Частное образовательное учреждение дополнительного профессионального образования

«ВЫШТЕХ» (ОАНО ДПО «ВЫШТЕХ»)

Факультет информационной безопасности

Отчёт по домашней работе № 1
по дисциплине «Эксплуатация средств и процессов ИБ»

Тема: «Развёртывание и настройка системы обнаружения и предотвращения вторжений (IDS/IPS) на базе Suricata с интеграцией SIEM (ELK Stack), мониторинг Windows-событий через Winlogbeat и Sysmon»

Выполнил:

Студент группы F-402-1

Наседкин Павел Николаевич

Проверил:

ex-инструктор академии Cisco,

кандидат педагогических наук, доцент

Шабалин Андрей Михайлович

Дата сдачи: «27» августа 2026 г.

Оценка: _____

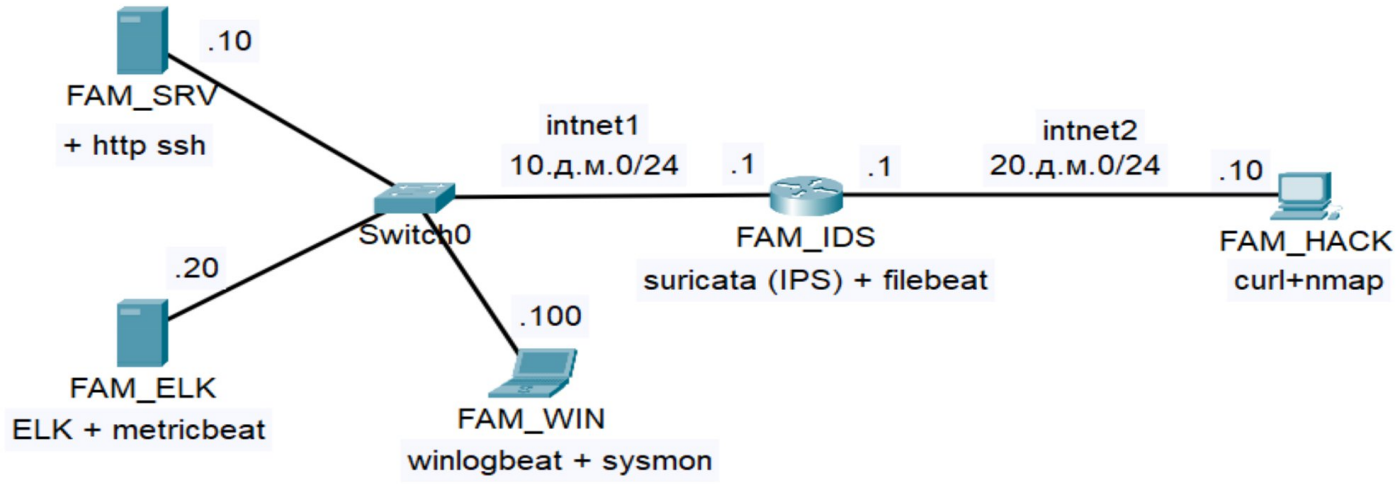
Наседкин Павел Николаевич

Подписано цифровой подписью: Наседкин Павел Николаевич
DN: c=RU, st=Иркутская область, l=Иркутск, o=ФГБОУ ВО ИрГУПС, ou=126714, cn=Наседкин Павел Николаевич
Дата: 2026.08.27 05:43:20 +08'00'

Содержание

1. Задание домашней работы 3
2. Цели и задачи работы 5
3. Ход выполнения 6
3.1. Таблица адресации 6
3.2. Кастомные сигнатуры Suricata 8
3.3. Конфигурация Filebeat на IDS 9
3.4. Конфигурация Winlogbeat на WIN 12
3.5. Конфигурация Logstash на ELK 14
3.6. Kibana-запросы для отчёта 15
4. Перечень скриншотов для отчета о выполнении 23
Заключение 37
Список использованных источников 39
ПРИЛОЖЕНИЕ А ВЫПОЛНЕНИЕ ЗАДАНИЯ 40

1 Задание (полный текст)



Все необходимое программное обеспечение доступно по ссылке: ***https://disk.360.yandex.ru/d/WuMMCiYqjUS7gQ***

1. Собрать топологию с использованием VBOX (Debian). Возможно использование GNS3. Осуществить базовую сетевую конфигурацию всех устройств: (имя устройства, IP-адрес, маска, шлюз).

2. На сервере SRV установить следующие серверные службы: ssh, http. На сервере ELK установить настроить ELK-стек и Metricbeat, осуществляющий мониторинг Elasticsearch.

3. На компьютере HACK установить curl и nmap (в качестве атакующей машины можно использовать Kali Linux). Провести SYN-сканирование сервера SRV и ping пакетами больше 1000 байт, а также просмотреть стартовую страницу веб-сервера средствами curl.

4. На IDS установить, настроить Suricata и обновить ее базу сигнатур. Включить и проверить режим IPS. Также добавить файлы с кастомными сигнатурами: детектирующими SYN-сканирование, ICMP-запросы большими пакетами и обращение к веб-серверу с помощью curl. Установить Filebeat на IDS, настроить с его помощью отправку событий безопасности в ELK.

5. На компьютере WIN создать пользователей Name и Name2. Пусть пользователь Name трижды введет неверно пароль при аутентификации и будет заблокирован, а пользователь Name2 в командной строке запустит утилиты ipconfig, whoami, ping и ssh-

подключение к SRV. Установить Winlogbeat и Sysmon, настроить с их помощью отправку событий безопасности в ELK.

Отчет по домашней работе: Отчет представляет собой набор подписанных скриншотов, подтверждающих выполнение задания. При создании скриншотов лучше всего пользоваться инструментом "Ножницы". Вырезанные скриншоты обычно копируются в текстовый документ (например, MS Word). Рекомендуемый формат файла-отчета pdf, который можно создать с помощью «Сохранить как…». Также в начало отчета вставьте вышеприведенное задание целиком.

Перечень скриншотов для отчета о выполнении:

1. Задание из данного файла. Топология, если используется эмулятор GNS3.

2. IDS -> cat /var/log/suricata/fast.log | grep … (по всем трем сигнатурам; на событиях виден drop).

3. ELK -> в Kibana вывести результаты работы Metricbeat, а также результаты запросов:

- по работе трех сигнатур (номер или описание сигнатуры).

- по событию журнала Security (заблокированные пользователи, событие 4740).

- по событиям журнала Sysmon о создании процессов пользователем Name2 (команды cmd).

Примечание на рисунке:

1. fam | name = фамилия слушателя = nasedkin (nasedkin_1) | name = pavel;
2. д.м. = дата.месяц. рождения слушателя = 10.20.11.0/24 и 20.20.11.0/24

2 Цели и задачи работы

Целью домашней работы №1 является: развёртывание комплексной системы мониторинга и защиты сетевой инфраструктуры на базе Suricata IDS/IPS и ELK Stack, а также настройка централизованного сбора событий безопасности с Windows-хоста с использованием Winlogbeat и Sysmon.

Задачи работы:

1. Собрать сетевую топологию на базе VirtualBox (Debian/Kali) с маршрутизацией между двумя подсетями.
2. Выполнить базовую сетевую конфигурацию всех устройств (IP-адреса, маски, шлюзы).
3. Развернуть серверные службы SSH и HTTP на сервере SRV.
4. Установить и настроить ELK Stack (Elasticsearch, Logstash, Kibana) и Metricbeat на сервере ELK.
5. Установить и настроить Suricata в режиме IPS с тремя кастомными сигнатурами (SYN-scan, ICMP DoS, curl User-Agent).
6. Настроить Filebeat на IDS для отправки событий Suricata в Elasticsearch.
7. На Windows-машине WIN создать двух пользователей, смоделировать инциденты (блокировка учётной записи, запуск команд) и настроить Winlogbeat + Sysmon для отправки событий в ELK.
8. Провести тестирование с атакующей машины HACK (nmap, ping, curl) и зафиксировать события в Kibana.
9. Оформить отчёт в соответствии с требованиями.

