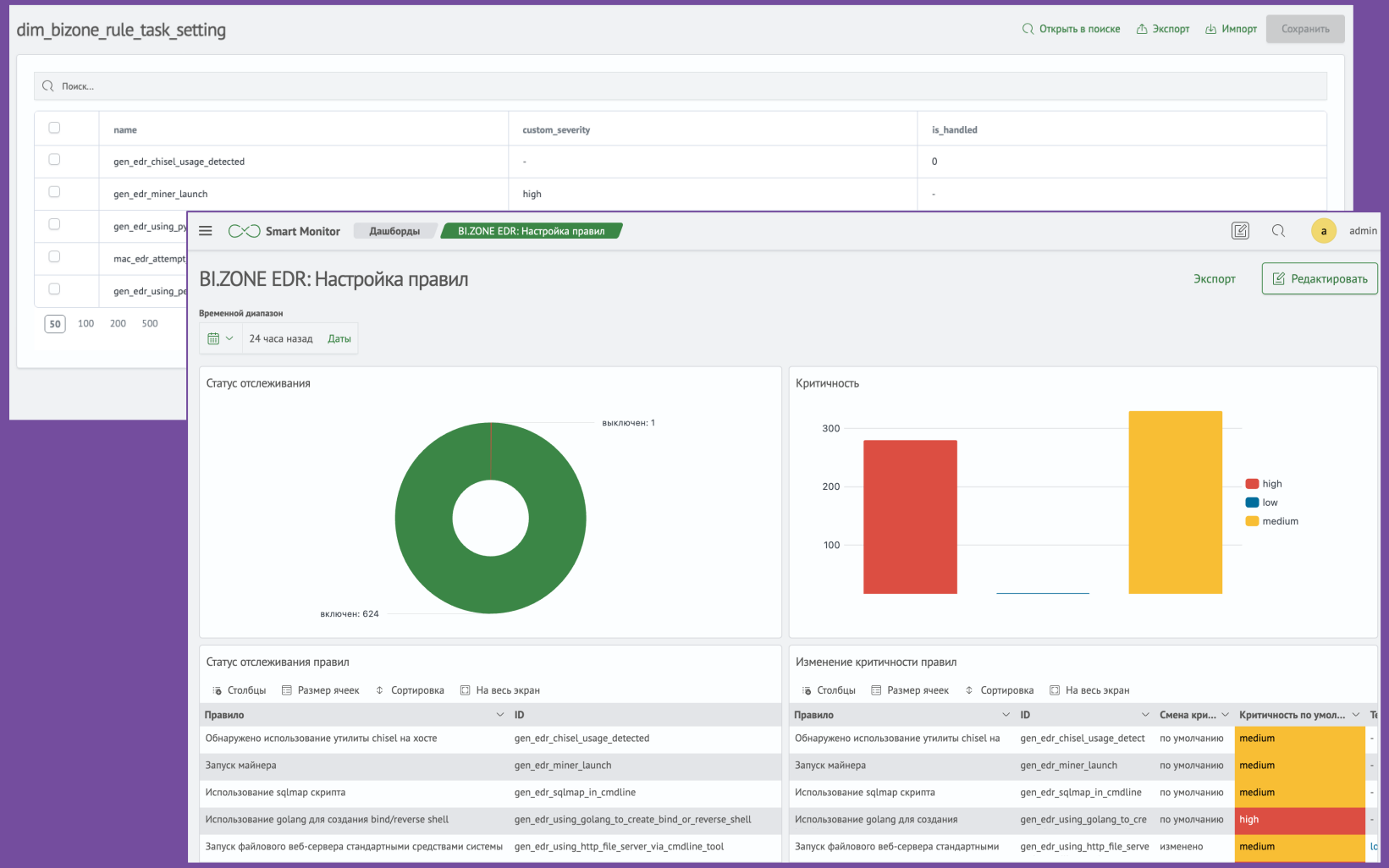
Алерты со всей мета-информацией

Гибкая настройка

Работа с инцидентами и анализ процесса

Реакции по кнопке

Дополнительные данные для расследования



VolgaBlob

Интеграция с менеджером инцидентов

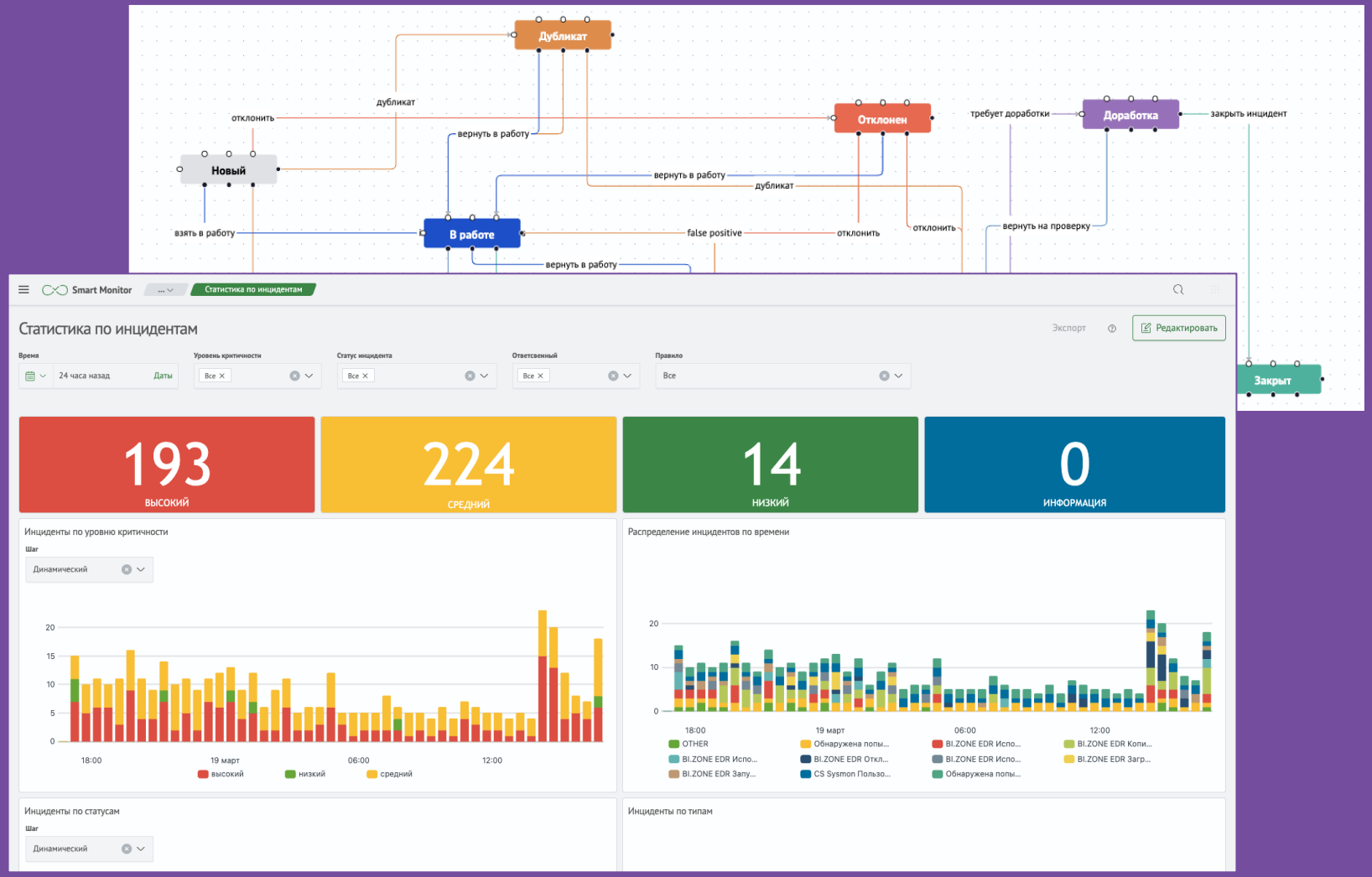
Алерты со всей мета-информацией

Гибкая настройка

Работа с инцидентами и анализ процесса

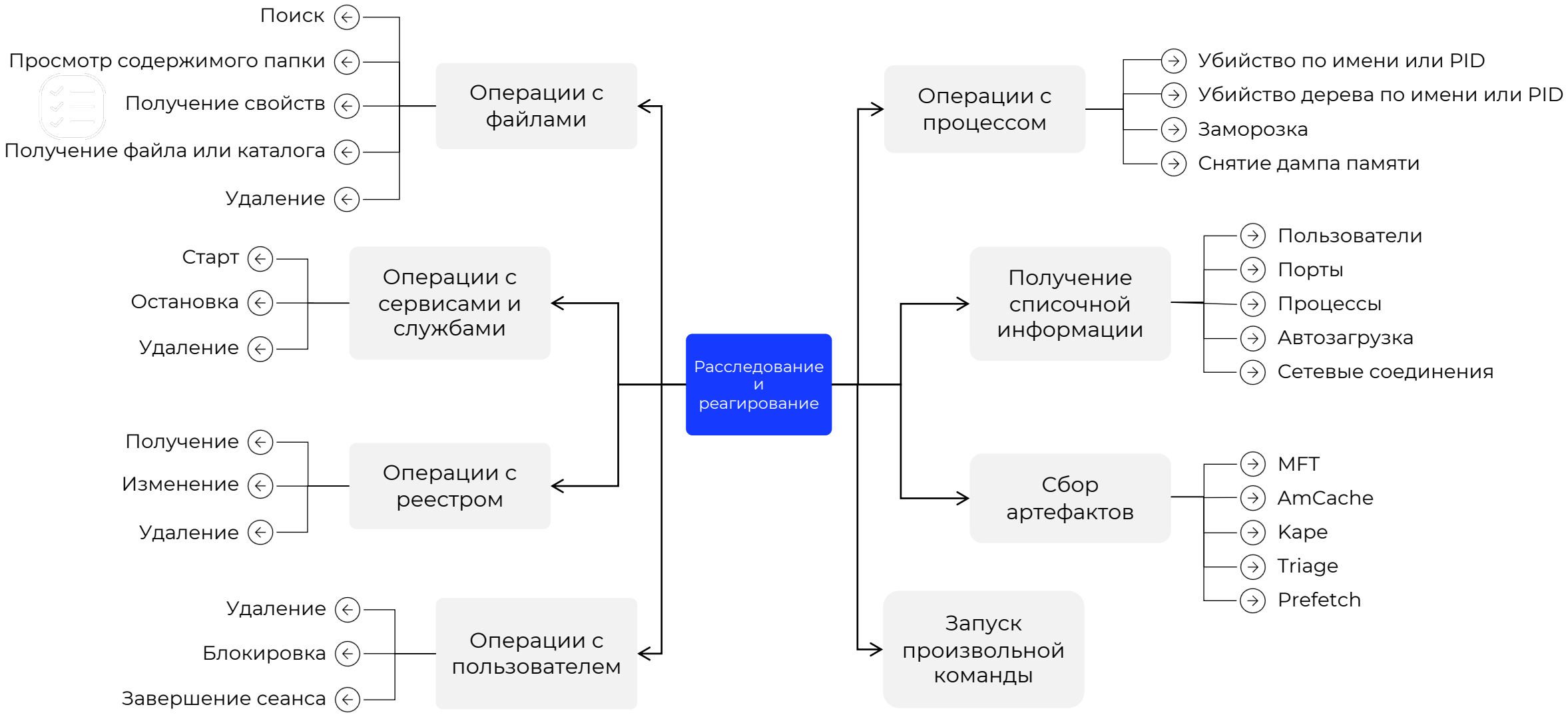
Реакции по кнопке

Дополнительные данные для расследования



VolgaBlob

Типы реакций BI.ZONE EDR



Библиотека задач реагирования BI.ZONE EDR

- Регулярно обновляемая библиотека задач
- Содержит задачи сбора данных для расследования и задачи сдерживания атаки
- В основе — опыт экспертов BI.ZONE по реагированию на инциденты и оценке инфраструктур на компрометацию

IR Identification

- [BZ] [Win] Collect a forensics package
- [BZ] [Nix] Collect a forensics package
- [BZ] [Nix] Get command history
- [BZ] [Nix] Get logon history
- [BZ] [Nix] List opened files
- [BZ] [Win] Run AV Scan (if host has AV)
- [BZ] [Win] YARA processes scan
- [BZ] [Win] YARA file system scan
- [BZ] [Win] YARA critical areas scan
- [BZ] [Nix] YARA processes scan
- [BZ] [Nix] YARA file system scan
- [BZ] [Nix] YARA critical areas scan
- [BZ] [All] File search
- [BZ] [All] Get file or directory
- [BZ] [All] Get file properties
- [BZ] [All] List directory content (depth 3)
- [BZ] [Win] List processes
