



VB-Trend 2025

АНТИХРУПКОСТЬ

БИЗНЕСА

Smart EDR: альянс с BI.ZONE

Smart EDR



Силкин Иван
VolgaBlob

Хеирхабаров Теймур
BI.ZONE





BI.ZONE EDR

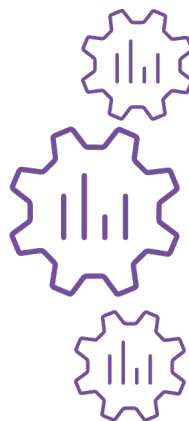
Сбор более 200 типов событий мониторинга и инвентаризации

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 TTP атакующих

✓ Мониторинг (сбор телеметрии)

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

Телеметрия

Передача собранных событий

Обнаружение

Передача обнаружений по внутренним правилам

Реагирование

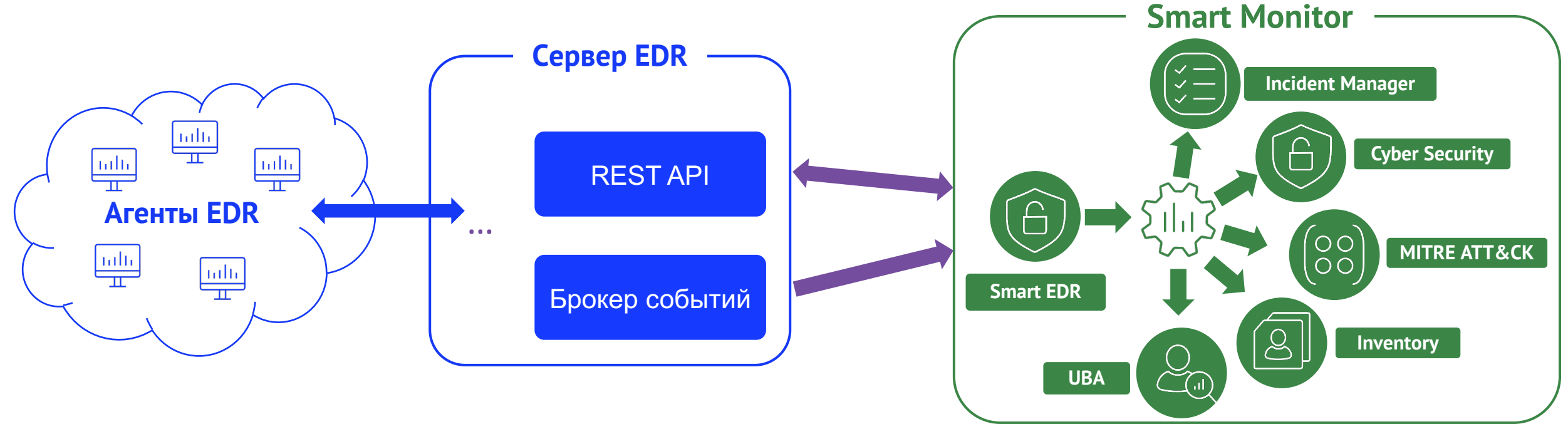
Возможность запуска задач реагирования извне

⚡ Расследование и реагирование

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

EDR

Схема интеграции



REST API

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

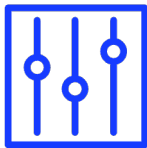
Забираем из брокера

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

Обнаружения с помощью VI.ZONE EDR



Различные технологии
обнаружения: IoC, YARA, IoA



Пользовательские
правила и исключения



Офлайн-детектирование
без общения с сервером



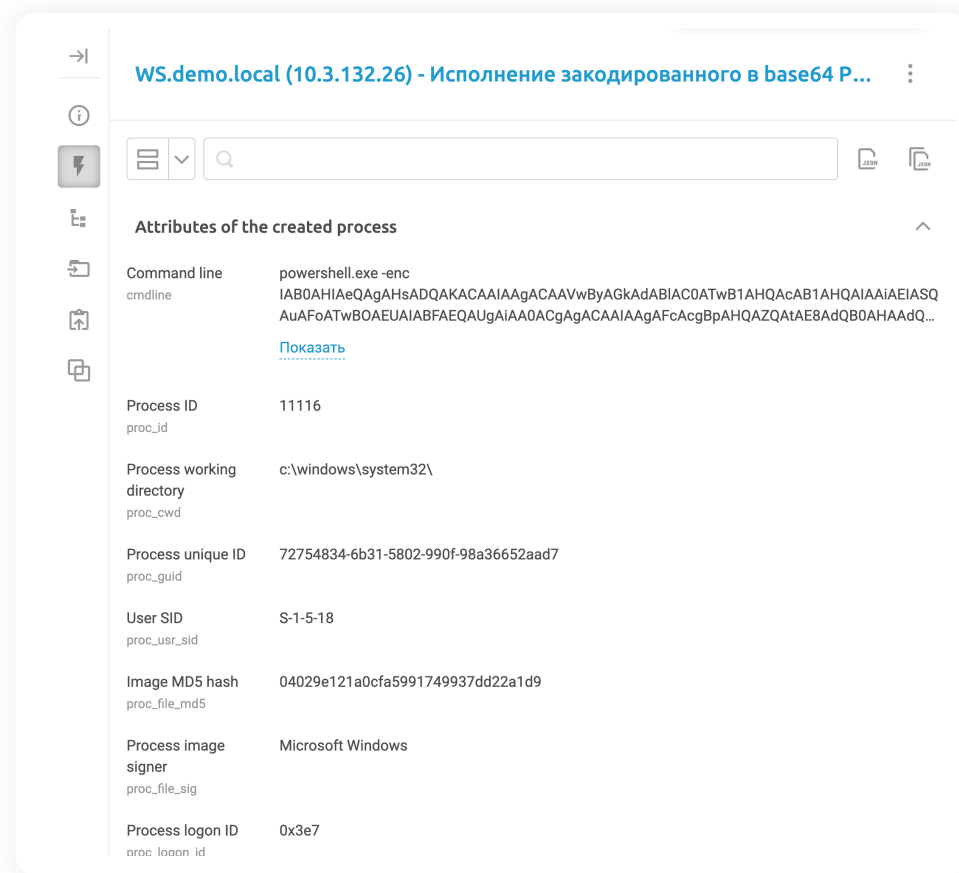
Встроенный модуль Desception,
хостовые приманки

700+

IoA-правил

2 500+

YARA-правил



Интеграция с менеджером инцидентов

Алерты со всей мета-информацией

Гибкая настройка

Работа с инцидентами и анализ процесса

Реакции по кнопке

Дополнительные данные для расследования

The screenshot displays the 'Менеджер инцидентов' (Incident Manager) interface. At the top, there's a navigation bar with 'Smart Monitor' and 'Менеджер инцидентов'. Below this, a summary section shows four colored boxes representing different incident levels: 69 (НОРМА - green), 116 (ПРЕДУПРЕЖДЕНИЕ - yellow), 81 (ТРЕВОГА - red), and 129 (ИНФОРМАЦИЯ - blue). The main area shows a list of incidents. The selected incident is titled '[BI.ZONE EDR] Использование стандартных системных утилит для добавления пользователя в привилегированную группу'. It has a status of 'В РАБОТЕ' (In Progress) and is assigned to 'Ирина Самоходкина'. The incident details are shown in a table-like format with fields for 'proc_p_cwd', 'event_utc_time', 'proc_start_time', 'proc_file_owner_fullname', 'proc_p_usr_fullname', 'cmdline', 'event_type', 'proc_cwd', 'event_logstash_created', 'alert_id', 'alert_source', 'alert_title', 'proc_usr_fullname', 'dev_ip4', 'win', and 'proc file size'. The 'cmdline' field shows a command to add a user to a privileged group. The 'event_type' field shows 'ProcessCreate'. The 'event_logstash_created' field shows a timestamp. The 'alert_title' field shows 'bizone-winctl (172.16.0.139) - Using standard system tools to add user to a privileged group'. The 'proc_usr_fullname' field shows 'bizone-winctl\akimovml'. The 'dev_ip4' field shows '172.16.0.139'. The 'win' field shows '1'. The 'proc file size' field shows '59904'. On the right side, there's a 'История' (History) section showing a log of changes to the incident status and assignee. At the bottom right, there's a 'MITRE ATT&CK' section showing the incident is related to 'Valid Accounts (T1078)', 'Domain Accounts (T1078.002)', 'Local Accounts (T1078.003)', and 'Account Manipulation (T1098)'.