3 Ход выполнения

3.1. Таблица адресации

Таблица № 1 – Общая информация

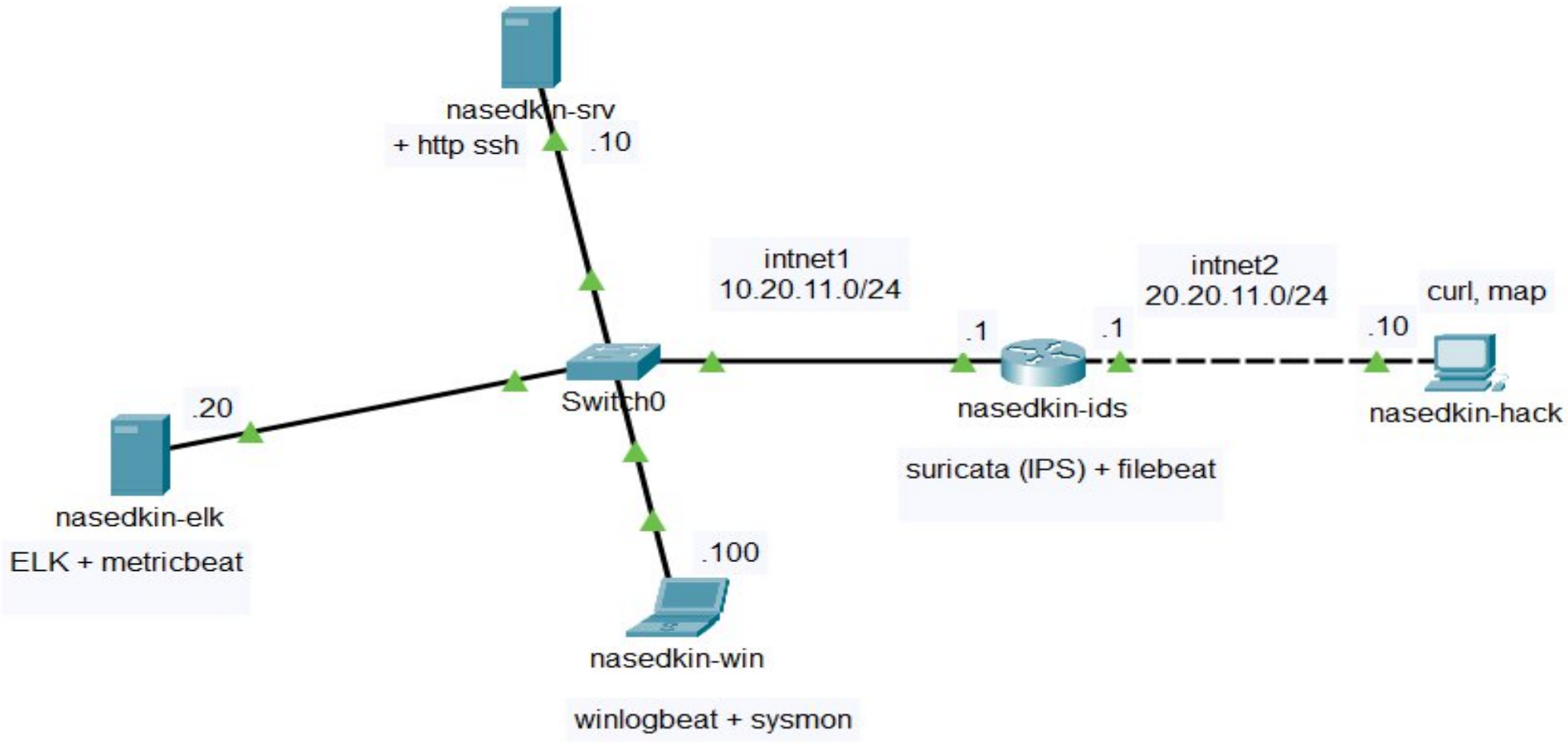
Параметр	Ваше значение
Фамилия (fam)	nasedkin
Имя (name)	pavel
Дата.месяц рождения (д.м.)	20.11 (пример из отчётов)
Сеть 1	10.20.11.0/24
Сеть 2	20.20.11.0/24

Таблица № 2 – Топология и таблица адресации (для Скриншота №1)

Устройство	Имя ВМ	IP-адрес	Маска	Шлюз
Сервер SRV	nasedkin-srv	10.20.11.10	/24	10.20.11.1
Сервер ELK	nasedkin-elk	10.20.11.20	/24	10.20.11.1
Windows WIN	nasedkin-win	10.20.11.100	/24	10.20.11.1
IDS/IPS	nasedkin-ids	enp0s3: 10.20.11.1 enp0s8: 20.20.11.1	/24	—

Устройство	Имя ВМ	IP-адрес	Маска	Шлюз
Хакер HACK	nasedkin-hack	20.20.11.10	/24	20.20.11.1

Ниже приведены скриншоты, подтверждающие выполнение каждого этапа. *Все виртуальные машины развёрнуты в VirtualBox.*



Скриншот №1 — Схема топологии в GNS3 с подписанными IP-адресами

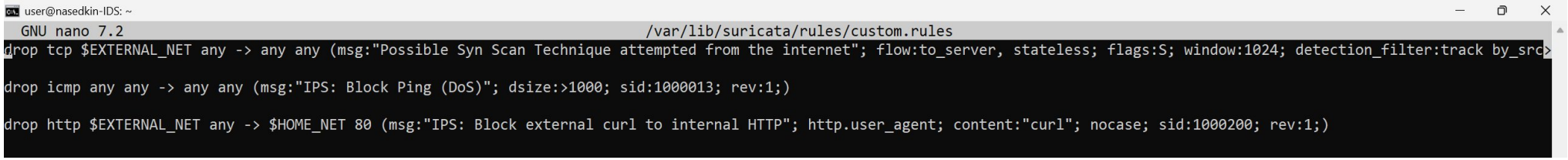
3.2. Кастомные сигнатуры Suricata

Файл /var/lib/suricata/rules/custom.rules (в соответствии с ips_sig.txt от преподавателя)

drop tcp $EXTERNAL_NET any -> any any (msg:"Possible Syn Scan Technique attempted from the internet"; flow:to_server, stateless; flags:S; window:1024; detection_filter:track by_src, count 10, seconds 15; classtype:attempted-recon; sid:40000003; rev:1;)

drop icmp any any -> any any (msg:"IPS: Block Ping (DoS)"; dsize:>1000; sid:1000013; rev:1;)

drop http $EXTERNAL_NET any -> $HOME_NET 80 (msg:"IPS: Block external curl to internal HTTP"; http.user_agent; content:"curl"; nocase; sid:1000200; rev:1;)



3.3. Конфигурация Filebeat на IDS

Файл /etc/filebeat/filebeat.yml:

yaml
```yaml
output.elasticsearch:
  hosts: ["http://10.20.11.20:9200"]
  indices:
    - index: "nasedkin_ids-%{+yyyy.MM.dd}"
```

```yaml
# ---------------------------- Elasticsearch Output ----------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["http://10.20.11.20:9200"]
  indices:
    - index: "nasedkin_ids-%{+yyyy.MM.dd}"

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"
```

setup.kibana:
  host: http://10.20.11.20:5601

```
# ================================== Kibana ==================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:
  host: "http://10.20.11.20:5601"
  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  #host: "localhost:5601"

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:
```

Файл /etc/filebeat/modules.d/suricata.yml:

yaml
```yaml
- module: suricata
  eve:
    enabled: true
    var.paths: ["/var/log/suricata/eve.json"]
```

user@nasedkin-IDS: ~

```
  GNU nano 7.2                    /etc/filebeat/modules.d/suricata.yml
# Module: suricata
# Docs: https://www.elastic.co/guide/en/beats/filebeat/8.10/filebeat-module-suricata.html

- module: suricata
  # All logs
  eve:
    enabled: true
    var.paths: ["/var/log/suricata/eve.json"]
    # Set custom paths for the log files. If left empty,
    # Filebeat will choose the paths depending on your OS.
    #var.paths:
```

3.4. Конфигурация Winlogbeat на WIN

Файл `C:\Program Files\winlogbeat\winlogbeat.yml`:

yaml
```yaml
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h
  - name: System
  - name: Security
    event_id: 4624, 4625, 4688, 4740
  - name: Microsoft-Windows-Sysmon/Operational
    event_id: 1
  - name: Windows PowerShell
    event_id: 400, 403, 600, 800
  - name: Microsoft-Windows-PowerShell/Operational
    event_id: 4103, 4104, 4105, 4106

tags: ["winagent"]

output.logstash:
  hosts: ["10.20.11.20:5044"]

logging.level: info
logging.to_files: true
logging.files:
  path: C:/Program Files/winlogbeat/logs
  name: winlogbeat
  keepfiles: 150
  permissions: 0644
```

nasedkin-win [Работает] - Oracle VM VirtualBox

Корзина

Microsoft Edge

winlogbeat – Блокнот

Файл Правка Формат Вид Справка

```
###################### Winlogbeat Configuration ########################

winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h
  - name: System
  - name: Security
    event_id: 4624, 4625, 4688, 4740
  - name: Microsoft-Windows-Sysmon/Operational
    event_id: 1
  - name: Windows PowerShell
    event_id: 400, 403, 600, 800
  - name: Microsoft-Windows-PowerShell/Operational
    event_id: 4103, 4104, 4105, 4106

tags: ["winagent"]

output.logstash:
  hosts: ["10.20.11.20:5044"]

logging.level: info
logging.to_files: true
logging.files:
  path: C:/Program Files/winlogbeat/logs
  name: winlogbeat
  keepfiles: 150
  permissions: 0644

processors:
  - add_host_metadata:
      when.not.contains.tags: forwarded
```