- [BZ] [Nix] List processes
- [BZ] [Win] Get autoruns
- [BZ] [Nix] Get autoruns
- [BZ] [Win] Get network connections
- [BZ] [Nix] Get network connections
- [BZ] [Win] Get event logs
- [BZ] [Win] Get MFT
- [BZ] [Win] Get system registry hives
- [BZ] [Win] Get amcache
- [BZ] [Win] Get prefetch files
- [BZ] [Win] Dump process by PID or procname
- [BZ] [Win] List group policies

IR Containment & Eradication

- [BZ] [All] Remove file or directory
- [BZ] [Win] Terminate user sessions
- [BZ] [Win] Remove registry key/value
- [BZ] [Win] Change registry key/value
- [BZ] [Win] Block domain user account
- [BZ] [Win] Block local user account
- [BZ] [Nix] Block local user account
- [BZ] [Win] Remove domain user
- [BZ] [Win] Remove local user
- [BZ] [Nix] Remove local user
- [BZ] [Win] Kill process by PID
- [BZ] [Nix] Kill process by PID
- [BZ] [Win] Kill process tree by PID
- [BZ] [Win] Kill process by procname
- [BZ] [Nix] Kill process by procname
- [BZ] [Win] Kill process tree by procname
- [BZ] [Win] Suspend process by PID or procname
- [BZ] [Win] Kill process by executable hash
- [BZ] [Win] Kill process tree by executable hash
- [BZ] [Nix] Kill process by executable hash
- [BZ] [Nix] Kill process tree by executable hash
- [BZ] [Nix] Suspend process by PID
- [BZ] [Win] Stop service
- [BZ] [Win] Remove service
- [BZ] [Win] Stop scheduled task
- [BZ] [Win] Remove scheduled task
- [BZ] [Win] Update group policies

