BI.ZONE

Комплексная защита Linux: от мониторинга до EDR и защиты микросервисов

BI.ZONE

Предпосылки

Эволюция мониторинга инфраструктуры

BI.ZONE

- Периметр
- СЗИ (AV, веб- и email-шлюз, NGFW и т. д.)
- Инфраструктурные сервисы (AD, Radius, VPN, DNS, Exchange и т. д.)
- Критичные APM/серверы

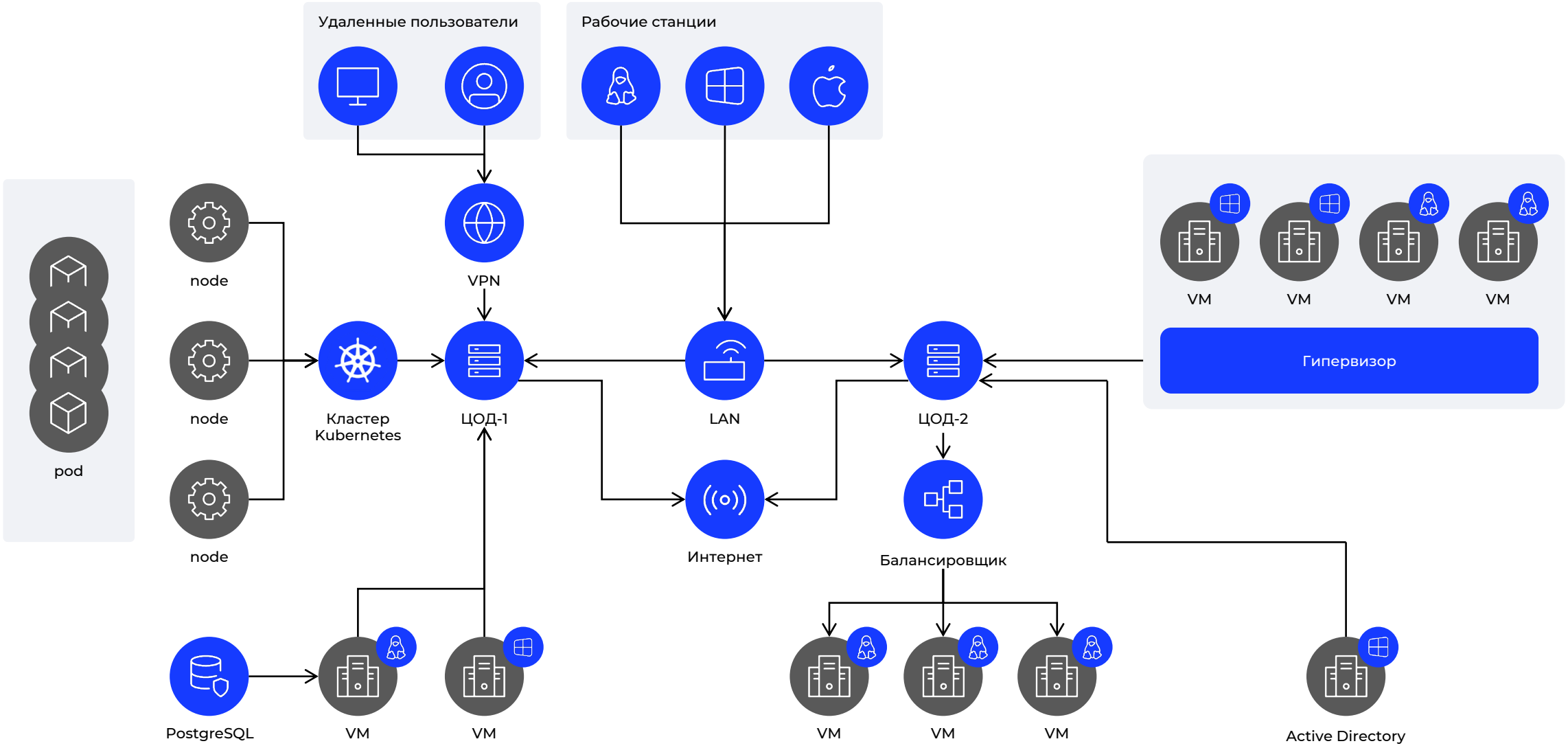
- Больше APM/серверов
- СУБД
- Приложения
- Веб
- NetFlow

- Sysmon
- Auditbeat
- Osquery

- EDR
- NTA
- Identity threat detection and response
- XDR

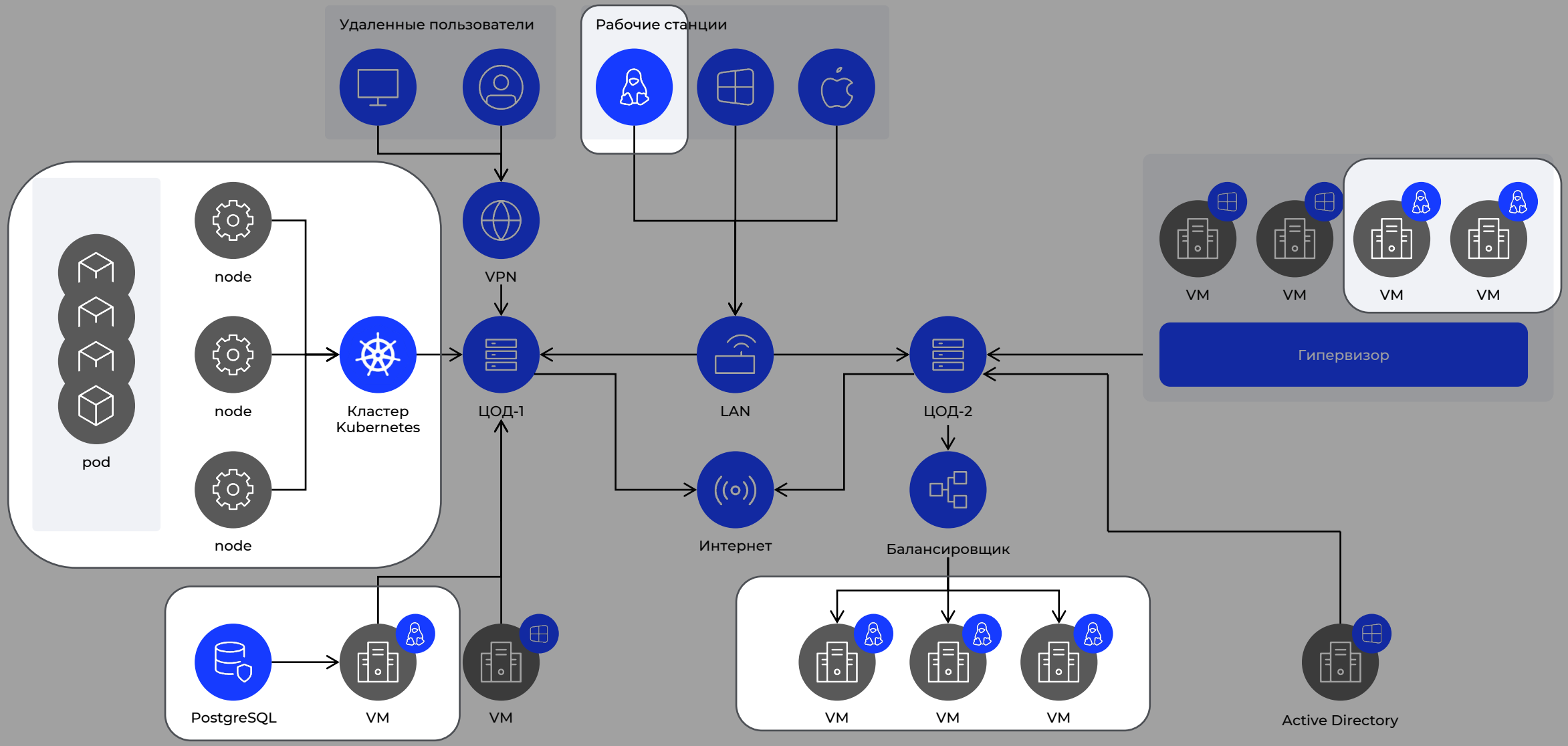
Типовая IT-архитектура

BI.ZONE



Типовая IT-архитектура

BI.ZONE



Тенденции

BI.ZONE

Рост серверной
Linux-инфраструктуры

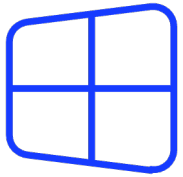
Kubernetes как стандарт платформы
для оркестрации контейнеров

Переход на Linux-десктопы
в российских организациях

Увеличение количества атак,
в которых затронуты Linux устройства

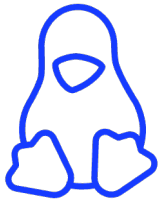
EDR для Linux

BI.ZONE



Высокая степень унификации:

- Единообразие между версиями ОС
- Драйверный API, не привязанный к версии ядра
- Стандартизированные источники расширенной информации (ETW, WMI и т.п)



Сильная фрагментация:

- разные дистрибутивы (Debian, RHEL, Alpine, SUSE и др.)
- разные ядра и версии системных библиотек
- Auditd с высокой нагрузкой при сборе данных
- Конкуренция за подписку на события аудита
- «Нормальная» поддержка eBPF только в «свежих ядрах»

EDR для Linux и контейнеров - челлендж

BI.ZONE

Требуется работать в сильно разнородной и динамичной среде

Собирать качественную телеметрию без ущерба для производительности

Уметь понимать контекст контейнеров и оркестраторов

Выявлять специфичные для Linux атаки

BI.ZONE

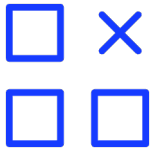
Как BI.ZONE EDR работает в Linux

BI.ZONE

Телеметрия

Сбор телеметрии

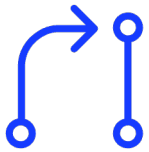
BI.ZONE



Нет необходимости
в сторонних программах

Собственный драйвер
на Windows

Лучшие технологии для
получения событий (eBPF, ESF)



