Константин Рудаков

Руководитель направления
по развитию продуктов для защиты
от целевых атак

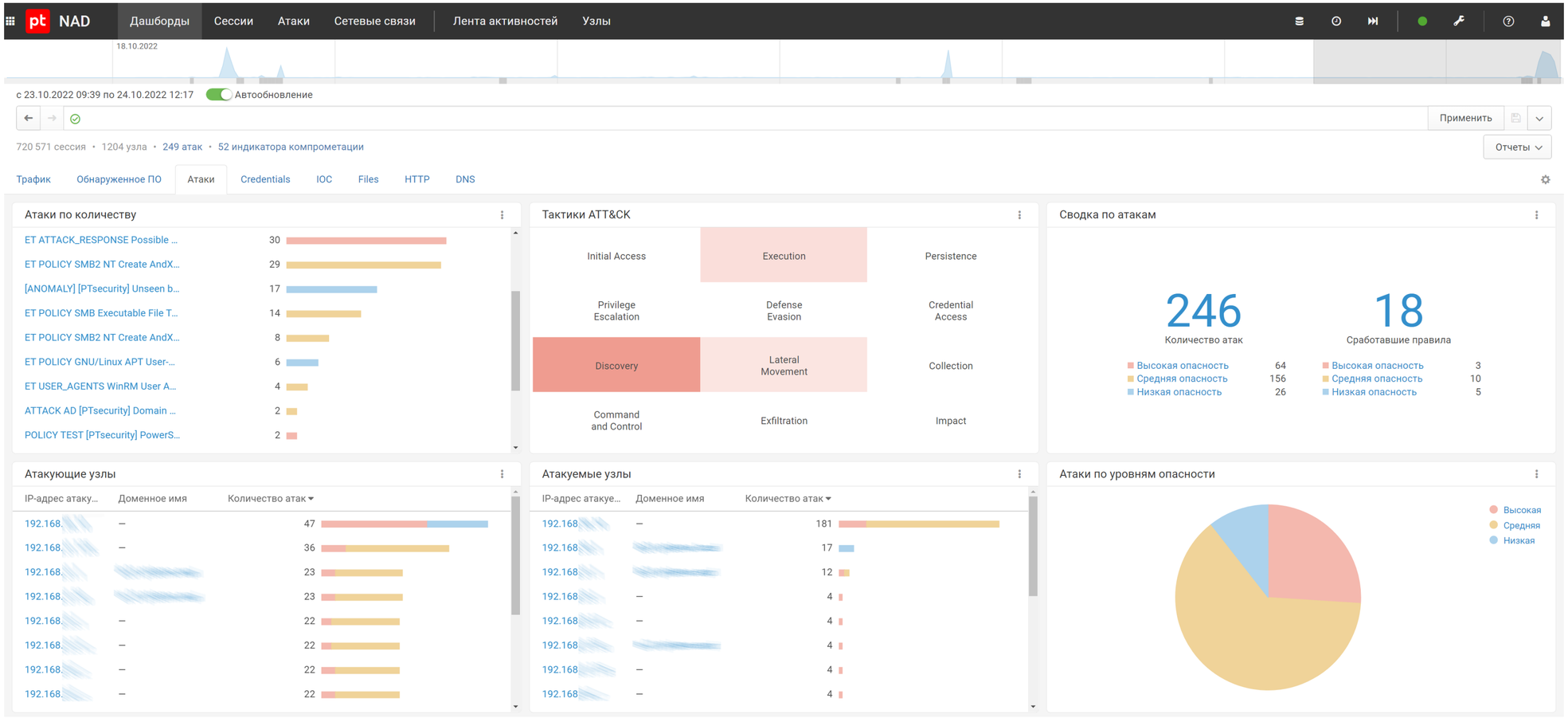
Владимир Клепче

Архитектор продуктов
для информационной безопасности

PT Network Attack Discovery 11.1

PT Network Attack Discovery

Система поведенческого анализа сетевого трафика
для выявления атак на периметре и внутри сети



Дашборды
PT NAD

PT NAD

Выявляет целевые атаки
на периметре и внутри сети

Обнаруживает
скрытые угрозы

Проверяет сетевую
активность узлов

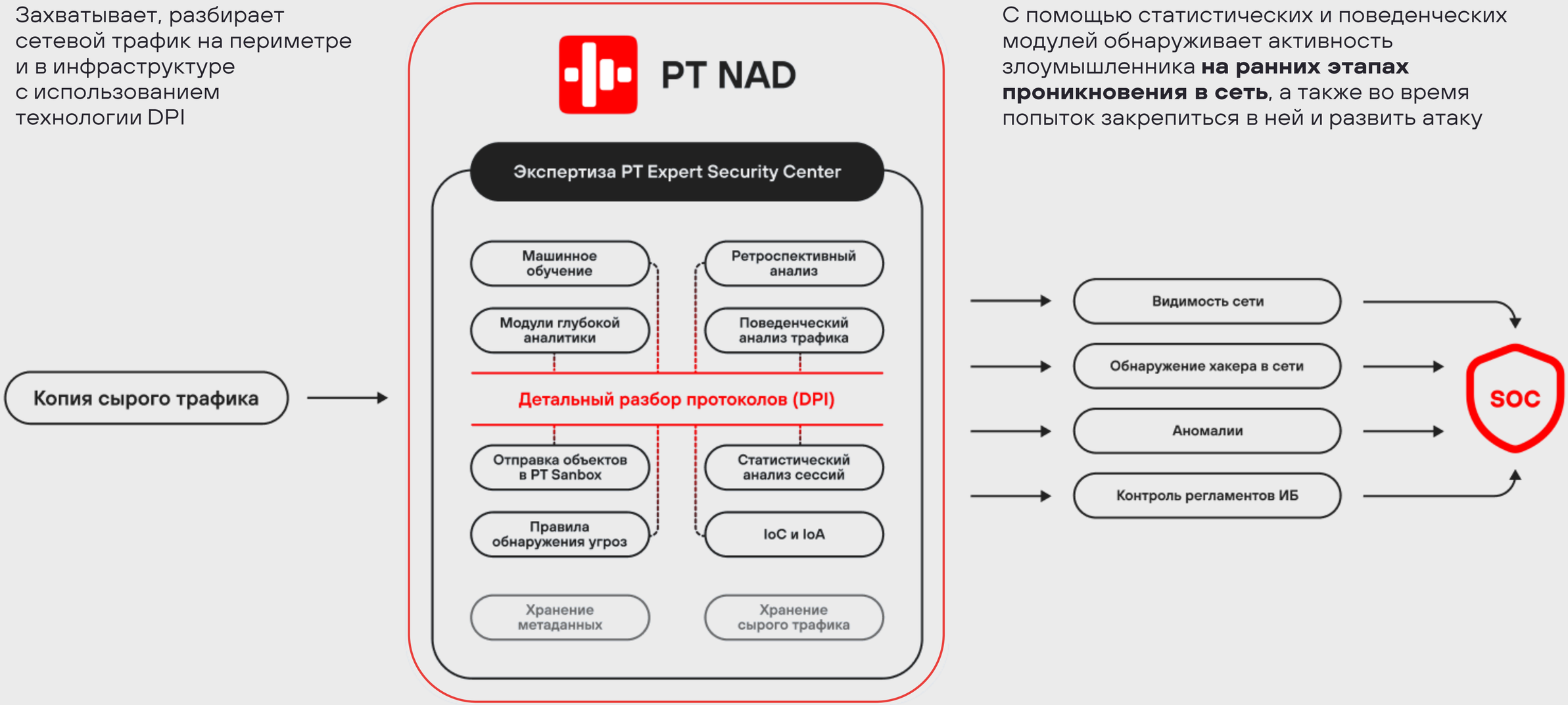
Результат

Сокращает время
присутствия
злоумышленника
в сети
**до считанных
минут**

Как работает PT NAD

Захватывает, разбирает сетевой трафик на периметре и в инфраструктуре с использованием технологии DPI

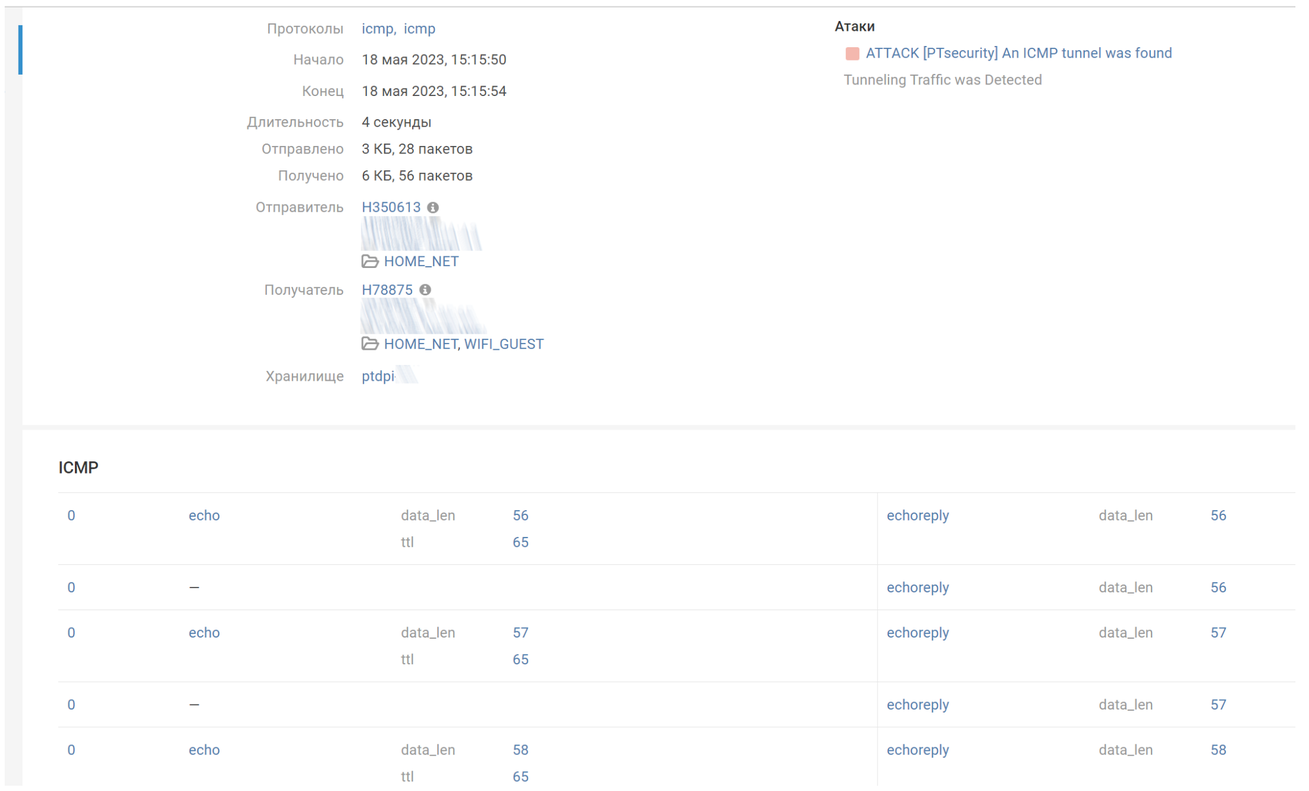
С помощью статистических и поведенческих модулей обнаруживает активность злоумышленника **на ранних этапах проникновения в сеть**, а также во время попыток закрепиться в ней и развить атаку