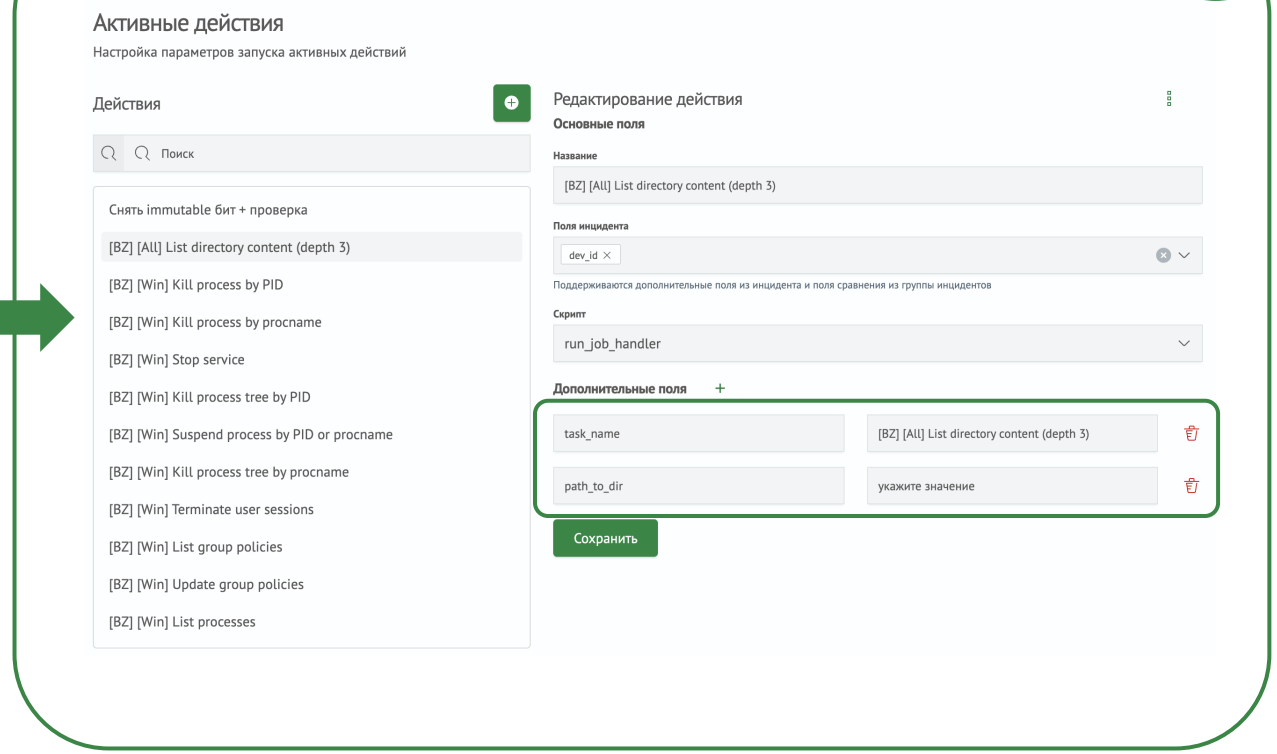
Интеграция с задачами BI.ZONE EDR

BI.ZONE EDR

Доступные задачи

Модуль Smart EDR

Активные действия



VolgaBlob

Интеграция с менеджером инцидентов

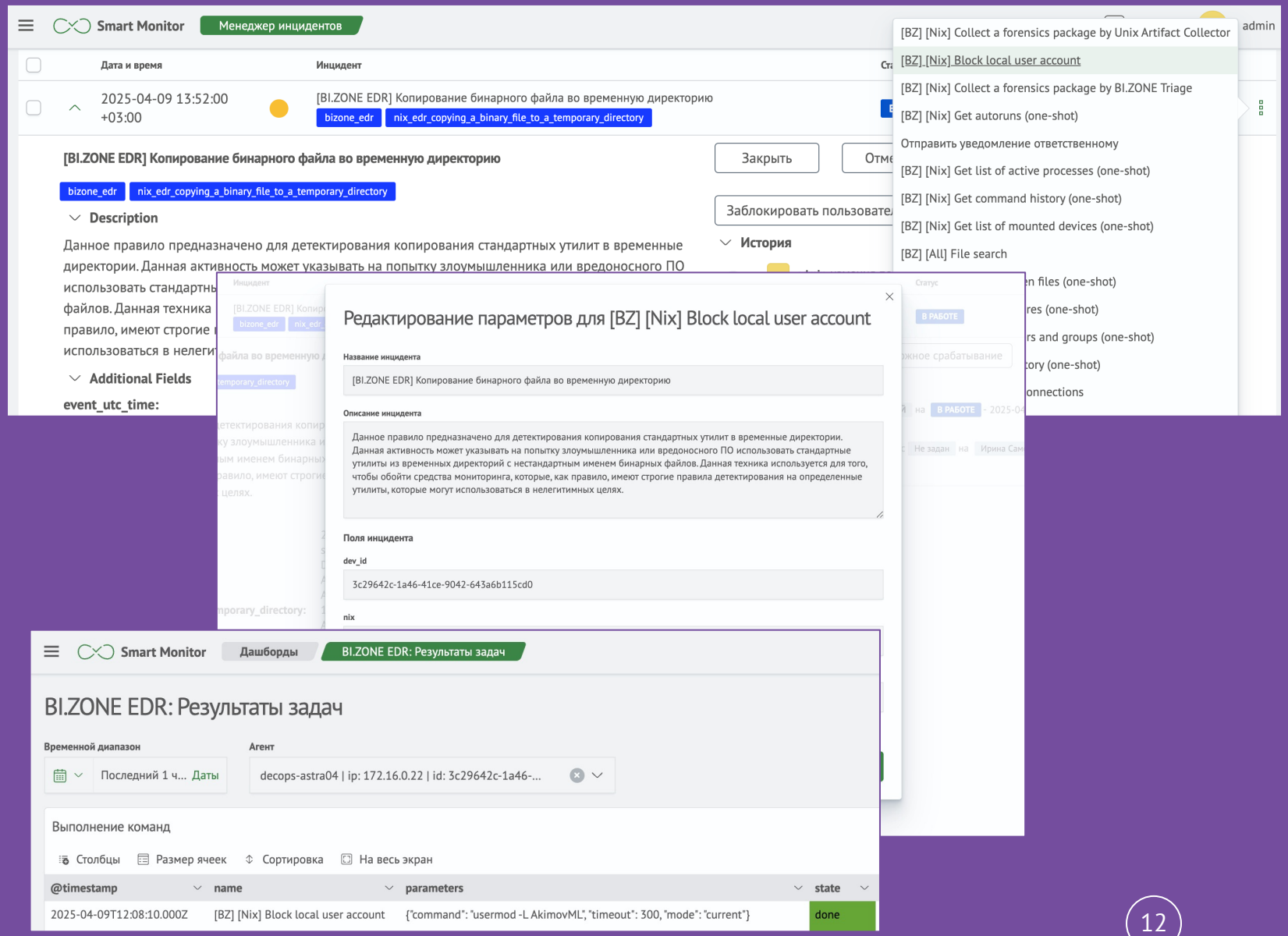
Алерты со всей мета-информацией

Гибкая настройка

Работа с инцидентами и анализ процесса

Реакции по кнопке

Дополнительные данные для расследования



VolgaBlob

Интеграция с менеджером инцидентов

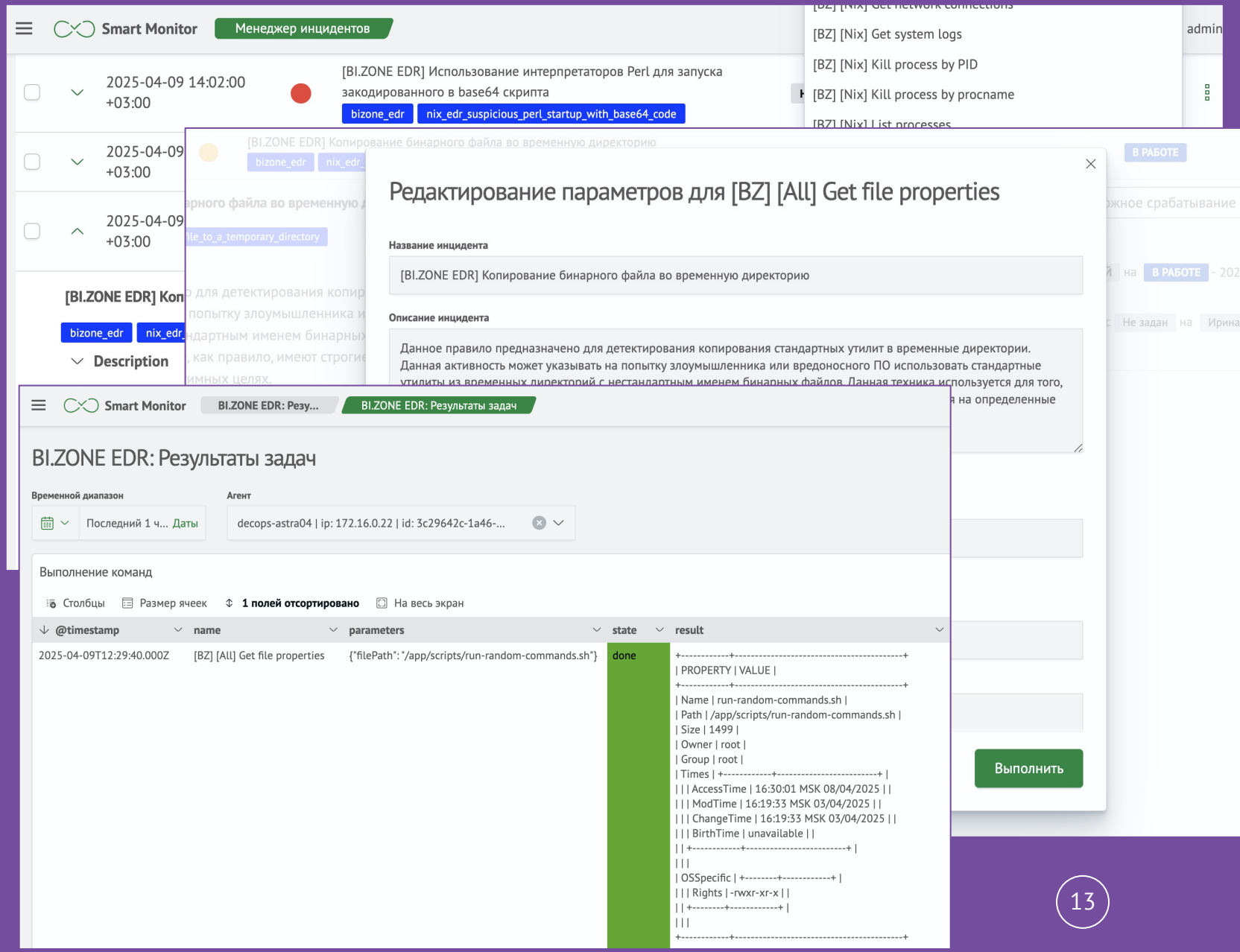
Алерты со всей мета-информацией

Гибкая настройка

Работа с инцидентами и анализ процесса

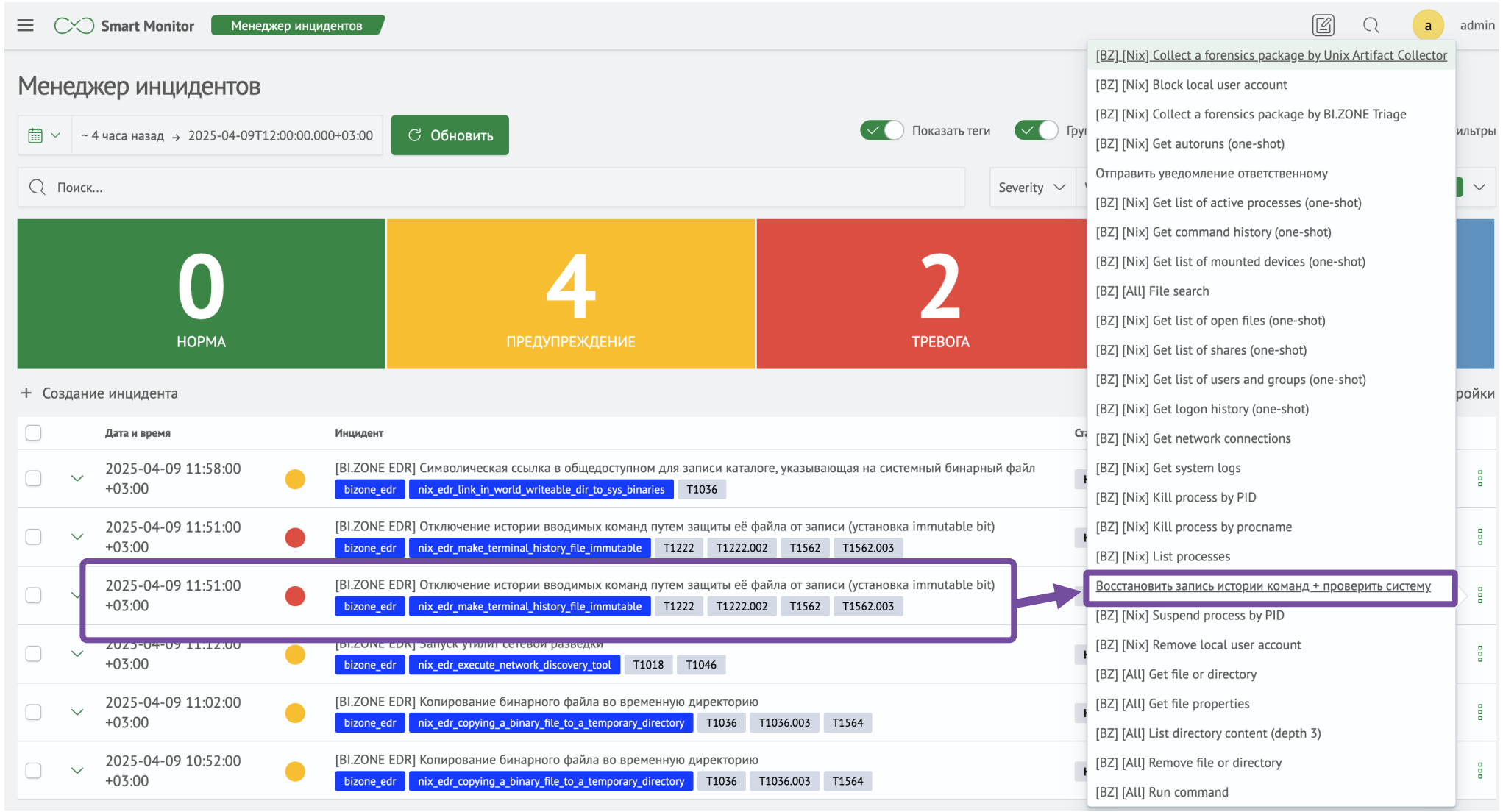
Реакции по кнопке