Стр 1, стлб 1 | 100% | UNIX (LF) | UTF-8 со специфи

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

Чтобы начать поиск, введите здесь запрос

ENG 2:58 27.08.2026

3.5. Конфигурация Logstash на ELK

Файл /etc/logstash/conf.d/03-winlogbeat-tag.conf:

bash

```
input {
  beats {
    port => 5044
  }
}

output {
  if "winagent" in [tags] {
    elasticsearch {
      hosts => ["http://localhost:9200"]
      index => "tag-winlogbeat-%{+YYYY.MM.dd}"
    }
  }
}
```

```
user@nasedkin-elk: ~
  GNU nano 7.2                    /etc/logstash/conf.d/03-winlogbeat-tag.conf
input {
  beats {
    port => 5044
  }
}

output {
  if "winagent" in [tags] {
    elasticsearch {
      hosts => ["http://localhost:9200"]
      index => "tag-winlogbeat-%{+YYYY.MM.dd}"
    }
  }
}
```

3.6. Kibana-запросы для отчёта

Запрос 1 (три сигнатуры Suricata):

event.kind: "alert" AND (suricata.eve.alert.signature_id: 40000003 OR 1000013 OR 1000200)

Запрос 2 (событие 4740, блокировка Name / Pavel):

winlog.event_id: 4740 AND winlog.event_data.TargetUserName: "pavel"

Запрос 3 (создание процессов Name2 / Pavel2, Sysmon Event ID 1):

winlog.event_id: 1 AND winlog.user_name: "nasedkin-win\pavel2"

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2026-08-26T13:58:24.363Z',to:'2026-08-26T17:26:10.376Z'))&_a=(columns:!(),dat...

Яндекс Почта Карты Маркет Новости Словари Видео Музыка Диск Mail.Ru Поиск в Интернете Foto.Mail.Ru Mail.Ru Video.Mail.Ru Предварительная... Все закладки

elastic Find apps, content, and more. ^/

D Discover Check out context-aware Discover Try ES|QL Inspect Alerts + Save

Data view nasedkin_ids

event.kind: "alert" AND (suricata.eve.alert.signature_id: 40000003 OR 1000013 OR 1000200)

Aug 26, 2026 @ 21:58:24.3... → Aug 27, 2026 @ 01:26:10.376 Refresh

event.original: exists

Search field names 0

Popular fields 1

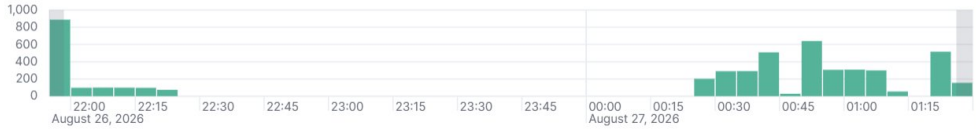
- event.original

Available fields 603

- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- destination.address
- destination.as.number
- destination.as.organization.name
- destination.bytes
- destination.domain
- destination.geo.city_name
- destination.geo.continent_name
- destination.geo.country_iso_code
- destination.geo.country_name
- destination.geo.location.lat
- destination.geo.location.lon

Add a field

Auto interval No breakdown



Aug 26, 2026 @ 21:58:24.363 - Aug 27, 2026 @ 01:26:10.376 (interval: Auto - 5 minutes)

Documents (4,931) Field statistics Sort fields 1

@timestamp	Summary
Aug 27, 2026 @ 01:25:08.404	event.kind alert @timestamp Aug 27, 2026 @ 01:25:08.404 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:25:08.243	event.kind alert @timestamp Aug 27, 2026 @ 01:25:08.243 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:25:08.078	event.kind alert event.original {"timestamp":"2026-08-26T22:25:08.078096+0500","flow_id":635724911925687,"event_type":"alert","src_ip":"20.20.11.10","dest_ip":"10.20.11.10","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire…
Aug 27, 2026 @ 01:25:08.072	event.kind alert @timestamp Aug 27, 2026 @ 01:25:08.072 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:25:07.899	event.kind alert @timestamp Aug 27, 2026 @ 01:25:07.899 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:25:07.736	event.kind alert @timestamp Aug 27, 2026 @ 01:25:07.736 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0

Rows per page: 100 1 2 3 4 5

Document 96 of 500

Actions: View single document View surrounding documents

Table JSON

event.original 0

Selected only

Field	Value
_ignored	event.original.keyword
event.original	{"timestamp":"2026-08-26T22:25:08.078096+0500","flow_id":635724911925687,"event_type":"alert","src_ip":"20.20.11.10","dest_ip":"10.20.11.10","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire/pcap","alert":{"action":"blocked","gid":1,"signature_id":10000013,"rev":1,"signa

Close

ENG 100% 1:41 27.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2026-08-26T13:58:24.363Z',to:'2026-08-26T17:26:10.376Z'))&_a=(columns:!(suric...

Яндекс | Почта | Карты | Маркет | Новости | Словари | Видео | Музыка | Диск | Mail.Ru | Поиск в Интернете | Foto.Mail.Ru | Mail.Ru | Video.Mail.Ru | Предварительная... | Все закладки

elastic | Find apps, content, and more. ^/

D | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: nasedkin_ids

event.kind: "alert" AND (suricata.eve.alert.signature_id: 40000003 OR 1000013 OR 1000200)

Aug 26, 2026 @ 21:58:24.3... → Aug 27, 2026 @ 01:26:10.376 | Refresh

Search field names | 0

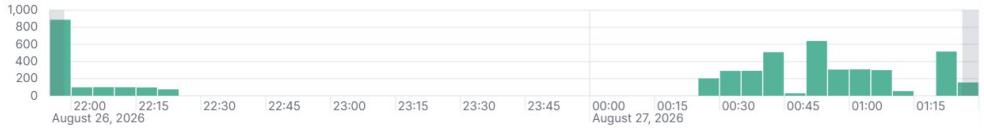
Selected fields 1
- suricata.eve.alert.signature

Popular fields 3
- suricata.eve.alert.signature_id
- event.original
- suricata.eve.alert.signature

Available fields 603
- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- destination.address
- destination.as.number
- destination.as.organization.name
- destination.bytes
- destination.domain
- destination.geo.city_name
- destination.geo.continent_name
- destination.geo.country_iso_code

Add a field

Auto interval | No breakdown



Aug 26, 2026 @ 21:58:24.363 - Aug 27, 2026 @ 01:26:10.376 (interval: Auto - 5 minutes)

Documents (4,931) | Field statistics | Columns 2 | Sort fields 1

@timestamp	suricata.eve.alert.signature
Aug 27, 2026 @ 01:26:10.376	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:26:09.376	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:26:08.372	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:26:07.120	IPS: Block Ping (DoS)
Aug 27, 2026 @ 01:26:06.100	IPS: Block Ping (DoS)
Aug 27, 2026 @ 01:26:05.071	IPS: Block Ping (DoS)

Rows per page: 100 | 1 2 3 4 5

Document 4 of 500

Actions: View single document | View surrounding documents

Table | JSON

Search field names or values | 0

Selected only

Field	Value
suricata.eve.alert.gid	1
suricata.eve.alert.rev	1
suricata.eve.alert.signature	IPS: Block Ping (DoS)
suricata.eve.alert.signature_id	1,000,013
suricata.eve.direction	to_server
suricata.eve.event_type	alert
suricata.eve.flow_id	635724911925687
suricata.eve.flow.dest_ip	10.20.11.10
suricata.eve.flow.src_ip	20.20.11.10
suricata.eve.icmp_code	0

Rows per page: 100 | 1

Close

ENG 100% 1:51 27.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2026-08-26T13:58:24.363Z',to:'2026-08-26T17:26:10.376Z'))&_a=(columns:!(),dat...