Гибкость сбора
и обогащения событий

40+

событий инвентаризации

190+

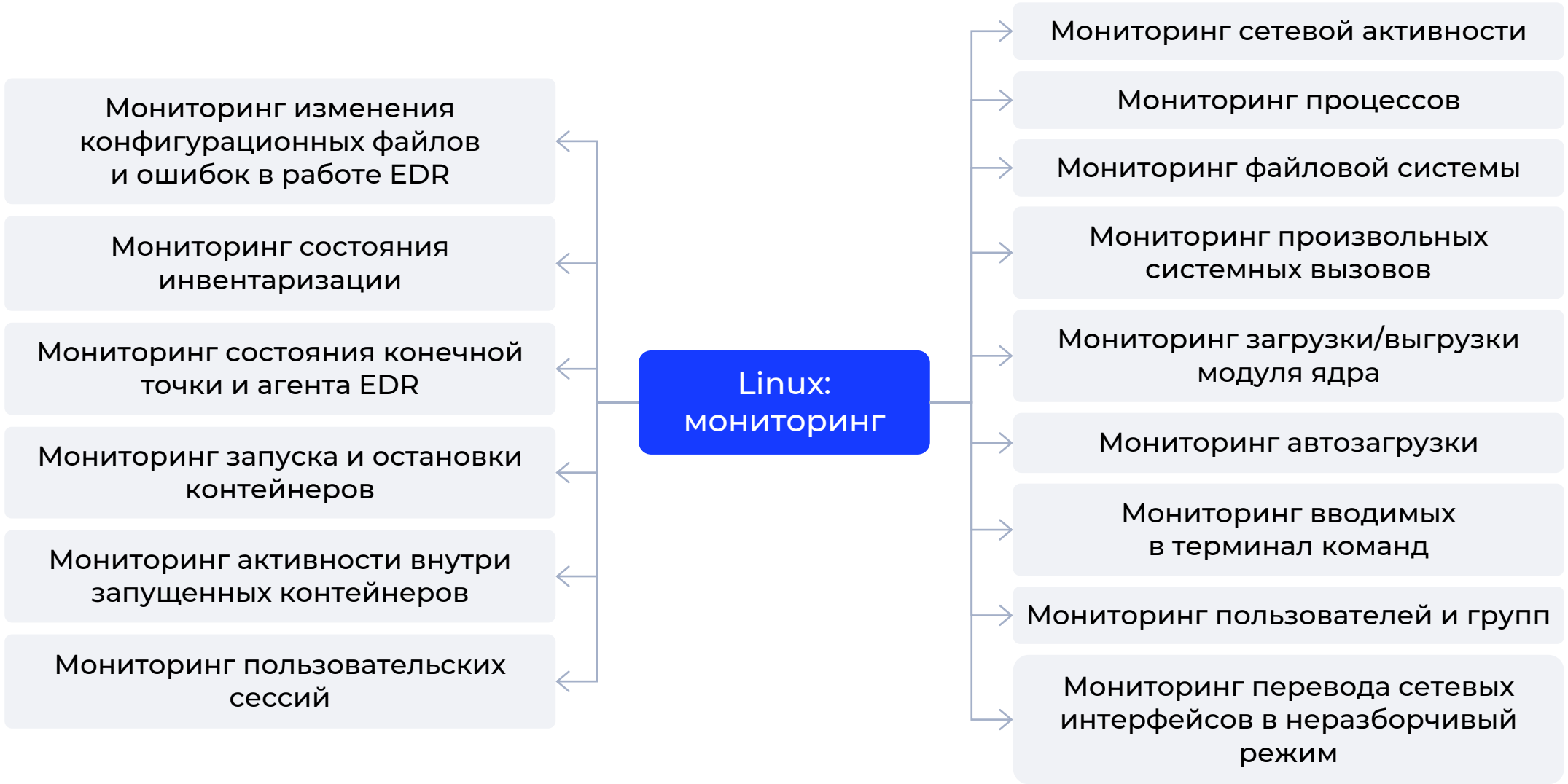
событий мониторинга

30 МБ

средний объем телеметрии
с одного агента в сутки

Категории событий EDR

BI.ZONE



Полнота телеметрии

BI.ZONE


```
{
  "type": "SYSCALL",
  "timestamp": "1737382118.989",
  "record_id": "314",
  "arch": "c00000b7",
  "syscall": "221",
  "success": "yes",
  "exit": "0",
  "a0": "b2bfe0395878",
  "a1": "b2bfe0307660",
  "a2": "b2bfe0396970",
  "a3": "b2bfe0396970",
  "items": "2",
  "ppid": "2334",
  "pid": "2335",
  "auid": "1000",
  "uid": "0",
  "gid": "0",
  "euid": "0",
  "suid": "0",
  "fsuid": "0",
  "egid": "0",
  "sgid": "0",
  "fsgid": "0",
  "tty": "pts2",
  "ses": "4",
  "comm": "ausearch",
  "exe": "/usr/sbin/ausearch",
  "subj": "unconfined",
  "key": "process_exec"
}
```


auditd
~30 полей


```
{
  "@timestamp": "2025-01-22T16:57:17.519Z",
  "@metadata.beat": "auditbeat",
  "@metadata.type": "_doc",
  "@metadata.version": "7.17.26",
  "process.name": "containerd-shim",
  "process.ppid": 1,
  "process.pid": 3132514,
  "process.working_directory": "/run/containerd/io.containerd.runtime.v2.task
  "process.executable": "/usr/bin/containerd-shim-runc-v2",
  "process.hash.sha1": "6054e1b50ba2b7998f4ad9e3f41bb044cf28a333",
  "process.entity_id": "K1eupUGWXdkVZpx/",
  "process.args": ["/usr/bin/containerd-shim-runc-v2", "-namespace", "moby",
  "process.start": "2025-01-22T16:57:11.950Z",
  "message": "Process containerd-shim (PID: 3132514) by user root STARTED",
  "user.name": "root",
  "user.id": "0",
  "user.group.id": "0",
  "user.group.name": "root",
  "user.effective.group.id": "0",
  "user.effective.id": "0",
  "user.saved.id": "0",
  "user.saved.group.id": "0",
  "service.type": "system",
  "event.module": "system",
  "event.dataset": "process",
  "event.kind": "event",
  "event.category": ["process"],
  "event.type": ["start"],
  "event.action": "process_started",
  "ecs.version": "1.12.0",
  "host.ip": ["10.3.132.91"],
  "host.mac": ["00:50:56:bd:cc:95"],
  "host.name": "msk03-<redacted>",
  "host.hostname": "msk03-<redacted>",
  "host.architecture": "x86_64",
  "host.os.family": "debian",
  "host.os.name": "Debian GNU/Linux",
  "host.os.kernel": "5.10.0-29-amd64",
  "host.os.codename": "bullseye",
  "host.os.type": "linux",
  "host.os.platform": "debian",
```


auditbeat
~45 полей


```
{
  "cmdline": "/bin/sh -e -u -c 'exec \"$@\"' sh /usr/lib/firefox/firefox-bin https://clck.ru/3<redacted>7",
  "cmdline_fingerprint": "b97321fc0d2360632e98262a5ffc2d38",
  "customer_id": "90000040",
  "customer_name": "<redacted>",
  "customer_system": "<redacted>
  "dev_fqdn": "<redacted>-ThinkP
  "dev_id": "c1e677ae-5bc0-4355-
  "dev_ipv4": "172.31.131.194",
  "dev_os": "Ubuntu 20.04.6 LTS
  "dev_os_type": "linux",
  "event_id": "40",
  "event_log_source": "LinuxProc
  "event_type": "ProcessCreate",
  "event_type_vendor": "Process(
  "event_utc_time": "2025-01-22T
  "event_uuid": "8814c90e-0a18-4
  "op_func_name": "sys_execve_ca
  "proc_cgroups": "/",
  "proc_cwd": "/home/<redacted>",
  "proc_env": "LC_NUMERIC=ru_RU.
  "proc_file_ace_mask": "012077
  "proc_file_age": 78815565,
  "proc_file_app_productname": "
  "proc_file_atime": "2025-01-22
  "proc_file_crtime": "2022-07-2
  "proc_file_exists": true,
  "proc_file_group_id": 0,
  "proc_file_group_name": "root"
  "proc_file_inode": 13632686,
  "proc_file_mage": 78815565,
  "proc_file_mtime": "2022-07-25
  "proc_file_name": "sh",
  "proc_file_nlink": 1,
  "proc_file_owner_id": 0,
  "proc_file_owner_name": "root"
  "proc_file_path": "/bin/sh",
  "proc_file_size": 4,
  "proc_file_tgt_ace_mask": "016
  "proc_file_tgt_name": "dash",
  "proc_file_tgt_path": "/bin/da
  "proc_file_tgt_size": 129816,
  "proc_file_type": "Link",
  "proc_group_e_id": 1000,
  "proc_group_e_name": "<redacted>",
  "proc_group_r_id": 1000,
  "proc_group_r_name": "<redacted>",
  "proc_guid": "5aa965db-4bed-5adf-bd0e-882c9c2264b8",
  "proc_id": 2679813,
  "proc_issnapshot": false,
  "proc_p_cap_pe": 2818844155,
  "proc_p_cap_pp": 2818844155,
  "proc_p_cmdline": "make libbzcpputils.so",
  "proc_p_cwd": "/usr/local/src/cpe/cpp/bz-cpp-utils",
  "proc_p_file_exists": true,
  "proc_p_file_name": "make",
  "proc_p_file_path": "/usr/bin/make",
  "proc_p_group_e_id": 0,
  "proc_p_group_r_id": 0,
  "proc_p_guid": "d4fe8399-919e-5257-8508-44f8af3013fb",
  "proc_p_id": 2300,
  "proc_p_session_id": 322933,
  "proc_p_uptime": 441618,
  "proc_p_usr_e_id": 0,
  "proc_p_usr_r_id": 0,
  "proc_session_id": 2613,
  "proc_start_time": "2025-01-22T16:08:55.520Z",
  "proc_term_session_id": 5,
  "proc_usr_audit_id": 1000,
  "proc_usr_audit_name": "vladislav",
  "proc_usr_e_id": 1000,
  "proc_usr_e_name": "vladislav",
  "proc_usr_r_id": 1000,
  "proc_usr_r_name": "vladislav",
  "rule_name": "ProcessCreate - Process Create Info",
  "sensor_cfg_profile": "default",
  "sensor_cfg_profile_id": "1",
  "sensor_cfg_version": "202409191126",
  "sensor_groups": "[Nix] PROD",
  "sensor_type": "bedr",
  "sensor_version": "1.9.0"
}
```


BI.ZONE EDR
~80 полей

Интересно отметить

BI.ZONE

Поля аутентификации

Количество неуспешных попыток входа в систему под пользовате... auth_wtmp_usr_count	6
Количество неуспешных попыток входа в систему с IP адреса (wtm... auth_wtmp_ip_count	1
Количество неуспешных попыток входа в систему под пользовате... auth_btmp_usr_count	1
Размер окна подсчета неуспешных попыток входа auth_btmp_time_window	300
Количество неуспешных попыток входа в систему с IP адреса (btmp) auth_btmp_ip_count	1

Поля события

Время генерации события на хосте в UTC event_utc_time	2025-06-04 10:48:20.294
Вендорский тип события event_type_vendor	UserLogonAttemptFail
Название правила формирования события rule_name	UserLogonAttemptFail - Use Info
Тип события event_type	LogonFailureNix

Интересно отметить

BI.ZONE

Поля события

Время генерации события на хосте в UTC event_utc_time	2025-09-01 08:45:28.346
Время записи события в хранилище event_storage_time	2025-09-01 08:43:48.394
Название источника события event_log_source	LinuxEBPF
Вендорский тип события event_type_vendor	FileCreate
Тип события event_type	FileCreateNix

Поля файла

Магические байты файла file_magic	23212F62696E2F626173680A0A6675
Имя файла file_name	cpuUsage.sh
Количество байт, записанных в файл file_bytes_count	1722

Интересно отметить

BI.ZONE

Поля, описывающие источник события

FQDN хоста dev_fqdn	linux.test
Операционная систем... dev_os	Ubuntu 20.04.6 LTS (Focal Fossa) x86_64 #5.15.0-139-generic

Поля DNS

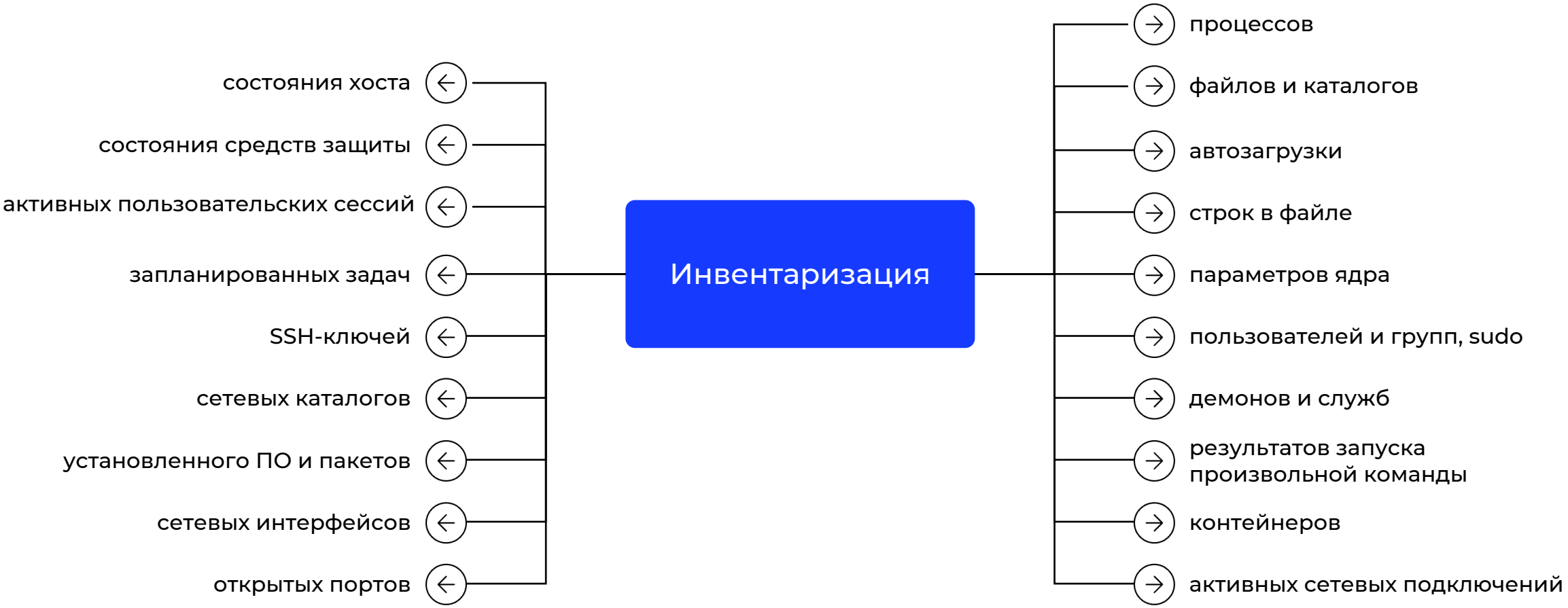
Запрашиваемое DNS ... dns_rname	bi.zone

Поля процесса

PID процесса proc_id	6728
Командная строка cmdline	dig +short A bi.zone
Время работы процес...	

