

# BI.ZONE

Комплексная защита  
Linux: от мониторинга  
до EDR и защиты  
микросервисов



# Предпосылки

# Эволюция мониторинга инфраструктуры

BI.ZONE

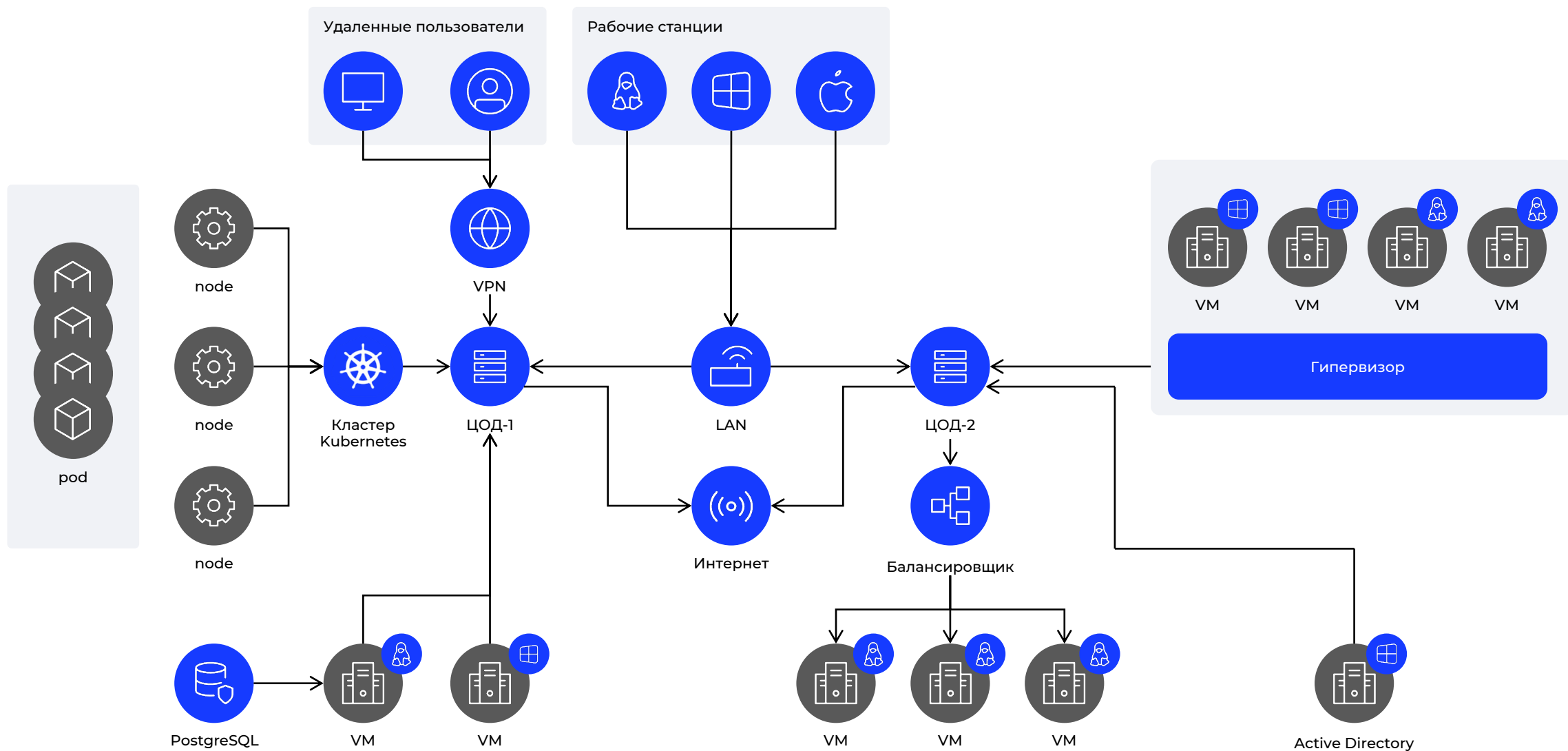
- Периметр
- СЗИ (AV, веб- и email-шлюз, NGFW и т. д.)
- Инфраструктурные сервисы (AD, Radius, VPN, DNS, Exchange и т. д.)
- Критичные APM/серверы

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

- Sysmon
- Auditbeat
- Osquery

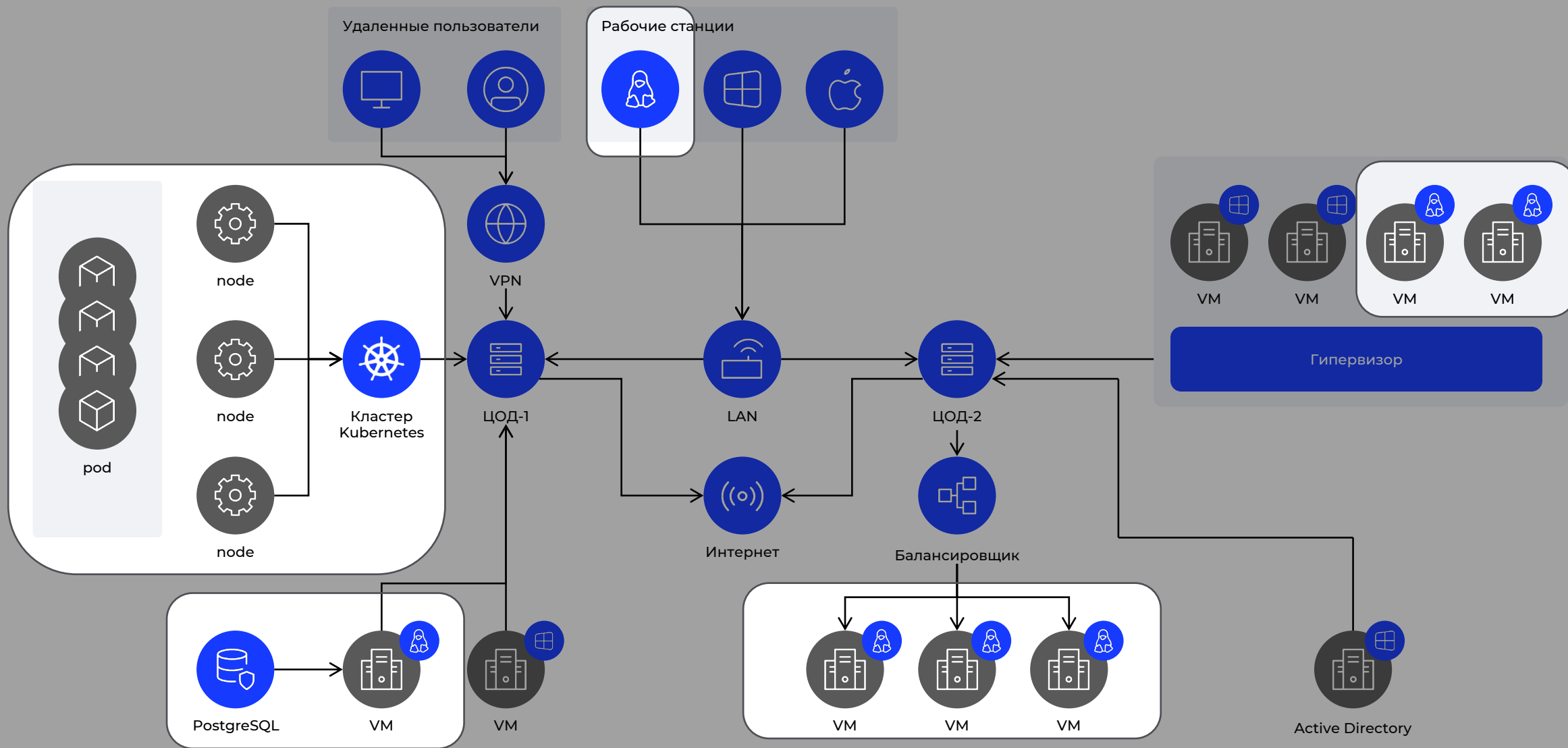
- EDR
- NTA
- Identity threat detection and response
- XDR