Яндекс | Почта | Карты | Маркет | Новости | Словари | Видео | Музыка | Диск | Mail.Ru | Поиск в Интернете | Foto.Mail.Ru | Mail.Ru | Video.Mail.Ru | Предварительная... | Все закладки

elastic | Find apps, content, and more. ^/

D | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: nasedkin_ids

event.kind: "alert" AND (suricata.eve.alert.signature_id: 40000003 OR 1000013 OR 1000200)

Aug 26, 2026 @ 21:58:24.3... → Aug 27, 2026 @ 01:26:10.376 | Refresh

Search field names | 0

Popular fields 2

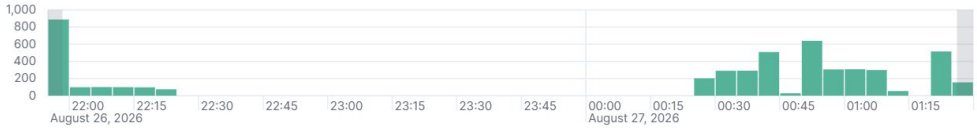
- suricata.eve.alert.signature_id
- event.original

Available fields 603

- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- destination.address
- destination.as.number
- destination.as.organization.name
- destination.bytes
- destination.domain
- destination.geo.city_name
- destination.geo.continent_name
- destination.geo.country_iso_code
- destination.geo.country_name
- destination.geo.location.lat
- destination.geo.location.lon
- destination.geo.region_iso_code

Add a field

Auto interval | No breakdown



Aug 26, 2026 @ 21:58:24.363 - Aug 27, 2026 @ 01:26:10.376 (interval: Auto - 5 minutes)

Documents (4,931) | **Field statistics** | Sort fields 1

@timestamp	Summary
Aug 27, 2026 @ 01:26:10.376	event.kind alert @timestamp Aug 27, 2026 @ 01:26:10.376 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:26:09.376	event.kind alert @timestamp Aug 27, 2026 @ 01:26:09.376 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:26:08.372	event.kind alert @timestamp Aug 27, 2026 @ 01:26:08.372 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:26:07.120	event.kind alert event.original {"timestamp":"2026-08-26T22:26:07.120089+0500","flow_id":635724911925687,"event_type":"alert","src_ip":"20.20.11.10","dest_ip":"10.20.11.10","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire…
Aug 27, 2026 @ 01:26:06.100	event.kind alert event.original {"timestamp":"2026-08-26T22:26:06.100580+0500","flow_id":635724911925687,"event_type":"alert","src_ip":"20.20.11.10","dest_ip":"10.20.11.10","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire…
Aug 27, 2026 @ 01:26:05.071	event.kind alert event.original {"timestamp":"2026-08-26T22:26:05.071238+0500","flow_id":635724911925687,"event_type":"alert","src_ip":"20.20.11.10","dest_ip":"10.20.11.10","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire…

Rows per page: 100 | 1 2 3 4 5

Document 470 of 500

Actions: View single document | View surrounding documents

Table | JSON

Search field names or values | 0

Selected only

Field	Value
source.geo.location.lon	-97.822
source.ip	20.20.11.10
source.packets	3
source.port	58,970
suricata.eve.alert.category	(empty)
suricata.eve.alert.gid	1
suricata.eve.alert.rev	1
suricata.eve.alert.signature	IPS: Block external curl to internal HTTP
suricata.eve.alert.signature_id	1,000,200
suricata.eve.direction	to_server
suricata.eve.event_type	alert

Rows per page: 100 | 1

Close

ENG 100% 1:49 27.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),time:(from:'2026-08-26T13:58:24.363Z',to:'2026-08-26T17:26:10.376Z'))&_a=(columns:!('@timestamp',suricata.eve.alert.signature),...

elastic | Find apps, content, and more. | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | Save

Data view: nasedkin_ids

event.kind: "alert" AND (suricata.eve.alert.signature_id: 1000200)

Aug 26, 2026 @ 21:58:24.3... → Aug 27, 2026 @ 01:26:10.376 | Refresh

Search field names

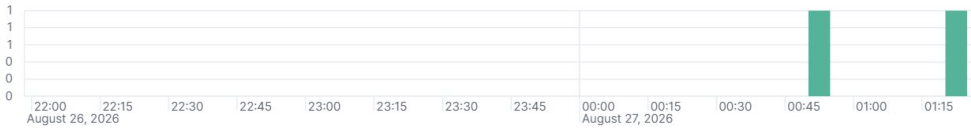
Selected fields 2
- @timestamp
- suricata.eve.alert.signature

Popular fields 6
- suricata.eve.alert.signature_id
- rule.id
- @timestamp
- event.original
- _id
- suricata.eve.alert.signature

Available fields 603
- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- destination.address
- destination.as.number
- destination.as.organization.name
- destination.bytes

Add a field

Auto interval | No breakdown



Aug 26, 2026 @ 21:58:24.363 - Aug 27, 2026 @ 01:26:10.376 (interval: Auto - 5 minutes)

Documents (2) | Field statistics | Columns 2 | Sort fields 1

@timestamp	suricata.eve.alert.signature
Aug 27, 2026 @ 01:24:25.794	IPS: Block external curl to internal HTTP
Aug 27, 2026 @ 00:54:55.281	IPS: Block external curl to internal HTTP

Document 1 of 2

Actions: View single document | View surrounding documents

Table | JSON

Search field names or values

Selected only

Field	Value
suricata.eve.alert.category	(empty)
suricata.eve.alert.gid	1
suricata.eve.alert.rev	1
suricata.eve.alert.signature	IPS: Block external curl to internal HTTP
suricata.eve.alert.signature_id	1,000,200
suricata.eve.direction	to_server
suricata.eve.event_type	alert
suricata.eve.flow_id	290847715078223
suricata.eve.flow.dest_ip	10.20.11.10
suricata.eve.flow.dest_port	80
suricata.eve.flow.sr	20.20.11.10

Rows per page: 100 | 1

Close

ENG 100% 2:10 27.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),time:(from:'2026-08-26T13:58:24.363Z',to:'2026-08-26T17:26:10.376Z'))&_a=(columns:!('@timestamp',rule.name),dataSource:(dat...

Яндекс | Почта | Карты | Маркет | Новости | Словари | Видео | Музыка | Диск | Mail.Ru | Поиск в Интернете | Foto.Mail.Ru | Mail.Ru | Video.Mail.Ru | Предварительная... | Все закладки

elastic | Find apps, content, and more. ^/

D | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: nasedkin_ids

event.kind: "alert" AND (suricata.eve.alert.signature_id: 40000003 OR 1000013 OR 1000200)

Aug 26, 2026 @ 21:58:24.3... → Aug 27, 2026 @ 01:26:10.376 | Refresh

rule.name: exists ×

Search field names | 0

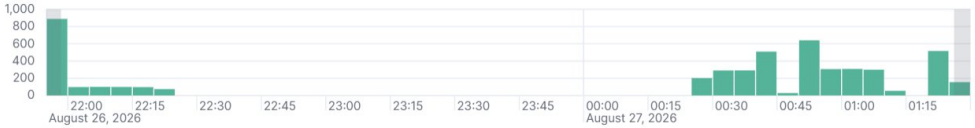
Selected fields 2
- @timestamp
- rule.name

Popular fields 7
- suricata.eve.alert.signature_id
- rule.id
- @timestamp
- event.original
- _id
- rule.name
- suricata.eve.alert.signature

Available fields 603
- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- destination.address

Add a field

Auto interval | No breakdown



Aug 26, 2026 @ 21:58:24.363 - Aug 27, 2026 @ 01:26:10.376 (interval: Auto - 5 minutes)

Documents (4,931) | Field statistics | Columns 2 | Sort fields 1

@timestamp	rule.name
Aug 27, 2026 @ 01:25:08.243	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:25:08.078	IPS: Block Ping (DoS)
Aug 27, 2026 @ 01:25:08.072	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:25:07.899	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:25:07.736	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:25:07.568	Possible Syn Scan Technique attempted from the internet

Rows per page: 100 | 1 2 3 4 5

Document 97 of 500

Actions: View single document | View surrounding documents

Table | JSON

Search field names or values | 0

Selected only

Field	Value
source.ip	20.20.11.10
source.packets	1
source.port	56,640
suricata.eve.alert.category	Attempted Information Leak
suricata.eve.alert.gid	1
suricata.eve.alert.rev	1
suricata.eve.alert.signature	Possible Syn Scan Technique attempted from the internet
suricata.eve.alert.signature_id	40,000,003
suricata.eve.direction	to_server
suricata.eve.event_type	alert
suricata.eve.flow_id	1155677955083555

Rows per page: 100 | 1

Close

ENG 100% 2:13 27.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2026-08-26T11:37:19.869Z',to:'2026-08-26T11:37:19.869Z'))&_a=(columns:!('@ti...