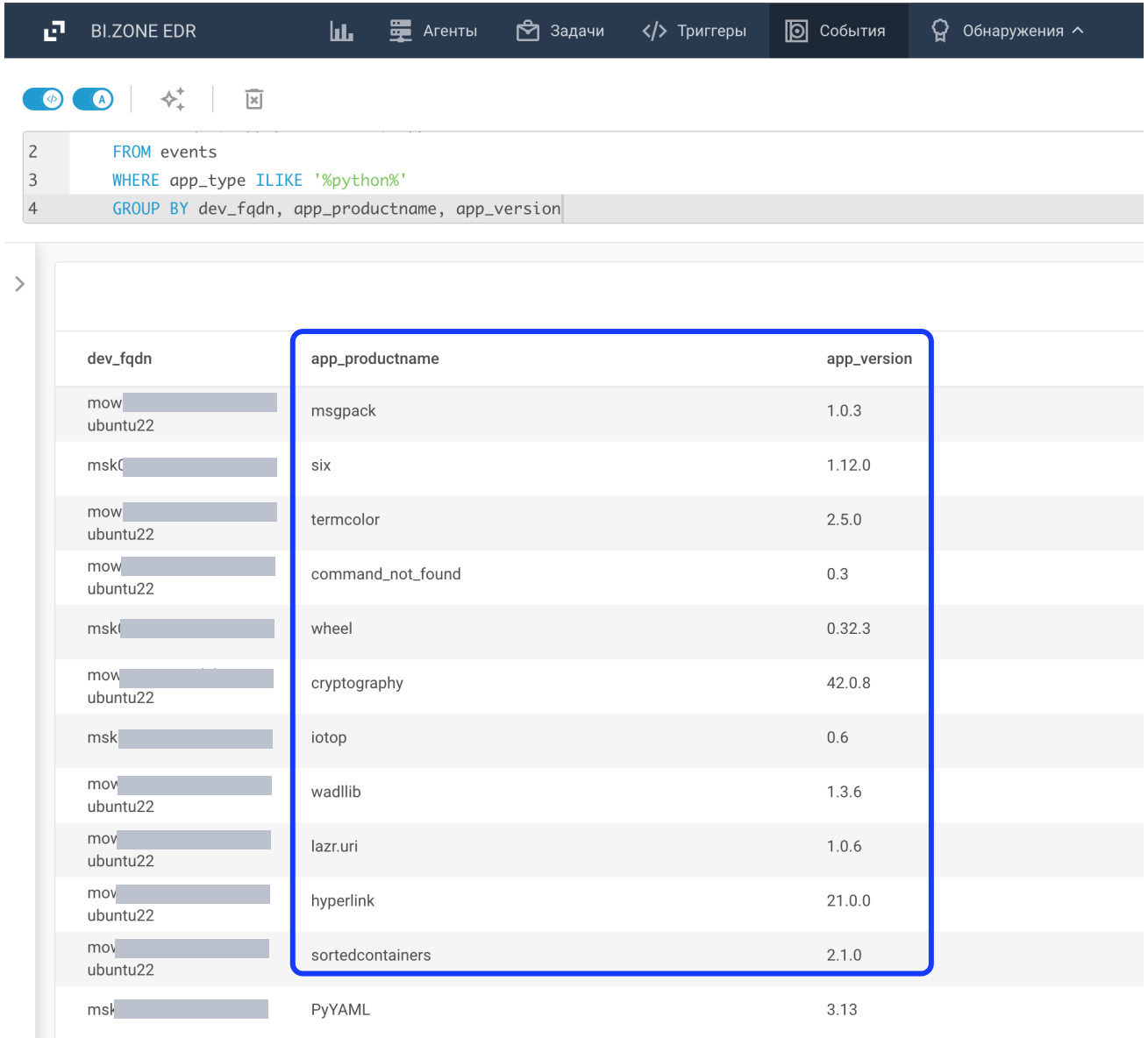
Категории инвентаризации

BI.ZONE



Интересно отметить

BI.ZONE



Интересно отметить

BI.ZONE

Тип события event_type	ShareInfoNix
Название источника события event_log_source	InventoryNG

Поля файла

Маска атрибутов директории file_dir_ace_mask	0040777
Имя группы директории file_dir_group_name	nfsserver
Содержимое директории file_dir_content	file_from_server|test_from_client
Идентификатор группы директории file_dir_group_id	1004
Идентификатор владельца директории file_dir_owner_id	1004
Путь к директории file_dir	/srv/nfs/share
Имя владельца директории file_dir_owner_name	nfsserver

Поля общего сетевого ресурса

Список аттрибутов общего сетевого ресурса share_attrib	nfsclient.example.local(sec=krb5p,rw,sync, no_subtree_check)

Прозрачность телеметрии

BI.ZONE

BI.ZONE
Cybersecurity

События E

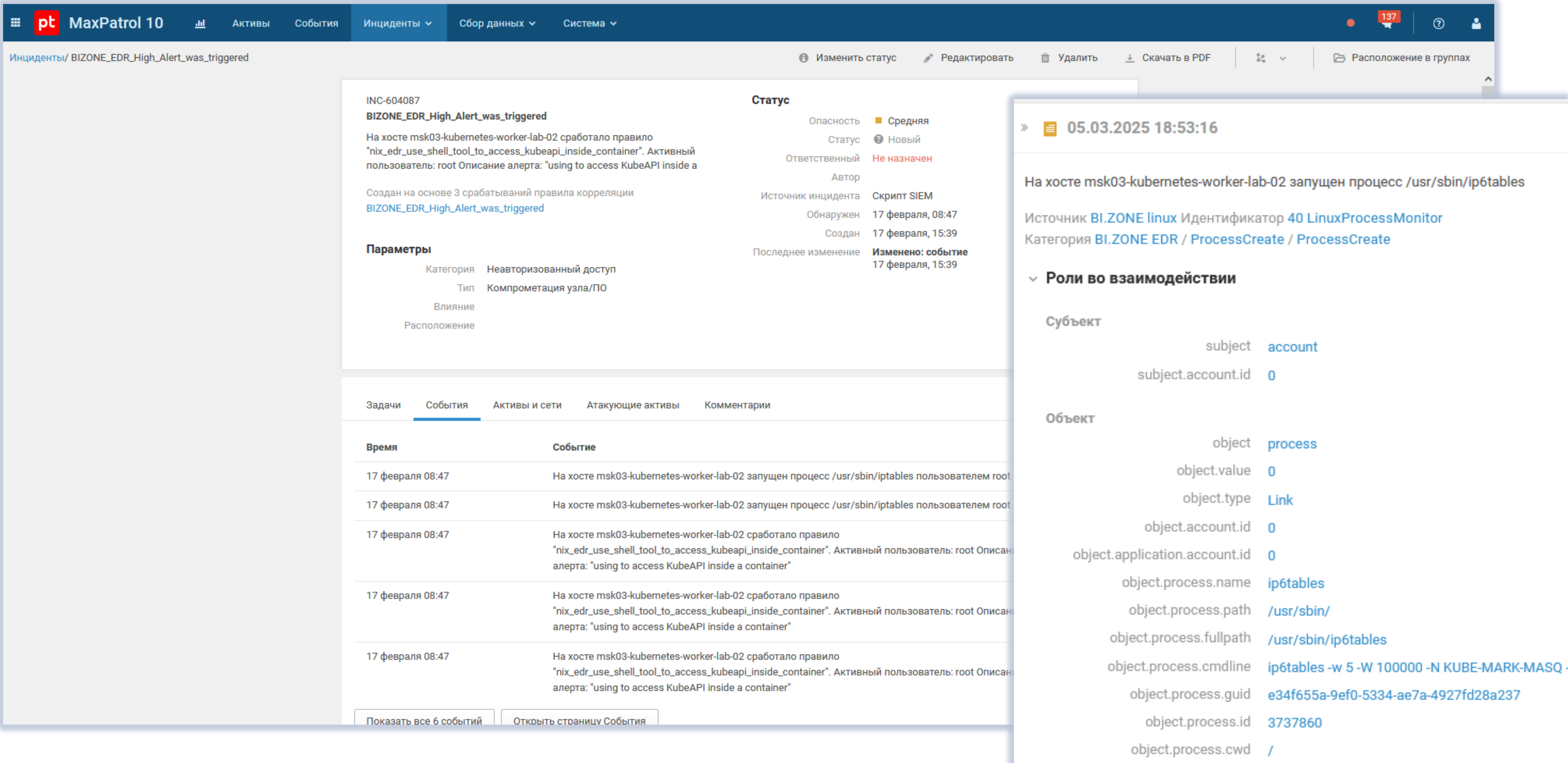
2.5. ProcessPrivChange — ProcessUIDChange

Событие генерируется при изменении идентификатора пользователя (UID) процесса. Отслеживаются изменения эффективного и реального идентификаторов пользователя процесса.

Поле	Тип	Описание	Пример значения
`event_id`	number	Внутренний номер исходного события агента, на базе которого было сформировано обогащенное итоговое событие	44
`event_type`	string	Тип события	ProcessPrivChange
`event_type_vendor`	string	Внутренний тип исходного события агента, на базе которого было сформировано обогащенное итоговое событие	ProcessUIDChange
`event_*` `rule_*`	EventFields	Набор полей, описывающих служебные атрибуты события	
`dev_*`	DeviceFields	Набор полей, описывающих хост, с которого было получено событие	
`sensor_*` `customer_*`	SensorFields	Набор полей, описывающих агента, выполнившего генерацию события, и использованную конфигурацию	
`proc_usr_e_id`	number	Идентификатор эффективного пользователя процесса после смены eUID. Подробнее см. `$ man 7 credentials`	0
`proc_usr_e_name`	string	Имя эффективного пользователя процесса после смены eUID. Подробнее см. `$ man 7 credentials`	root
`proc_usr_e_id_old`	number	Идентификатор эффективного пользователя процесса до смены eUID.	42