# Типовая IT-архитектура



# Типовая IT-архитектура

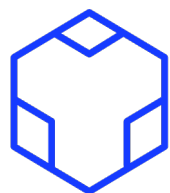
BI.ZONE



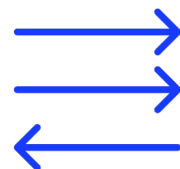
# Тенденции



Рост серверной  
Linux-инфраструктуры



Kubernetes как стандарт платформы  
для оркестрации контейнеров

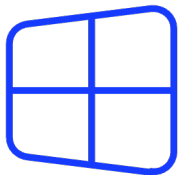


Переход на Linux-десктопы  
в российских организациях



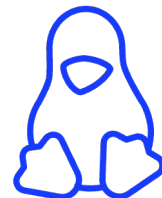
Увеличение количества атак,  
в которых затронуты Linux устройства





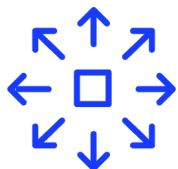
## Высокая степень унификации:

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



## Сильная фрагментация:

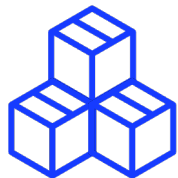
- разные дистрибутивы (Debian, RHEL, Alpine, SUSE и др.)
- разные ядра и версии системных библиотек
- Auditd с высокой нагрузкой при сборе данных
- Конкуренция за подписку на события аудита
- «Нормальная» поддержка eBPF только в «свежих ядрах»



Требуется работать в сильно разнородной и динамичной среде



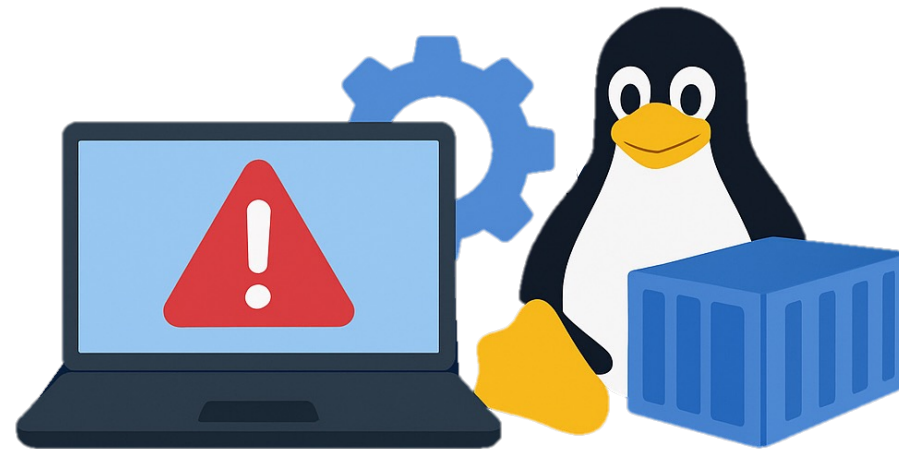
Собирать качественную телеметрию без ущерба для производительности



Уметь понимать контекст контейнеров и оркестраторов



Выявлять специфичные для Linux атаки

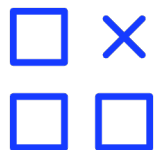


# Как BI.ZONE EDR работает в Linux

# Телеметрия

# Сбор телеметрии

BI.ZONE



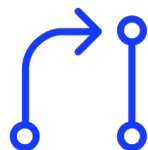
Нет необходимости  
в сторонних программах



Собственный драйвер  
на Windows



Лучшие технологии для  
получения событий (eBPF, ESF)



Гибкость сбора  
и обогащения событий

40+

событий инвентаризации

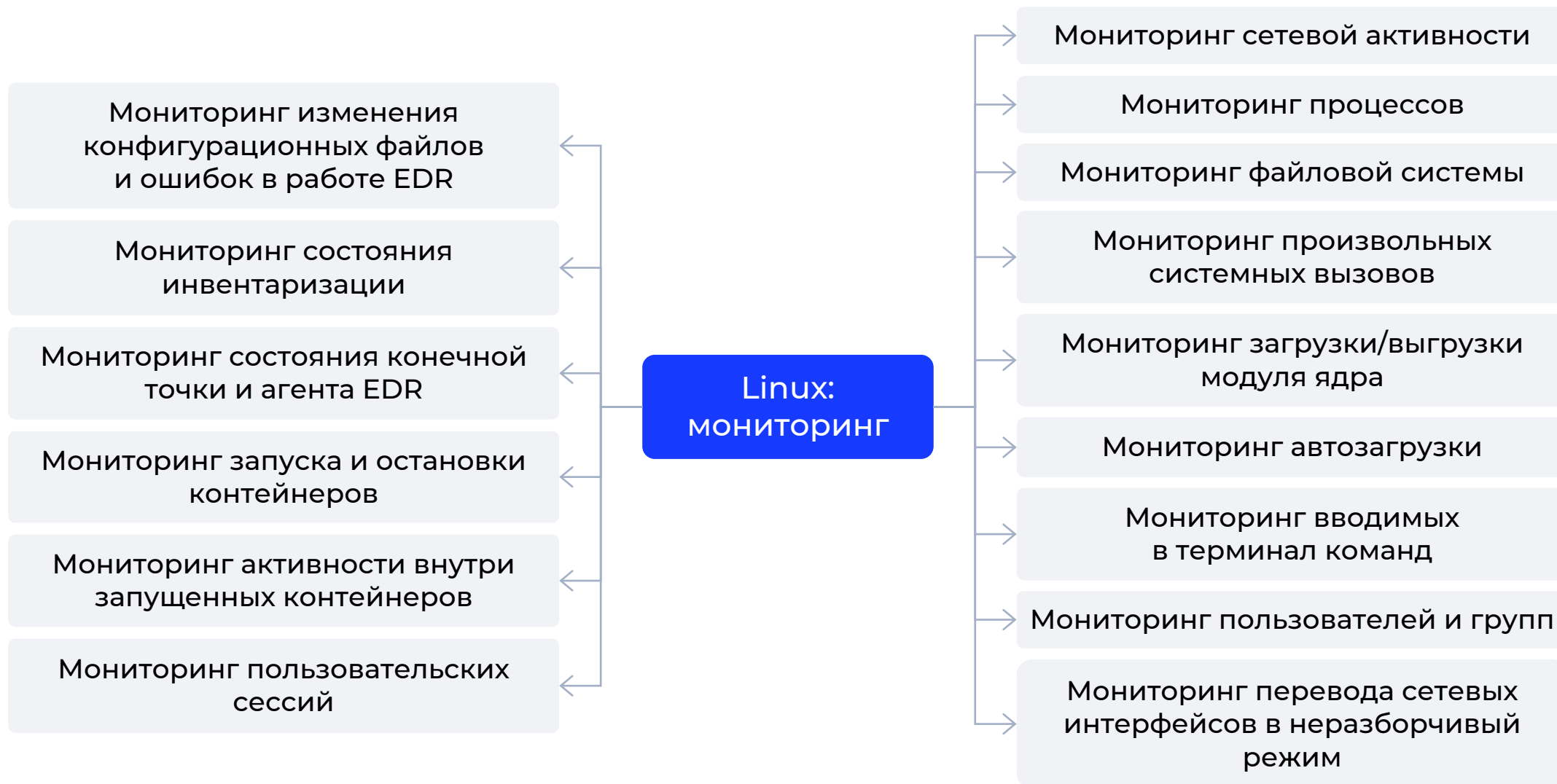
190+

событий мониторинга

30 МБ

средний объем телеметрии  
с одного агента в сутки

# Категории событий EDR



# Полнота телеметрии

```
1 {
2   "type": "SYSCALL",
3   "timestamp": "1737382118.989",
4   "record_id": "314",
5   "arch": "c00000b7",
6   "syscall": "221",
7   "success": "yes",
8   "exit": "0",
9   "a0": "b2bfe0395878",
10  "a1": "b2bfe0307660",
11  "a2": "b2bfe0396970",
12  "a3": "b2bfe0396970",
13  "items": "2",
14  "ppid": "2334",
15  "pid": "2335",
16  "aid": "1000",
17  "uid": "0",
18  "gid": "0",
19  "euid": "0",
20  "suid": "0",
21  "fsuid": "0",
22  "egid": "0",
23  "sgid": "0",
24  "fsgid": "0",
25  "tty": "pts2",
26  "ses": "4",
27  "comm": "ausearch",
28  "exe": "/usr/sbin/ausearch",
29  "subj": "unconfined",
30  "key": "process_exec"
31 }
```