PT NAD 11.1. Новые способы обнаружения атак

PT NAD 11.1. Новые способы обнаружения атак

Обнаружение ICMP-туннелей



Протоколы	icmp, icmp
Начало	18 мая 2023, 15:15:50
Конец	18 мая 2023, 15:15:54
Длительность	4 секунды
Отправлено	3 КБ, 28 пакетов
Получено	6 КБ, 56 пакетов
Отправитель	H350613 [redacted] HOME_NET
Получатель	H78875 [redacted] HOME_NET, WIFI_GUEST
Хранилище	ptdpi

Атаки

ATTACK [PTsecurity] An ICMP tunnel was found

Tunneling Traffic was Detected

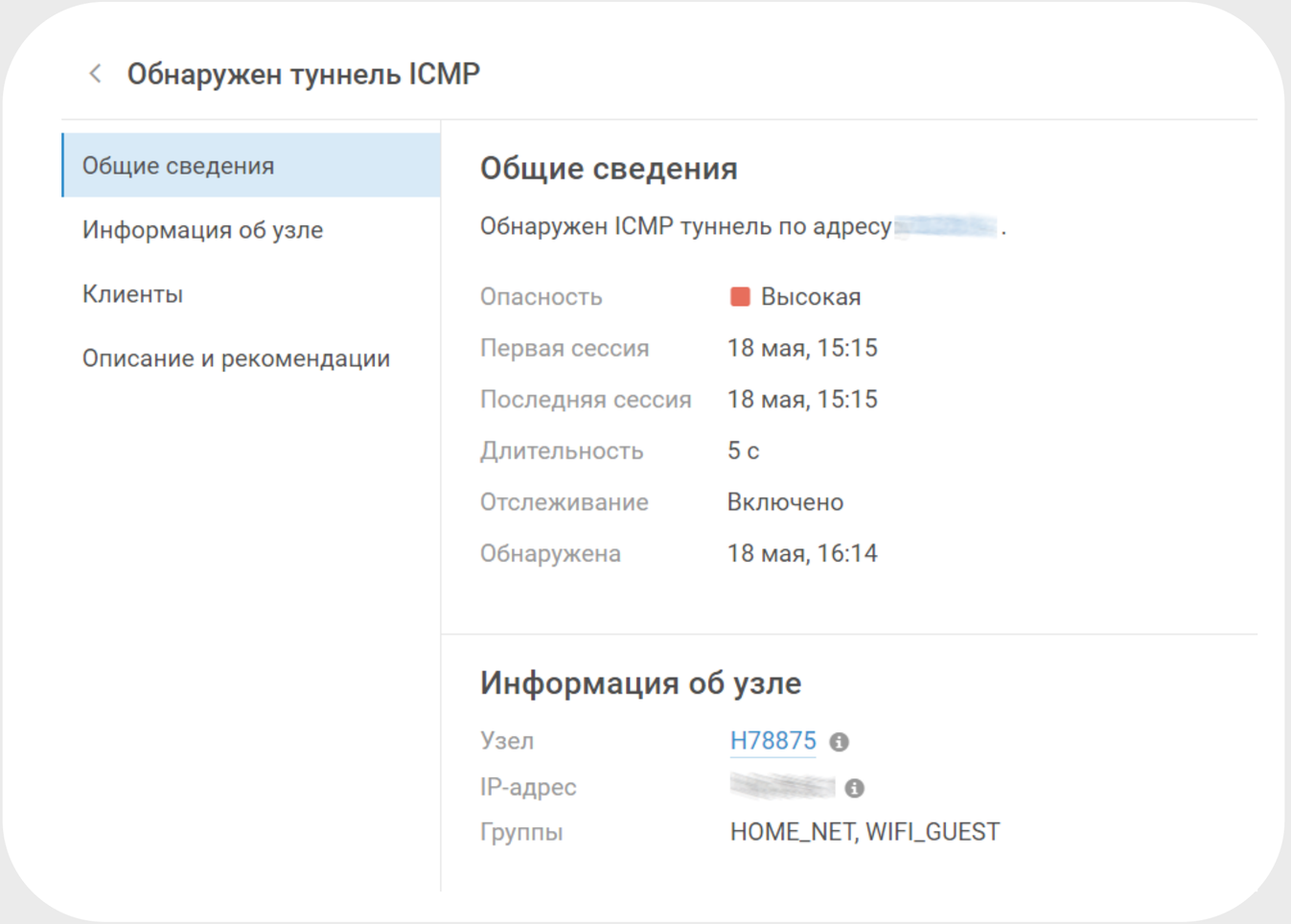
ICMP

0	echo	data_len ttl	56 65		echoreply	data_len	56
0	–				echoreply	data_len	56
0	echo	data_len ttl	57 65		echoreply	data_len	57
0	–				echoreply	data_len	57
0	echo	data_len ttl	58 65		echoreply	data_len	58

PT NAD 11.1. Новые способы обнаружения атак

PT NAD обнаруживает установление ICMP-туннелей по накопленным статистическим данным пакетов ICMP

Модуль позволяет выявлять любые хакерские инструменты



PT NAD 11.1. Новые способы обнаружения атак

PT NAD 11.1. Новые способы обнаружения атак

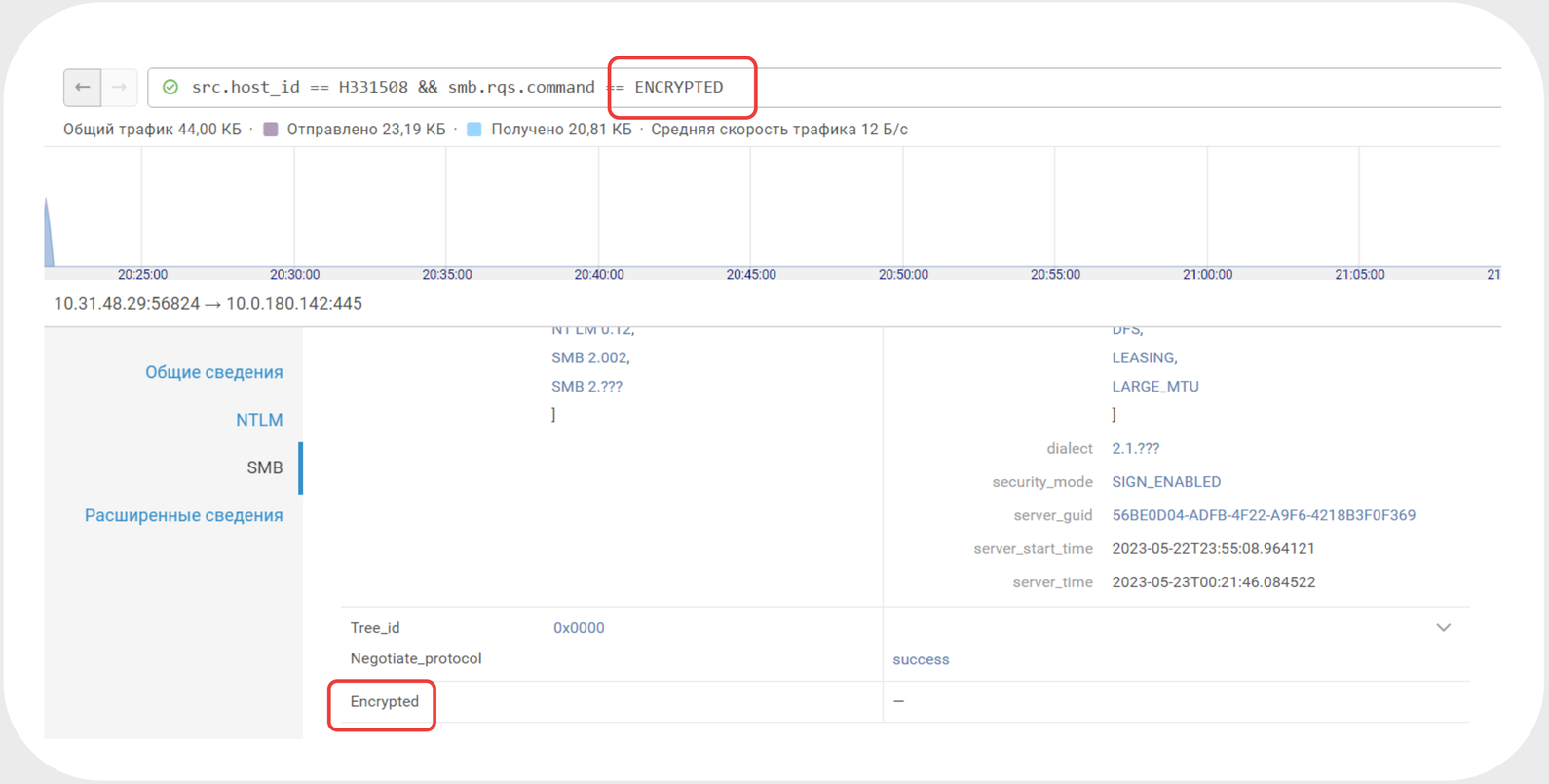
- Выявление зашифрованного SMB-трафика
- Обнаружение неизвестных пайпов SMB