Интеграция с менеджером инцидентов

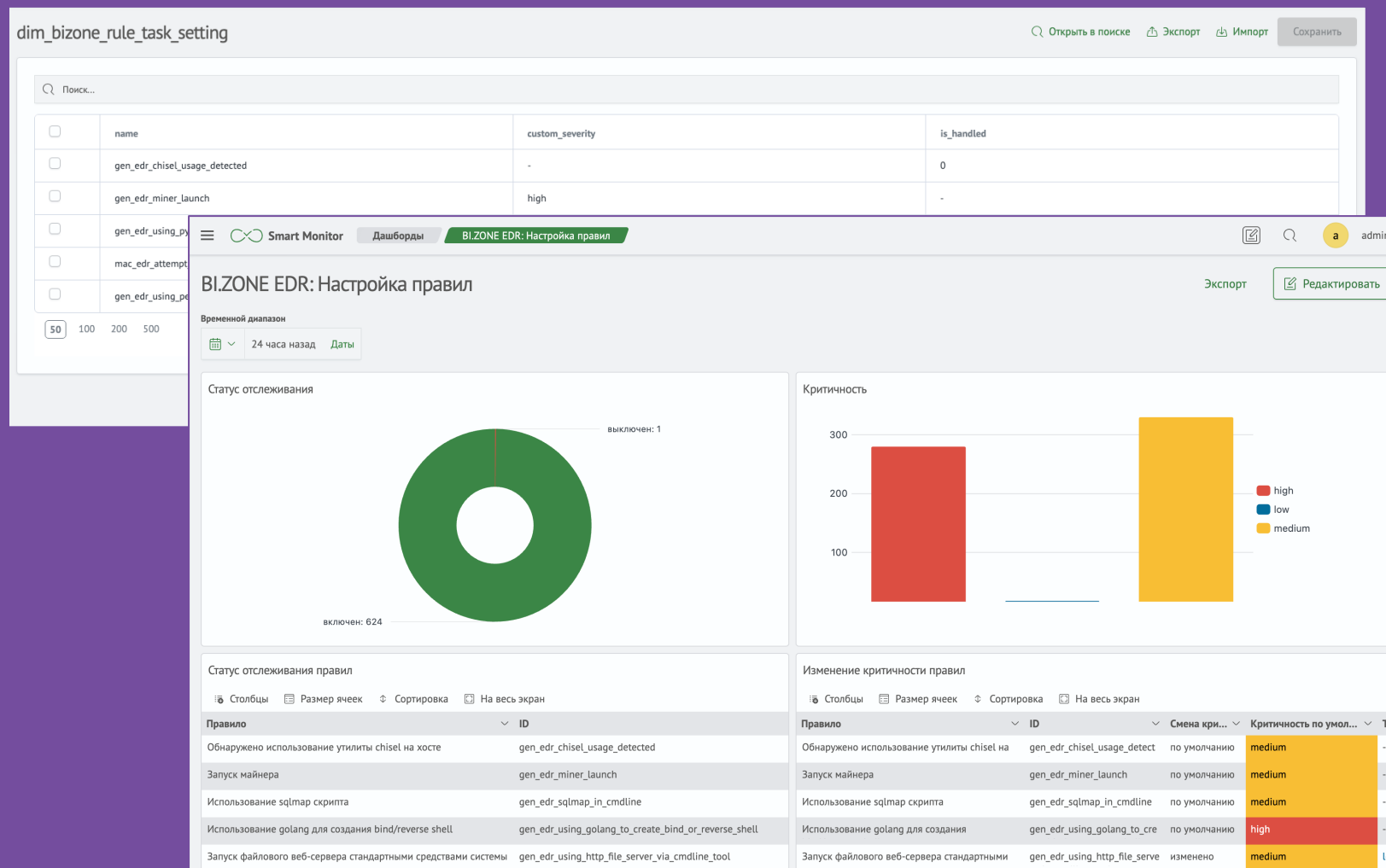
Алерты со всей мета-информацией

Гибкая настройка

Работа с инцидентами и анализ процесса

Реакции по кнопке

Дополнительные данные для расследования



Интеграция с менеджером инцидентов

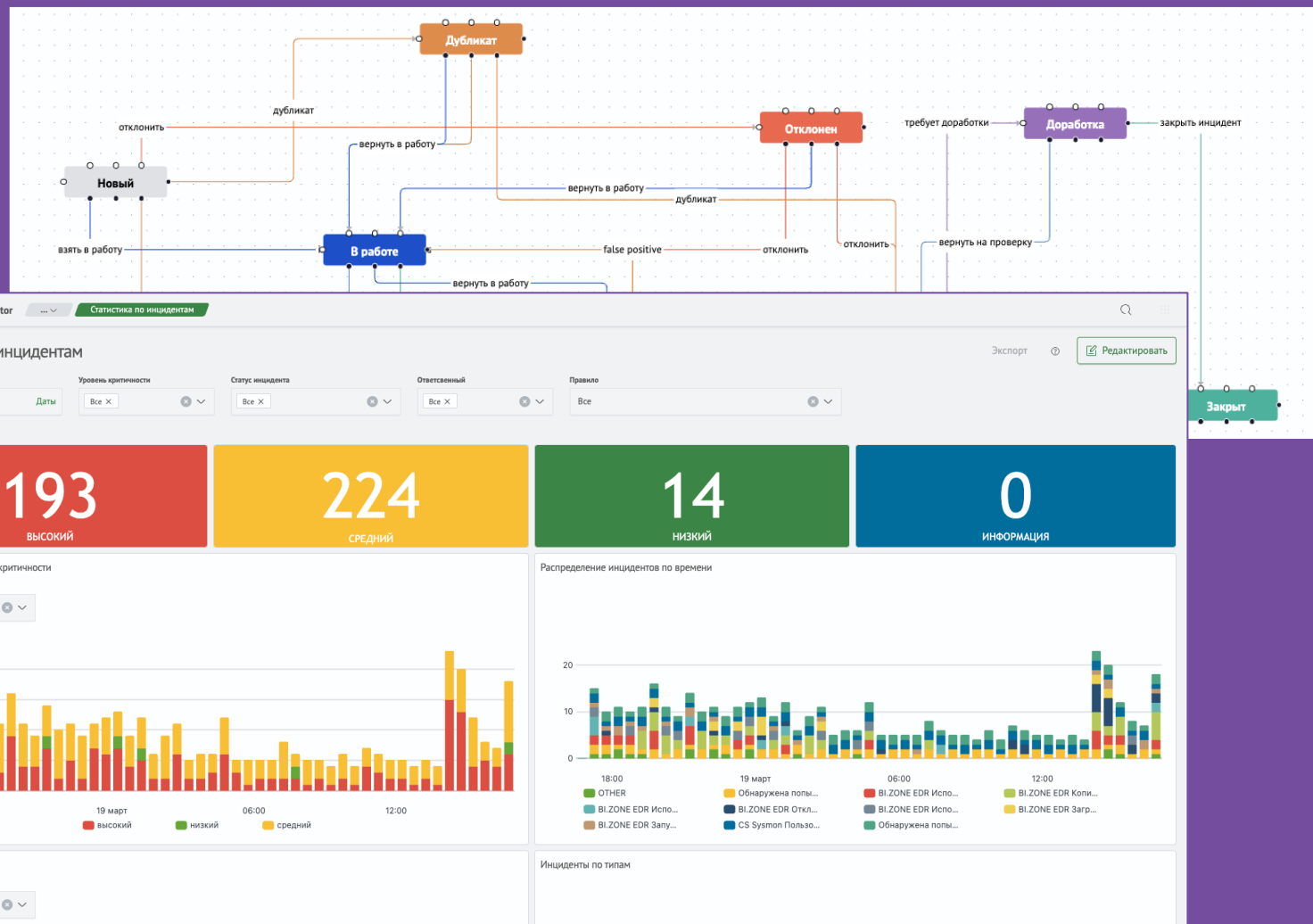
Алерты со всей мета-информацией

Гибкая настройка

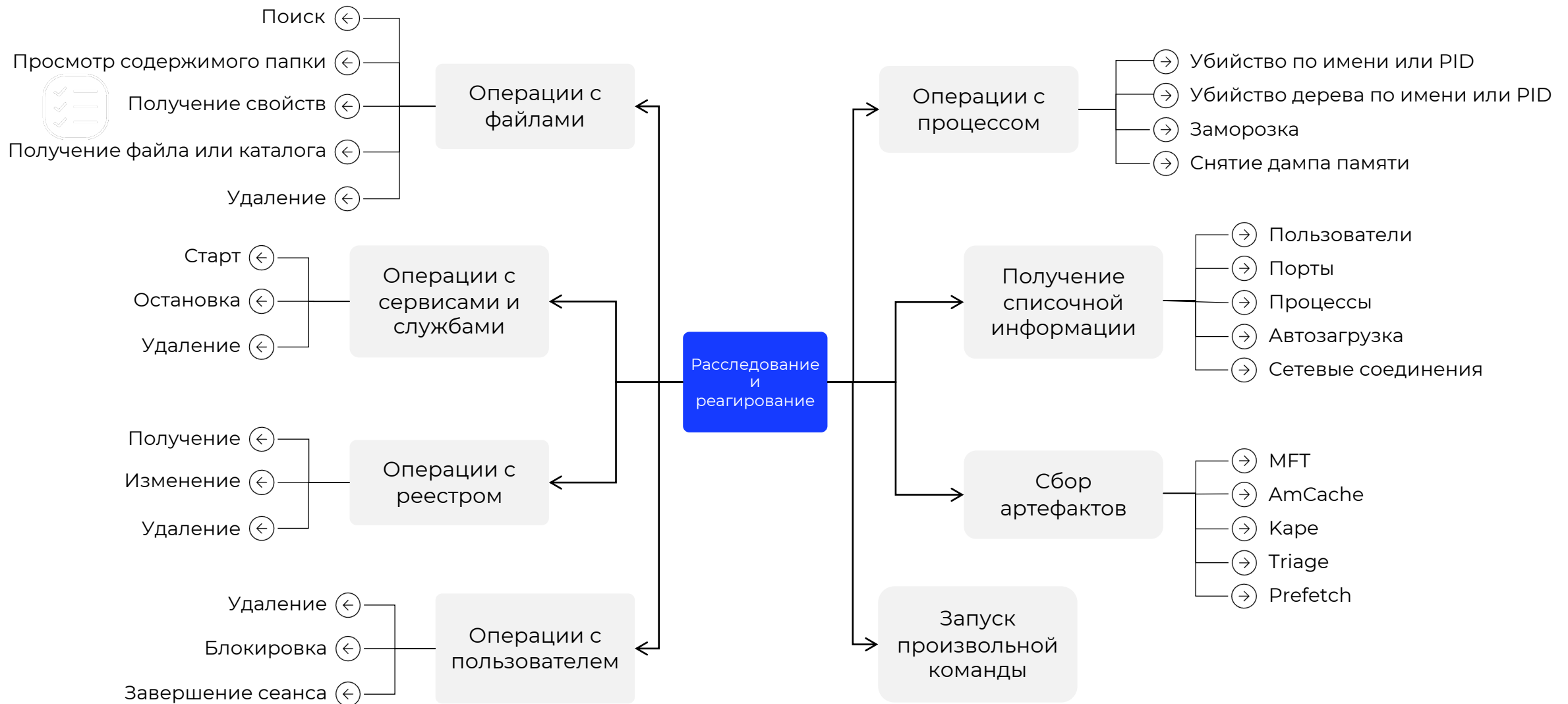
Работа с инцидентами и анализ процесса

Реакции по кнопке

Дополнительные данные для расследования



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

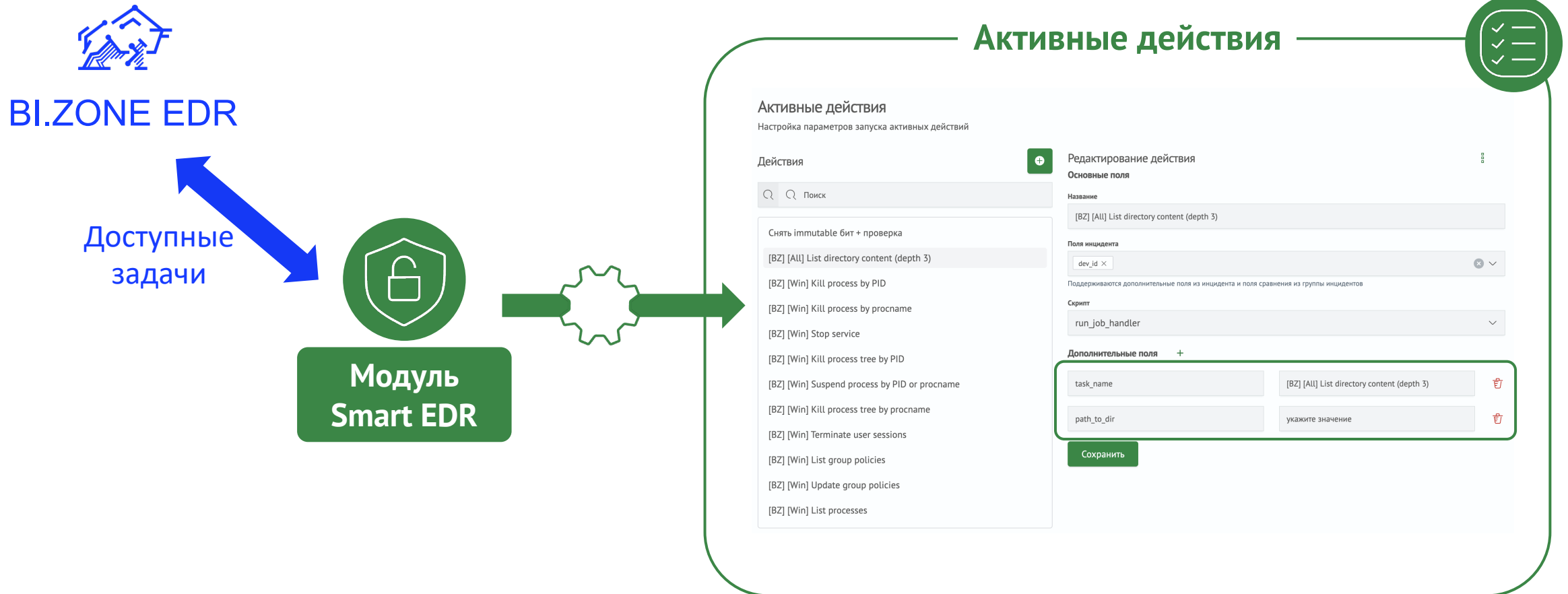
IR Identification

- [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



Интеграция с менеджером инцидентов

Алерты со всей мета-информацией

Гибкая настройка

Работа с инцидентами и анализ процесса

Реакции по кнопке

Дополнительные данные для расследования

Smart Monitor

Менеджер инцидентов

Дата и время

Инцидент

2025-04-09 13:52:00 +03:00

[BI.ZONE EDR] Копирование бинарного файла во временную директорию

bizone_edr nix_edr_copying_a_binary_file_to_a_temporary_directory

[BI.ZONE EDR] Копирование бинарного файла во временную директорию

bizone_edr nix_edr_copying_a_binary_file_to_a_temporary_directory

Description

Данное правило предназначено для детектирования копирования стандартных утилит в временные директории. Данная активность может указывать на попытку злоумышленника или вредоносного ПО использовать стандартные утилиты из временных директорий с нестандартным именем бинарных файлов. Данная техника используется для того, чтобы обойти средства мониторинга, которые, как правило, имеют строгие правила детектирования на определенные утилиты, которые могут использоваться в нелегитимных целях.

Additional Fields

event_utc_time:

Закреть

Отменить

Заблокировать пользователя

История

Редактирование параметров для [BZ] [Nix] Block local user account

Название инцидента

[BI.ZONE EDR] Копирование бинарного файла во временную директорию

Описание инцидента

Данное правило предназначено для детектирования копирования стандартных утилит в временные директории. Данная активность может указывать на попытку злоумышленника или вредоносного ПО использовать стандартные утилиты из временных директорий с нестандартным именем бинарных файлов. Данная техника используется для того, чтобы обойти средства мониторинга, которые, как правило, имеют строгие правила детектирования на определенные утилиты, которые могут использоваться в нелегитимных целях.