auditd  
~30 полей

```
1 {
2   "@timestamp": "2025-01-22T16:57:17.519Z",
3   "@metadata.beat": "auditbeat",
4   "@metadata.type": "_doc",
5   "@metadata.version": "7.17.26",
6   "process.name": "containerd-shim",
7   "process.ppid": 1,
8   "process.pid": 3132514,
9   "process.working_directory": "/run/containerd/io.containerd.runtime.v2.task",
10  "process.executable": "/usr/bin/containerd-shim-runc-v2",
11  "process.hash.sha1": "6054e1b50ba2b7998f4ad9e3f41bb044cf28a333",
12  "process.entity_id": "K1eupUGWxdkVZpx/",
13  "process.args": ["/usr/bin/containerd-shim-runc-v2", "--namespace", "moby",
14  "message": "Process containerd-shim (PID: 3132514) by user root STARTED",
15  "user.name": "root",
16  "user.id": "0",
17  "user.group.id": "0",
18  "user.group.name": "root",
19  "user.effective.group.id": "0",
20  "user.effective.id": "0",
21  "user.saved.id": "0",
22  "user.saved.group.id": "0",
23  "service.type": "system",
24  "event.module": "system",
25  "event.dataset": "process",
26  "event.kind": "event",
27  "event.category": ["process"],
28  "event.type": ["start"],
29  "event.action": "process_started",
30  "ecs.version": "1.12.0",
31  "host.ip": ["10.3.132.91"],
32  "host.mac": ["00:50:56:bd:cc:95"],
33  "host.name": "msk03-<redacted>",
34  "host.hostname": "msk03-<redacted>",
35  "host.architecture": "x86_64",
36  "host.os.family": "debian",
37  "host.os.name": "Debian GNU/Linux",
38  "host.os.kernel": "5.10.0-29-amd64",
39  "host.os.codename": "bullseye",
40  "host.os.type": "linux",
41  "host.os.platform": "debian",
42 }
```

auditbeat  
~45 полей

```
1 {
2   "cmdline": "/bin/sh -e -u -c 'exec \"$@\" sh /usr/lib/firefox/firefox-bin https://clck.ru/3<redacted>7'",
3   "cmdline_fingerprint": "b97321fc0d2360632e9826a5ffc2d38",
4   "customer_id": "90000040",
5   "customer_name": "<redacted>",
6   "customer_system": "<redacted>",
7   "dev_fqdn": "<redacted>-Thinkf",
8   "dev_id": "c1e677ae-5bc0-4355-",
9   "dev_ipv4": "172.31.131.194",
10  "dev_os": "Ubuntu 20.04.6 LTS",
11  "dev_os_type": "linux",
12  "event_id": "40",
13  "event_log_source": "LinuxProc",
14  "event_type": "ProcessCreate",
15  "event_type_vendor": "Process",
16  "event_utc_time": "2025-01-22T16:57:17.519Z",
17  "event_uuid": "8814c90e-0a18-4",
18  "op_func_name": "sys_execve_c",
19  "proc_cgroups": "/",
20  "proc_cwd": "/home/<redacted>",
21  "proc_env": "LC_NUMERIC=ru_RU",
22  "proc_file_ace_mask": "012077",
23  "proc_file_age": 78815565,
24  "proc_file_app_productname": "dash",
25  "proc_file_atime": "2025-01-22T16:57:17.519Z",
26  "proc_file_crtime": "2022-07-27T16:57:17.519Z",
27  "proc_file_exists": true,
28  "proc_file_group_id": 0,
29  "proc_file_group_name": "root",
30  "proc_file_inode": 13632686,
31  "proc_file_mage": 78815565,
32  "proc_file_mtime": "2022-07-27T16:57:17.519Z",
33  "proc_file_name": "sh",
34  "proc_file_nlink": 1,
35  "proc_file_owner_id": 0,
36  "proc_file_owner_name": "root",
37  "proc_file_path": "/bin/sh",
38  "proc_file_size": 4,
39  "proc_file_tgt_ace_mask": "012077",
40  "proc_file_tgt_name": "dash",
41  "proc_file_tgt_path": "/bin/dash",
42  "proc_file_tgt_size": 129816,
43  "proc_file_type": "Link",
44  "proc_group_e_id": 1000,
45  "proc_group_e_name": "<redacted>",
46  "proc_group_r_id": 1000,
47  "proc_group_r_name": "<redacted>",
48  "proc_guid": "5aa965db-4bed-5adf-bd0e-882c9c2264b8",
49  "proc_id": 2679813,
50  "proc_issnapshot": false,
51  "proc_p_cap_pe": 2818844155,
52  "proc_p_cap_pp": 2818844155,
53  "proc_p_cmdline": "make libzcpputils.so",
54  "proc_p_cwd": "/usr/local/src/cpe/cpp/bz-cpp-utils",
55  "proc_p_file_exists": true,
56  "proc_p_file_name": "make",
57  "proc_p_file_path": "/usr/bin/make",
58  "proc_p_group_e_id": 0,
59  "proc_p_group_r_id": 0,
60  "proc_p_guid": "d4fe8399-919e-5257-8508-44f8af3013fb",
61  "proc_p_id": 2300,
62  "proc_p_session_id": 322933,
63  "proc_p_uptime": 441618,
64  "proc_p_usr_e_id": 0,
65  "proc_p_usr_r_id": 0,
66  "proc_session_id": 2613,
67  "proc_start_time": "2025-01-22T16:08:55.520Z",
68  "proc_term_session_id": 5,
69  "proc_usr_audit_id": 1000,
70  "proc_usr_audit_name": "vladislav",
71  "proc_usr_e_id": 1000,
72  "proc_usr_e_name": "vladislav",
73  "proc_usr_r_id": 1000,
74  "proc_usr_r_name": "vladislav",
75  "rule_name": "ProcessCreate - Process Create Info",
76  "sensor_cfg_profile": "default",
77  "sensor_cfg_profile_id": "1",
78  "sensor_cfg_version": "202409191126",
79  "sensor_groups": "[Nix] PROD",
80  "sensor_type": "bedr",
81  "sensor_version": "1.9.0"
82 }
```

BI.ZONE EDR  
~80 полей

# Интересно отметить

## 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

## 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

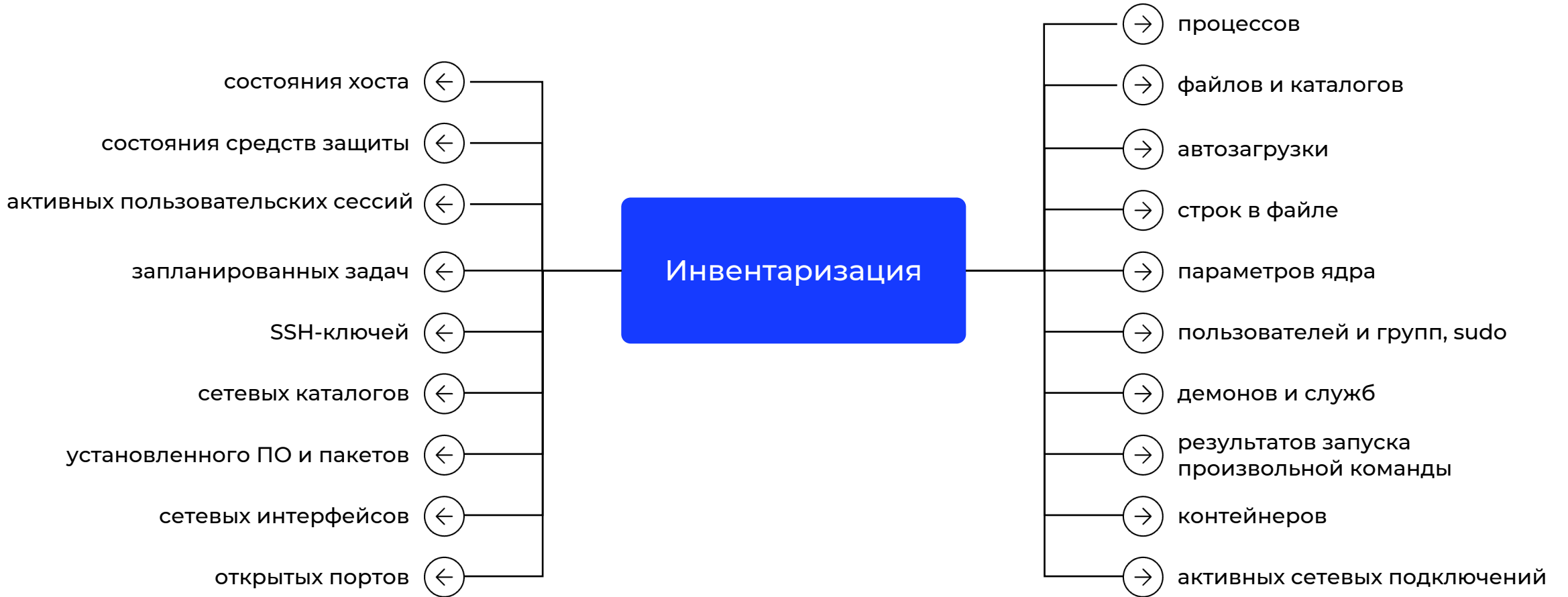
cmdline

dig +short A bi.zone

Время работы процес...