Злоумышленники могут скрывать свою активность внутри шифрованных SMB-пакетов

Если узел неожиданно начнет использовать шифрованную версию протокола SMB, **PT NAD это выявит**

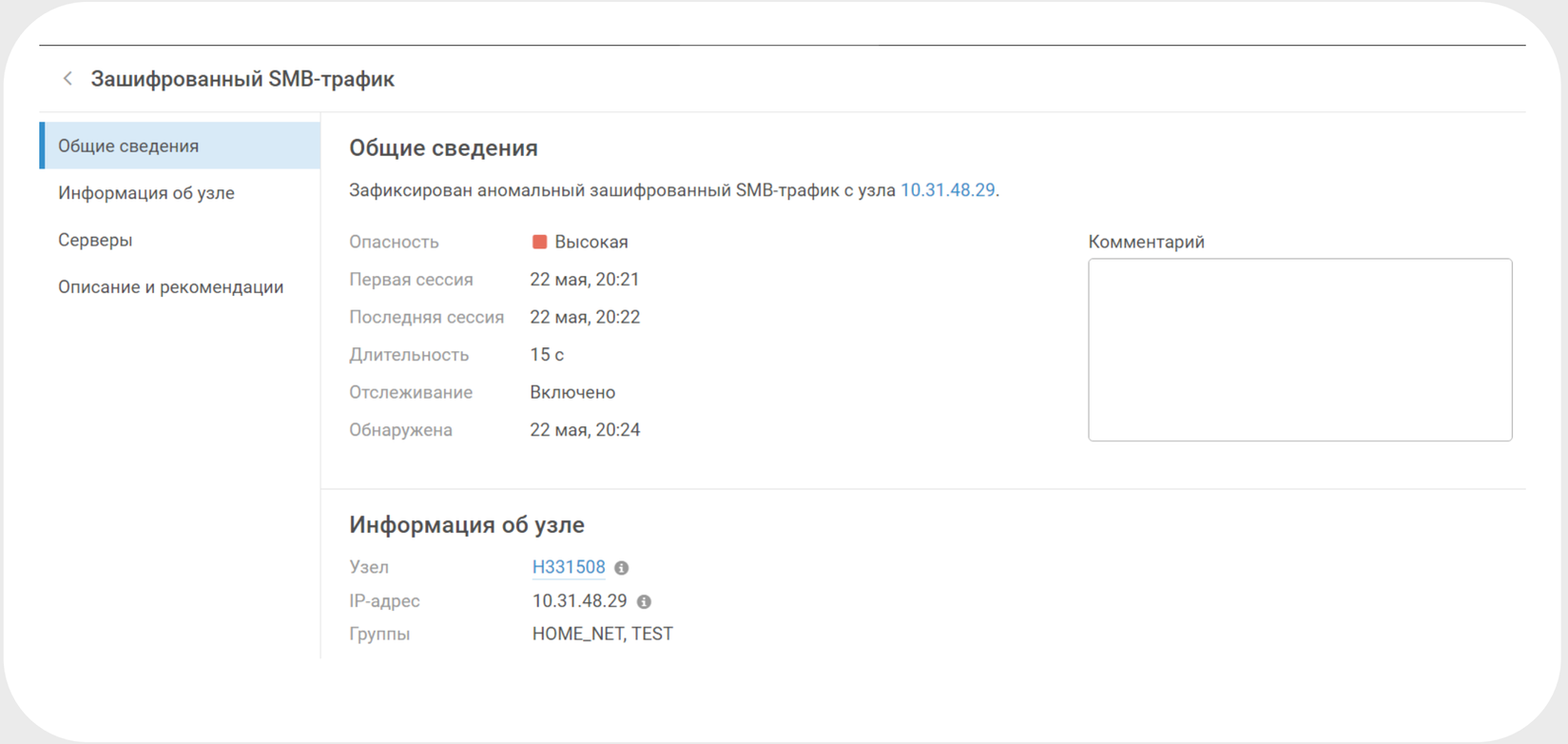
PT NAD 11.1. Новые способы обнаружения атак

Выявление зашифрованного SMB-трафика



PT NAD 11.1. Новые способы обнаружения атак

Выявление зашифрованного SMB-трафика



PT NAD 11.1. Новые способы обнаружения атак

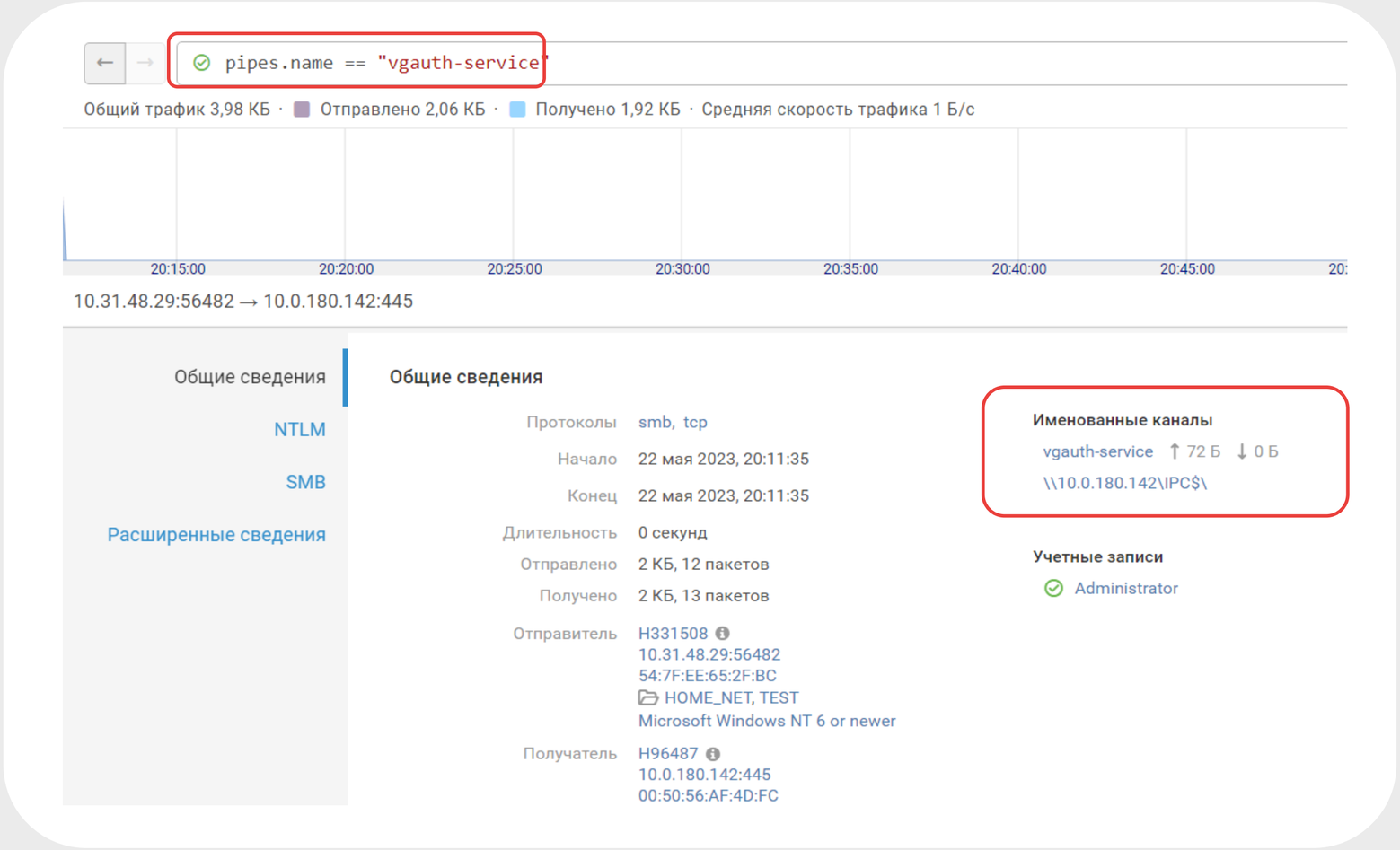
- Выявление зашифрованного SMB-трафика
- Обнаружение неизвестных пайпов SMB

Именованные каналы SMB (пайпы) могут использоваться инструментами атакующих и вредоносным ПО для коммуникации с агентами

PT NAD определяет новые пайпы SMB в сети

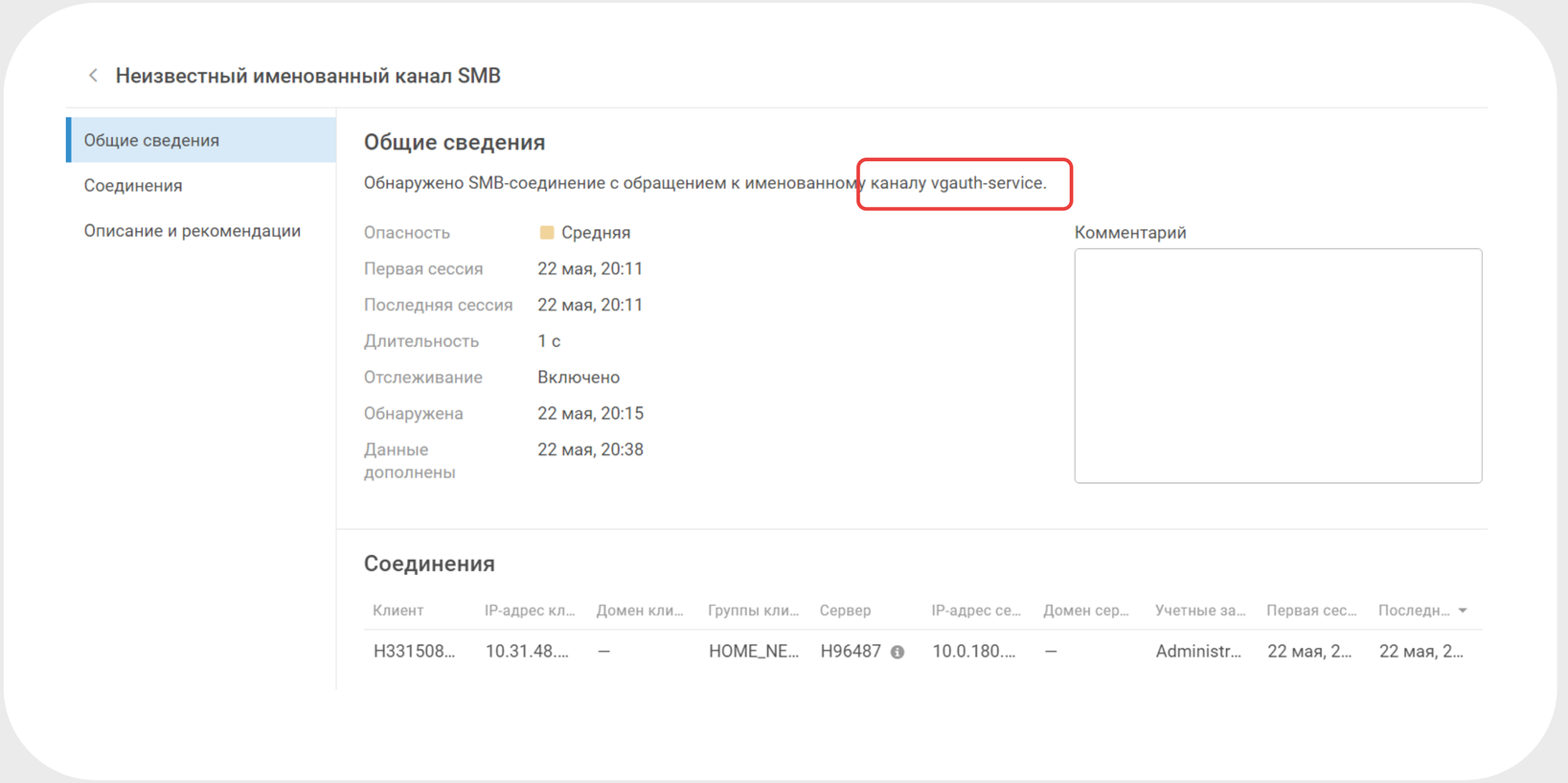
PT NAD 11.1. Новые способы обнаружения атак