Поля инцидента

dev_id

3c29642c-1a46-41ce-9042-643a6b115cd0

nix

Smart Monitor

Дашборды

BI.ZONE EDR: Результаты задач

BI.ZONE EDR: Результаты задач

Временной диапазон

Агент

Последний 1 ч... Даты

decops-astra04 | ip: 172.16.0.22 | id: 3c29642c-1a46-...

Выполнение команд

Столбцы Размер ячейки Сортировка На весь экран

@timestamp	name	parameters	state
2025-04-09T12:08:10.000Z	[BZ] [Nix] Block local user account	{ "command": "usermod -L AkimovML", "timeout": 300, "mode": "current" }	done

VolgaBlob

12

Интеграция с менеджером инцидентов

Алерты со всей мета-информацией

Гибкая настройка

Работа с инцидентами и анализ процесса

Реакции по кнопке

Дополнительные данные для расследования

Smart Monitor Менеджер инцидентов

2025-04-09 14:02:00 +03:00

✓

[BI.ZONE EDR] Использование интерпретаторов Perl для запуска закодированного в base64 скрипта

bizone_edr nix_edr_suspicious_perl_startup_with_base64_code

2025-04-09 14:02:00 +03:00

✓

[BI.ZONE EDR] Копирование бинарного файла во временную директорию

bizone_edr nix_edr

2025-04-09 14:02:00 +03:00

^

[BI.ZONE EDR] Копирование бинарного файла во временную директорию

bizone_edr nix_edr

Description

[BI.ZONE EDR] Копирование бинарного файла во временную директорию для детектирования копирования стандартных утилит в временные директории. Данная активность может указывать на попытку злоумышленника или вредоносного ПО использовать стандартные утилиты из временных директорий с нестандартным именем бинарных файлов. Данная техника используется для того, чтобы избежать обнаружения на определенных...

Редктирование параметров для [BZ] [All] Get file properties

Название инцидента

[BI.ZONE EDR] Копирование бинарного файла во временную директорию

Описание инцидента

Данное правило предназначено для детектирования копирования стандартных утилит в временные директории. Данная активность может указывать на попытку злоумышленника или вредоносного ПО использовать стандартные утилиты из временных директорий с нестандартным именем бинарных файлов. Данная техника используется для того, чтобы избежать обнаружения на определенных...