Дополнительные данные для расследования



VolgaBlob

Пользовательская задача (комбинированная)



Пользовательская задача (комбинированная)

Снять immutable бит + проверка

Восстановить состояние системы

1. Снять immutable bit

[BZ] [All] Run command
command: sudo chattr -i ~/.bash_history

2. Проверка, что атрибут снят

[BZ] [All] Get file properties
filePath: /root/.bash_history

3. Проверить файл истории на наличие подозрительных команд

[BZ] [Nix] Get command history (one-shot)

Проверить систему на наличие других признаков компрометации

4. Подозрительные процессы

[BZ] [Nix] List processes

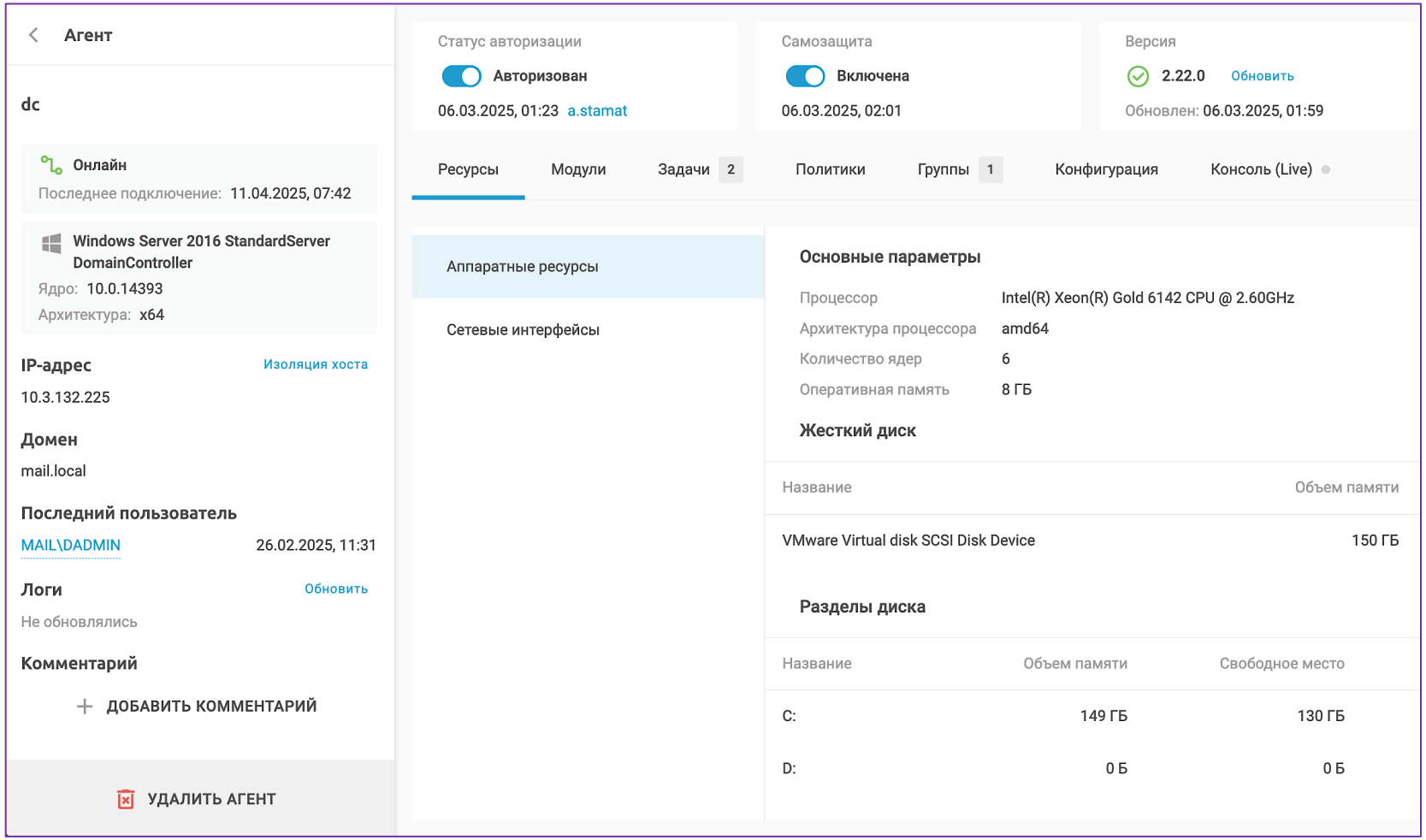