Обнаружение неизвестных пайпов SMB



PT NAD 11.1. Новые способы обнаружения атак

Обнаружение неизвестных пайпов SMB



PT NAD 11.1. Новые способы обнаружения атак

PT NAD 11.1. Новые способы обнаружения атак

Обнаружение использования Cobalt Strike и Brute Ratel C4*

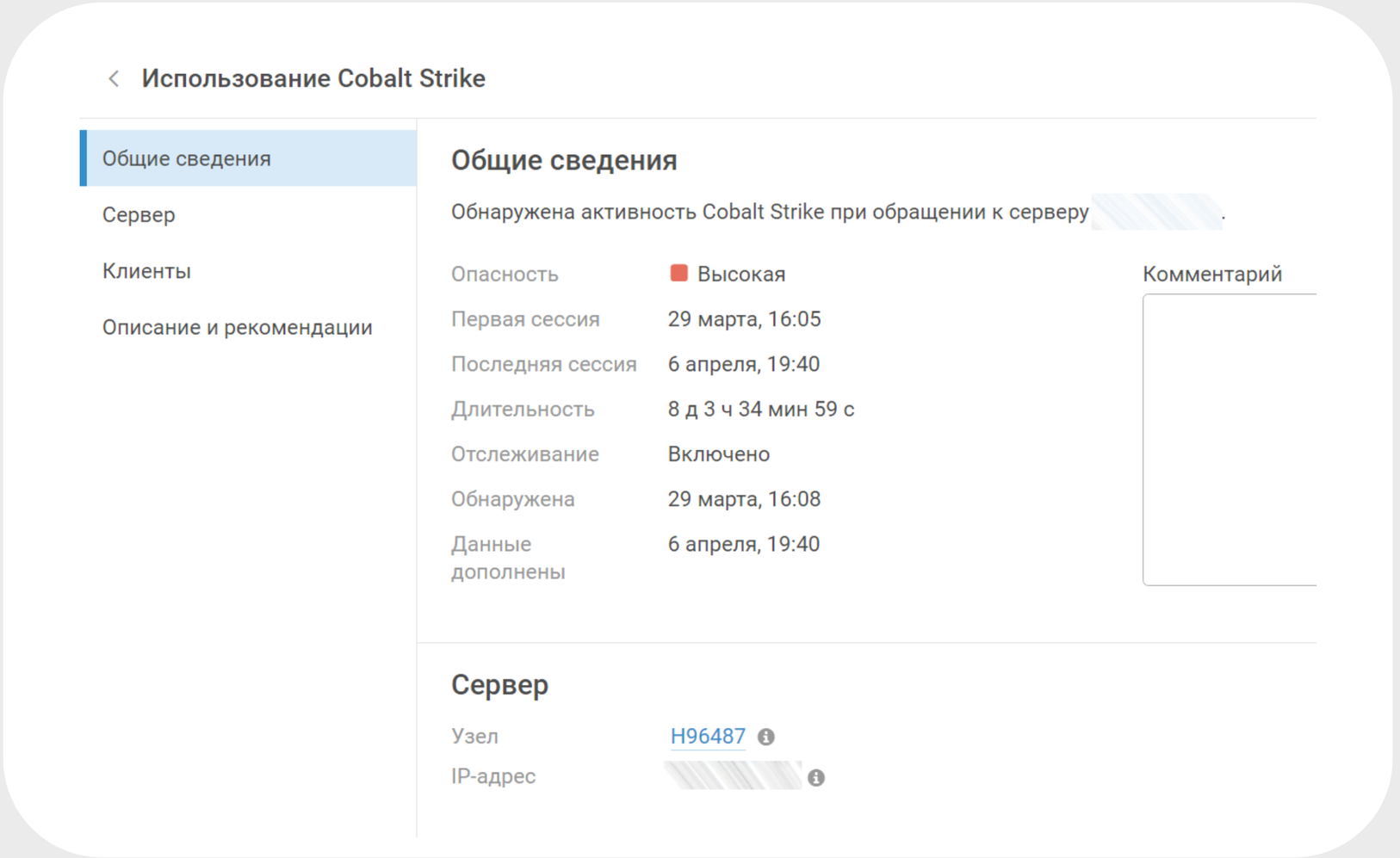
PT NAD обнаруживает маяки и агенты по периодическим HTTP-запросам к управляющему серверу (C2), которые используются для взаимодействия, получения команд и предоставления отчета о результатах их выполнения

* Cobalt Strike и Brute Ratel C4 — фреймворки для постэксплуатации зараженных систем

Ищем иголку вредоносных запросов в стоге трафика:
PT NAD vs. Cobalt Strike и Brute Ratel C4

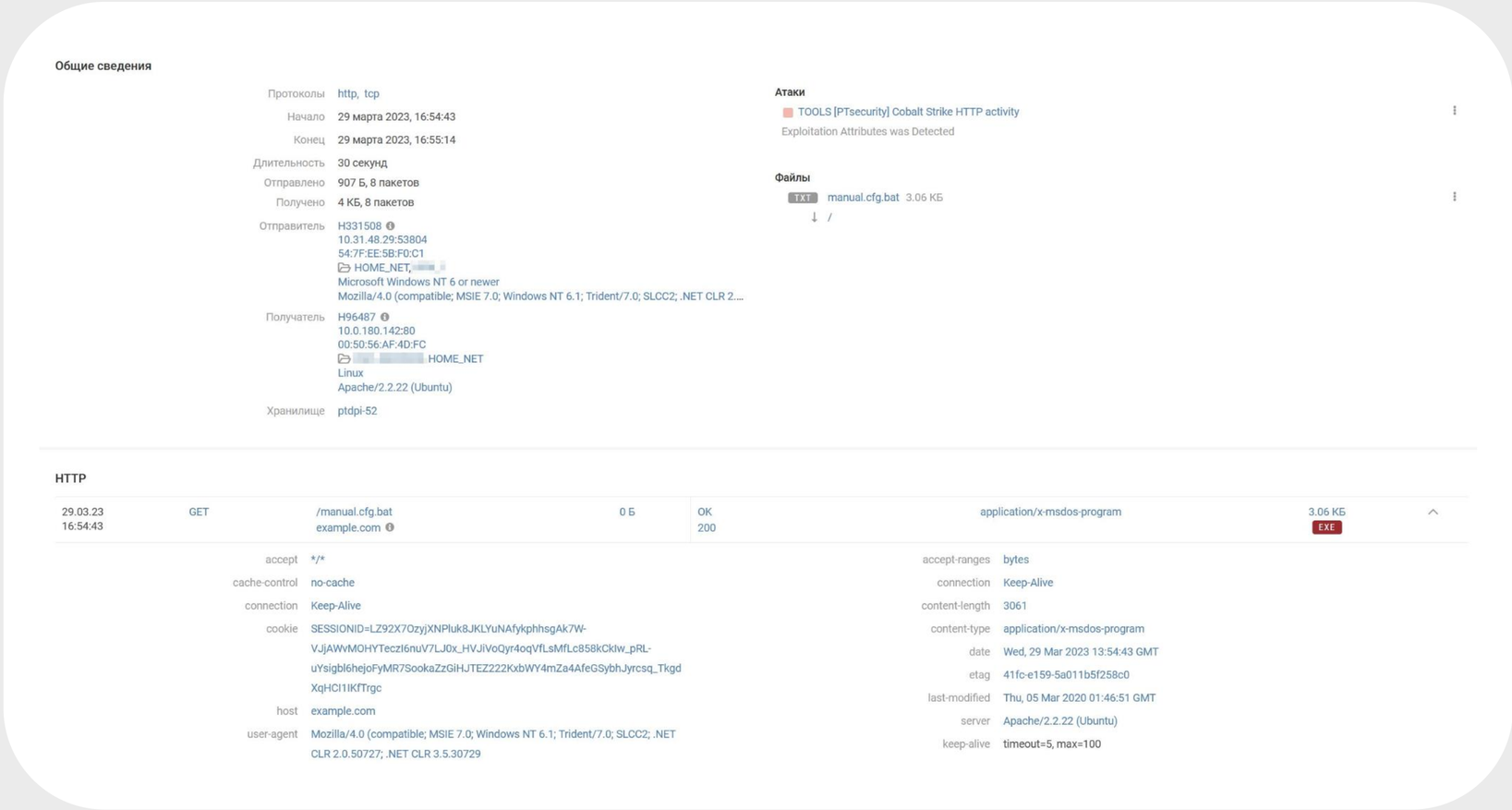
PT NAD 11.1. Новые способы обнаружения атак