2260272

# Категории инвентаризации



# Интересно отметить

BI.ZONE EDR | | | | | |

```
2 FROM events
3 WHERE app_type ILIKE '%python%'
4 GROUP BY dev_fqdn, app_productname, app_version
```

dev_fqdn	app_productname	app_version
mow-ubuntu22	msgpack	1.0.3
msk-	six	1.12.0
mow-ubuntu22	termcolor	2.5.0
mow-ubuntu22	command_not_found	0.3
msk-	wheel	0.32.3
mow-ubuntu22	cryptography	42.0.8
msk-	iotop	0.6
mow-ubuntu22	wadllib	1.3.6
mow-ubuntu22	lazr.uri	1.0.6
mow-ubuntu22	hyperlink	21.0.0
mow-ubuntu22	sortedcontainers	2.1.0
msk-	PyYAML	3.13

# Интересно отметить

**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 nfserver

**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 nfserver

## Поля общего сетевого ресурса ^

**Список атрибутов общего сетевого ресурса**  
share\_attr nfsclient.example.local(sec=krb5p,rw,sync,  
no\_subtree\_check)



## 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_*	<a href="#">EventFields</a>	Набор полей, описывающих служебные атрибуты события	
dev_*	<a href="#">DeviceFields</a>	Набор полей, описывающих хост, с которого было получено событие	
sensor_* customer_*	<a href="#">SensorFields</a>	Набор полей, описывающих агента, выполнившего генерацию события, и использованную конфигурацию	
proc_usr_e_id	number	Идентификатор эффективного пользователя процесса после смены eUID. Подробнее см. <code>\$ man 7 credentials</code>	0
proc_usr_e_name	string	Имя эффективного пользователя процесса после смены eUID. Подробнее см. <code>\$ man 7 credentials</code>	root
proc_usr_e_id_old	number	Идентификатор эффективного пользователя процесса до смены eUID.	42

- ..... 250
- ..... 252
- ..... 254
- ..... 257
- ..... 257
- ..... 258
- ..... 260
- ..... 261
- ..... 261
- ..... 262
- ..... 262
- ..... 263
- ..... 265
- ..... 265
- ..... 266
- ..... 270

# Интеграция с SIEM

BI.ZONE

The screenshot displays the MaxPatrol 10 SIEM interface. The top navigation bar includes the MaxPatrol 10 logo and menu items: Активы, События, Инциденты, Сбор данных, Система. The current view is for an incident with ID INC-604087, titled "BIZONE\_EDR\_High\_Alert\_was\_triggered".

**Инциденты / BIZONE\_EDR\_High\_Alert\_was\_triggered**

**Статус**

- Опасность: Средняя
- Статус: Новый
- Ответственный: Не назначен
- Автор:
- Источник инцидента: Скрипт SIEM
- Обнаружен: 17 февраля, 08:47
- Создан: 17 февраля, 15:39
- Последнее изменение: Изменено: событие 17 февраля, 15:39

**Параметры**

- Категория: Неавторизованный доступ
- Тип: Компрометация узла/ПО
- Влияние:
- Расположение:

**События**

Время	Событие
17 февраля 08:47	На хосте msk03-kubernetes-worker-lab-02 запущен процесс /usr/sbin/iptables пользователем root
17 февраля 08:47	На хосте msk03-kubernetes-worker-lab-02 запущен процесс /usr/sbin/iptables пользователем root
17 февраля 08:47	На хосте msk03-kubernetes-worker-lab-02 сработало правило "nix_edr_use_shell_tool_to_access_kubeapi_inside_container". Активный пользователь: root Описание алерта: "using to access KubeAPI inside a container"
17 февраля 08:47	На хосте msk03-kubernetes-worker-lab-02 сработало правило "nix_edr_use_shell_tool_to_access_kubeapi_inside_container". Активный пользователь: root Описание алерта: "using to access KubeAPI inside a container"
17 февраля 08:47	На хосте msk03-kubernetes-worker-lab-02 сработало правило "nix_edr_use_shell_tool_to_access_kubeapi_inside_container". Активный пользователь: root Описание алерта: "using to access KubeAPI inside a container"

**05.03.2025 18:53:16**

На хосте msk03-kubernetes-worker-lab-02 запущен процесс /usr/sbin/ip6tables

Источник [BI.ZONE linux](#) Идентификатор [40 LinuxProcessMonitor](#)  
Категория [BI.ZONE EDR / ProcessCreate / ProcessCreate](#)


**Роли во взаимодействии**

**Субъект**

- subject: account
- subject.account.id: 0

**Объект**

- object: process
- object.value: 0
- object.type: Link
- object.account.id: 0
- object.application.account.id: 0
- object.process.name: ip6tables
- object.process.path: /usr/sbin/
- object.process.fullpath: /usr/sbin/ip6tables
- object.process.cmdline: ip6tables -w 5 -W 100000 -N KUBE-MARK-MASQ
- object.process.guid: e34f655a-9ef0-5334-ae7a-4927fd28a237
- object.process.id: 3737860
- object.process.cwd: /



**Kaspersky**  
**Unified Monitoring and Analysis Platform**

---

Выбрано тенантов: 1

---

Панель мониторинга

**Алерты**

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

[Алерты >](#)

BIZONE\_EDR\_High\_Alert [redacted] win\_edr\_dns\_server\_level\_plugin\_dll\_configuration\_in\_registry) Новый

Уровень важности: Высокий Назначить: Не назначено Закреть алерт

## Информация об алерте

Уровень важности правила корреляции	Первое появление	Тенант
<b>Высокий</b>	22.08.2025 15:48:17	Main
Наивысшая важность категории активов	Последнее появление	Правило корреляции
Нет значения	22.08.2025 17:37:41	<a href="#">BIZONE EDR High Alert</a>

Идентификатор алерта

07d83f87-7d96-431a-a272-d66e995eaac1

## Связанные события

Время ↓	Информация о событии
<p>&gt; <span style="color: red;">■</span> 01.12.2022 17:37:41</p>	<p>Severity: High , Technique: alert , Tactic: win_edr_dns_server_level_plugin_dll_conf DeviceProduct: windows , DeviceAddress: [redacted] [redacted] - DNS server level plugin DLL configuration via Windows registry. The "hkey_local_machine\system\controlset001\services\dns\parameters\serverlevelplugin_dll" registry value may indicate the modification of the registry key responsible for configuring the DNS Server Level Plugin DLL mechanism, which may indicate either an attempt by an attacker to gain persistence on a compromised system using the Server Level Plugin DLL, or an attempt at privilege escalation.</p>
<p>&gt; <span style="color: red;">■</span> 30.11.2022 21:34:15</p>	<p>Severity: High , Technique: alert , Tactic: win_edr_dns_server_level_plugin_dll_conf DeviceProduct: windows , DeviceAddress: [redacted] [redacted] - DNS server level plugin DLL configuration via Windows registry. The "hkey_local_machine\system\controlset001\services\dns\parameters\serverlevelp</p>