5. Неизвестные пользователи или группы

[BZ] [Nix] Get list of users and groups (one-shot)

6. Неизвестные сетевые соединения

[BZ] [Nix] Get network connections

Данные инвентаризации BI.ZONE EDR



Доступно на сервере

- список хостов с агентами
- версии установленных агентов и модулей
- операционная система
- активные пользователи
- аппаратное обеспечение

Доступно в телеметрии

- установленное ПО
- ОС и установленные роли
- сервисы
- пользователи и группы
- контейнеры
- сетевые шары
- открытые порты
- сетевые интерфейсы
- настройки ОС и приложений

VolgaBlob

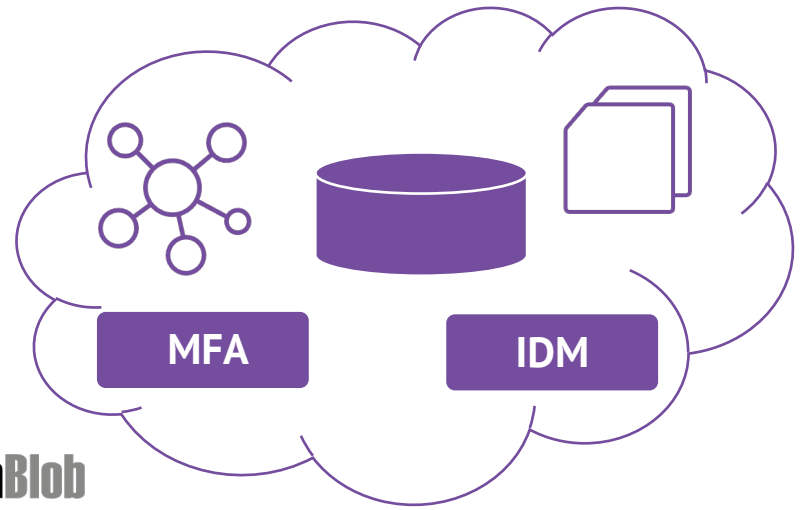
Обогащение объектов модуля инвентаризации