Обнаружение использования Cobalt Strike и Brute Ratel C4



PT NAD 11.1. Новые способы обнаружения атак

Обнаружение использования Cobalt Strike и Brute Ratel C4

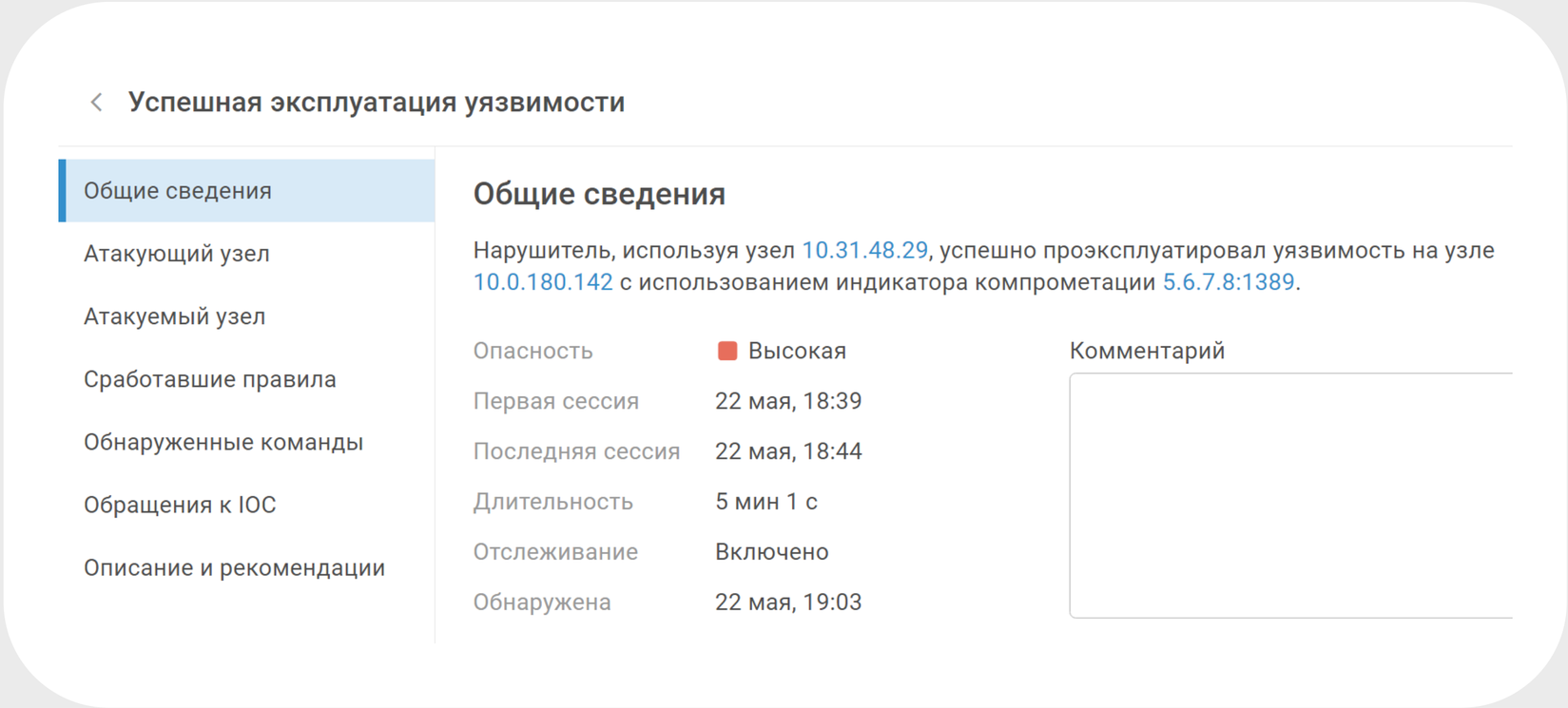


PT NAD 11.1. Новые способы обнаружения атак

PT NAD 11.1. Новые способы обнаружения атак

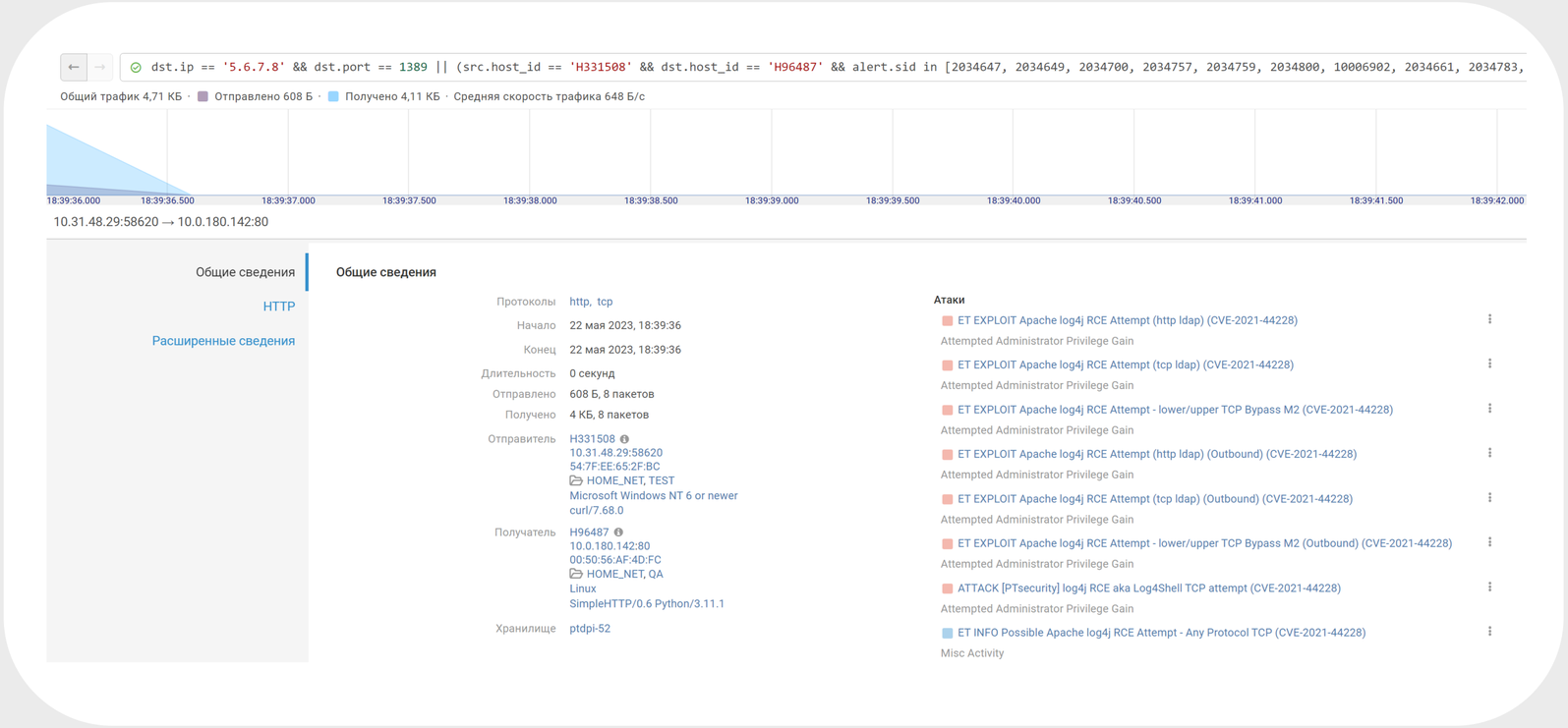
Обнаружение успешной эксплуатации уязвимостей

PT NAD автоматически извлекает индикаторы компрометации из сетевых запросов и проверяет факты обращения к ним



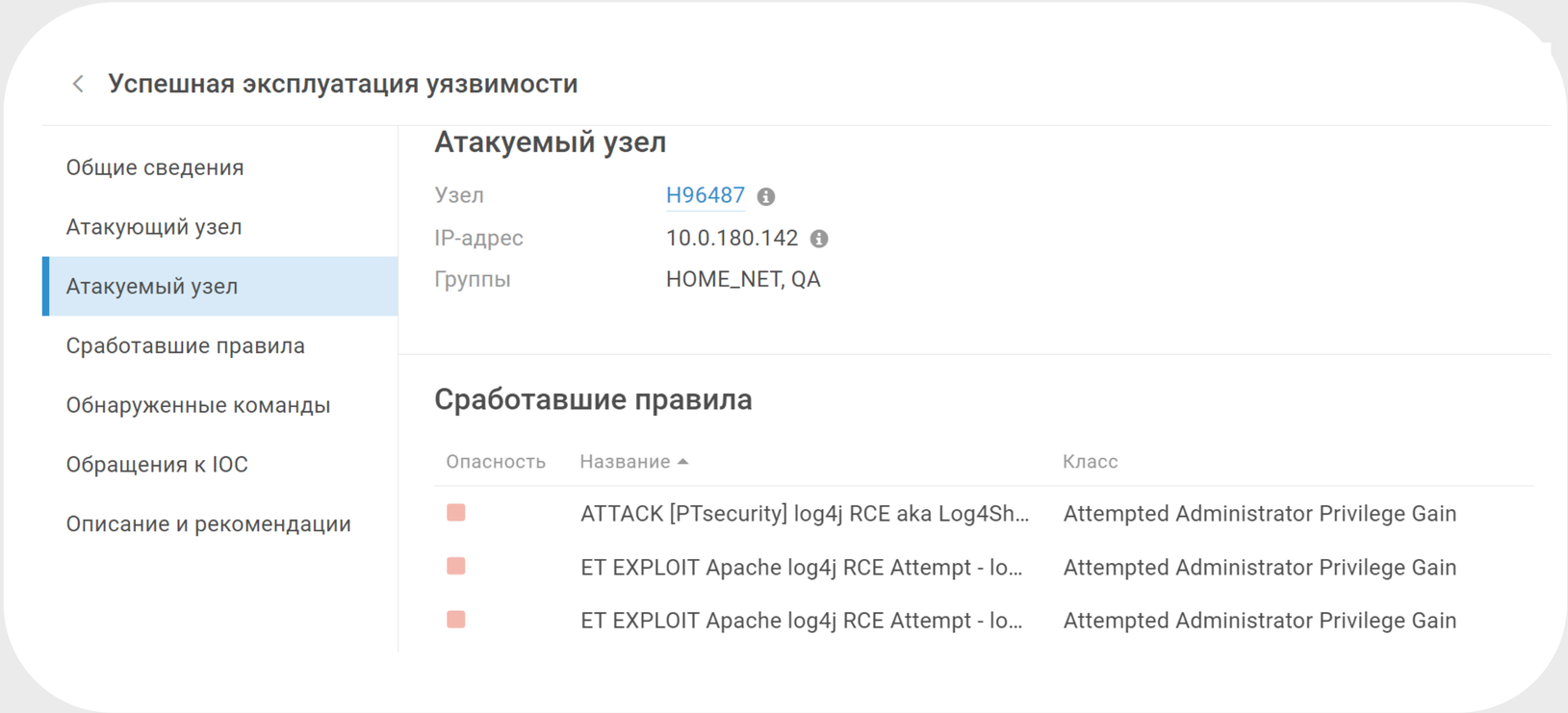
PT NAD 11.1. Новые способы обнаружения атак