## Информация о корреляционном событии

Копировать Подробные сведения

TenantName	Main
Timestamp	22.08.2025 17:37:41 :172
Name	BIZONE_EDR_High_Alert
StartTime	22.08.2025 17:37:41 :719
EndTime	22.08.2025 17:37:41 :719
Message	The "hkey_local_machine\system\controlset001\services\dns\parameters\serverlevelplugin_dll" registry value may indicate the modification of the registry key responsible for configuring the DNS Server Level Plugin DLL mechanism, which may indicate either an attempt by an attacker to gain persistence on a compromised system using the Server Level Plugin DLL, or an attempt at privilege escalation.
DeviceAddress	[redacted]
DeviceHostName	[redacted]
DeviceProduct	windows
DeviceTimeZone	+03:00
DeviceVendor	BI.ZONE
CorrelationRule	<a href="#">BIZONE EDR High Alert</a>
Service	<a href="#">[OOTB] Correlator</a>
BaseEventCount	1
Priority	Высокий
Reason	[redacted] - DNS server level plugin DLL configuration via Windows registry

# Жизнь в хайлоад

# Профили сбора данных



Базовый профиль



Мониторинг

Инвентаризация

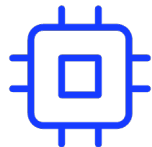


Высокая сетевая активность



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

The screenshot displays the BI.ZONE EDR interface, divided into three main sections:

- System Resource Usage (Left Panel):** A terminal-style display showing system metrics and a process list. The top part shows CPU usage (0.0%, 2.6%, 3.3%, 2.0%) and memory usage (1.70G/2.91G). Below is a table of running processes.
- Agent Information (Middle Panel):** Details for the agent 'linux.demo.local'. It shows the agent is online, last connected on 01.09.2025, 19:37. It lists the OS as 'Debian GNU/Linux 10 (buster)', kernel '4.19.0-26-amd64', and architecture 'x64'. The IP address is 10.3.132.24, and the last user was 'p.kutsenko' on 01.09.2025, 17:08.
- Task Management (Right Panel):** A table of tasks with columns for status, name, runs/results, launch mode, and data source. Tasks include configuration updates, diagnostic checks, and agent updates.

PID	USER	PRI	NI	VRT	RES	SHR	S	CPU%
391	root	20	0	22624	4976	3448	S	0.0
589	systemd-t	20	0	93096	5776	4916	S	0.0
527	systemd-t	20	0	93096	5776	4916	S	0.0
528	root	20	0	46196	9680	8148	S	0.0
597	_lldpd	20	0	26172	7132	6040	S	0.0
601	root	20	0	8500	2776	2512	S	0.0
632	root	20	0	714M	56068	16852	S	0.0
644	root	20	0	714M	56068	16852	S	0.0
645	root	20	0	714M	56068	16852	S	0.0
635	root	20	0	2189M	43772	24068	S	0.0
636	root	20	0	2189M	43772	24068	S	0.0
637	root	20	0	2189M	43772	24068	S	0.0
638	root	20	0	2189M	43772	24068	S	0.0
641	root	20	0	2189M	43772	24068	S	0.0
654	root	20	0	2189M	43772	24068	S	0.0
655	root	20	0	2189M	43772	24068	S	0.0
1064	root	20	0	2189M	43772	24068	S	0.0
1149	root	20	0	2189M	43772	24068	S	0.0
605	root	20	0	5608	1492	1380	S	0.0
623	root	20	0	13816	6144	5308	S	0.0
643	root	20	0	190M	19296	12940	S	0.0
649	www-data	20	0	190M	9280	2896	S	0.0
650	www-data	20	0	190M	9280	2896	S	0.0
651	www-data	20	0	190M	9280	2896	S	0.0
652	www-data	20	0	190M	9280	2896	S	0.0
653	www-data	20	0	190M	9280	2896	S	0.0
668	root	20	0	3579M	86192	38332	S	0.0
669	root	20	0	3579M	86192	38332	S	0.0
670	root	20	0	3579M	86192	38332	S	0.0

Задачи	Статус	Название	Запуски \ Результаты	Режим запуска	Источник данных
<input type="checkbox"/>	🔄	[EDR][Nix][PROD] Apply config	<a href="#">Просмотр</a> 2 01.09.2025, 19:41	Постоянный	<a href="#">Показать 7</a>
<input type="checkbox"/>	✅	[EDR][Nix] Get Diagnostic	<a href="#">Просмотр</a> 2 01.09.2025, 17:06	Ручной	
<input type="checkbox"/>	✅	[Int] [Auth] Agent	<a href="#">Просмотр</a> 6 01.09.2025, 19:41	Ручной	
<input type="checkbox"/>	✅	[EDR][Nix][TEST] Apply config	<a href="#">Просмотр</a> 18 01.09.2025, 17:20	Постоянный	<a href="#">Показать 7</a>
<input type="checkbox"/>	✅	[INT][Nix][PROD] install/update	<a href="#">Просмотр</a> 5 01.09.2025, 19:41	Ручной	
<input type="checkbox"/>	✅	[INT][Agent][Nix][PROD] update	<a href="#">Просмотр</a> 6 01.09.2025, 19:41	Ручной	
<input type="checkbox"/>	✅	[INT][Fg & Sa][PROD] install/update	<a href="#">Просмотр</a> 5 01.09.2025, 19:41	Ручной	

# Контейнеры

# Проблема мониторинга контейнеров



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

## 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.

Поля командной строки	
Командная строка cmdline	go list github.com/google/go-github/github
Тип события event_type	ProcessCreateNix

Поля контейнера	
Идентификатор конте... container_id	20d5c6c0e01f4bc0294d6010349a19331e96b78e93aed95b0a3827d3ce890427
Имя образа контейнера container_img_name	caldera:latest
Имя контейнера container_name	caldera_old-caldera-1
Список меток контейн... container_labels	io.cri-containerd.kind=container, io.kubernetes.container.name=caldera_old-caldera-1, io.kubernetes.pod.name=runner-test-1, io.kubernetes.pod.namespace=test, io.kubernetes.pod.uid=18c54e2e-3642-445c-8f25-9d4d88a8e9b1

## Инвентаризация

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

event_type	dev_fqdn	container_name	container_state
ContainerInfoNix	linux.demo.local	www-wordpress-1	running
ContainerInfoNix	linux.demo.local	strange_kirch	exited
ContainerInfoNix	linux.demo.local	grafana	running
ContainerInfoNix	linux.demo.local	stoic_colden	exited
ContainerInfoNix	linux.demo.local	epic_perlman	exited

Поля конфигурации

Значение параметра конфигурации (cfg_param_value)	NodeRestriction
Название параметра конфигурации (cfg_param)	--enable-admission-plugins

Поля события

Вендорский тип события (event_type_vendor)	ConfigurationParameterFound
Название правила фильтрации (rule_name)	ConfigurationParameterFound - Configuration Kubernetes (MASTER-NODE - KUBE-APISERVER) Parameter Info Three
Уникальный идентификатор (customer_id)	90000052
Идентификатор события (event_id)	405
Тип события (event_type)	ConfigParamInfoNix

Поиск

### Поля контейнера

Список смониторованных контейнеров (container_mounts)	/var/lib/docker/volumes/7a6a96a07f63d68449e2f8ef0e1f493f6c6e7b1f945576a1f6f72/_data:/var/www/html:
Имя контейнера (container_name)	www-wordpress-1
Имя образа контейнера (container_img_name)	wordpress:latest
Список переменных среды (container_env)	APACHE_CONFDIR=/etc/apache2 APACHE_ENVVARS=/etc/vvvars GPG_KEYS=39B641343D8C104B2B146DC3F9C39D6E60913E4DF209907 SHRINK
Командная строка исполнения (container_cmdline)	docker-entrypoint.sh apache2-foreground
Список IP адресов контейнера (container_ipaddr)	172.18.0.4
Идентификатор родительского контейнера (container_state_pid)	79040
Идентификатор образа (container_img_id)	sha256:c4d738408447e12b4ef6fa0a6413ed68eeec4af6abb998261e13
Состояние контейнера (container_state)	running
Время старта контейнера (container_start_time)	2025-09-02 06:11:04.147
Секунды с момента старта (container_uptime)	1026