BI.ZONE EDR

Модуль Smart EDR

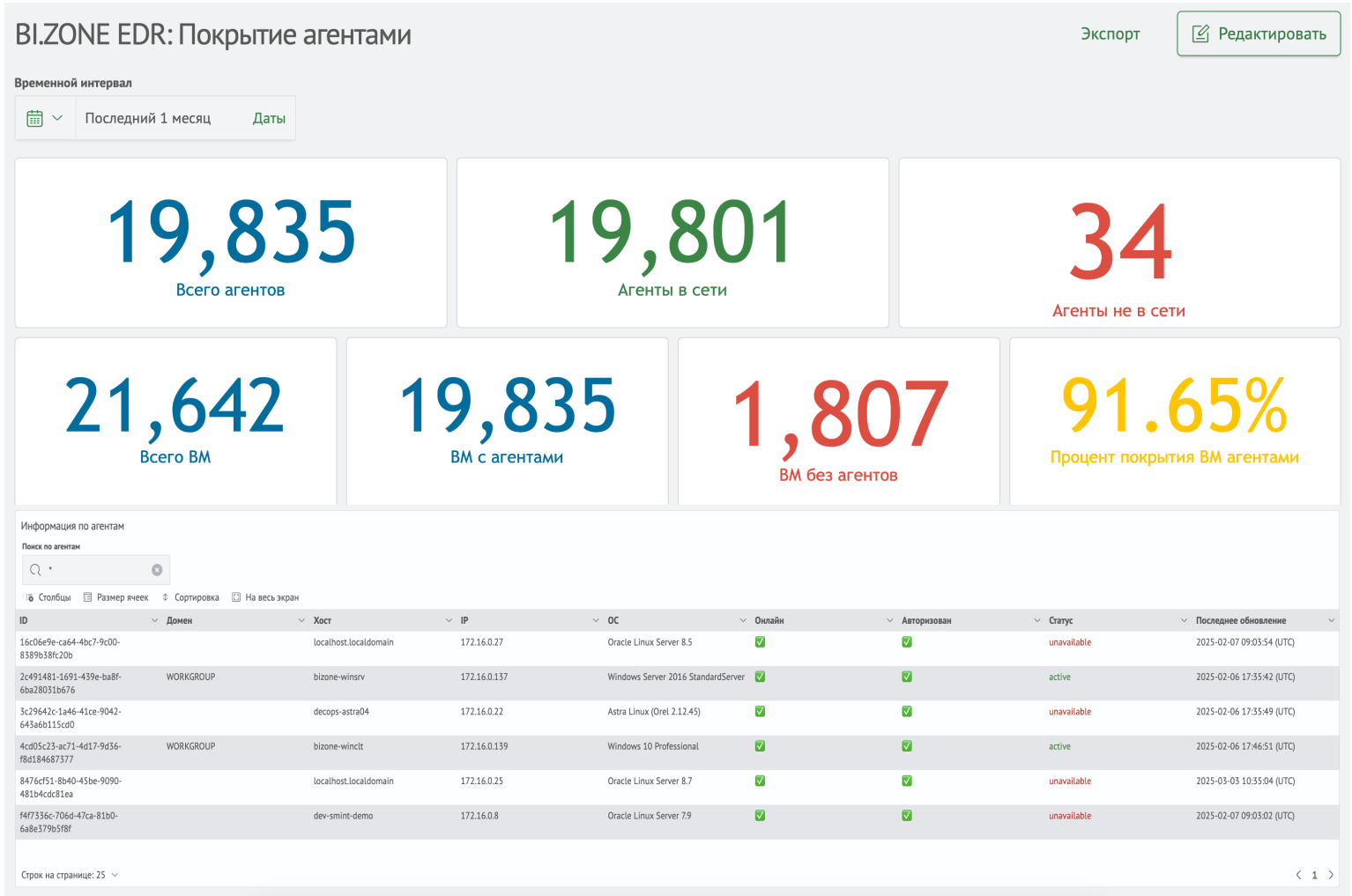
+

- Наличие агентов
- Текущее состояние
- Параметры конфигурации
- Инвентарные данные (аппаратное обеспечение, пользователи, ОС)



VolgaBlob

Анализ покрытия хостов агентами EDR



Сравниваем

- данные о **активных агентах EDR**
- перечень защищаемых активов

Определяем

- Процент **покрытых** активов
- **Количество** «проблемных» активов
- **Списки** «проблемных» активов