Smart Monitor BI.ZONE EDR: Резуль... BI.ZONE EDR: Результаты задач

Временной диапазон

Агент

Последний 1 ч... Даты

decops-astra04 | ip: 172.16.0.22 | id: 3c29642c-1a46-...

Выполнение команд

Столбцы Размер ячейки 1 полей отсортировано На весь экран

@timestamp	name	parameters	state	result
2025-04-09T12:29:40.000Z	[BZ] [All] Get file properties	{\"filePath\": \"/app/scripts/run-random-commands.sh\"}	done	PROPERTY VALUE Name run-random-commands.sh Path /app/scripts/run-random-commands.sh Size 1499 Owner root Group root Times AccessTime 16:30:01 MSK 08/04/2025 ModTime 16:19:33 MSK 03/04/2025 ChangeTime 16:19:33 MSK 03/04/2025 BirthTime unavailable OSSpecific Rights -rwxr-xr-x

Выполнить

Пользовательская задача (комбинированная)

Smart Monitor Менеджер инцидентов

Менеджер инцидентов

~ 4 часа назад → 2025-04-09T12:00:00.000+03:00 Обновить

Поиск... Severity

0 НОРМА 4 ПРЕДУПРЕЖДЕНИЕ 2 ТРЕВОГА

+ Создание инцидента

	Дата и время	Инцидент
☐	✓ 2025-04-09 11:58:00 +03:00	[BI.ZONE EDR] Символическая ссылка в общедоступном для записи каталоге, указывающая на системный бинарный файл bizone_edr nix_edr_link_in_world_writeable_dir_to_sys_binaries T1036
☐	✓ 2025-04-09 11:51:00 +03:00	[BI.ZONE EDR] Отключение истории вводимых команд путем защиты её файла от записи (установка immutable bit) bizone_edr nix_edr_make_terminal_history_file_immutable T1222 T1222.002 T1562 T1562.003
☐	✓ 2025-04-09 11:51:00 +03:00	[BI.ZONE EDR] Отключение истории вводимых команд путем защиты её файла от записи (установка immutable bit) bizone_edr nix_edr_make_terminal_history_file_immutable T1222 T1222.002 T1562 T1562.003
☐	✓ 2025-04-09 11:12:00 +03:00	[BI.ZONE EDR] Запуск утилит сетевой разведки bizone_edr nix_edr_execute_network_discovery_tool T1018 T1046
☐	✓ 2025-04-09 11:02:00 +03:00	[BI.ZONE EDR] Копирование бинарного файла во временную директорию bizone_edr nix_edr_copying_a_binary_file_to_a_temporary_directory T1036 T1036.003 T1564
☐	✓ 2025-04-09 10:52:00 +03:00	[BI.ZONE EDR] Копирование бинарного файла во временную директорию bizone_edr nix_edr_copying_a_binary_file_to_a_temporary_directory T1036 T1036.003 T1564