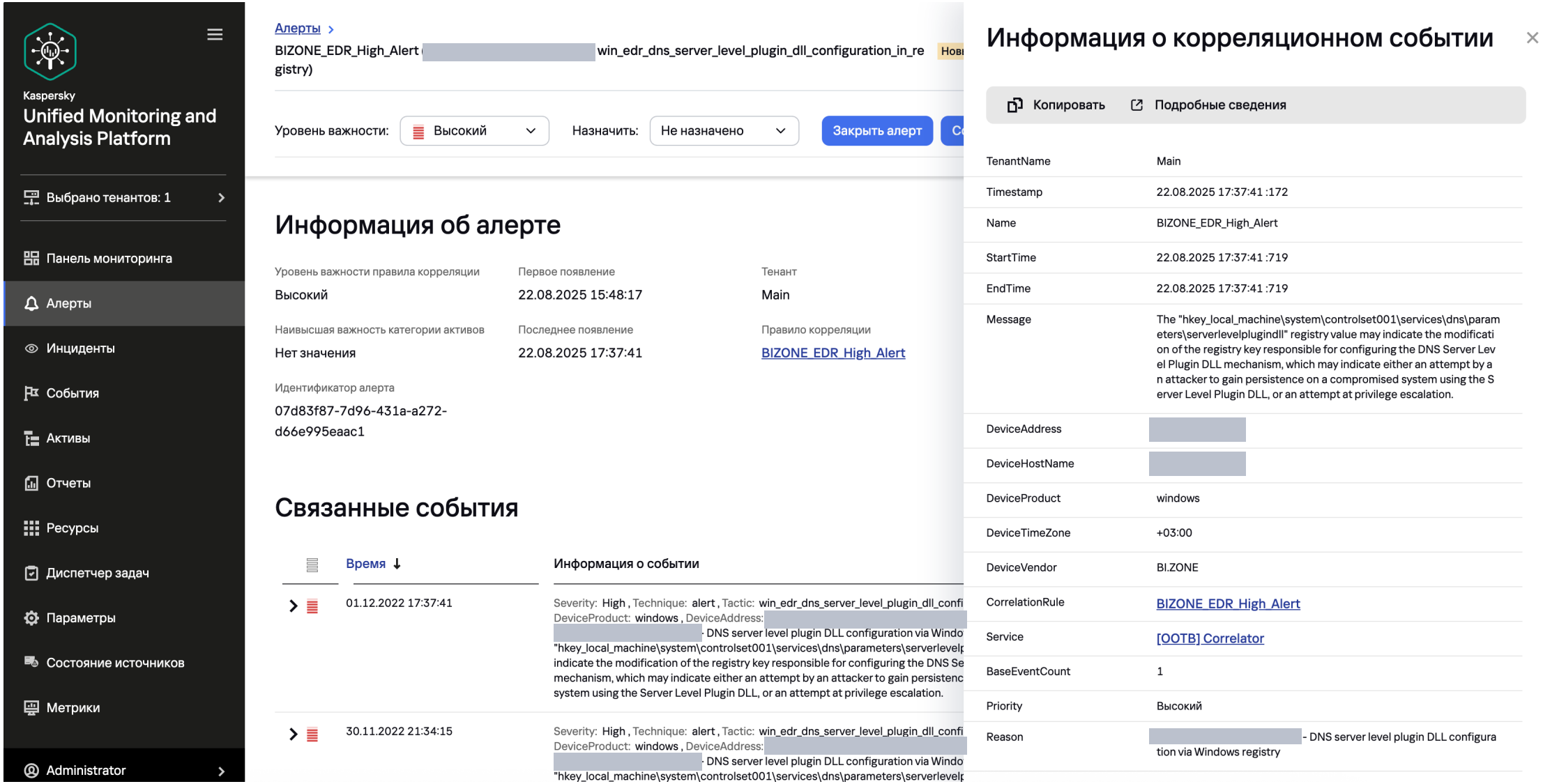
Интеграция с SIEM

BI.ZONE



Интеграция с SIEM

BI.ZONE



BI.ZONE

Жизнь в хайлоад

Профили сбора данных

BI.ZONE

Базовый профиль

Мониторинг

Инвентаризация

Высокая сетевая активность

Убираем мониторинг сети

Фокусируемся на инвентаризации долгоживущих соединений

Высокая процессная активность

Убираем мониторинг запуска процессов

Фокусируемся на инвентаризации процессов в polling-режиме

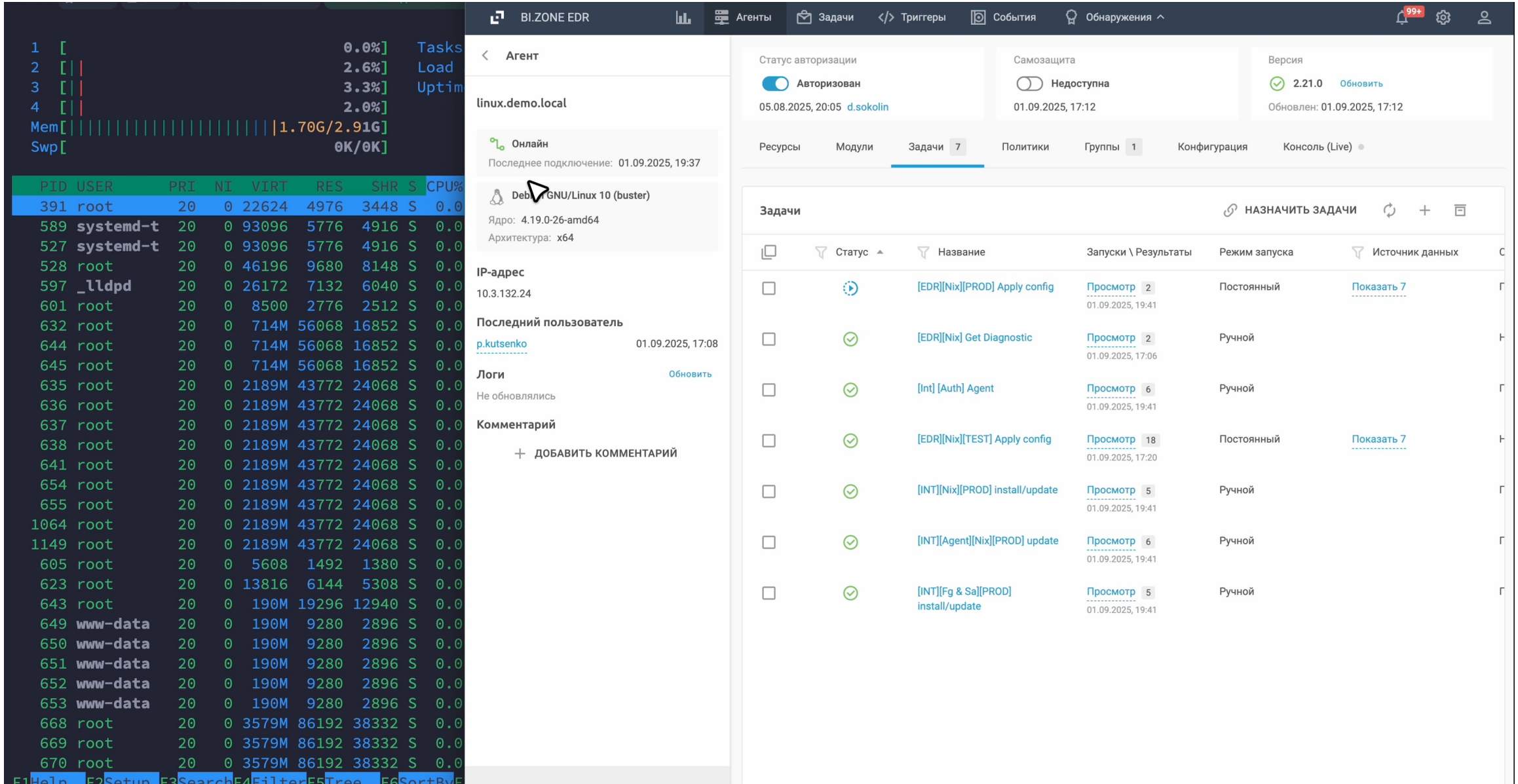
Высокая файловая активность

Убираем мониторинг файловых операций

Фокусируемся на инвентаризации критичных файлов

Графики потребления с профилями

BI.ZONE



BI.ZONE

Контейнеры

Проблема мониторинга контейнеров

BI.ZONE

Контейнеры делят одно ядро –
не понятно действие произошло
в контейнере или на хосте

Короткоживущие контейнеры —
угроза может исчезнуть вместе
с контейнером до того, как её заметят

Сложно контролировать
конфигурацию без использования
оркестратора

Fileless-атаки, вредоносные скрипты
и lateral movement остаются
незамеченными

BI.ZONE EDR и контейнеры

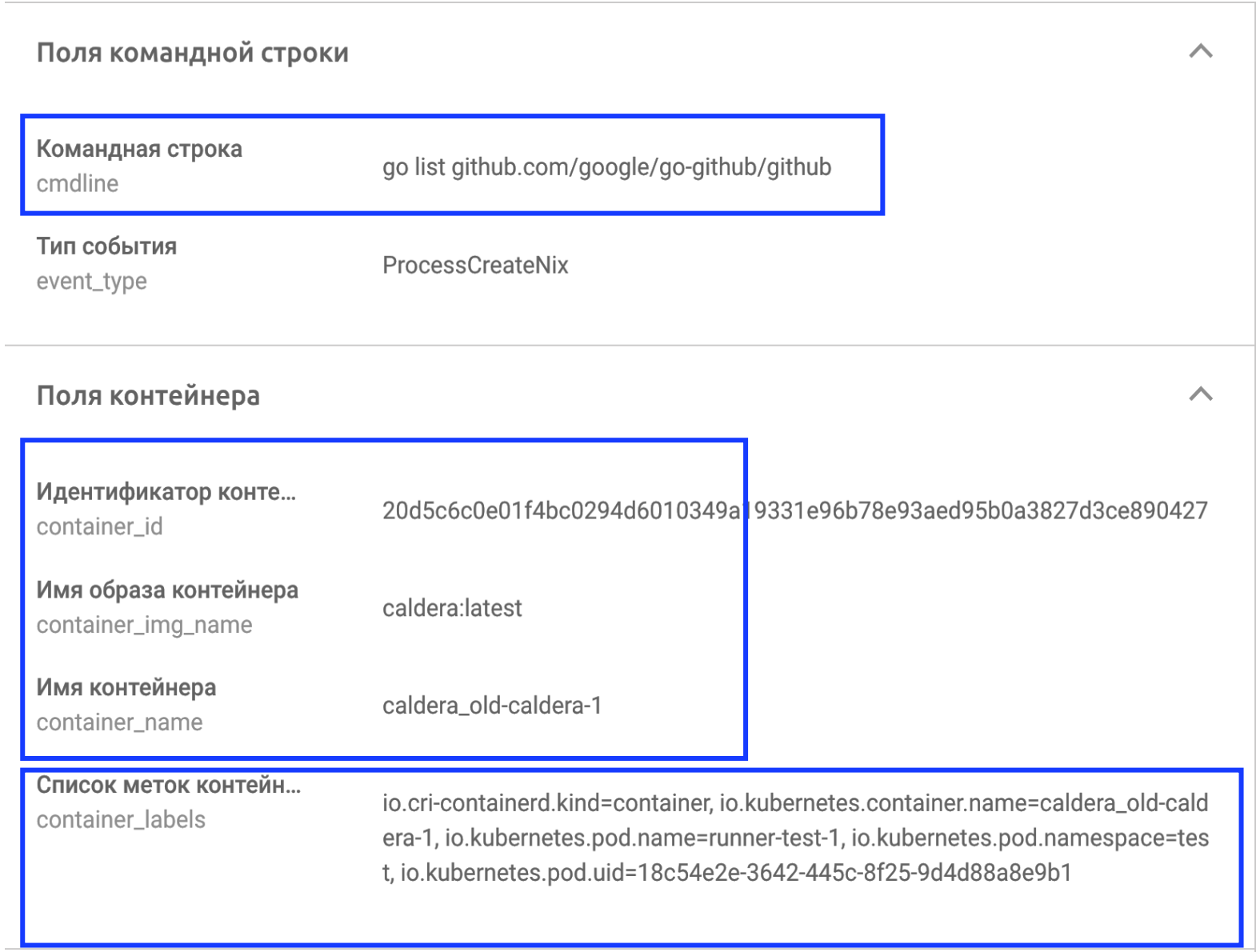
BI.ZONE

Привязка событий к контейнеру и поду

не просто "процесс go запустился", а "процесс go запустился в контейнере caldera_old-caldera-1".

Контекст Kubernetes

EDR может связать событие с namespace, deployment, service account.