## 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	
<b>Заголовок</b>	Подозрительное использование клиента docker для удаленного запуска контейнера
<b>Критичность</b>	Medium
<b>Достоверность</b>	Medium
<b>MITRE ATT&amp;CK</b>	<b>Execution:</b> T1059: Command and Scripting Interpretation T1059.004: Unix Shell <b>Initial Access:</b> T1133: External Remote Services <b>Lateral Movement:</b>

nix_edr_attempt_to_load_kernel_module_via_insmod_in_privileged_container	
<b>Заголовок</b>	Попытка загрузить модуль ядра командой привилегированного контейнера
<b>Критичность</b>	Medium
<b>Достоверность</b>	Medium
<b>MITRE ATT&amp;CK</b>	<b>privilege-escalation:</b> T1611: Escape to Host

nix_edr_run_privileged_container_via_docker_api	
<b>Заголовок</b>	Запуск привилегированного контейнера внутри контейнера через docker api
<b>Номер</b>	
<b>Версия</b>	
<b>Дата последнего изменения</b>	
<b>Критичность</b>	Medium

nix_edr_use_shell_tool_to_access_kubeapi_inside_container	
<b>Заголовок</b>	Использование стандартных утилит для доступа к KubeAPI внутри контейнера
<b>Критичность</b>	Medium
<b>Достоверность</b>	High
<b>MITRE ATT&amp;CK</b>	<b>discovery:</b> T1613: Container and Resource Discovery



Инвентаризация контейнеров, обнаруженных на хосте



Мониторинг активности внутри контейнеров:

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

## Поддерживаемые движки:



DaemonSet\*



> Информация о событии

Начните вводить название

Командная строка cmdline	mysqldump -u root -p wordpress
ID контейнера container_id	a6dff0ca47bc6a11e7e26b86d0cdca280e8c3e6e12b87194a570fc4b839f8e87
ID образа контейнера container_img_id	sha256:5107333e08a87b836d48ff7528b1e84b9c86781cc9f1748bbc1b8c42a870d933
Имя образа контейнера container_img_name	mysql:5.7
Метаданные контейнера container_labels	com.docker.compose.config-hash=680603d59355140b3d655c1e6a3c48bf862a90234e029332b707c43d2a70ae4a com.docker.compose.container-number=1 com.docker.compose.depends_on=com.docker.compose.image=sha256:5107333e08a87b836d48ff7528b1e84b9c86781cc9f1748bbc1b8c42a870d933 com.docker.compose.oneoff=False com.docker.compose.project.config_files=/var/www/docker-compose.yml com.docker.compose.project.working_dir=/var/www com.docker.compose.project=www com.docker.compose.service=db com.docker.compose.version=2.27.0
Имя контейнера container_name	www-db-1
Runtime контейнера container_runtime	docker
Время старта контейнера container_start_time	2024-05-15 22:58:52
FQDN источника события dev_fqdn	linux.demo.local