Восстановить запись истории команд + проверить систему

- [BZ].[Nix] Collect a forensics package by Unix Artifact Collector
- [BZ] [Nix] Block local user account
- [BZ] [Nix] Collect a forensics package by BI.ZONE Triage
- [BZ] [Nix] Get autoruns (one-shot)
- Отправить уведомление ответственному
- [BZ] [Nix] Get list of active processes (one-shot)
- [BZ] [Nix] Get command history (one-shot)
- [BZ] [Nix] Get list of mounted devices (one-shot)
- [BZ] [All] File search
- [BZ] [Nix] Get list of open files (one-shot)
- [BZ] [Nix] Get list of shares (one-shot)
- [BZ] [Nix] Get list of users and groups (one-shot)
- [BZ] [Nix] Get logon history (one-shot)
- [BZ] [Nix] Get network connections
- [BZ] [Nix] Get system logs
- [BZ] [Nix] Kill process by PID
- [BZ] [Nix] Kill process by procname
- [BZ] [Nix] List processes
- [BZ] [Nix] Suspend process by PID
- [BZ] [Nix] Remove local user account
- [BZ] [All] Get file or directory
- [BZ] [All] Get file properties
- [BZ] [All] List directory content (depth 3)
- [BZ] [All] Remove file or directory
- [BZ] [All] Run command

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)

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

Проверить
систему
на наличие
других признаков
компрометации

Данные инвентаризации BI.ZONE EDR

Агент

dc

Онлайн
Последнее подключение: 11.04.2025, 07:42

Windows Server 2016 StandardServer
DomainController
Ядро: 10.0.14393
Архитектура: x64

IP-адрес
10.3.132.225
Изоляция хоста

Домен
mail.local

Последний пользователь
MAIL\ADMIN
26.02.2025, 11:31

Логи
Не обновлялись
Обновить

Комментарий
+ ДОБАВИТЬ КОММЕНТАРИЙ

УДАЛИТЬ АГЕНТ

Статус авторизации
Авторизован
06.03.2025, 01:23 a.stamat

Самозащита
Включена
06.03.2025, 02:01

Версия
2.22.0
Обновить
Обновлен: 06.03.2025, 01:59

Ресурсы

Модули

Задачи 2

Политики

Группы 1

Конфигурация

Консоль (Live)

Аппаратные ресурсы

Сетевые интерфейсы

Основные параметры

Жесткий диск

Процессор
Архитектура процессора
Количество ядер
Оперативная память

Intel(R) Xeon(R) Gold 6142 CPU @ 2.60GHz
amd64
6
8 ГБ

Название

Объем памяти

VMware Virtual disk SCSI Disk Device

150 ГБ

Разделы диска

Название

Объем памяти

Свободное место

C:

149 ГБ

130 ГБ

D:

0 Б

0 Б

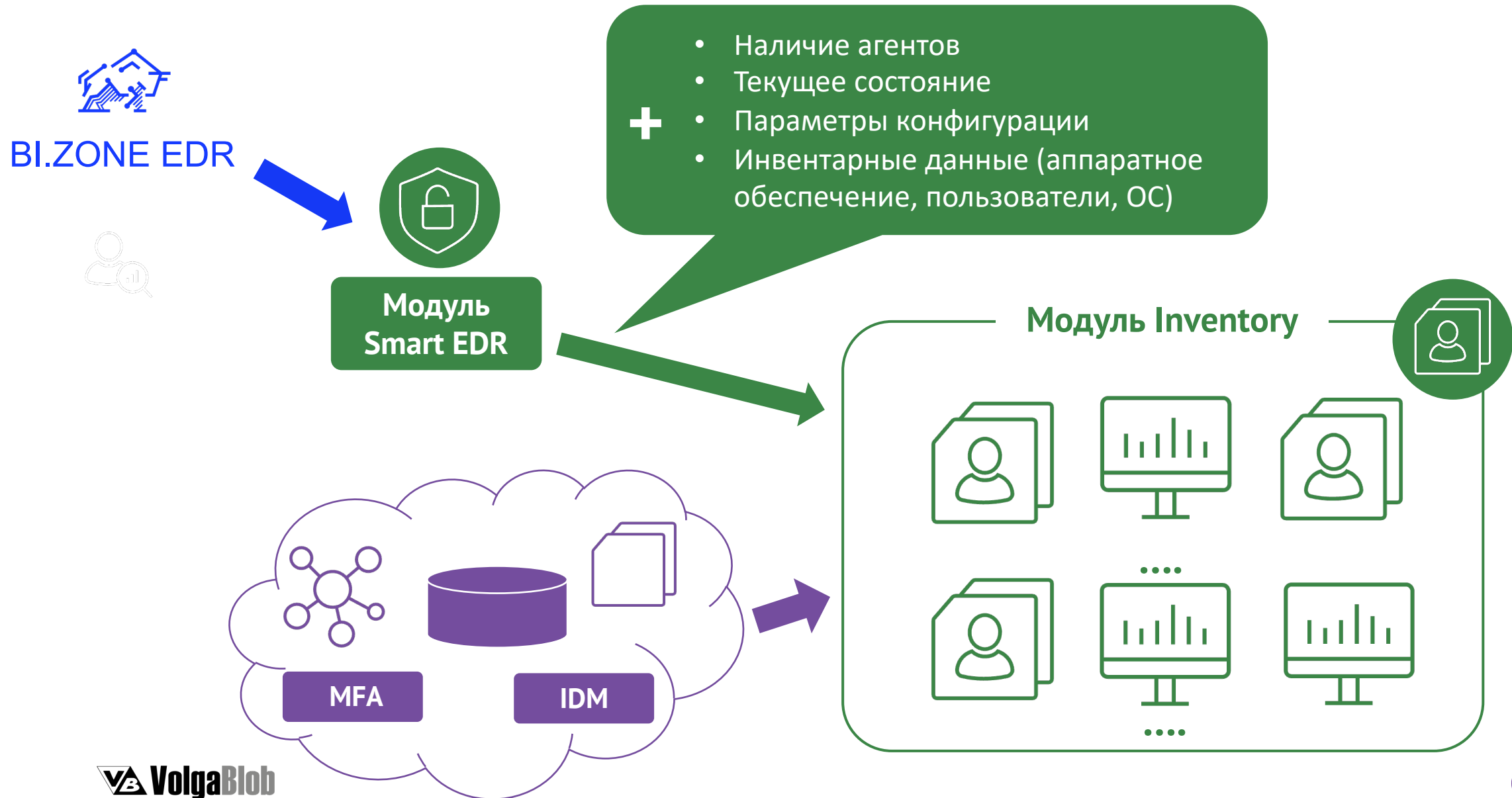
Доступно на сервере

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

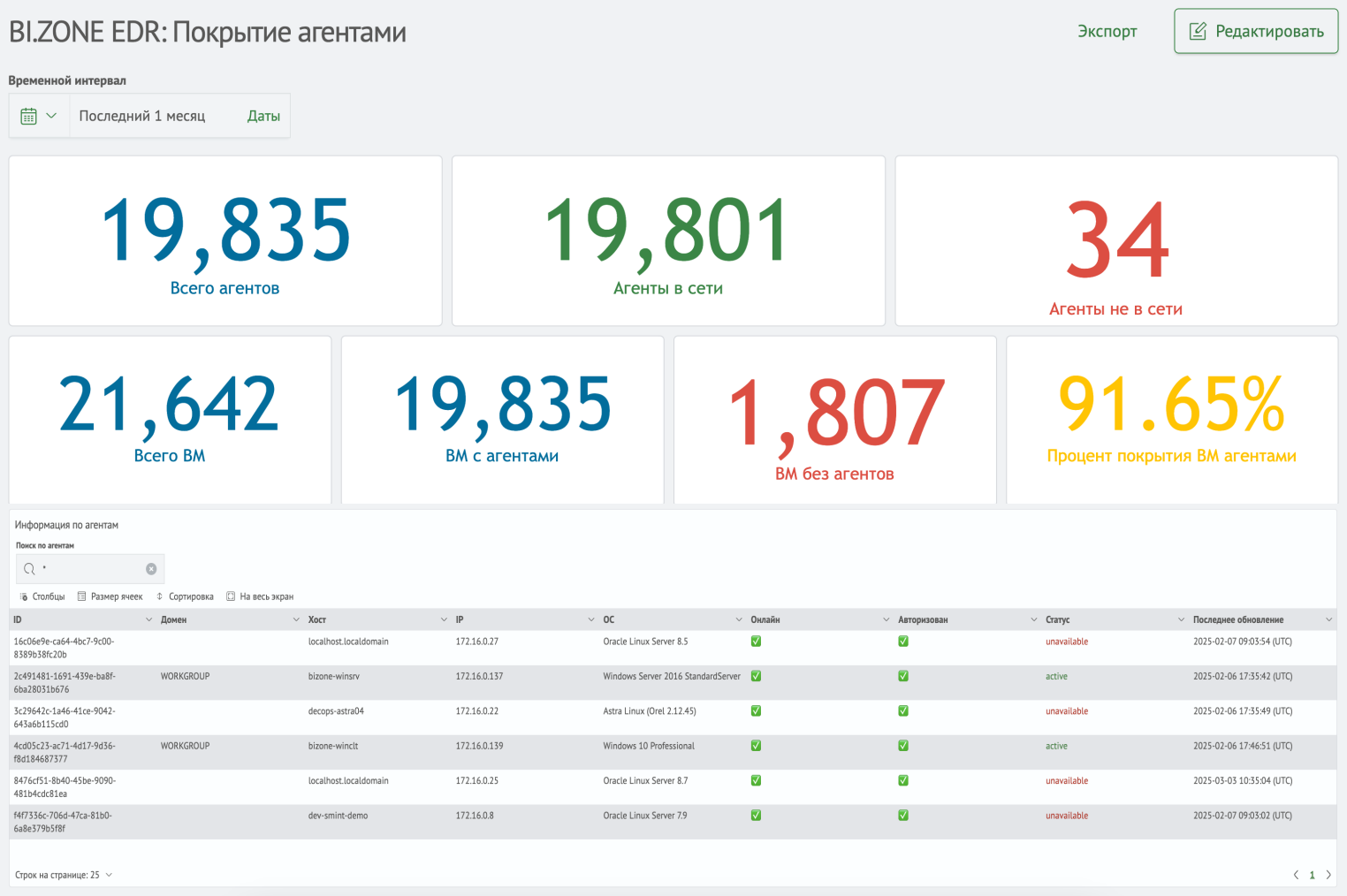
Доступно в телеметрии

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

Обогащение объектов модуля инвентаризации