Яндекс Почта Карты Маркет Новости Словари Видео Музыка Диск Mail.Ru Поиск в Интернете Foto.Mail.Ru Mail.Ru Video.Mail.Ru Предварительная... Все закладки

elastic | Find apps, content, and more. ^/

D Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: winlogbeat

winlog.event_id: 4740 AND winlog.event_data.TargetUserName: "pavel"

Aug 26, 2026 @ 19:37:19.869 → Aug 26, 2026 @ 19:37:19.869 | Update

Search field names 0

Selected fields 2
- @timestamp
- event.original

Popular fields 2
- winlog.event_data.CommandLine
- event.original

Available fields 221
- @timestamp
- @version
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- ecs.version
- event.action
- event.code
- event.created
- event.kind
- event.original
- event.outcome

Add a field

Auto interval | No breakdown

Aug 26, 2026 @ 19:37:19.869 - Aug 26, 2026 @ 19:37:19.869 (interval: Auto - millisecond)

Documents (1) | **Field statistics** | Columns 2 | Sort fields 1

@timestamp	ginal
Aug 26, 2026 @ 19:37:19.869	Заблокирована учетная запись пользователя. Субъект: Идентификатор безопасности: S-1-5-18 Имя учетной записи: NASEDKIN-WIN$ Домен учетной записи: WORKGROUP Идентификатор входа: 0x3E7 Заблокированная учетная запись: Идентификатор безопасности: S-1-5-21-28584859-90745515-1943227453-1002 Имя учетной записи: Pavel Дополнительные сведения: Имя вызывающего компьютера: NASEDKIN-WIN

Filter for | Filter out | Copy value

Document

Actions: View single document | View surrounding documents

Table | JSON

Search field names or values 0

Selected only

Field	Value
event.kind	event
event.original	Заблокирована учетная запись пользователя. Субъект: Идентификатор безопасности: S-1-5-18 Имя учетной записи: NASEDKIN-WIN$ Домен учетной записи: WORKGROUP Идентификатор входа: 0x3E7 Заблокированная учетная запись: Идентификатор безопасности: S-1-5-21-28584859-90745515-1943227453-1002
event.outcome	success
event.provider	Microsoft-Windows-Security-Auditing
host.architecture	x86_64

Rows per page: 100 | 1

Close

13° ENG 100% 2:20 27.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(time:(from:'2026-08-26T11:25:25.746Z',to:'2026-08-26T13:25:27.442Z'))&_a=(columns:!('@timestamp',winlog.event_data.CommandLine),d...

Яндекс | Почта | Карты | Маркет | Новости | Словари | Видео | Музыка | Диск | Mail.Ru | Поиск в Интернете | Foto.Mail.Ru | Mail.Ru | Video.Mail.Ru | Предварительная... | Все закладки

elastic | Find apps, content, and more. ^/

D | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: winlogbeat

winlog.event_id: 1 AND winlog.event_data.User: "nasedkin-win\pavel2"

Aug 26, 2026 @ 19:25:25.7... → Aug 26, 2026 @ 21:25:27.442 | Refresh

Search field names | 0

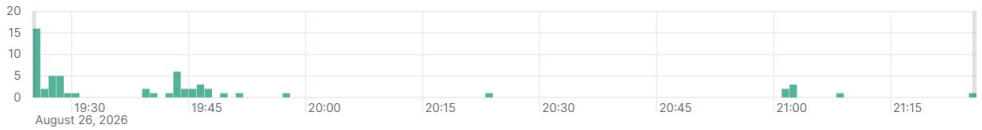
Selected fields 2
- @timestamp
- winlog.event_data.CommandLine

Popular fields 2
- winlog.event_data.CommandLine
- event.original

Available fields 221
- @timestamp
- @version
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- ecs.version
- event.action
- event.code
- event.created
- event.kind
- event.original
- event.outcome

Add a field

Auto interval | No breakdown



Aug 26, 2026 @ 19:25:25.746 - Aug 26, 2026 @ 21:25:27.442 (interval: Auto - minute)

Documents (60) | **Field statistics** | Columns 2 | Sort fields 1

@timestamp	winlog.event_data.CommandLine
Aug 26, 2026 @ 19:49:42.639	"C:\Windows\system32\mmc.exe" "C:\Windows\system32\eventvwr.msc" /s
Aug 26, 2026 @ 19:47:22.594	ssh user@10.20.11.10
Aug 26, 2026 @ 19:47:01.768	whoami
Aug 26, 2026 @ 19:46:54.924	ipconfig
Aug 26, 2026 @ 19:46:34.736	ping 10.20.11.10
Aug 26, 2026 @ 19:46:25.704	ping ping 10.20.11.10

Rows per page: 100 | 1

Document 3 of 60

Actions: View single document | View surrounding documents

Table | JSON

com | 0

Selected only

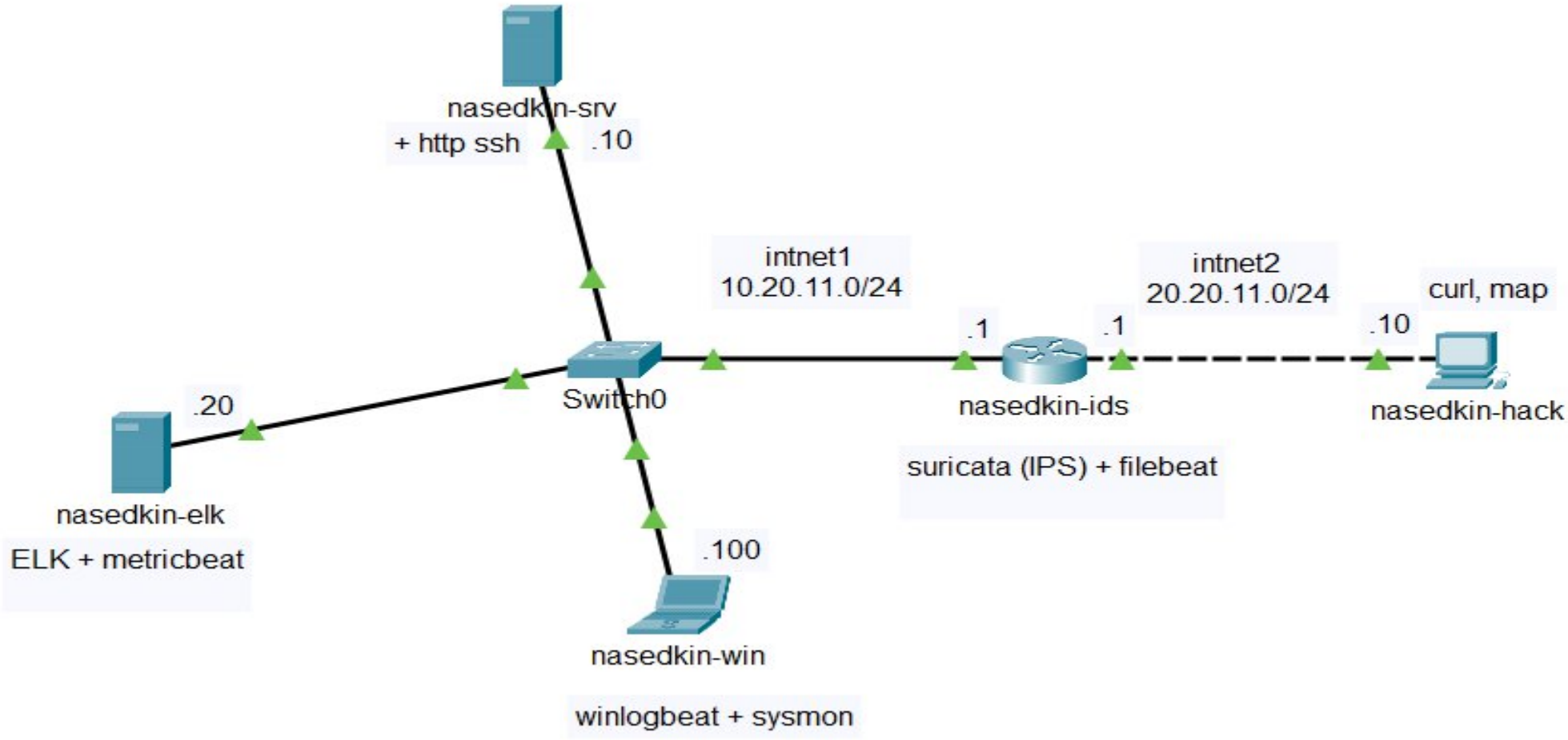
Field	Value
event.original	Process Create: RuleName: - UtcTime: 2026-08-26 13:02:15.809 ProcessGuid: {821b00f7-e3d7-6a8e-5f04-000000000e00} ProcessId: 1768

Close

ENG 100% 2:25 27.08.2026

4. Перечень скриншотов для отчёта о выполнении

Ниже приведены скриншоты, подтверждающие выполнение каждого этапа. ***Все виртуальные машины развёрнуты в VirtualBox.***



Скриншот №1 — Схема топологии в GNS3 с подписанными IP-адресами

root@nasedkin-IDS:~# ip -4 -br a

lo UNKNOWN 127.0.0.1/8

enp0s3 UP 10.20.11.1/24

enp0s8 UP 20.20.11.1/24

root@nasedkin-IDS:~# suricata -T -c /etc/suricata/suricata.yaml -v

[...]