Обнаружение успешной эксплуатации уязвимостей



PT NAD 11.1. Новые способы обнаружения атак

Обнаружение успешной эксплуатации уязвимостей

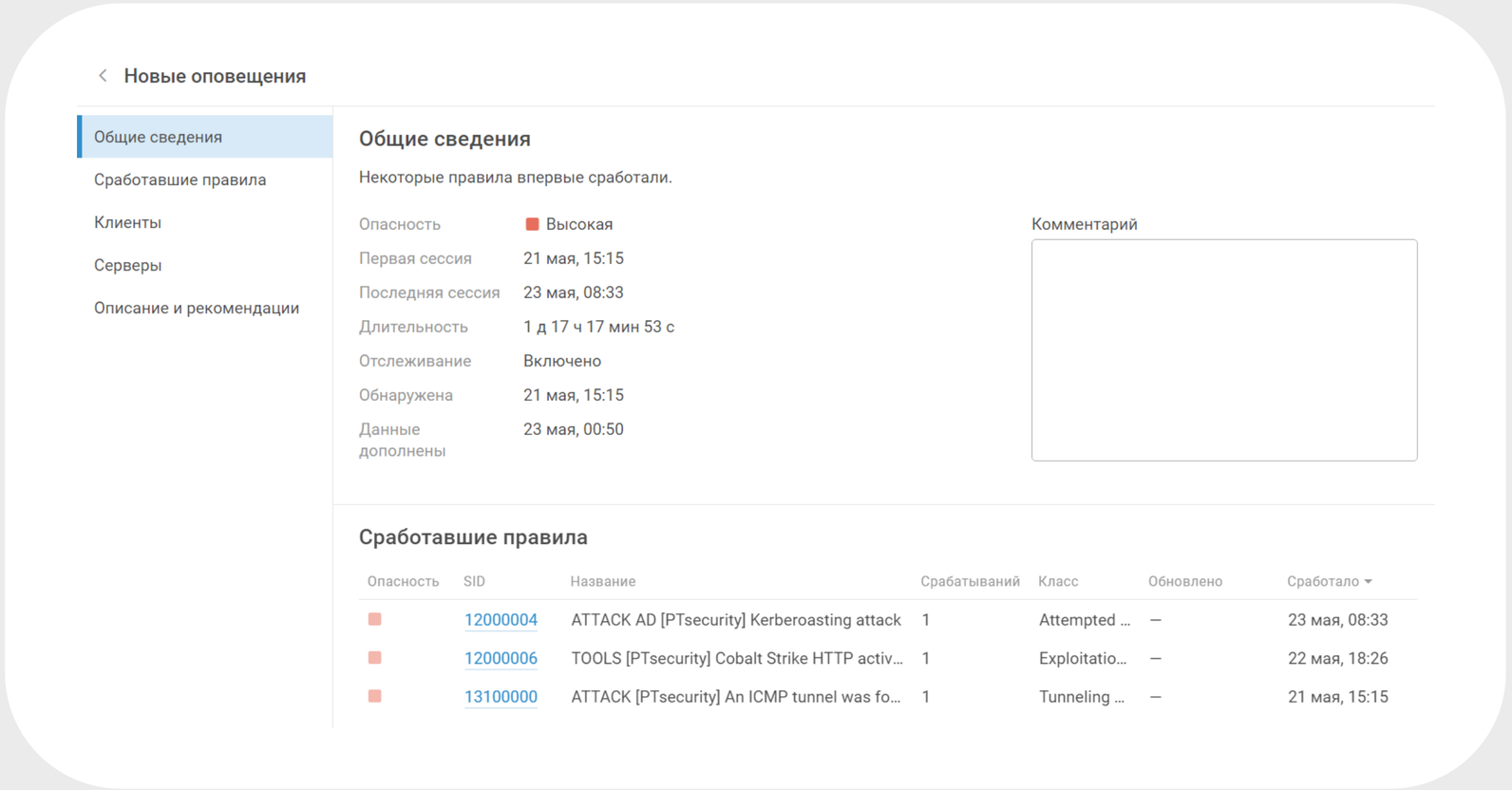


PT NAD 11.1. Новые способы обнаружения атак

PT NAD 11.1. Удобство

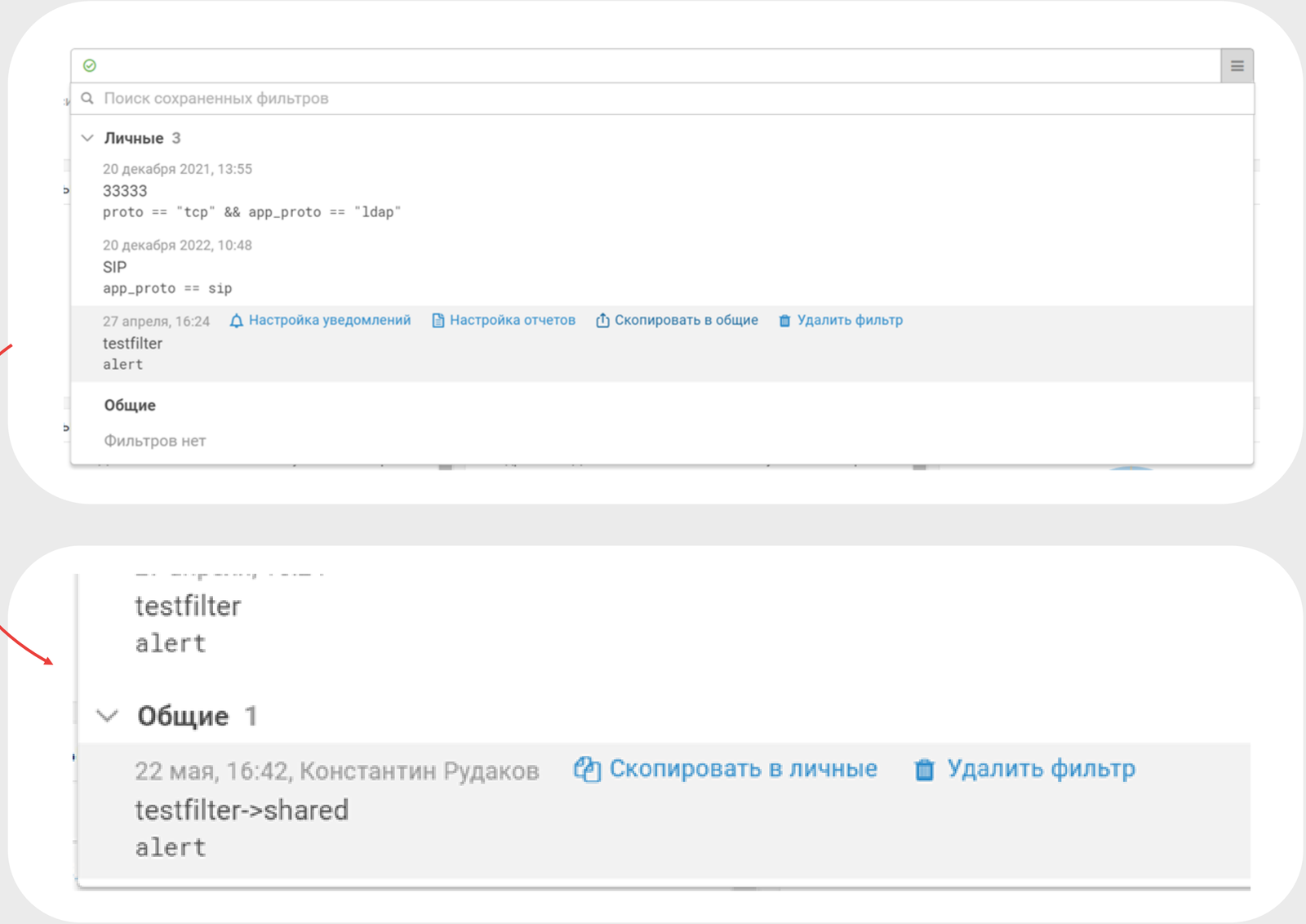
Оповещение о срабатывании потенциально важных новых правил

PT NAD подсвечивает срабатывания, которые не регистрировались до этого и могли остаться незамеченными