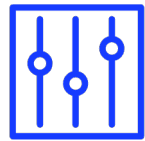
Обогащение события  
КОНТЕКСТОМ

Обнаружение

# Обнаружение Linux



Различные технологии обнаружения: IoA, YARA, IoC



Пользовательские правила и исключения

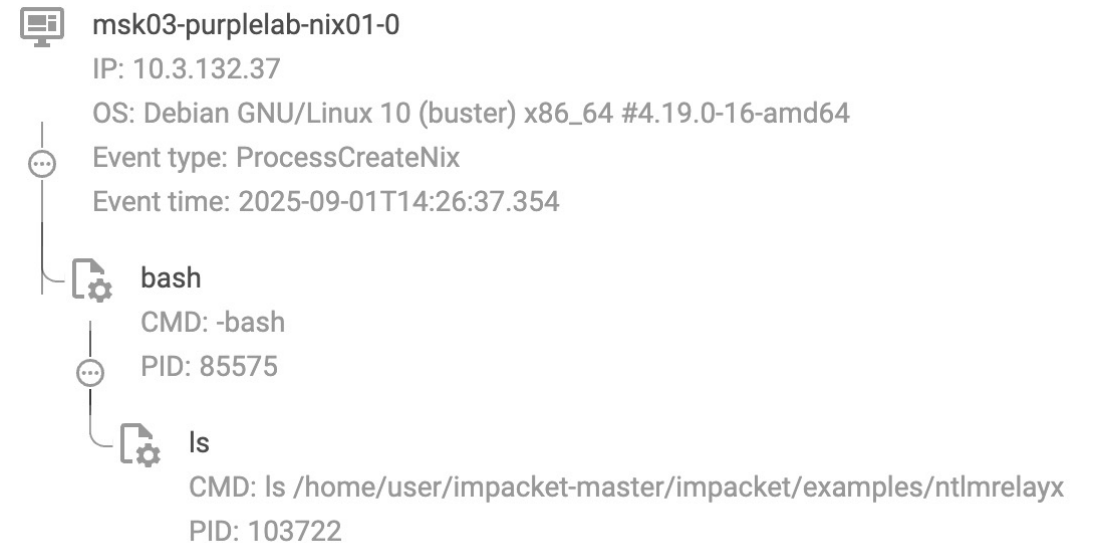


Deception-приманки

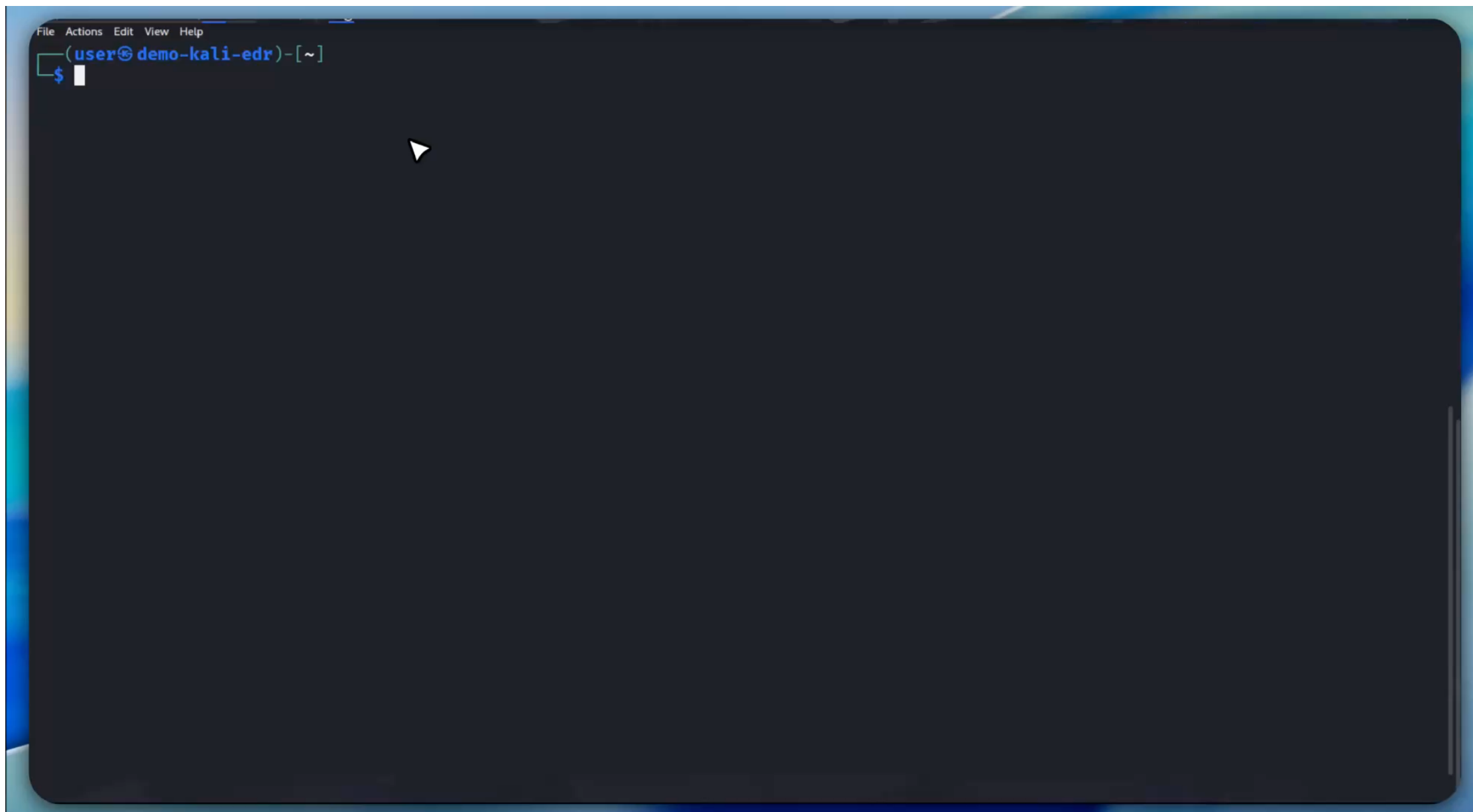


Самозащита

## nix\_edr\_usage\_impacket\_tool\_in\_cmdline



# Обнаружение Linux



# Прозрачность политики обнаружения угроз

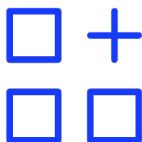
BI.ZONE



Список экспертных правил



Подробное описание правил



Упрощение адаптации под инфраструктуру



Минимизация ошибок

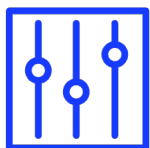
The screenshot displays the BI.ZONE EDR management console. At the top, there are navigation tabs for 'Агенты', 'Задачи', and 'Триггеры'. The main area shows a list of rules under the heading 'Правила выявления угроз'. Rule 335100 is selected, and its details are shown on the right. The details include the rule name, technical name, importance level (Medium), and trust level (High). Below the details, there is a 'Конструктор исключений' (Exclusion Builder) section, which allows users to define exclusion conditions for the rule. The interface is clean and modern, with a dark theme and clear typography.



Различные источники идей:  
CIS, NSA, ФСТЭК



Разработка на основе  
экспертного опыта



Пользовательские  
правила и исключения



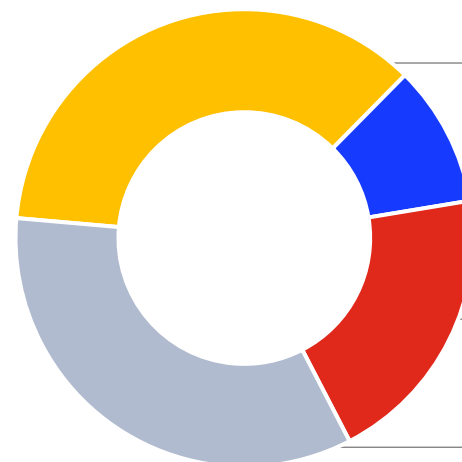
Офлайн-детектирование  
без общения с сервером