Configuration provided was successfully loaded. Exiting.

```
user@nasedkin-IDS: ~
root@nasedkin-IDS:~# nano /var/lib/suricata/rules/custom.rules
root@nasedkin-IDS:~# nano /etc/filebeat/filebeat.yml
root@nasedkin-IDS:~# nano /etc/filebeat/modules.d/suricata.yml
root@nasedkin-IDS:~# ip -4 -br a
lo               UNKNOWN        127.0.0.1/8
enp0s3           UP             10.20.11.1/24
enp0s8           UP             20.20.11.1/24
enp0s9           UP             10.0.4.15/24
enp0s10          UP             192.168.0.28/24
root@nasedkin-IDS:~# suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: alert-syslog: Syslog output initialized
Info: detect: 1 rule files processed. 3 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 3 signatures processed. 0 are IP-only rules, 0 are inspecting packet payload, 1 inspect ap
plication layer, 0 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
root@nasedkin-IDS:~#
```

Скриншот №2 – IDS: проверка конфигурации Suricata

root@nasedkin-IDS:~# cat /var/log/suricata/fast.log | grep 40000003 | head -5

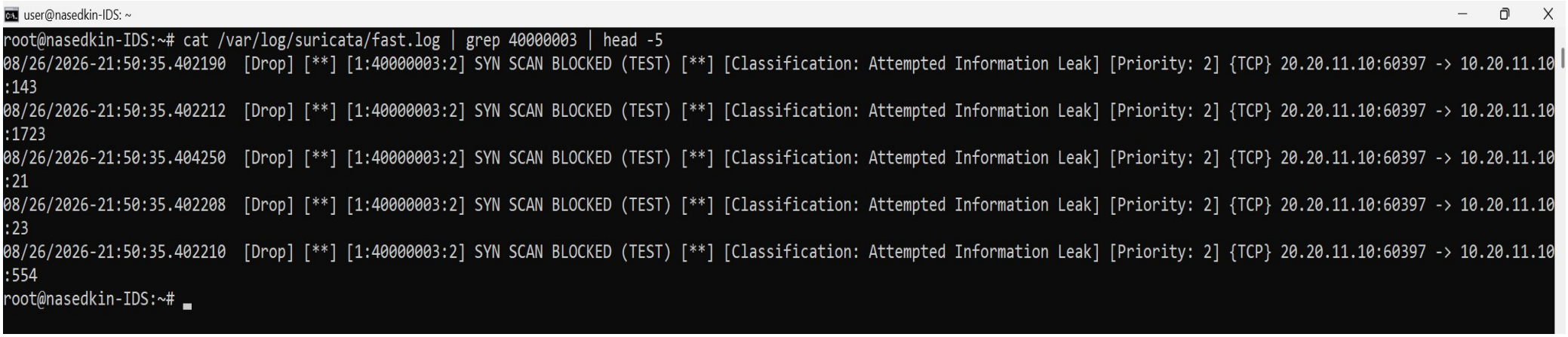
08/26/2026-21:50:35.402190 [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10:143

08/26/2026-21:50:35.402212 [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10:1723

08/26/2026-21:50:35.404250 [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10:21

08/26/2026-21:50:35.402208 [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10:23

08/26/2026-21:50:35.402210 [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10:554



Скриншот №3 – IDS: SYN-сканирование (sid:40000003)

root@nasedkin-IDS:~# cat /var/log/suricata/fast.log | grep 1000013 | head -5

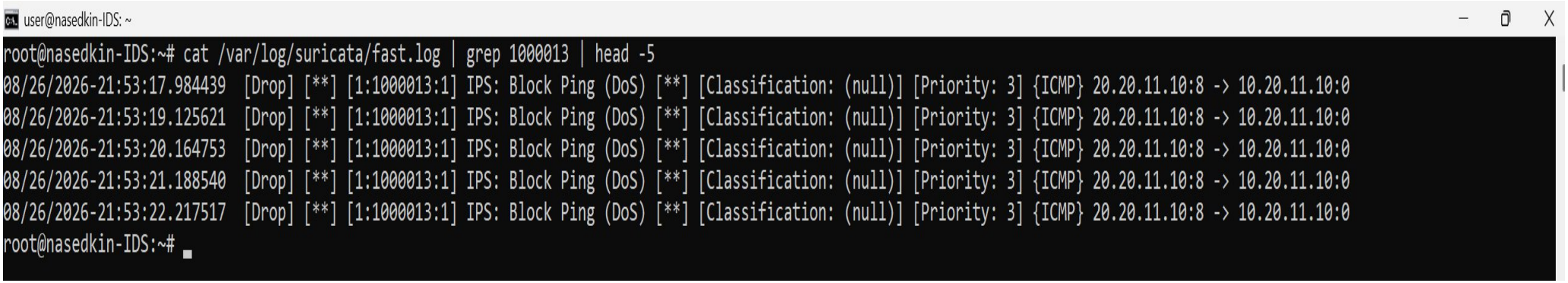
08/26/2026-21:53:17.984439 [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0

08/26/2026-21:53:19.125621 [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0

08/26/2026-21:53:20.164753 [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0

08/26/2026-21:53:21.188540 [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0

08/26/2026-21:53:22.217517 [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0



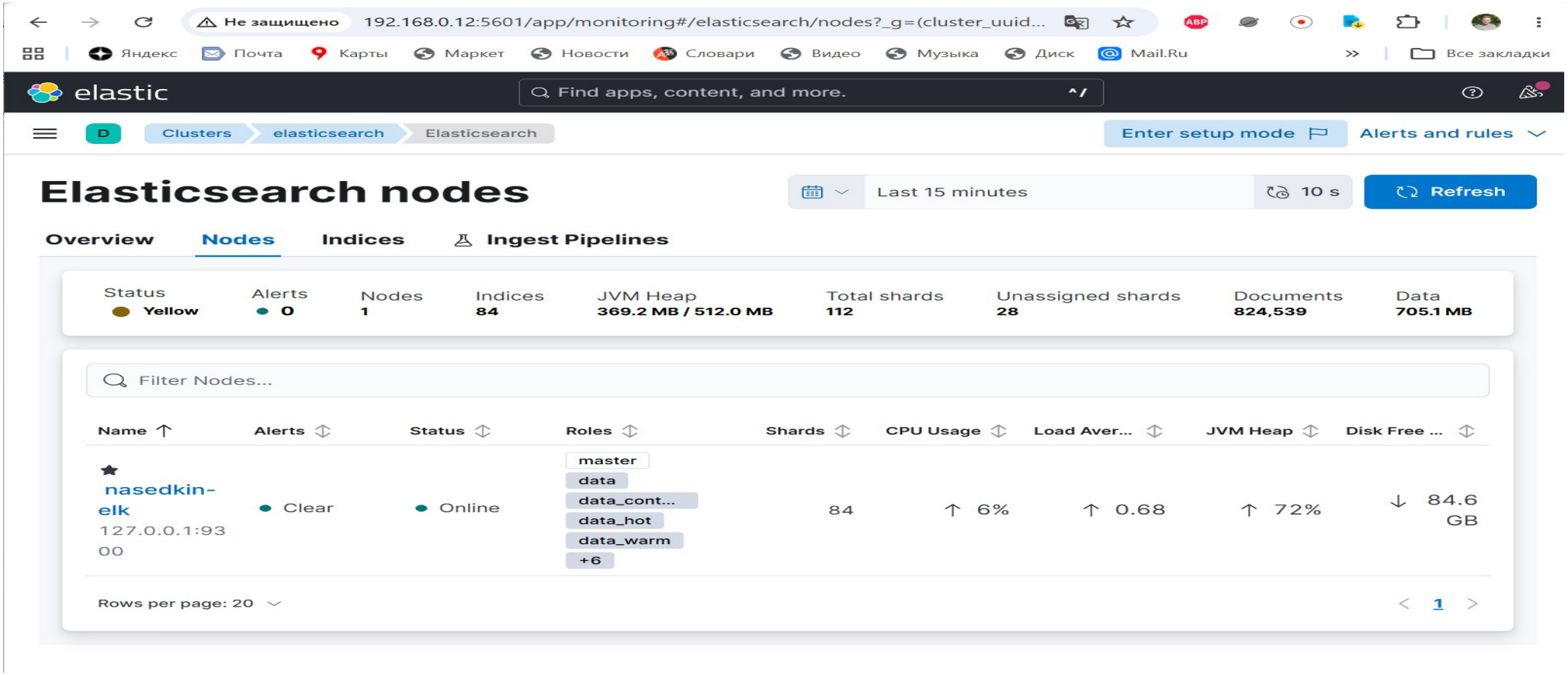
Скриншот №4 – IDS: ICMP DoS (sid:1000013)