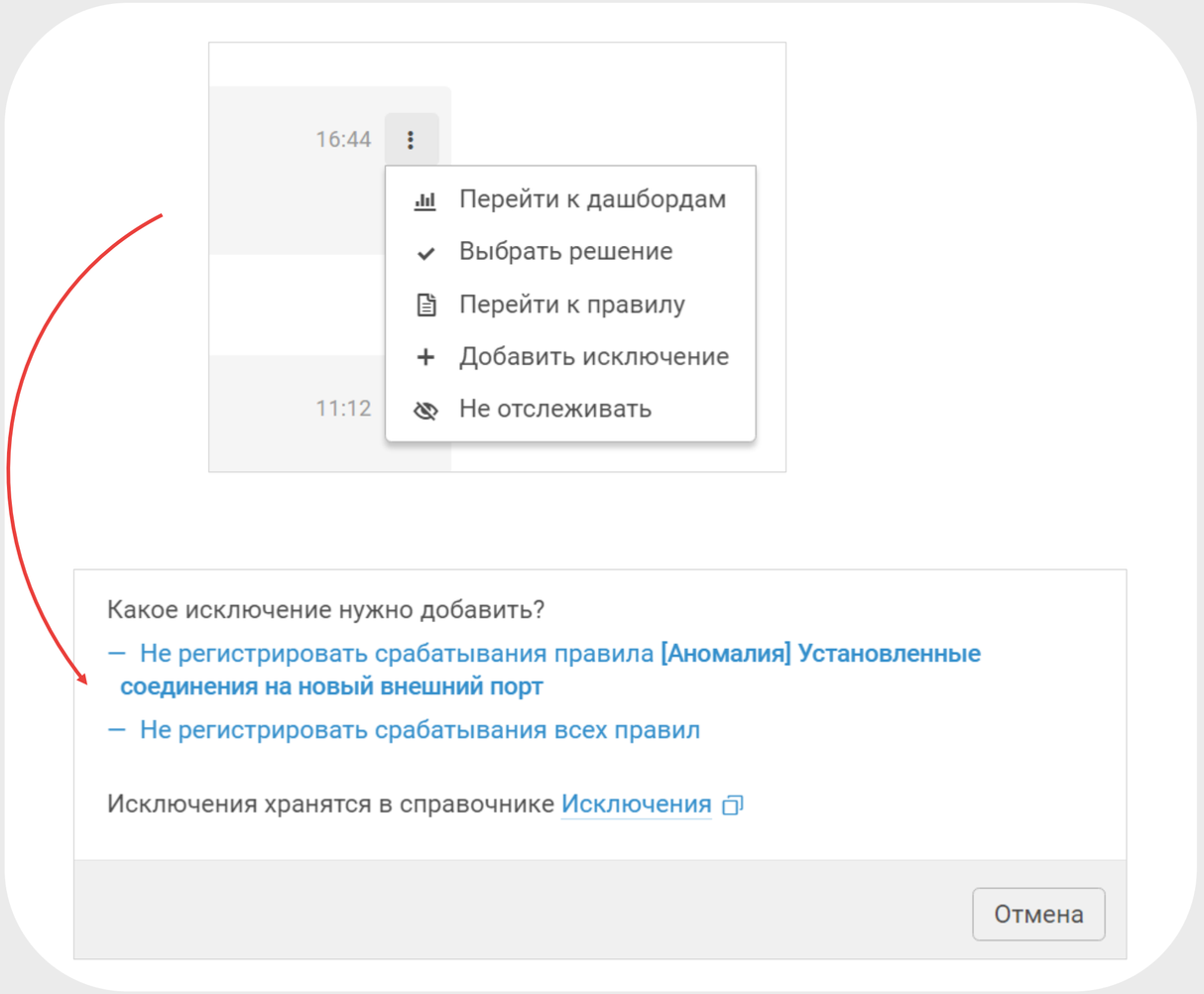
PT NAD 11.1. Фильтры

Добавление личных и общих фильтров



PT NAD 11.1. Управление исключениями

Управление исключениями из ленты активностей



PT NAD 11.1. Управление исключениями

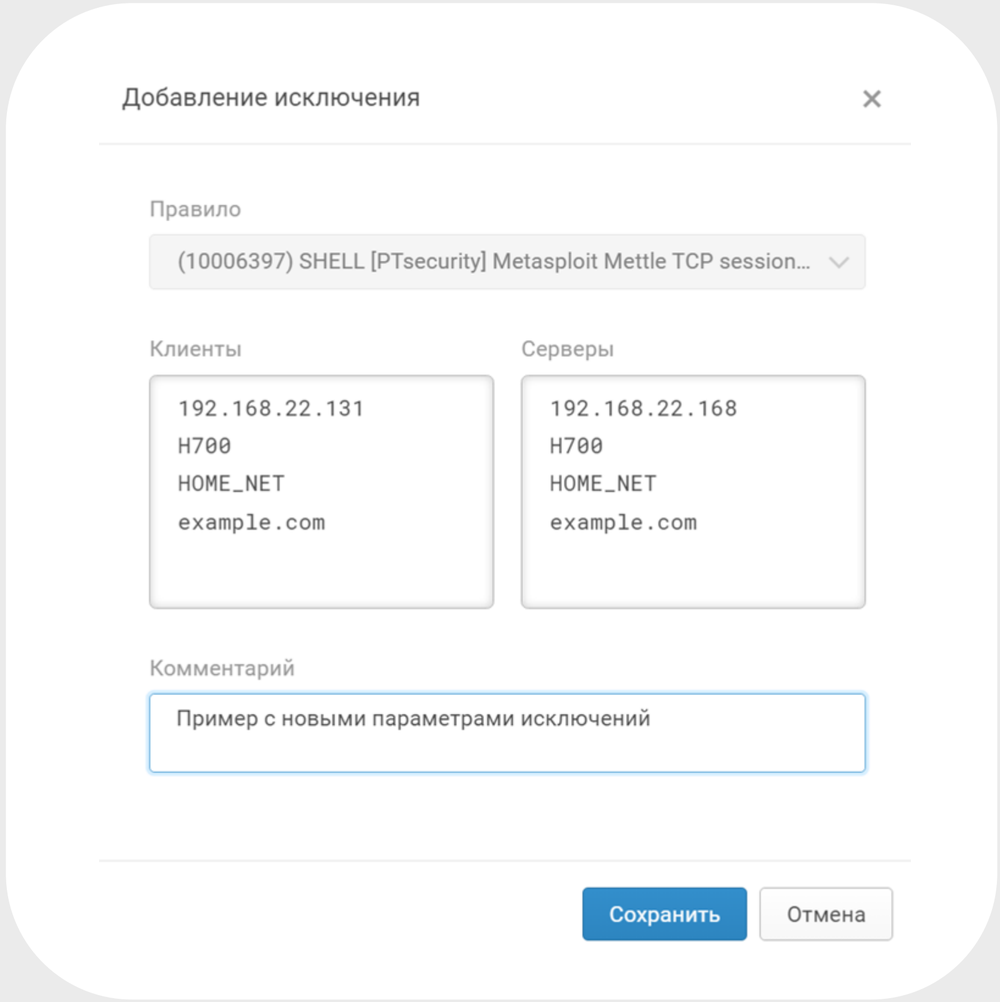
Расширение механизма исключений для атак

В PT NAD 11.1 появились новые параметры исключения для правил обнаружения атак:

— идентификаторы узлов

— группы узлов

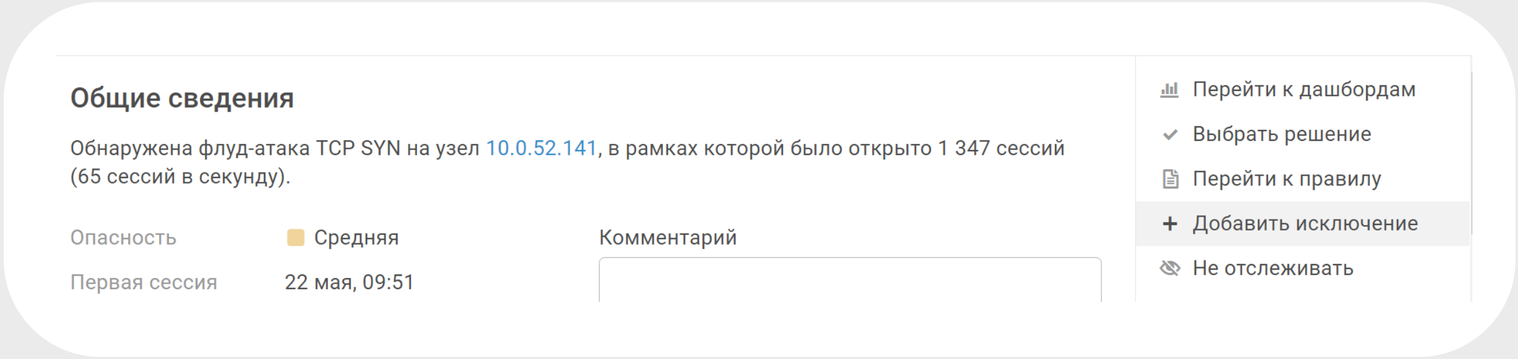
— доменные имена



PT NAD 11.1. Управление исключениями

Исключения для флуд-атак и сканирований

В PT NAD 11.1 можно добавить в исключения сетевой флуд и сканирование сети, которые определяются несигнатурными механизмами



PT NAD 11.1. Инженерные улучшения

Мастер настройки

Переход от механизма захвата трафика PF_RING к DPDK

Добавление инструмента для определения проблем с захватом и обработкой трафика

PT NAD 11.1. Конфигуратор

PT NAD 11

Инсталлятор

Устанавливает PT NAD

PT NAD 11.1

Конфигуратор

Настраивает базовые параметры PT NAD

PT NAD 11.1. Конфигуратор

Поддерживает

- Односерверную и многосерверную конфигурации
- PT NAD, установленный и обновленный через инсталлятор