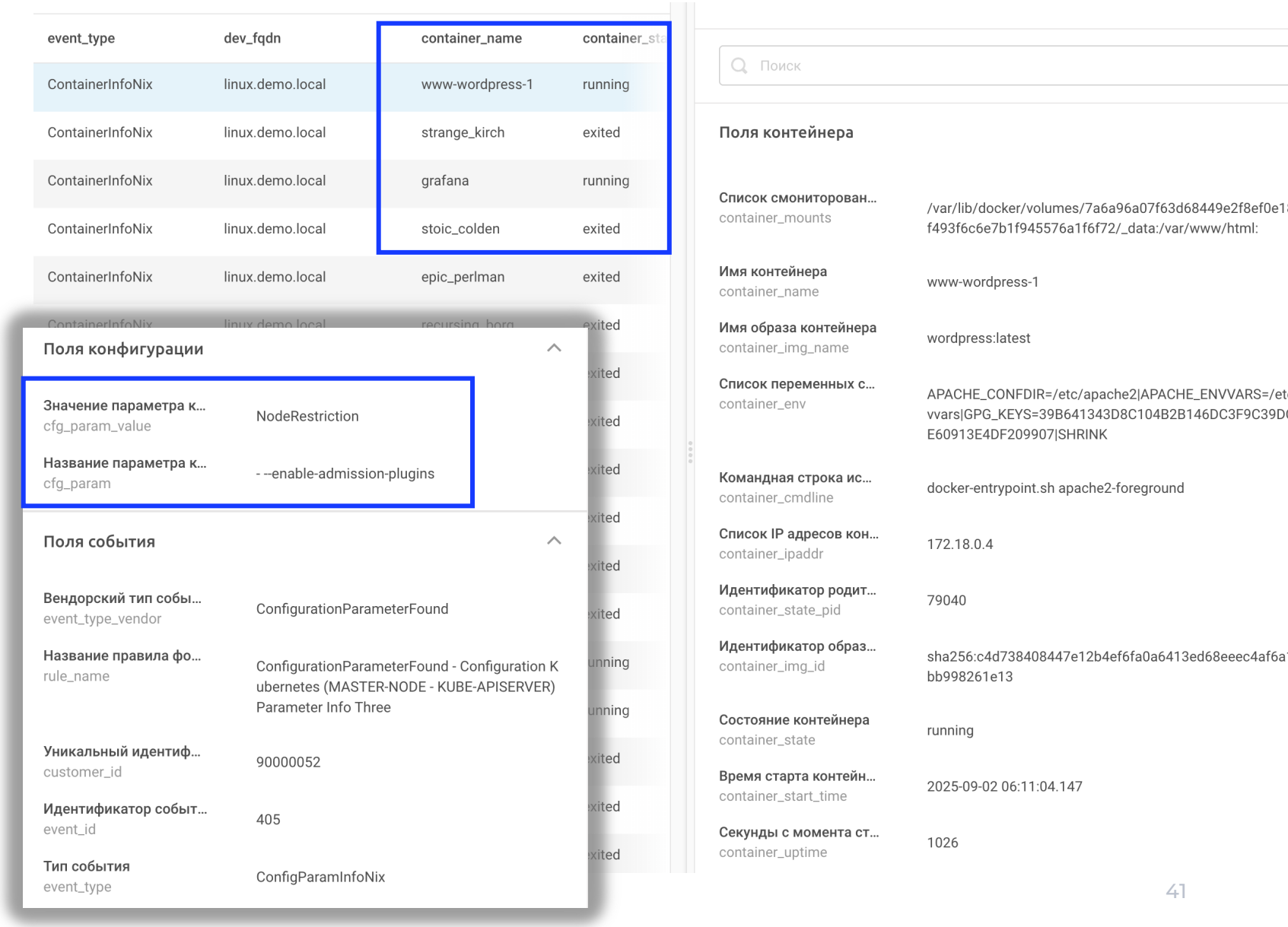


BI.ZONE EDR и контейнеры

BI.ZONE

Инвентаризация

- запущенные контейнеры
- остановленные контейнеры
- запуск и остановка контейнеров
- аудит конфигурации систем оркестрации

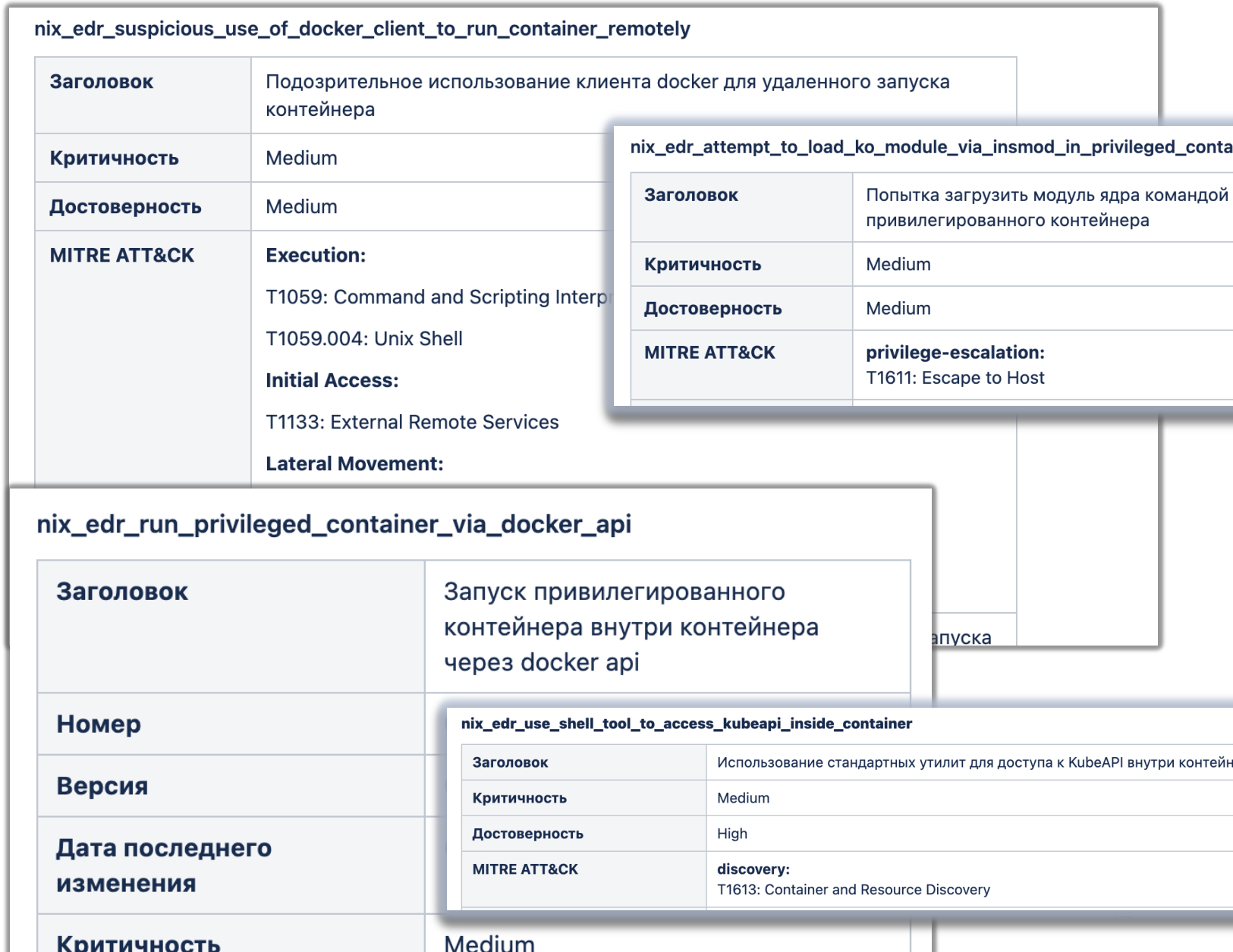


BI.ZONE EDR и контейнеры

BI.ZONE

Детектирование MITRE ATT&CK for Containers техник

- побег из контейнера
- повышение привилегий
- злоупотребление capabilities
- криптомайнинг



nix_edr_suspicious_use_of_docker_client_to_run_container_remotely

Заголовок	Подозрительное использование клиента docker для удаленного запуска контейнера
Критичность	Medium
Достоверность	Medium
MITRE ATT&CK	**Execution:** T1059: Command and Scripting Interp T1059.004: Unix Shell **Initial Access:** T1133: External Remote Services **Lateral Movement:**

nix_edr_attempt_to_load_ko_module_via_insmod_in_privileged_conta

Заголовок	Попытка загрузить модуль ядра командой привилегированного контейнера
Критичность	Medium
Достоверность	Medium
MITRE ATT&CK	**privilege-escalation:** T1611: Escape to Host

nix_edr_run_privileged_container_via_docker_api

Заголовок	Запуск привилегированного контейнера внутри контейнера через docker api
Номер	
Версия	
Дата последнего изменения	
Критичность	Medium

nix_edr_use_shell_tool_to_access_kubeapi_inside_container

Заголовок	Использование стандартных утилит для доступа к KubeAPI внутри контейн
Критичность	Medium
Достоверность	High
MITRE ATT&CK	**discovery:** T1613: Container and Resource Discovery

BI.ZONE EDR и контейнеры

BI.ZONE

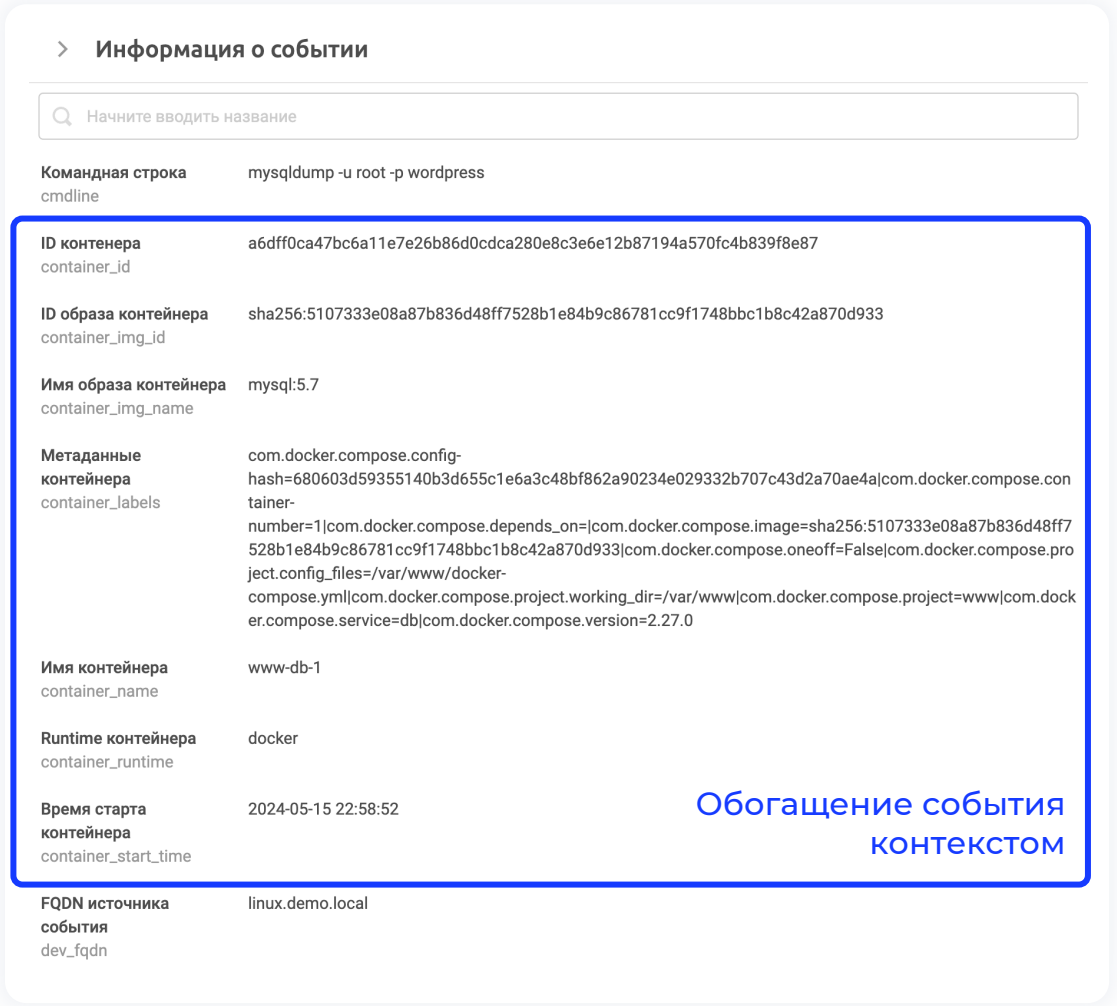
Инвентаризация контейнеров, обнаруженных на хосте

Мониторинг активности внутри контейнеров:

- запуск процессов
- файловые операции
- сетевая активность
- и многое другое

Поддерживаемые движки:

DaemonSet*



*– Roadmap

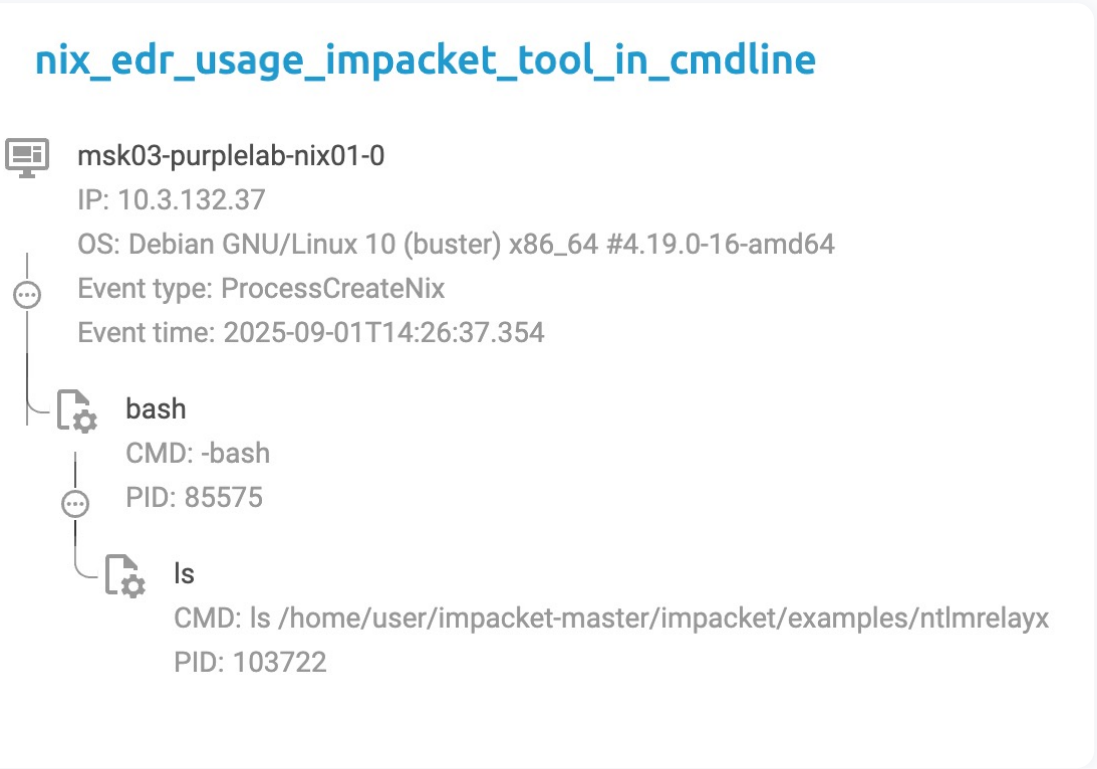
BI.ZONE

Обнаружение

Обнаружение Linux

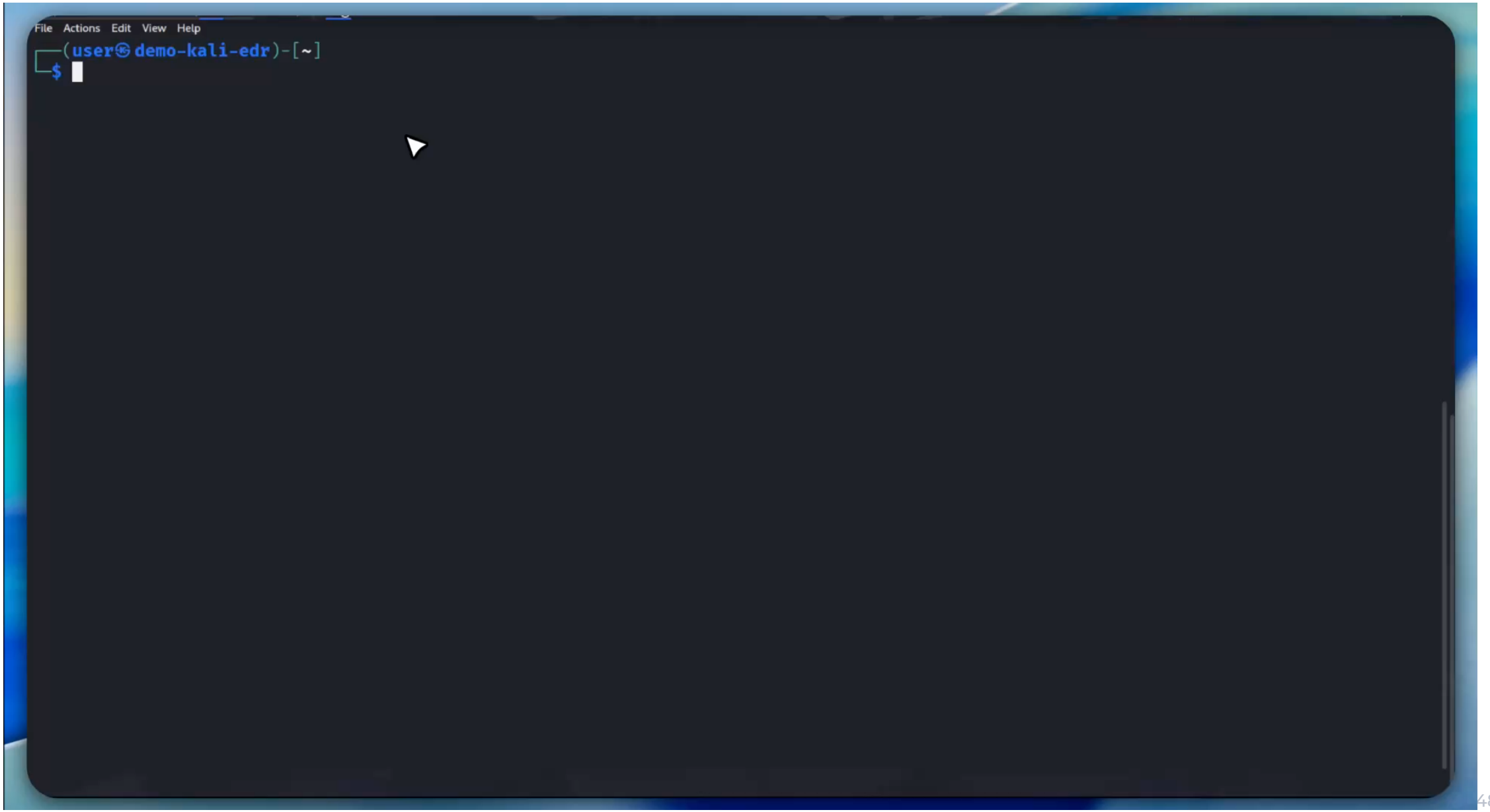
BI.ZONE

- Различные технологии обнаружения: IoA, YARA, IoC
- Пользовательские правила и исключения
- Deception-приманки
- Самозащита



Обнаружение Linux

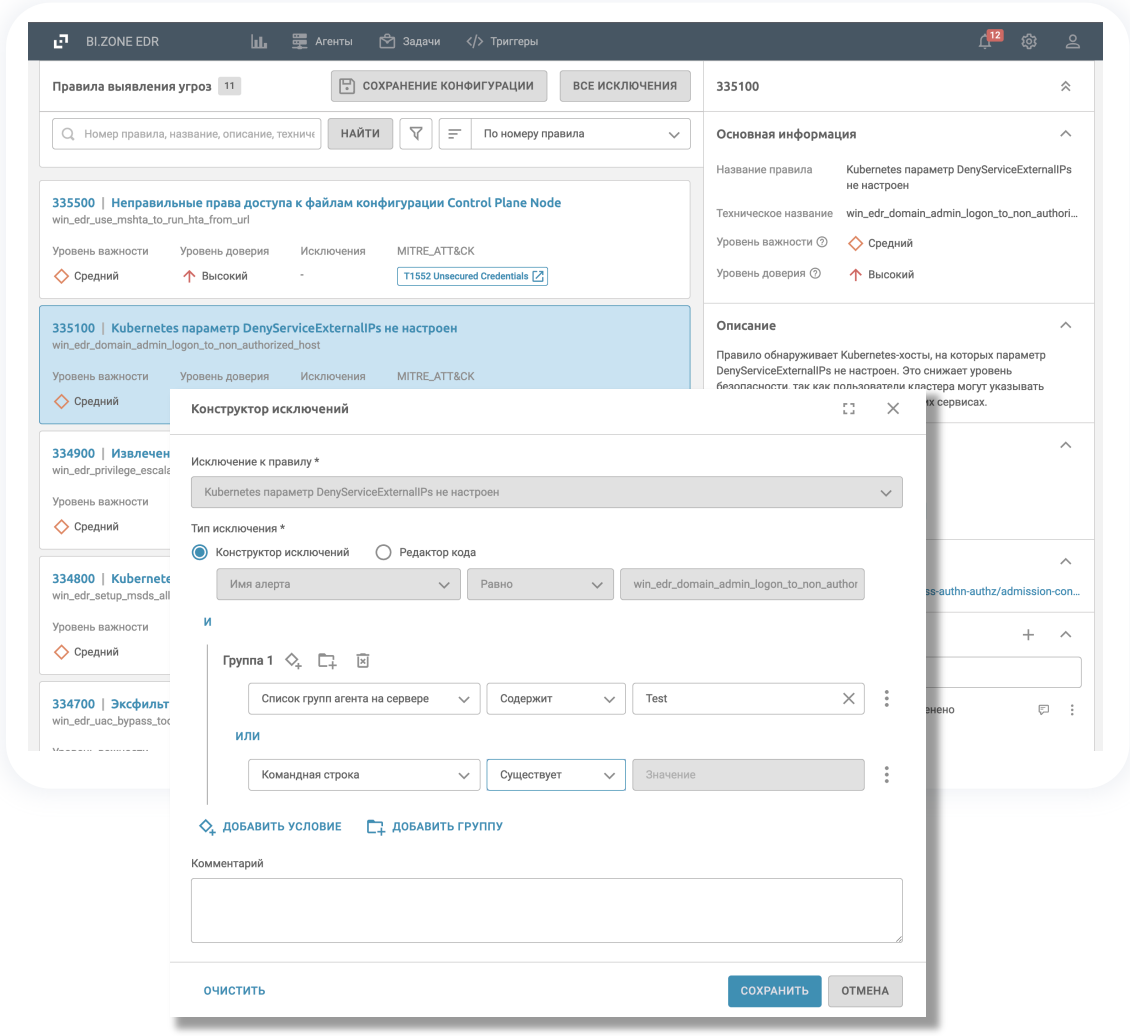
BI.ZONE



Прозрачность политики обнаружения угроз

BI.ZONE

- Список экспертных правил
- Подробное описание правил
- Упрощение адаптации под инфраструктуру
- Минимизация ошибок



Технический аудит ОС и ПО

BI.ZONE

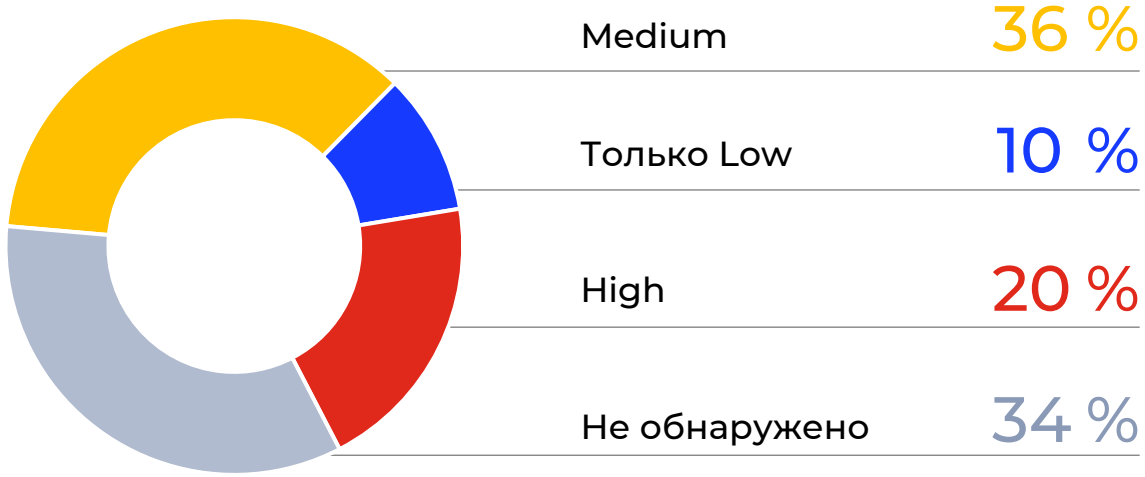
- Различные источники идей: CIS, NSA, ФСТЭК
- Разработка на основе экспертного опыта
- Пользовательские правила и исключения
- Офлайн-детектирование без общения с сервером