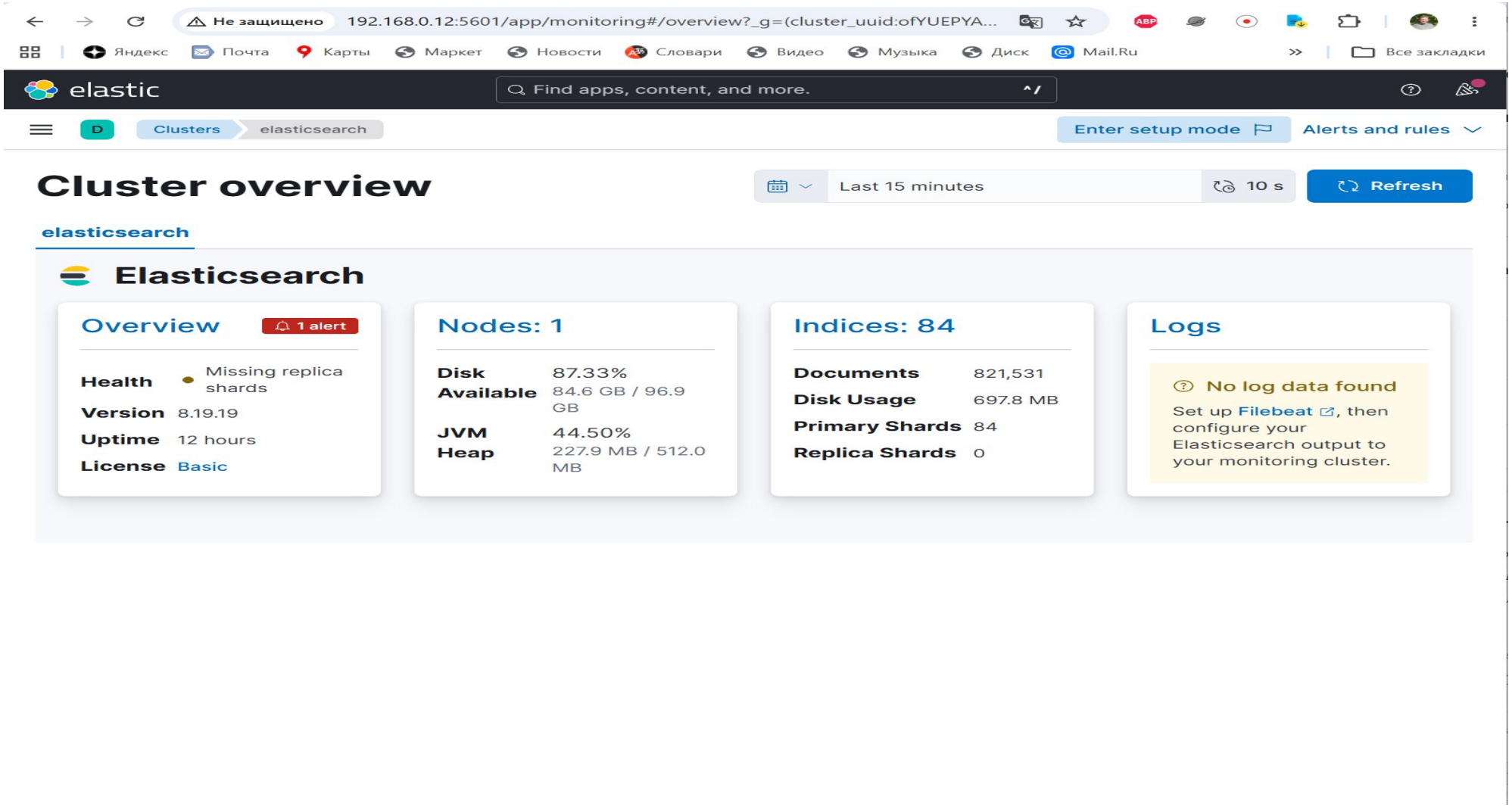
root@nasedkin-IDS:~# cat /var/log/suricata/fast.log | grep 1000200

08/26/2026-21:54:55.281805 [Drop] [**] [1:1000200:1] IPS: Block external curl to internal HTTP [**] [Classification: (null)] [Priority: 3] {TCP} 20.20.11.10:36044 -> 10.20.11.10:80

```
user@nasedkin-IDS: ~
root@nasedkin-IDS:~# cat /var/log/suricata/fast.log | grep 1000200
08/26/2026-21:54:55.281805  [Drop] [**] [1:1000200:1] IPS: Block external curl to internal HTTP [**] [Classification: (null)] [Priority: 3] {TCP} 20.20.11.10:36044 -> 10.20.11.10:80
08/26/2026-22:24:25.794927  [Drop] [**] [1:1000200:1] IPS: Block external curl to internal HTTP [**] [Classification: (null)] [Priority: 3] {TCP} 20.20.11.10:58970 -> 10.20.11.10:80
root@nasedkin-IDS:~#
```

Скриншот №5 – IDS: curl (sid:1000200)





Скриншот №6 — Дашборд мониторинга Elasticsearch (Metricbeat) в Kibana

На скриншоте представлена информация о состоянии кластера Elasticsearch, собранная с помощью Metricbeat: состояние кластера, использование JVM, количество индексов и документов, использование дискового пространства

Запрос 1 (три сигнатуры Suricata):