PT NAD 11.1. Конфигуратор

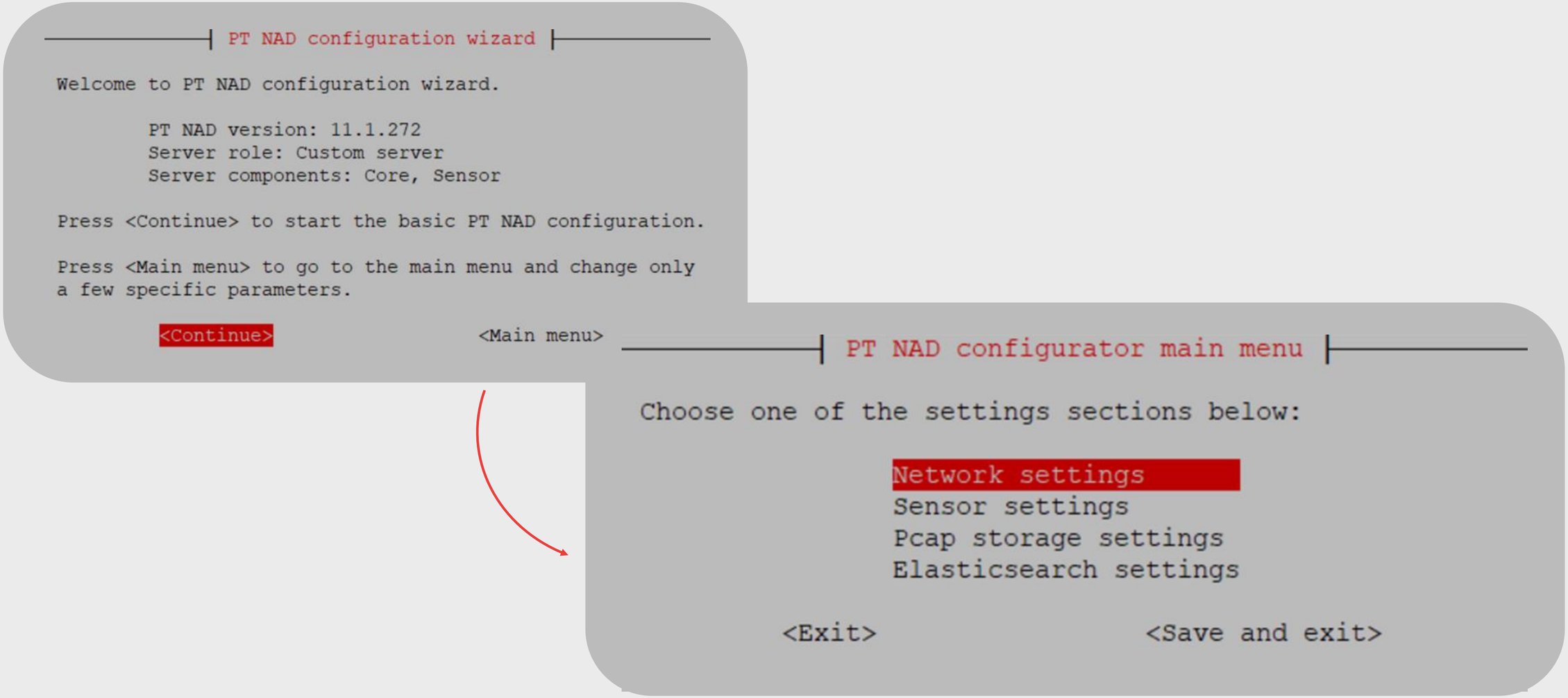
Настраивает

- GRUB
- Параметры захвата трафика
- Сроки хранения файлов PCAP и ES

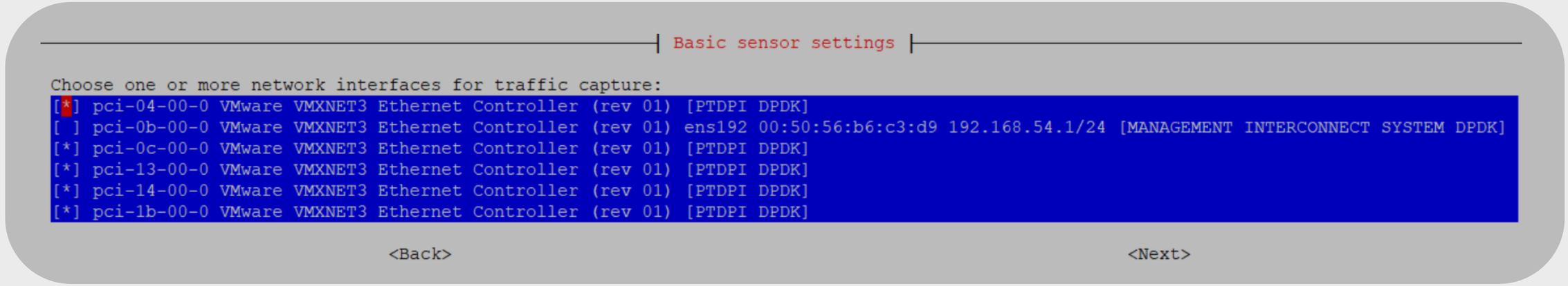
Сетевые интерфейсы (порты):

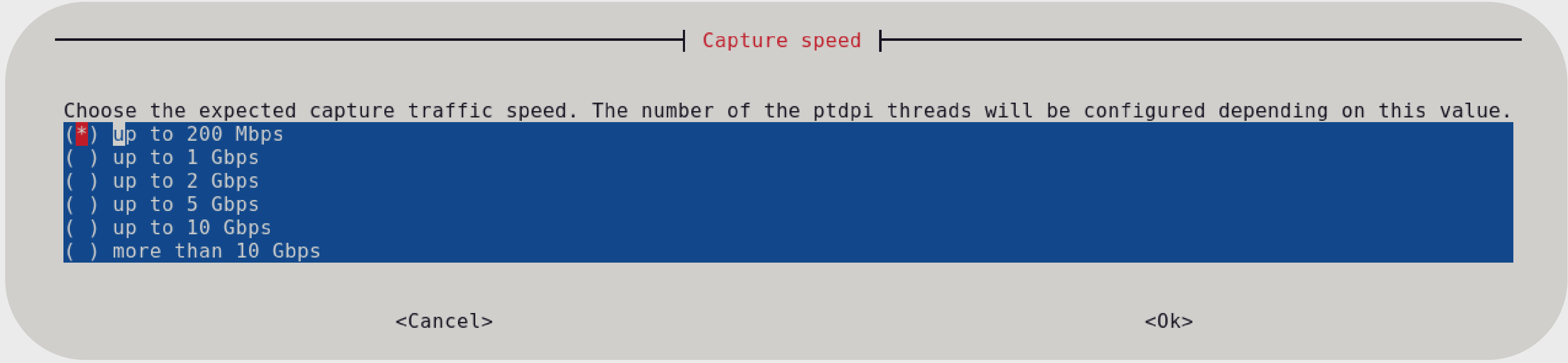
- управления
- межкомпонентного взаимодействия
- захвата

PT NAD 11.1. Конфигуратор



PT NAD 11.1. Конфигуратор





PT NAD 11.1. Режимы захвата трафика

DPDK —
рекомендуется
для всех
физических карт

AF-PACKET —
остается только
для совместимости
с существующими
внедрениями

PF-RING —
не поддерживается
PT NAD версии 11.1
и выше

PT NAD 11.1. Режимы захвата трафика

DPDK — рекомендуется для всех физических карт

AF-PACKET — остается только для совместимости с существующими внедрениями

Унифицированная конфигурация: для новых инсталляций всегда указывается DPDK

На одном сенсоре могут одновременно работать карты с поддержкой нативного DPDK и без нее

PT NAD 11.1. Режимы захвата трафика

nadadmin@localhost:~$ sudo **ptdpictl devlist**
ptdpictl devlist...
pci-02-00-0 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
Driver: ixgbe
Drivers available: ixgbe
Local cpu: 0,4, 1,5, 2,6, 3,7
Usage: **[DPDK_NATIVE]**

pci-05-00-1 Ethernet controller: Broadcom Limited NetXtreme BCM5720 Gigabit Ethernet PCIe
Driver: tg3
Drivers available: tg3
Local cpu: 0,4, 1,5, 2,6, 3,7

В параметрах указываются идентификаторы PCI

Например:

- capture_type: **dpdk**
- capture_if: **pci-02-00-0 pci-05-00-1**

PT NAD 11.1. Инструмент для определения проблем с захватом и обработкой трафика

```
ptuser@ptnad-01:/tmp/11.1$ ptdpictl traf
ptdpictl traf...  2023-05-22 15:24:24,379 - INFO - run:20 - NAD traffic analyzer
2023-05-22 15:24:24,516 - INFO - run:37 - Host 127.0.0.1; Start 22/05/2023, 11:24; End 22/05/2023, 12:24
-2023-05-22 15:24:24,994 - INFO - run:67 - Source live1
```

metric	total	%	bytes.total	bytes.recv	bytes.sent
TCP	4610	_	267 MB	133 MB	134 MB
BAD_CHECKSUM	0	0.00	0 B	0 B	0 B
Errors	569	12.34	20 MB	11 MB	9 MB
ASYNC	1	0.02	64 kB	0 B	64 kB
Errors & !ASYNC	568	12.32	20 MB	11 MB	9 MB
GAP_DETECT	1	0.02	705 kB	505 kB	199 kB
OUT_OF_WINDOW	0	0.00	0 B	0 B	0 B
GAP_DETECT & OUT_OF_WINDOW & !ASYNC	0	0.00	0 B	0 B	0 B
TUNNELS	0	0.00	0 B	0 B	0 B
TUNNELS_VLAN	0	0.00	0 B	0 B	0 B
TUNNELS_GRE	0	0.00	0 B	0 B	0 B
TUNNELS_TEREDO	0	0.00	0 B	0 B	0 B
TUNNELS_VLAN & ASYNC	0	0.00	0 B	0 B	0 B

PT NAD 11.1. Инструмент для определения проблем с захватом и обработкой трафика

```
+--------------------+-----------------------------------+
| Sensor name        |                                   |
| Stat time          | 2023-05-22T12:24:35.008535 (UTC)  |
| Up time            | 0d 02h 39m 38s                    |
+--------------------+-----------------------------------+
| Interface name     | pci-04-00-0                       |
| Speed              | 3.96 MB/sec    (31.64 Mb/sec)     |
| Packets            | 4582 pkt/sec                      |
| Kernel drops       | 0 pkt/sec (0 abs)                 |
| Other drops        | 0 pkt/sec (0 abs)                 |
| Invalid checksums  | 0 pkt/sec (0 abs)                 |
| Packet size max    | 1514 bytes                        |
+--------------------+-----------------------------------+
| Interface name     | pci-0c-00-0                       |
| Speed              | 194.0 B/sec    (1.55 kb/sec)      |
| Packets            | 2 pkt/sec                         |
| Kernel drops       | 0 pkt/sec (0 abs)                 |
| Other drops        | 0 pkt/sec (0 abs)                 |
| Invalid checksums  | 0 pkt/sec (0 abs)                 |
| Packet size max    | 98 bytes                          |
+--------------------+-----------------------------------+
```

PT NAD 11.1. Прочие улучшения

- Добавление команд в интерфейс командной строки

  nad-status

- Улучшение отображения репутационных списков в транзакциях DNS

- Разбор протокола DTLS

Полезные ссылки

Телеграм-чат
о PT NAD
t.me/PTNADChat

Дополнительные
материалы о PT NAD
clck.ru/33f7PP

pt@ptsecurity.com

ptsecurity.com