## 2 из 3

корп. компьютеров  
содержат хотя бы одну  
мiskonfigurацию\*

## 1 из 50

корпоративных локальных  
пользователей использует  
слабый пароль\*



Medium **36 %**

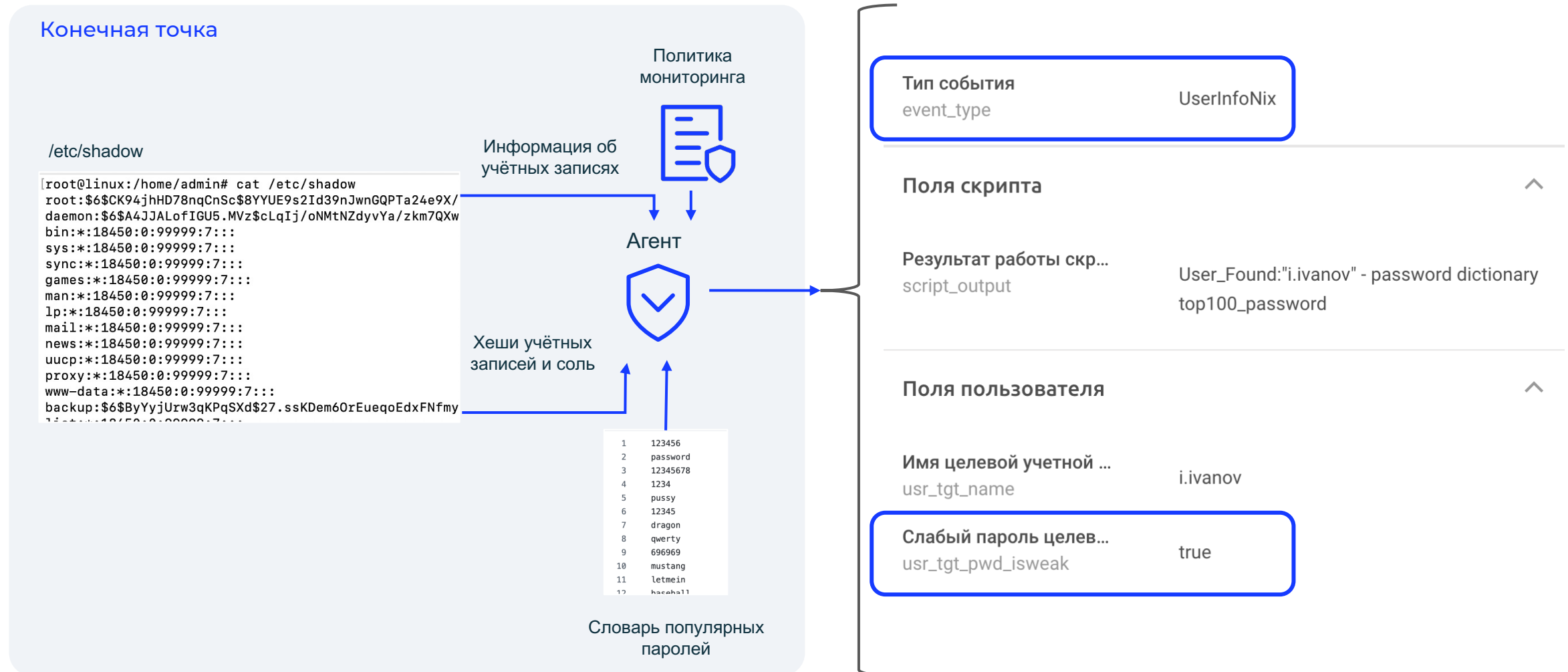
Только Low **10 %**

High **20 %**

Не обнаружено **34 %**

Распределение хостов по критичности  
выявленных мiskonfigurаций

# Слабые пароли



# Популярные мисконфиги\*

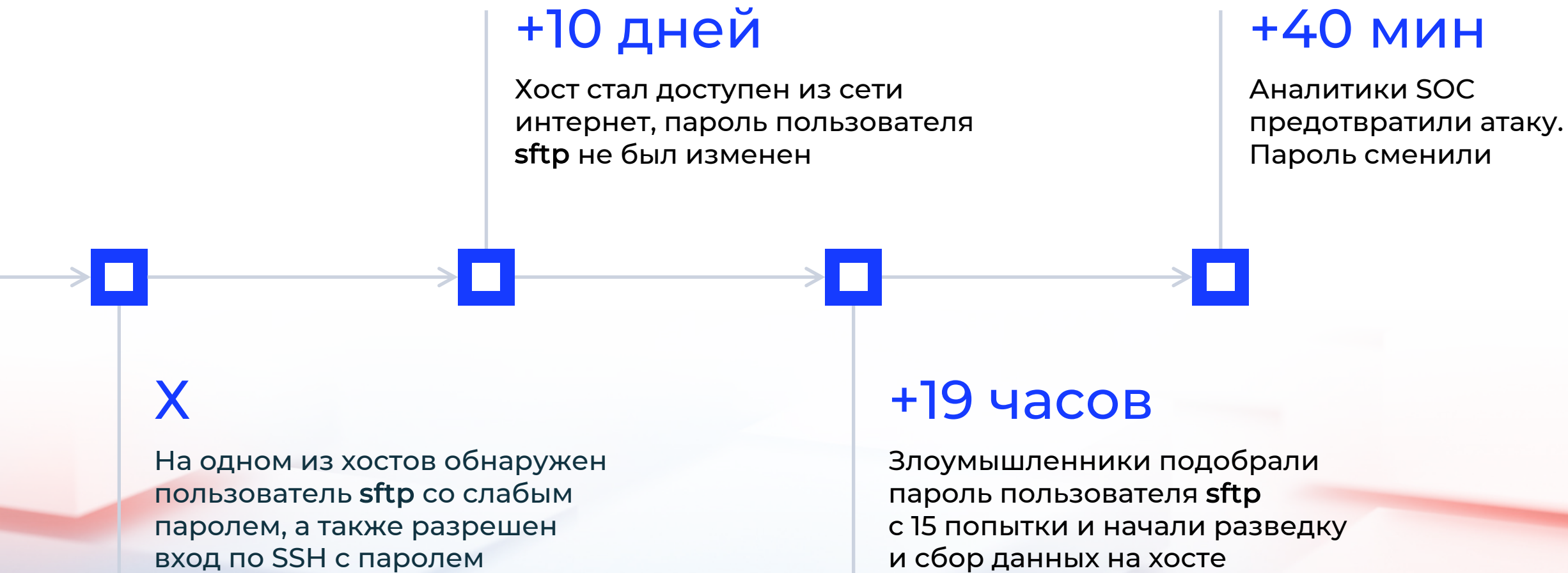
BI.ZONE



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

# Случай из практики

BI.ZONE

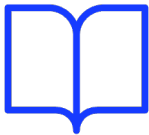


# Реагирование

# Реагирование



Автоматическое (онлайн/офлайн)  
и ручное реагирование



Библиотека готовых сценариев  
расследования и реагирования



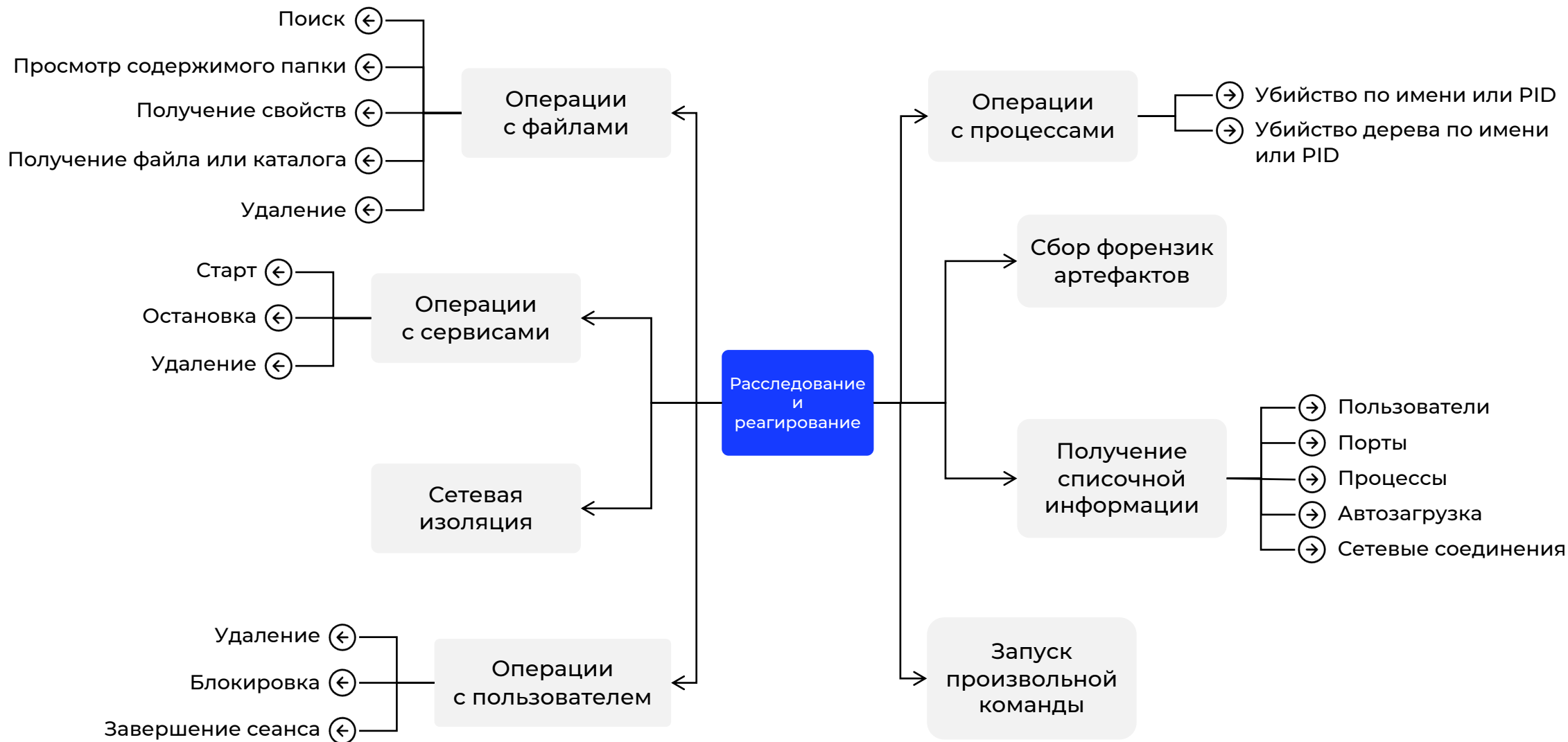
Live-консоль  
из веб-интерфейса



Сетевая изоляция

The screenshot displays the BI.ZONE EDR web interface. The top navigation bar includes 'Агенты', 'Задачи', 'Триггеры', 'События', and 'Обнаружения'. The main content area shows details for an agent named 'admins-Mac-mini'. Key information includes: 'Статус авторизации' (Authorized), 'Самозащита' (Self-protection: Disabled), 'Версия' (Version: 2), 'IP-адрес' (10.1.135.2), 'Последний пользователь' (admin), and 'Логи' (Logs). A 'Консоль' (Console) tab is active, showing a terminal output for 'system\_profiler SPSoftwareDataType Software'. The output includes system details like 'System Version: macOS 14.2 (23C64)', 'Kernel Version: Darwin 23.2.0', and 'User Name: System Administrator (root)'. A dropdown menu is open, showing options for 'Модуль' (File grabber), 'Инструмент' (Delete files/folder), and 'Параметры задачи' (Task parameters) with a 'Показать' (Show) link.

# Реагирования через сервер EDR



# Автоматическое реагирование

BI.ZONE

BI.ZONE EDR

Агенты | Задачи | Триггеры | События | Обнаружения

99+

### Агент

ubuntu2204.localdomain

Онлайн  
Последнее подключение: 10.10.2025, 12:39

Ubuntu 22.04.3 LTS (Jammy Jellyfish)  
Ядро: 5.15.0-91-generic  
Архитектура: x64

IP-адрес  
10.0.2.15

Последний пользователь  
[vagrant](#) 10.10.2025, 12:35

Логи [Обновить](#)  
Не обновлялись

Комментарий  
[+ ДОБАВИТЬ КОММЕНТАРИЙ](#)

Статус авторизации  
 Авторизован  
09.10.2025, 16:01

Самозащита  
 Недоступна  
09.10.2025, 16:01 system

Версия  
 2.21.0 [Обновить](#)  
Обновлен: 09.10.2025, 16:01

Ресурсы | Модули | **Задачи 1** | Политики | Группы | Конфигурация | Консоль (Live)

### Задачи

[НАЗНАЧИТЬ ЗАДАЧИ](#)

Статус	Название	Запуски \ Результаты	Режим запуска	Источник данных	Способ назначения
<input checked="" type="checkbox"/>	<a href="#">[EDR][Nix][PROD] Apply config</a>	<a href="#">Просмотр</a> 15 10.10.2025, 12:39	Постоянный	<a href="#">Показать 4</a>	Напрямую

# 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 TTP атакующих

## 🔍 Мониторинг (сбор телеметрии)

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

T1110.001

T1562.001

T1078.002

T1087.002

T1078.003

T1069.002

EDR

### Телеметрия

Передача собранных событий

### Обнаружение

Передача обнаружений по внутренним правилам

### Реагирование

Возможность запуска команд по расследованию и реагированию

## ⚡ 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

## 🔗 Интеграции с внешними СЗИ

## 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)

Ключевые преимущества VI.ZONE EDR в сравнении с другими EDR

## 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



Реестр  
отечественного ПО



Сертификат ОАЦ при Президенте  
Республики Беларусь



Сертификаты ФСТЭК:

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



Сертификаты совместимости  
с российским ОС:

- Astra Linux
- ALT Linux
- «РЕД ОС»



Совместимость с популярными  
СABЗ и DLP-решениями

# 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

VI.ZONE

[Изучить исследование на сайте](#)



Спасибо!  
Вопросы?



[BI.ZONE в telegram](#)



[Узнать больше о BI.ZONE EDR](#)