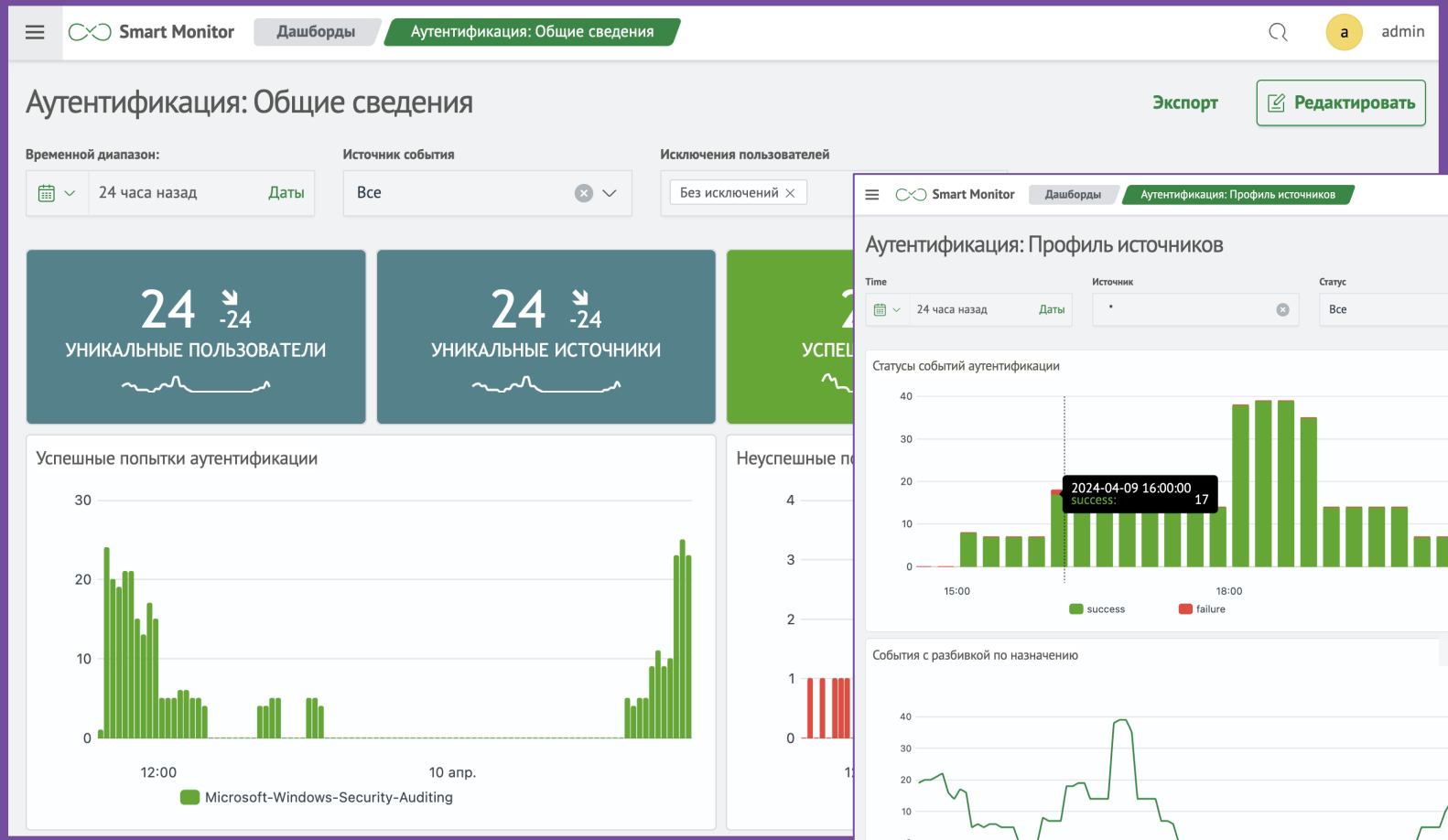
Автоматизируем

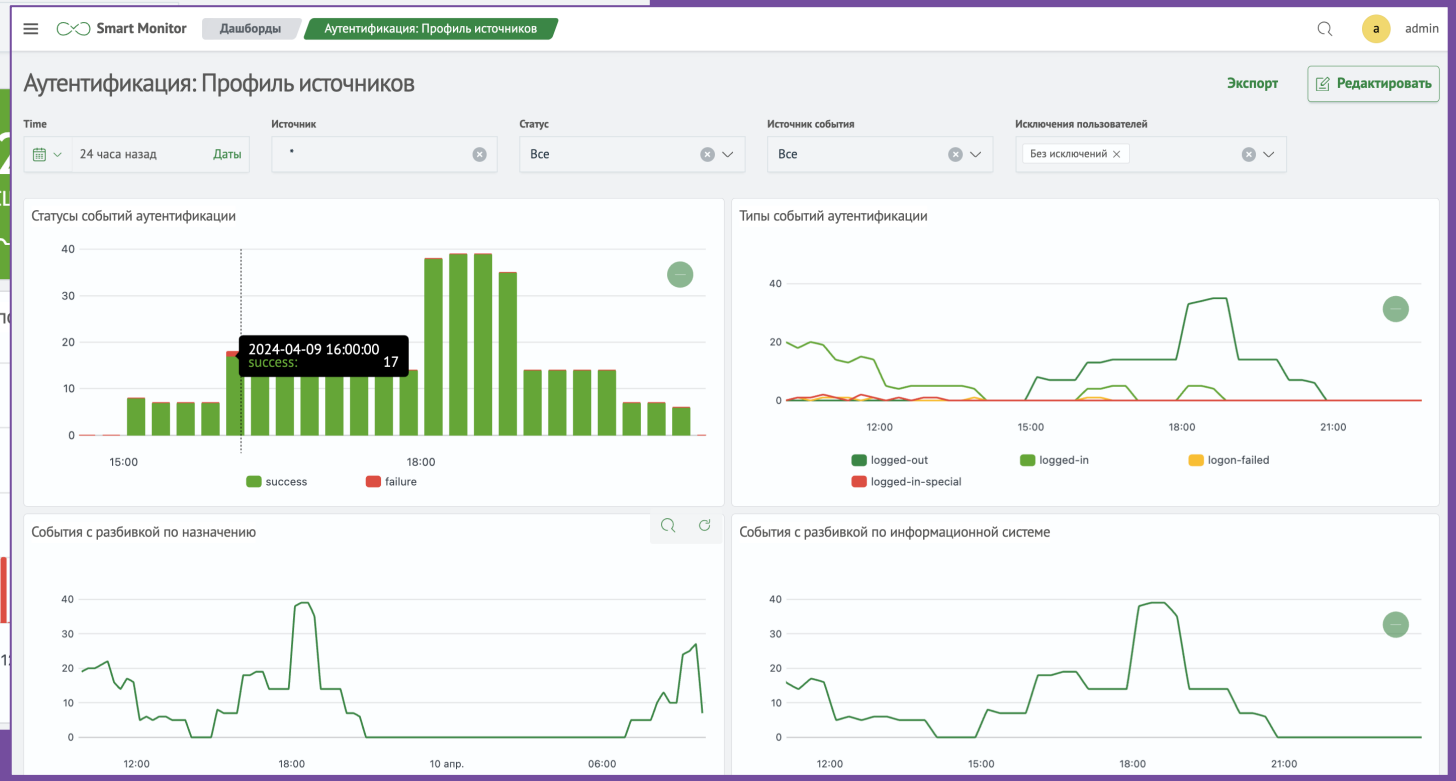
- **Автоматические** рассылки для **устранения недостатков** в покрытии