Анализ покрытия хостов агентами EDR



Сравниваем

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

Определяем

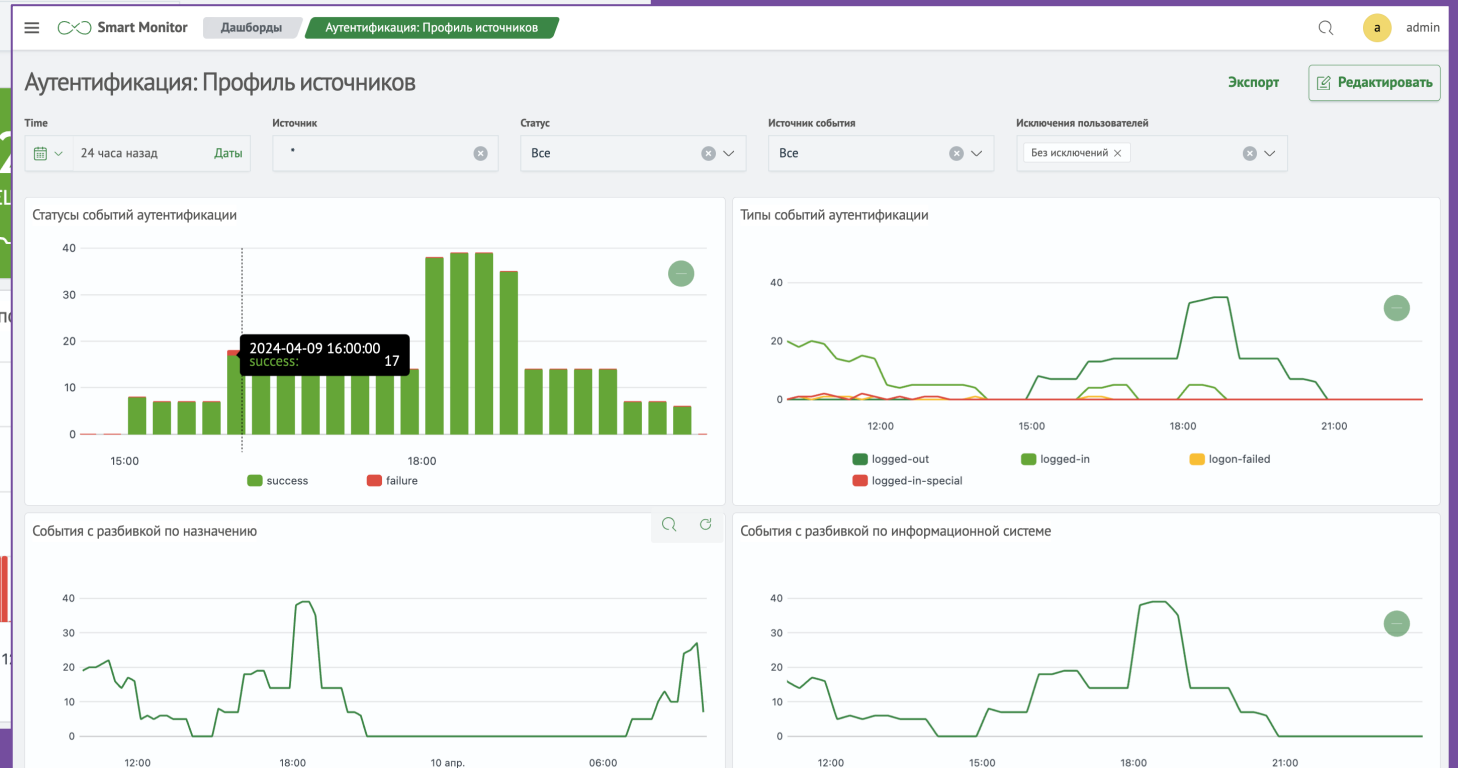
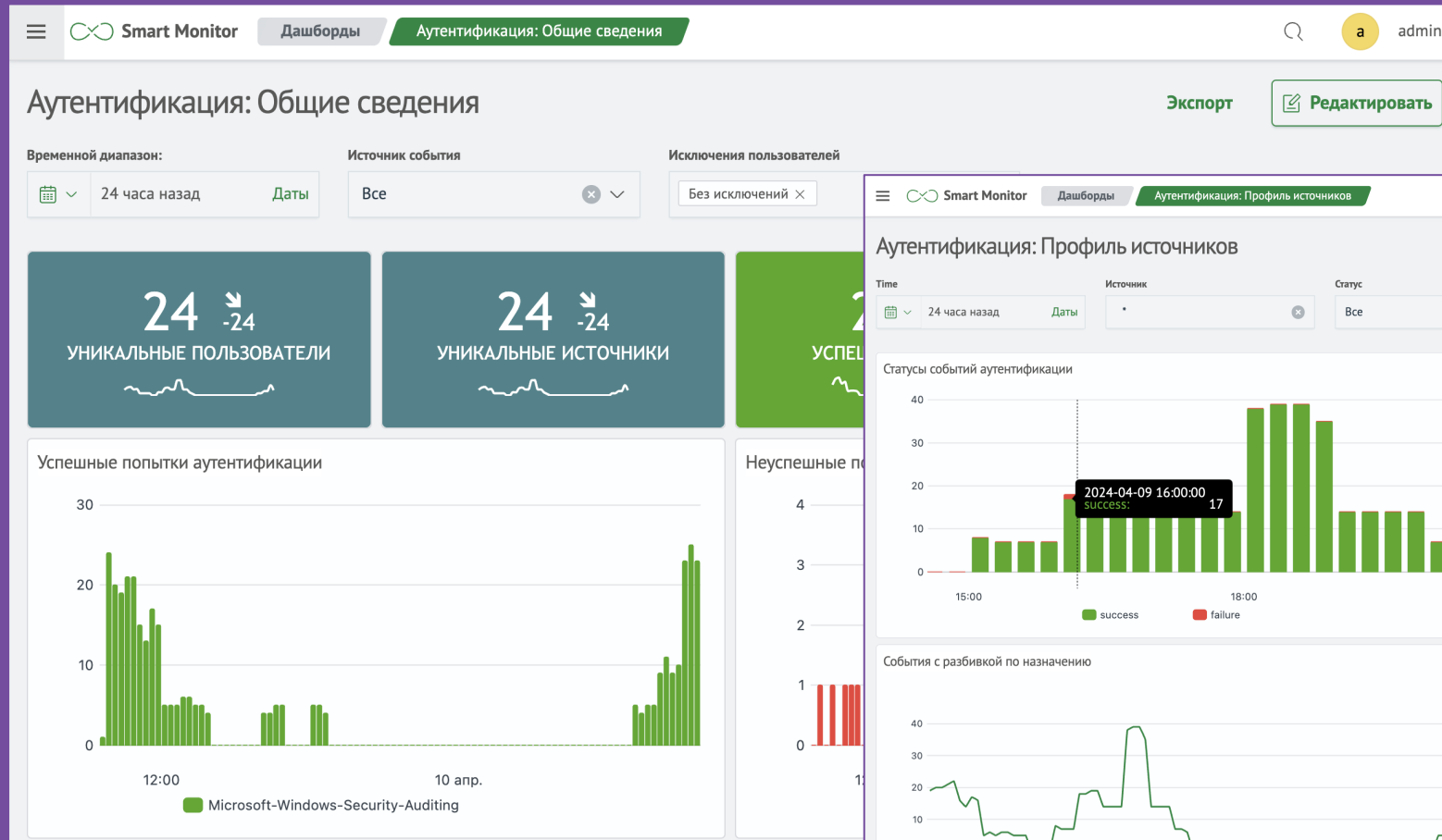
- Процент **покрытых** активов
- **Количество** «проблемных» активов
- **Списки** «проблемных» активов