2 из 3

корп. компьютеров содержат хотя бы одну мисконфигурацию*

1 из 50

корпоративных локальных пользователей использует слабый пароль*

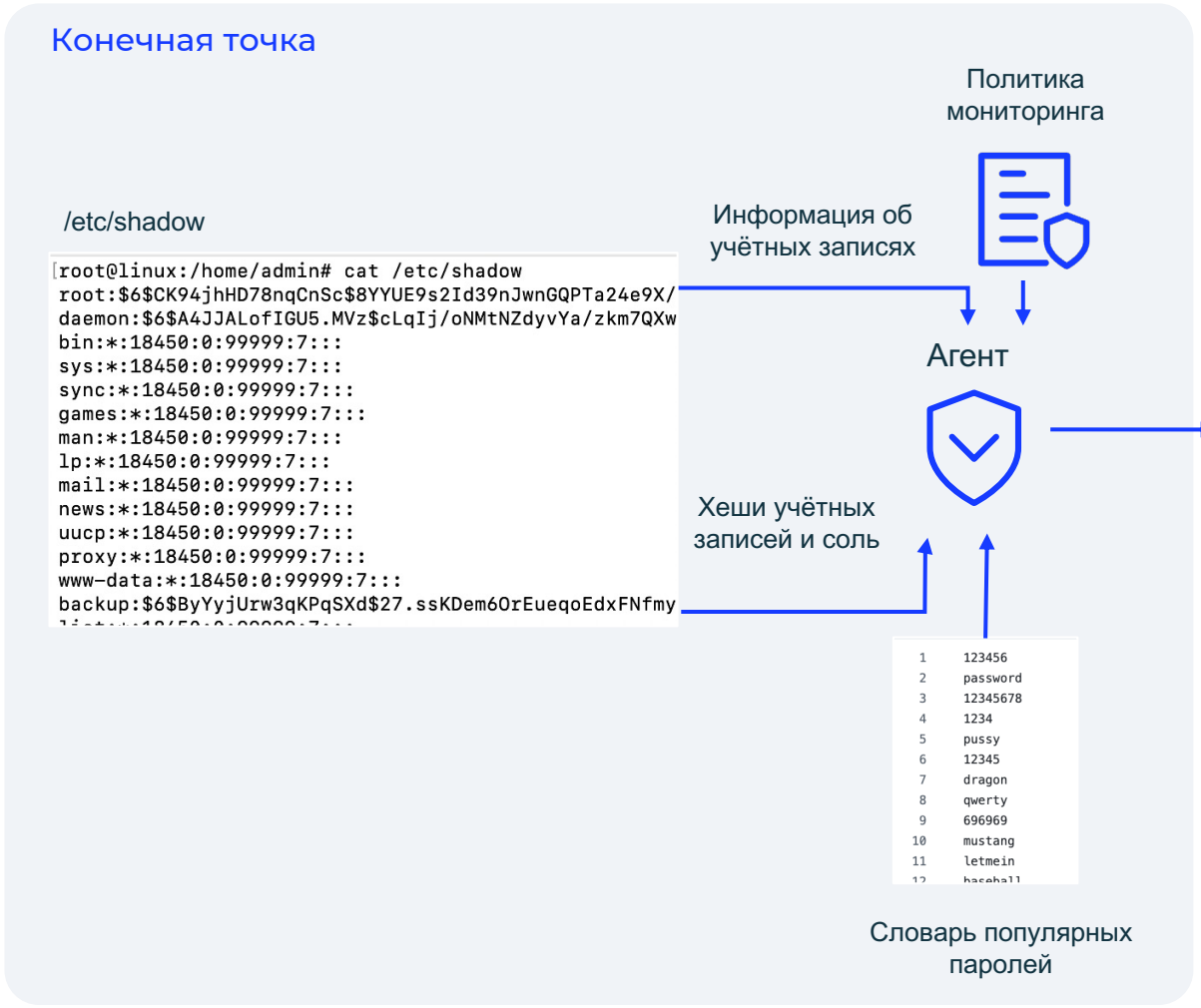


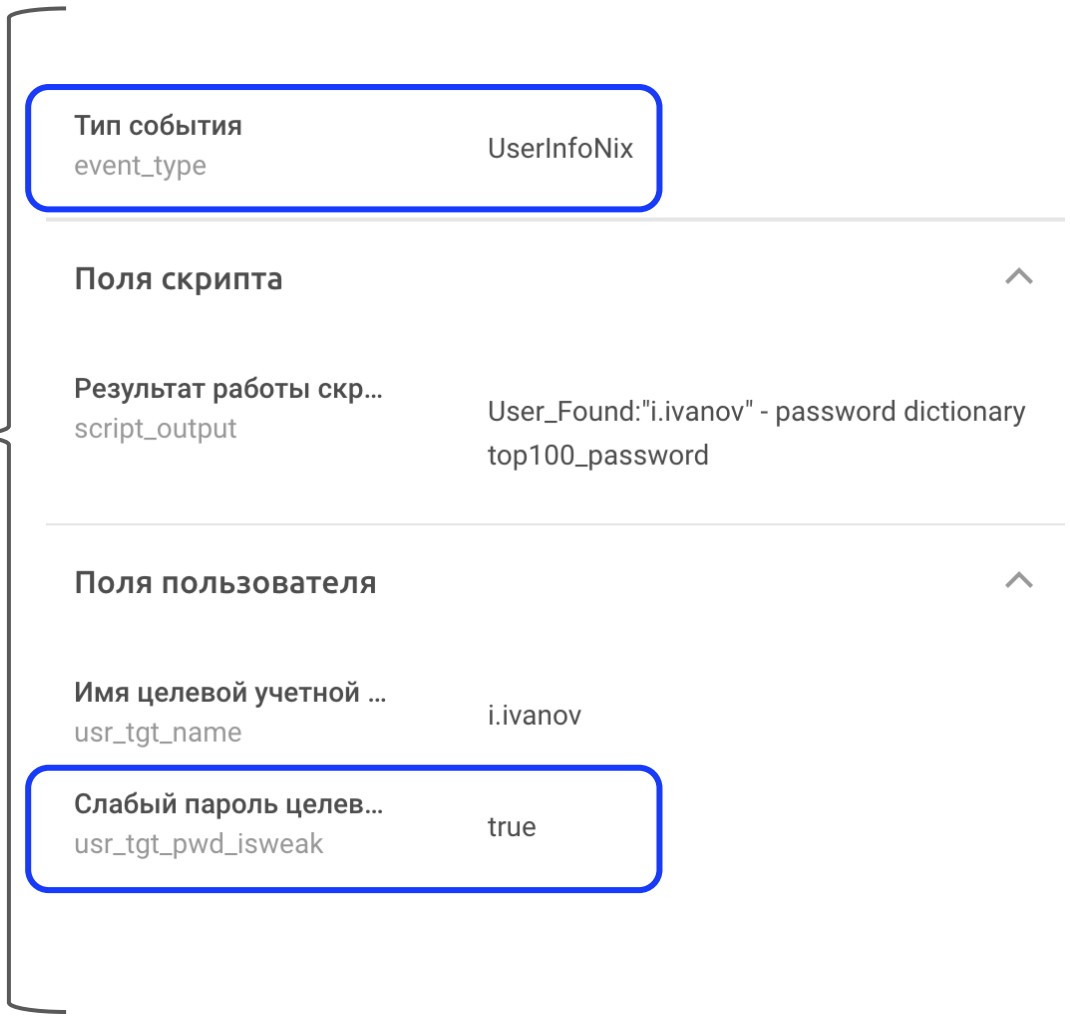
Распределение хостов по критичности выявленных мисконфигураций

* По данным BI.ZONE TDR – 150+ компаний и 290 000+ конечных точек

Слабые пароли

BI.ZONE





Популярные мисконфиги*

BI.ZONE

* По данным BI.ZONE TDR – 150+ компаний и 290 000+ конечных точек

Случай из практики

BI.ZONE

X

На одном из хостов обнаружен пользователь **sftp** со слабым паролем, а также разрешен вход по SSH с паролем

+10 дней

Хост стал доступен из сети интернет, пароль пользователя **sftp** не был изменен

+19 часов

Злоумышленники подобрали пароль пользователя **sftp** с 15 попытки и начали разведку и сбор данных на хосте