VolgaBlob

Модуль Cyber Security

Обогащение дашбордов событиями телеметрии EDR



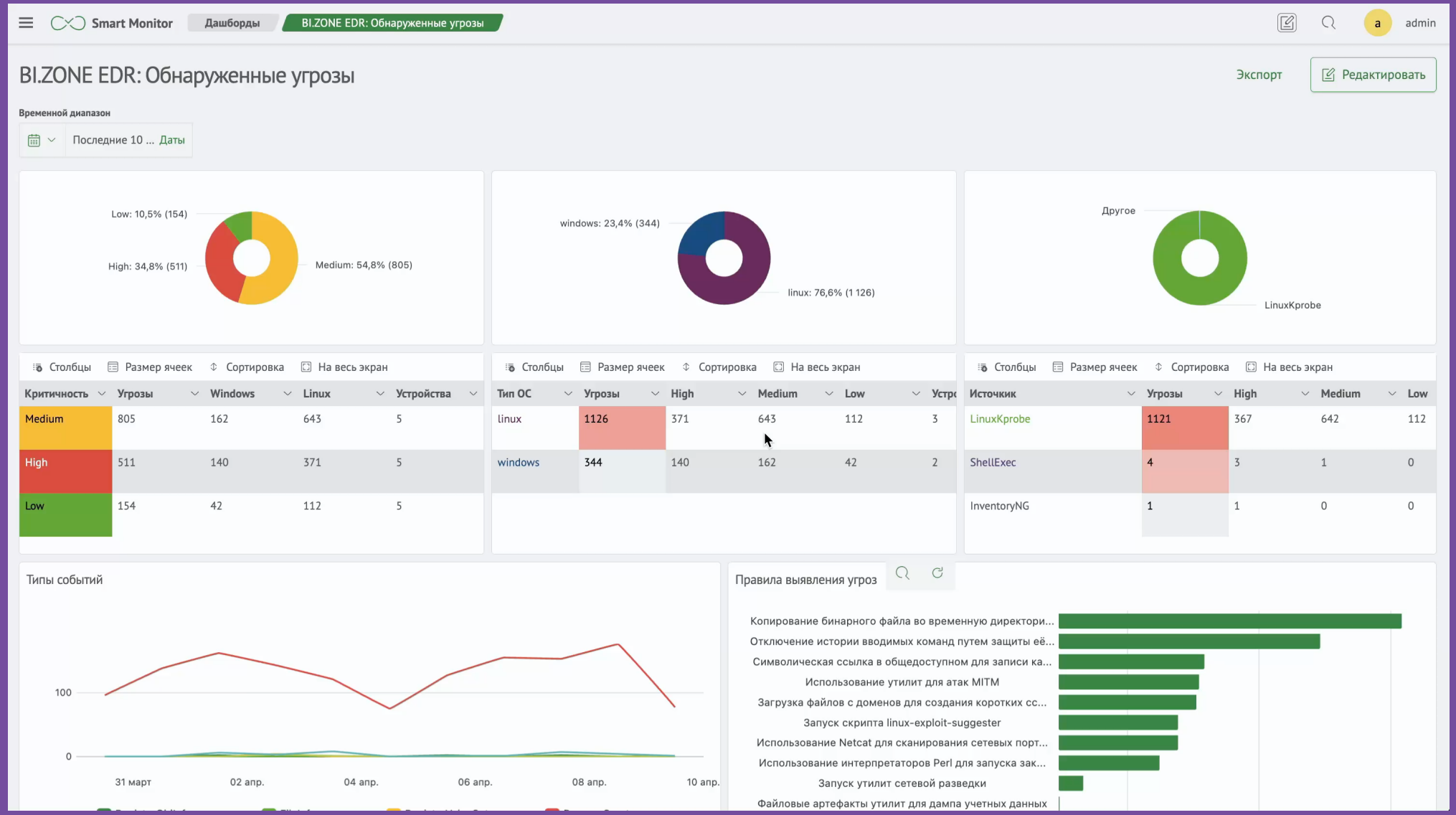


Аутентификация | Вредоносное ПО | Сеть | Электронная почта

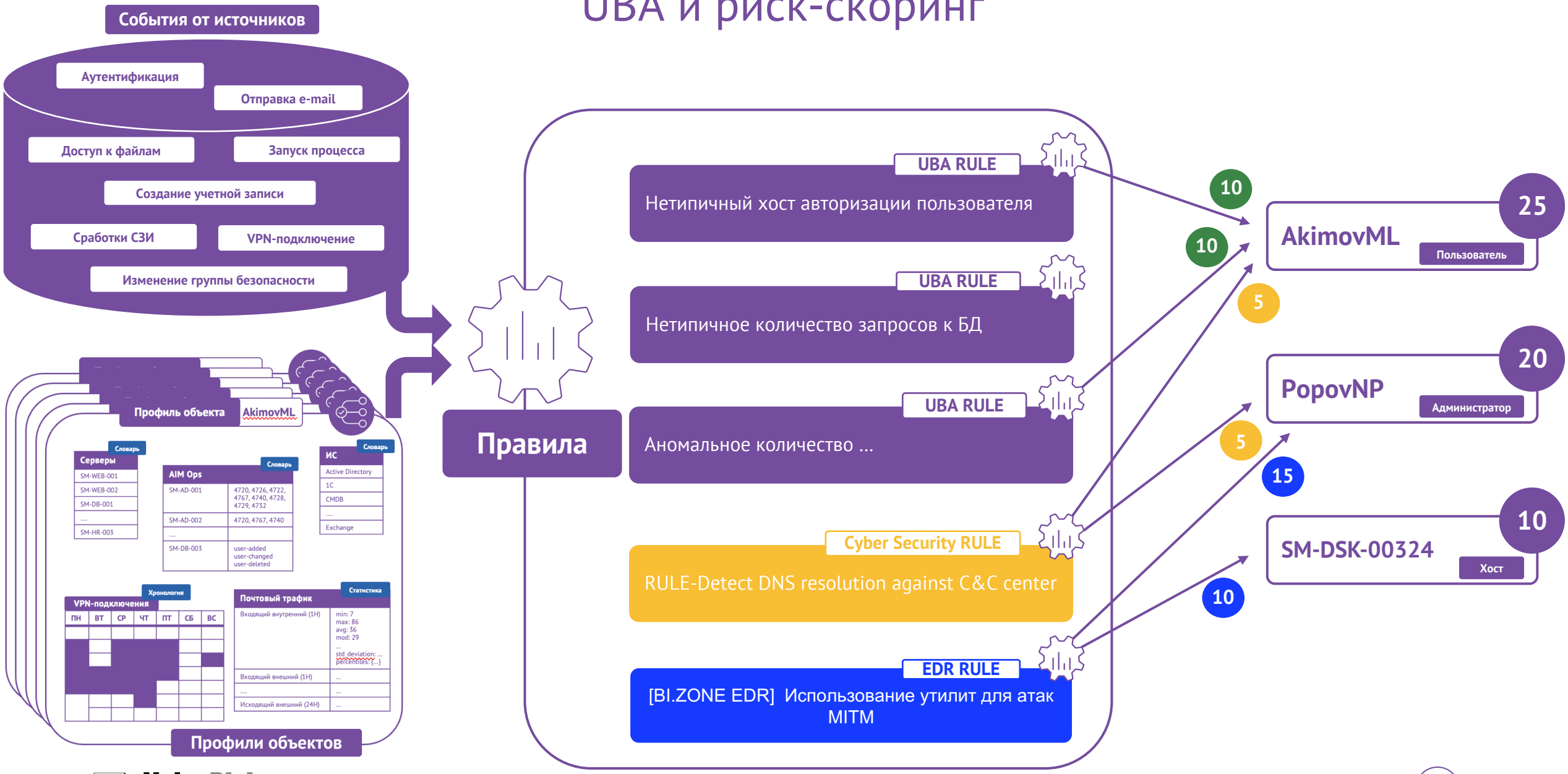
Управление учётными записями | Уязвимости | Web

VolgaBlob

Функциональные дашборды для BI.ZONE EDR



UBA и риск-скоринг



VolgaBlob

Развитие BI.ZONE EDR

- Конструктор исключений
- IOC сканер
- CMDB
- Самозащита Linux
- Сетевая изоляция Linux
- Мониторинг консольного ввода Windows
- Разовые задачи Windows

- Prevention: блокировка запуска и открытия файлов
- FIM (File Integrity Monitoring)
- Коррелятор на сервере
- Deception (новые ОС и приманки)

- Поиск неуправляемых устройств
- Конструктор правил в UI
- macOS: мониторинг сети

Развитие Smart EDR

Интеграция с модулем Deception

Данные об утилизации хостовых ловушек используются в SM для своевременного реагирования

Health-мониторинг

Функциональный мониторинг состояния компонентов BI.ZONE EDR

Телеметрия

Развитие интеграция данных телеметрии в части формирования объектов знаний (дашбордов, алертов, отчетов) для проактивного поиска следов атакующих и удобного анализа угроз в разрезе отлеживаемых объектов.

Спасибо за внимание!