Автоматизируем

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

Модуль Cyber Security

Обогащение дашбордов
событиями телеметрии EDR



Аутентификация

Вредоносное ПО

Сеть

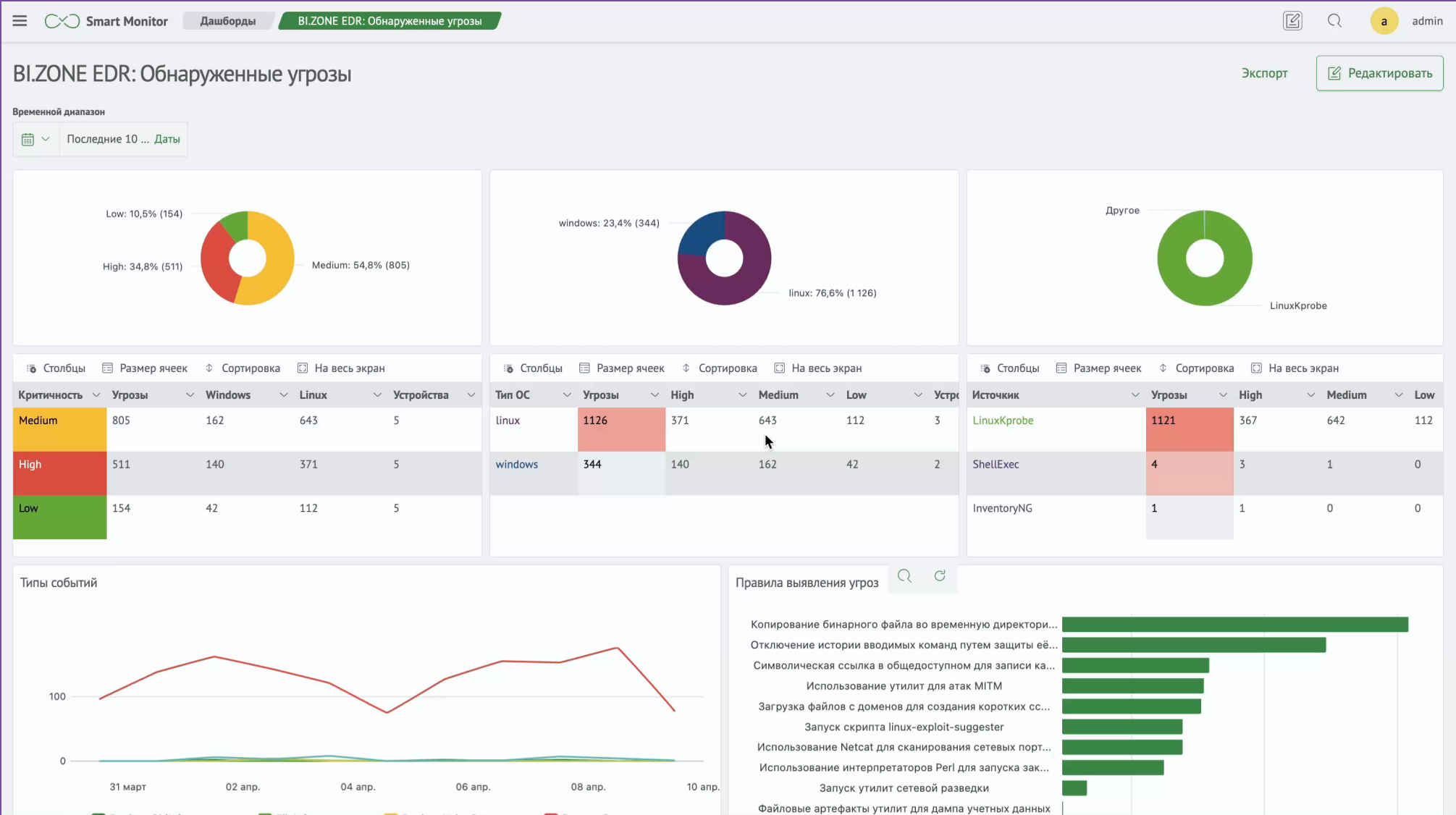
Электронная почта

Управление учётными записями

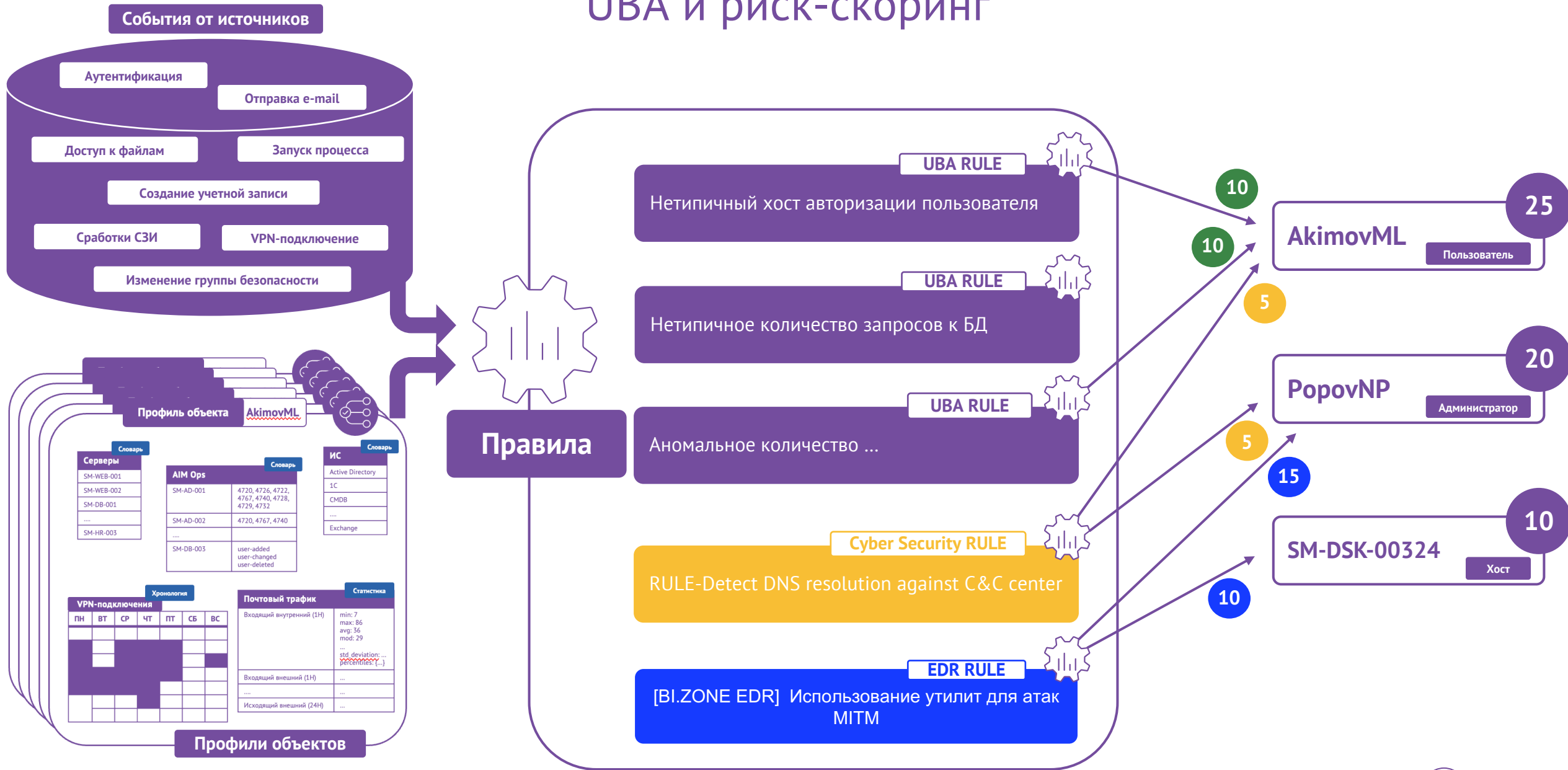
Уязвимости

Web

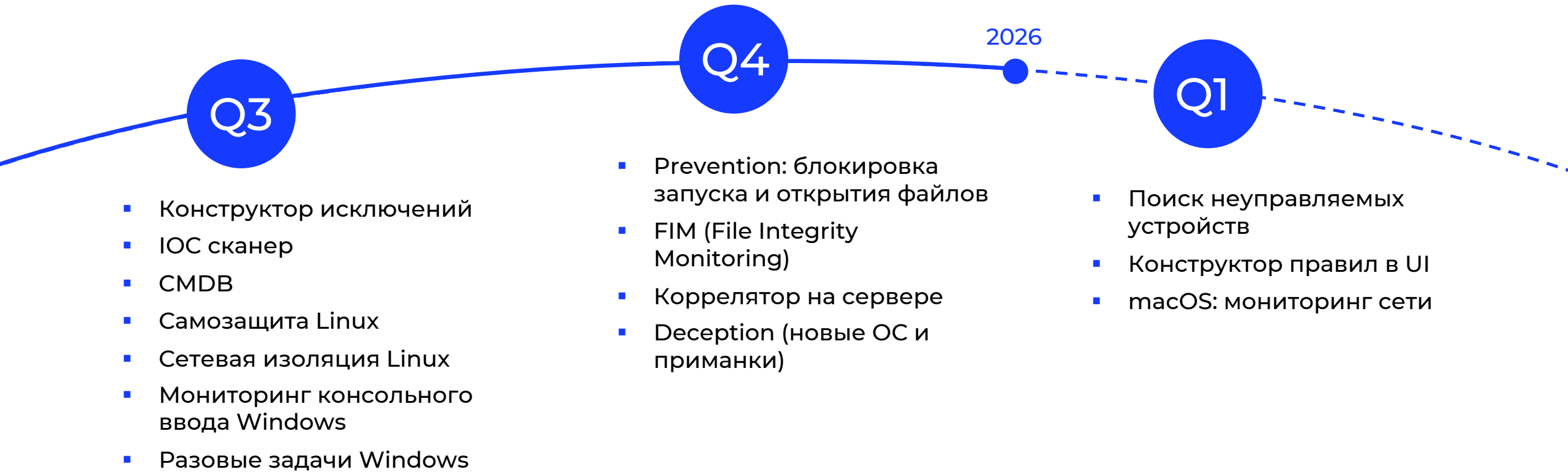
Функциональные дашборды для BI.ZONE EDR



UBA и риск-скоринг



Развитие BI.ZONE EDR



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 отслеживаемых объектов.

**Спасибо за
внимание!**