+40 мин

Аналитики SOC предотвратили атаку. Пароль сменили

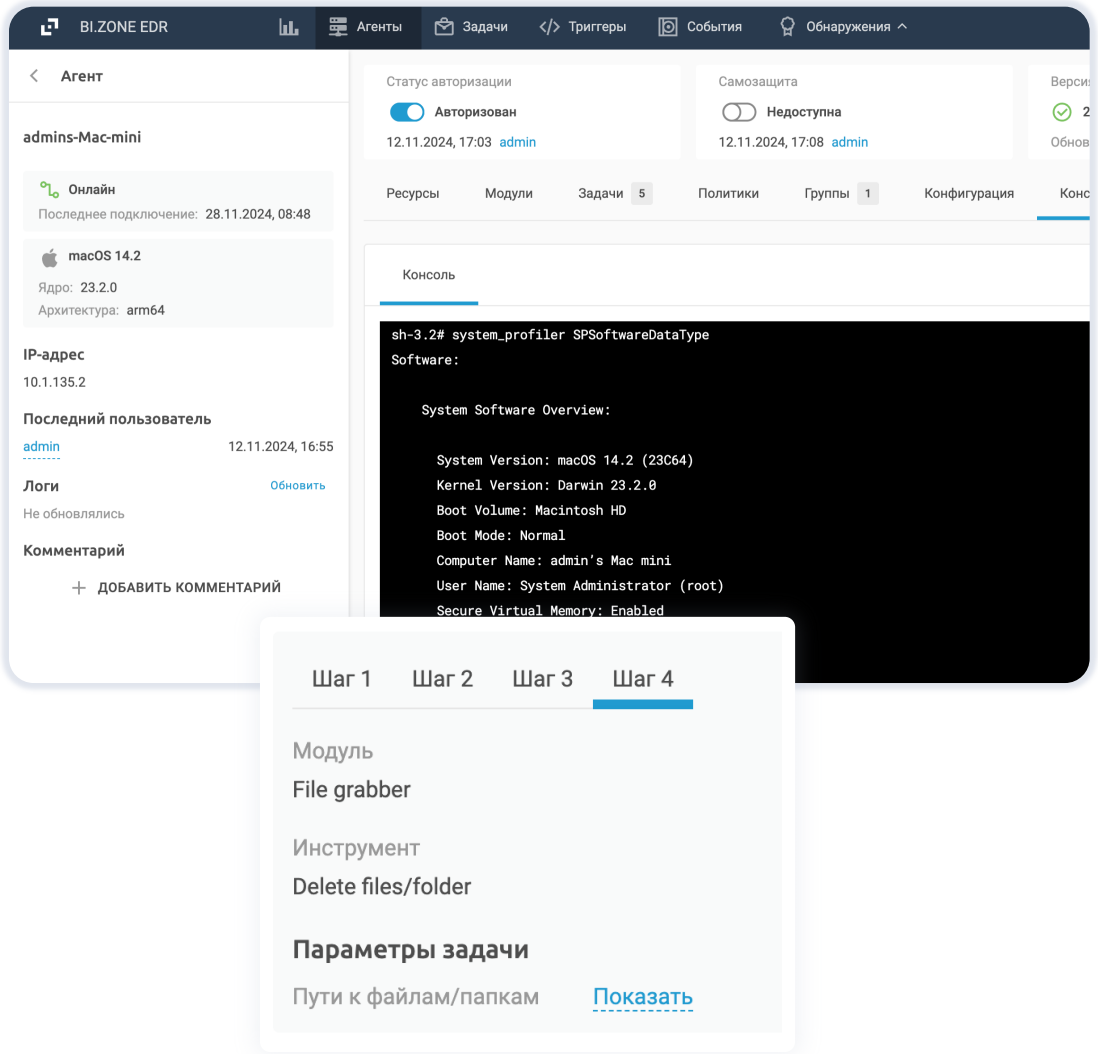
BI.ZONE

Реагирование

Реагирование

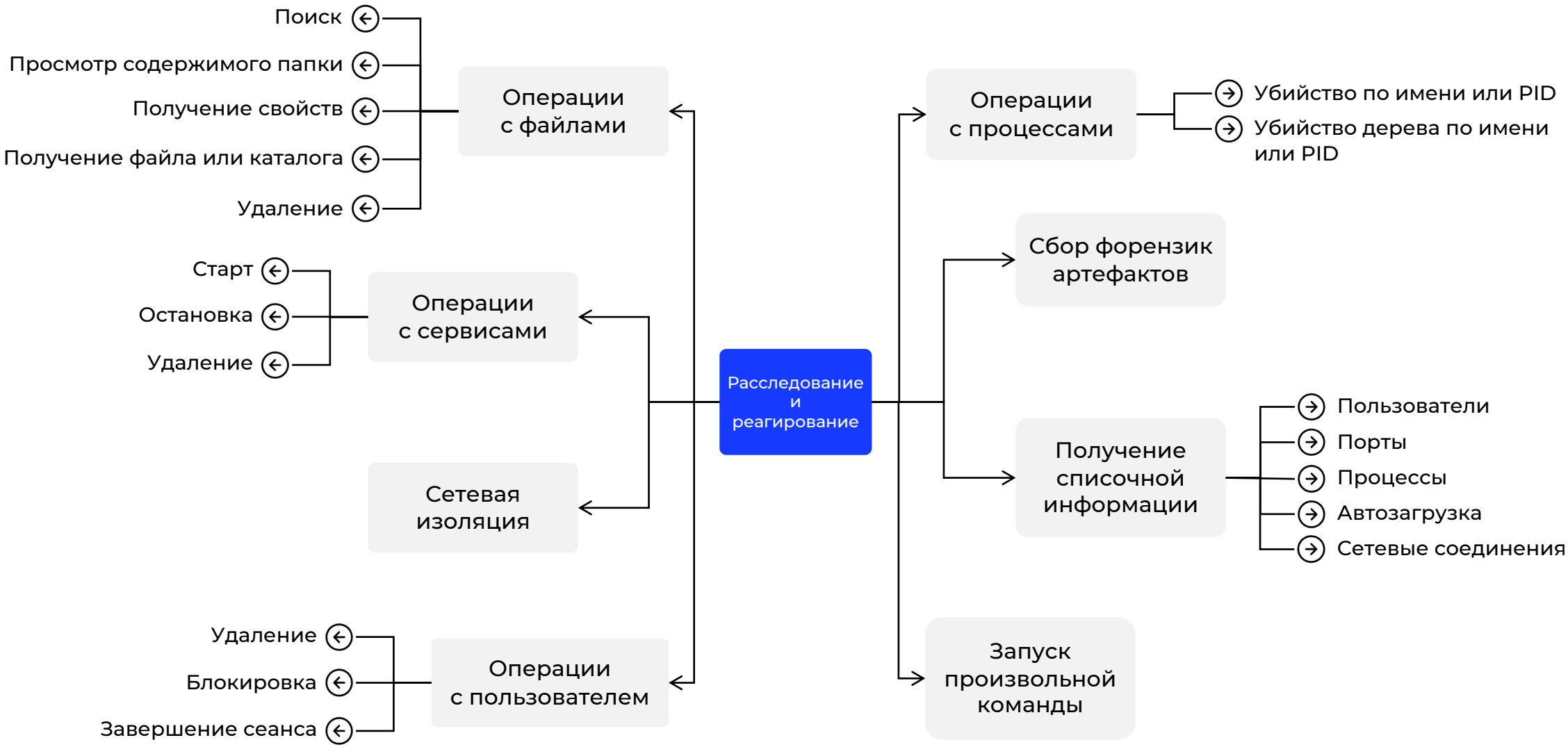
BI.ZONE

- Автоматическое (онлайн/офлайн) и ручное реагирование
- Библиотека готовых сценариев расследования и реагирования
- Live-консоль из веб-интерфейса
- Сетевая изоляция



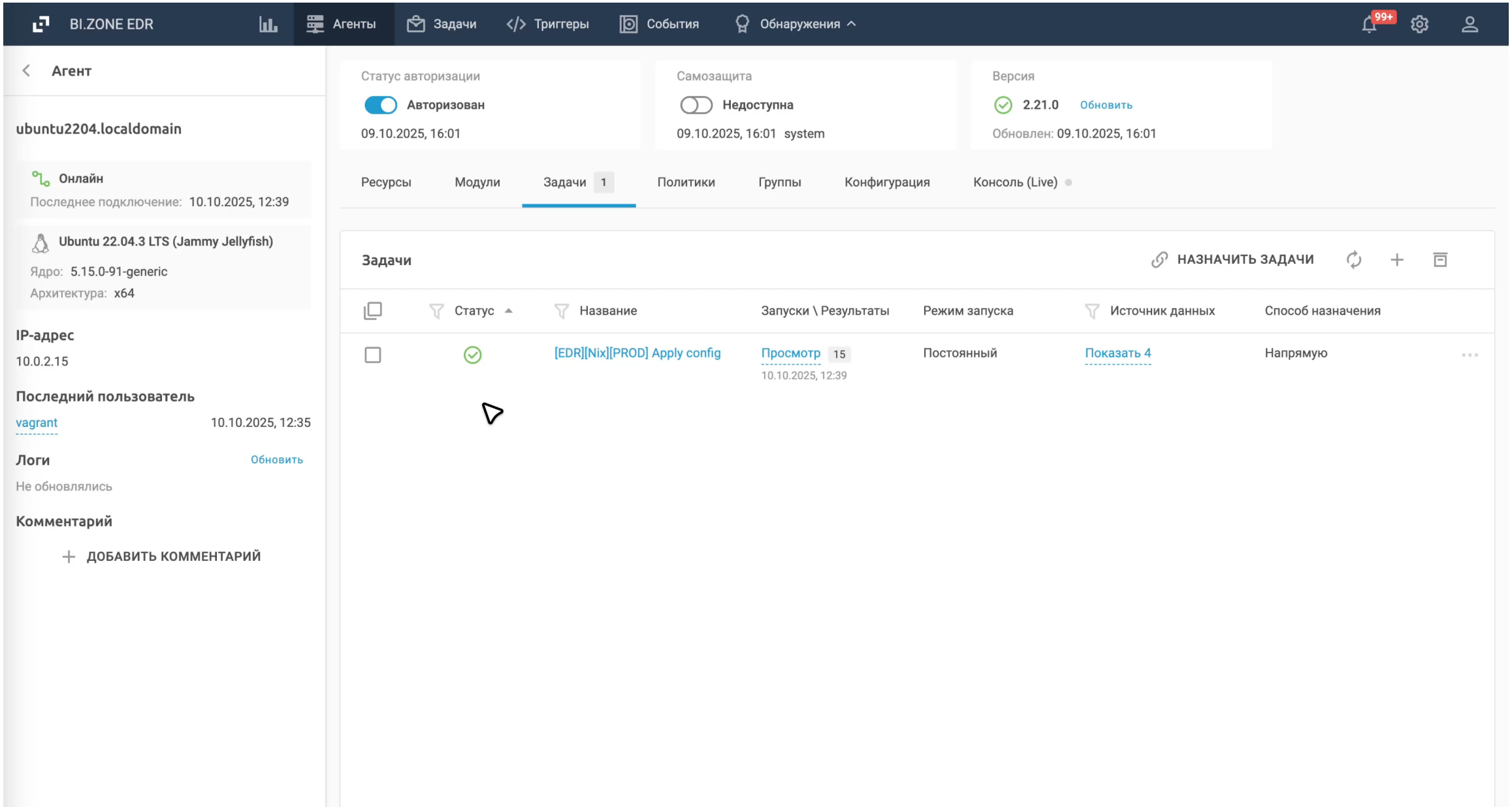
Реагирования через сервер EDR

BI.ZONE



Автоматическое реагирование

BI.ZONE



Возможности BI.ZONE EDR

BI.ZONE

Обнаружение

Threat prediction
Автоматизированное выявление недостатков инфраструктуры

IoC
Автоматизированное выявление следов атакующих

Офлайн
Выявление атак без доступа к серверу управления

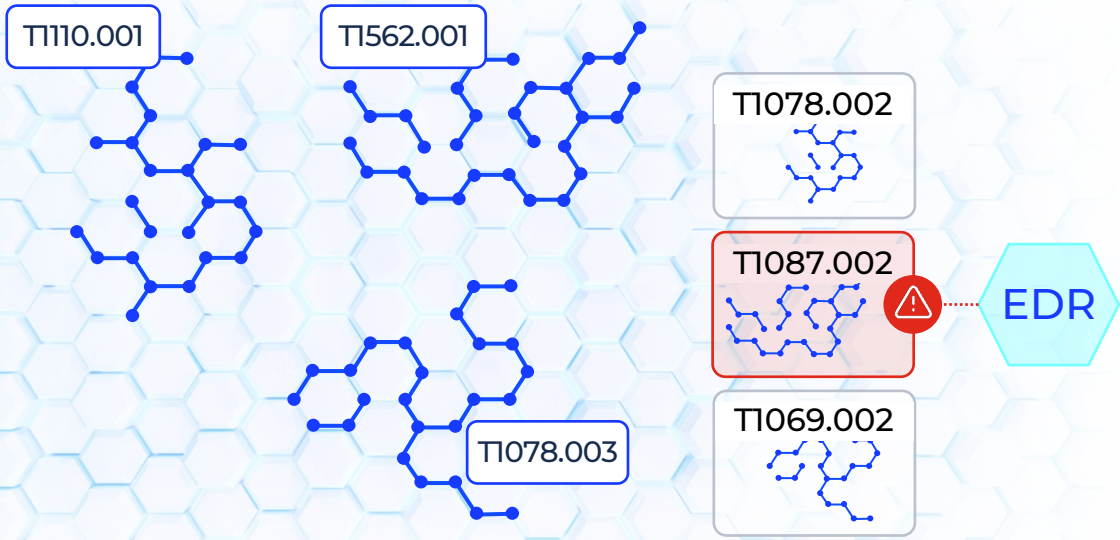
IoA
Автоматизированное выявление TTP атакующих

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
- Выполнение действий через API
- Изоляция хоста
- Интерактивная консоль
- Запуск команд и скриптов
- Автоматическое реагирование

Телеметрия
Передача собранных событий

Обнаружение
Передача обнаружений по внутренним правилам

Реагирование
Возможность запуска команд по расследованию и реагированию

Интеграции с внешними СЗИ

Возможности BI.ZONE EDR

BI.ZONE

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)

Ключевые преимущества BI.ZONE EDR в сравнении с другими EDR

T1078.003

T1069.002

Расследование и реагирование

- Скачивание и загрузка файлов
- Завершение процесса
- Удаление файлов
- Выполнение действий через API
- Изоляция хоста
- Интерактивная консоль
- Запуск команд и скриптов
- Автоматическое реагирование

Телеметрия
Передача собранных событий

Обнаружение
Передача обнаружений по внутренним правилам

Реагирование
Возможность запуска команд по расследованию и реагированию

Интеграции с внешними СЗИ

Сертификация и партнерства

BI.ZONE

Реестр
отечественного ПО

Сертификат ОАЦ при Президенте
Республики Беларусь

Сертификаты ФСТЭК:

- СОВ 4-го класса
(ноябрь 2025 г.)
- Антивирус (скоро)
- EDR (скоро)

Сертификаты совместимости
с российским ОС:

- Astra Linux
- ALT Linux
- «РЕД ОС»

Совместимость с популярными
САВЗ и DLP-решениями

BI.ZONE

Выводы

Преимущества BI.ZONE EDR в Linux

BI.ZONE

Уникальная телеметрия.
В режиме мониторинга и инвентаризации

Мониторинг происходящего в контейнерах.
Инвентаризация контейнеров

Управляемая нагрузка на хосты.
Профили потребления для Linux

Выявление уязвимостей и недостатков конфигурации ОС и ПО

Гибкость политик мониторинга. Возможность расширения правил телеметрии и выявления угроз

AD CS: инфраструктура и методы обнаружения атак

BI.ZONE

Изучить исследование на сайте

BI.ZONE

Спасибо!
Вопросы?

BI.ZONE в telegram

Узнать больше о BI.ZONE EDR