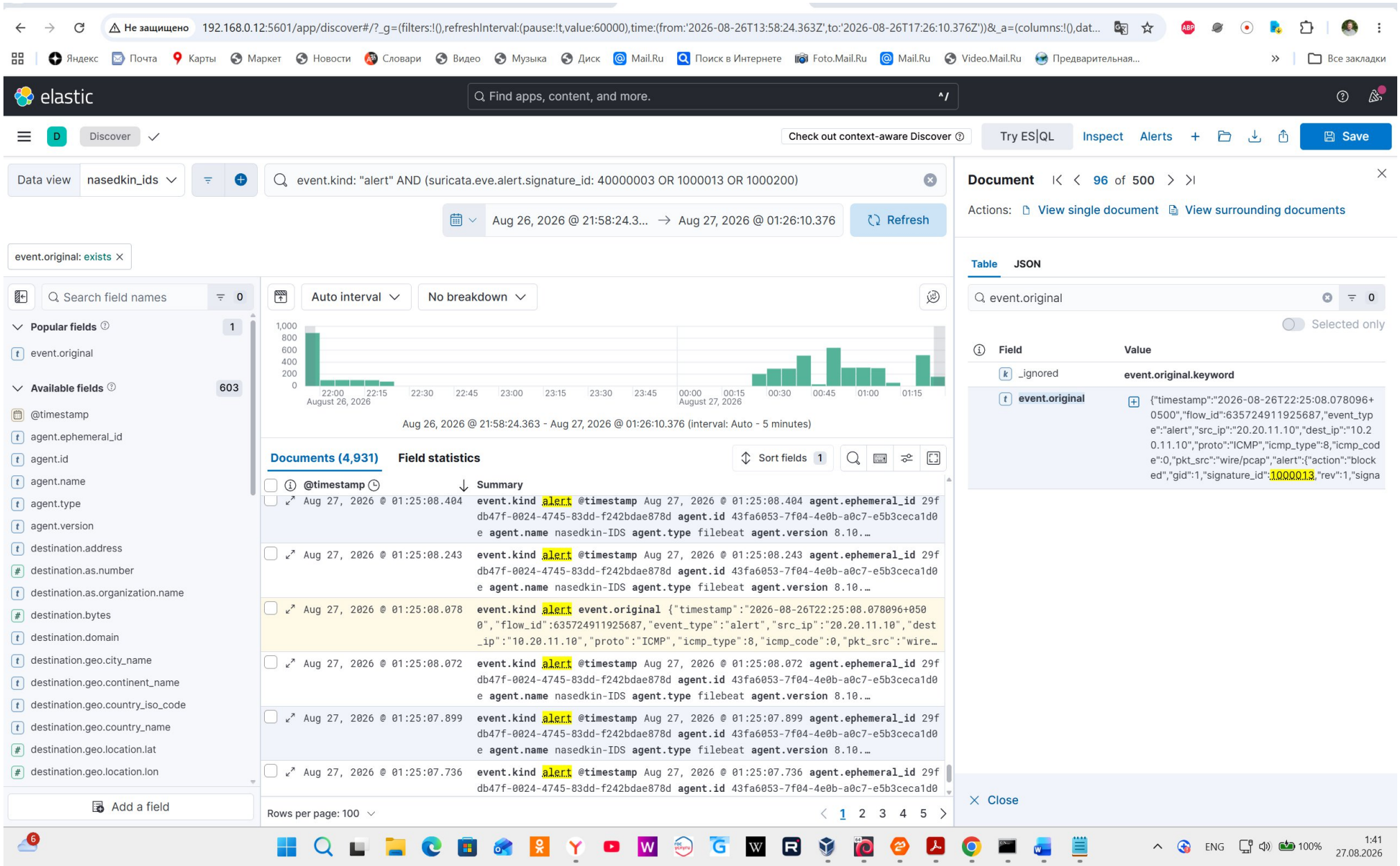
event.kind: "alert" AND (suricata.eve.alert.signature_id: 40000003 OR 1000013 OR 1000200)

Запрос 2 (событие 4740, блокировка Name / pavel):

winlog.event_id: 4740 AND winlog.event_data.TargetUserName: "pavel"

Запрос 3 (создание процессов Name2 / pavel2, Sysmon Event ID 1):

winlog.event_id: 1 AND winlog.user_name: "nasedkin-win\pavel2"



Скриншот №7 – ELK: сигнатура Suricata «1000013» (часть 1)

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2026-08-26T13:58:24.363Z',to:'2026-08-26T17:26:10.376Z'))&_a=(columns:!(suric...

Яндекс Почта Карты Маркет Новости Словари Видео Музыка Диск Mail.Ru Поиск в Интернете Foto.Mail.Ru Mail.Ru Video.Mail.Ru Предварительная... Все закладки

elastic | Find apps, content, and more. | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | Save

Data view: nasedkin_ids

event.kind: "alert" AND (suricata.eve.alert.signature_id: 40000003 OR 1000013 OR 1000200)

Aug 26, 2026 @ 21:58:24.3... → Aug 27, 2026 @ 01:26:10.376 | Refresh

Search field names

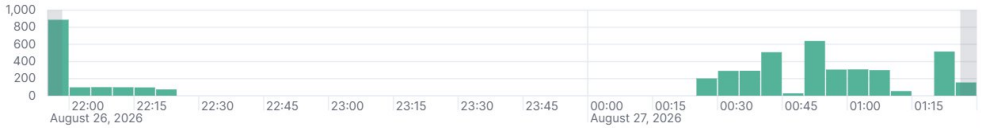
Selected fields 1
- suricata.eve.alert.signature

Popular fields 3
- suricata.eve.alert.signature_id
- event.original
- suricata.eve.alert.signature

Available fields 603
- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- destination.address
- destination.as.number
- destination.as.organization.name
- destination.bytes
- destination.domain
- destination.geo.city_name
- destination.geo.continent_name
- destination.geo.country_iso_code

Add a field

Auto interval | No breakdown



Aug 26, 2026 @ 21:58:24.363 - Aug 27, 2026 @ 01:26:10.376 (interval: Auto - 5 minutes)

Documents (4,931) | Field statistics | Columns 2 | Sort fields 1

@timestamp	suricata.eve.alert.signature
Aug 27, 2026 @ 01:26:10.376	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:26:09.376	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:26:08.372	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:26:07.120	IPS: Block Ping (DoS)
Aug 27, 2026 @ 01:26:06.100	IPS: Block Ping (DoS)
Aug 27, 2026 @ 01:26:05.071	IPS: Block Ping (DoS)

Rows per page: 100 | 1 2 3 4 5

Document 4 of 500

Actions: View single document | View surrounding documents

Table | JSON

Search field names or values | Selected only

Field	Value
suricata.eve.alert.gid	1
suricata.eve.alert.rev	1
suricata.eve.alert.signature	IPS: Block Ping (DoS)
suricata.eve.alert.signature_id	1,000,013
suricata.eve.direction	to_server
suricata.eve.event_type	alert
suricata.eve.flow_id	635724911925687
suricata.eve.flow.dest_ip	10.20.11.10
suricata.eve.flow.src_ip	20.20.11.10
suricata.eve.icmp_code	0

Rows per page: 100 | 1

Close

ENG 100% 1:51 27.08.2026

Скриншот №8 – ELK: сигнатура Suricata «1000013» (часть 2)

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2026-08-26T13:58:24.363Z',to:'2026-08-26T17:26:10.376Z'))&_a=(columns:!(),dat...

Яндекс Почта Карты Маркет Новости Словари Видео Музыка Диск Mail.Ru Поиск в Интернете Foto.Mail.Ru Mail.Ru Video.Mail.Ru Предварительная... Все закладки

elastic | Find apps, content, and more. | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | Save

Data view: nasedkin_ids

event.kind: "alert" AND (suricata.eve.alert.signature_id: 40000003 OR 1000013 OR 1000200)

Aug 26, 2026 @ 21:58:24.3... → Aug 27, 2026 @ 01:26:10.376 | Refresh

Search field names

Popular fields 2

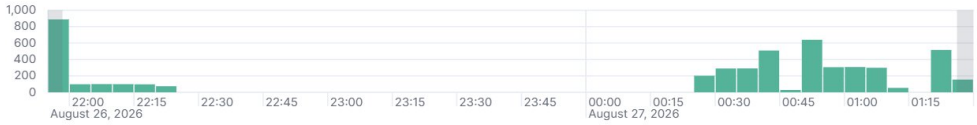
- suricata.eve.alert.signature_id
- event.original

Available fields 603

- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- destination.address
- destination.as.number
- destination.as.organization.name
- destination.bytes
- destination.domain
- destination.geo.city_name
- destination.geo.continent_name
- destination.geo.country_iso_code
- destination.geo.country_name
- destination.geo.location.lat
- destination.geo.location.lon
- destination.geo.region_iso_code

Add a field

Auto interval | No breakdown



Aug 26, 2026 @ 21:58:24.363 - Aug 27, 2026 @ 01:26:10.376 (interval: Auto - 5 minutes)

Documents (4,931) | Field statistics | Sort fields 1

@timestamp	Summary
Aug 27, 2026 @ 01:26:10.376	event.kind alert @timestamp Aug 27, 2026 @ 01:26:10.376 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:26:09.376	event.kind alert @timestamp Aug 27, 2026 @ 01:26:09.376 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:26:08.372	event.kind alert @timestamp Aug 27, 2026 @ 01:26:08.372 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:26:07.120	event.kind alert event.original {"timestamp":"2026-08-26T22:26:07.120089+0500","flow_id":635724911925687,"event_type":"alert","src_ip":"20.20.11.10","dest_ip":"10.20.11.10","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire…
Aug 27, 2026 @ 01:26:06.100	event.kind alert event.original {"timestamp":"2026-08-26T22:26:06.100580+0500","flow_id":635724911925687,"event_type":"alert","src_ip":"20.20.11.10","dest_ip":"10.20.11.10","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire…
Aug 27, 2026 @ 01:26:05.071	event.kind alert event.original {"timestamp":"2026-08-26T22:26:05.071238+0500","flow_id":635724911925687,"event_type":"alert","src_ip":"20.20.11.10","dest_ip":"10.20.11.10","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire…

Rows per page: 100 | 1 2 3 4 5

Document 470 of 500

Actions: View single document | View surrounding documents

Table | JSON

Search field names or values | Selected only

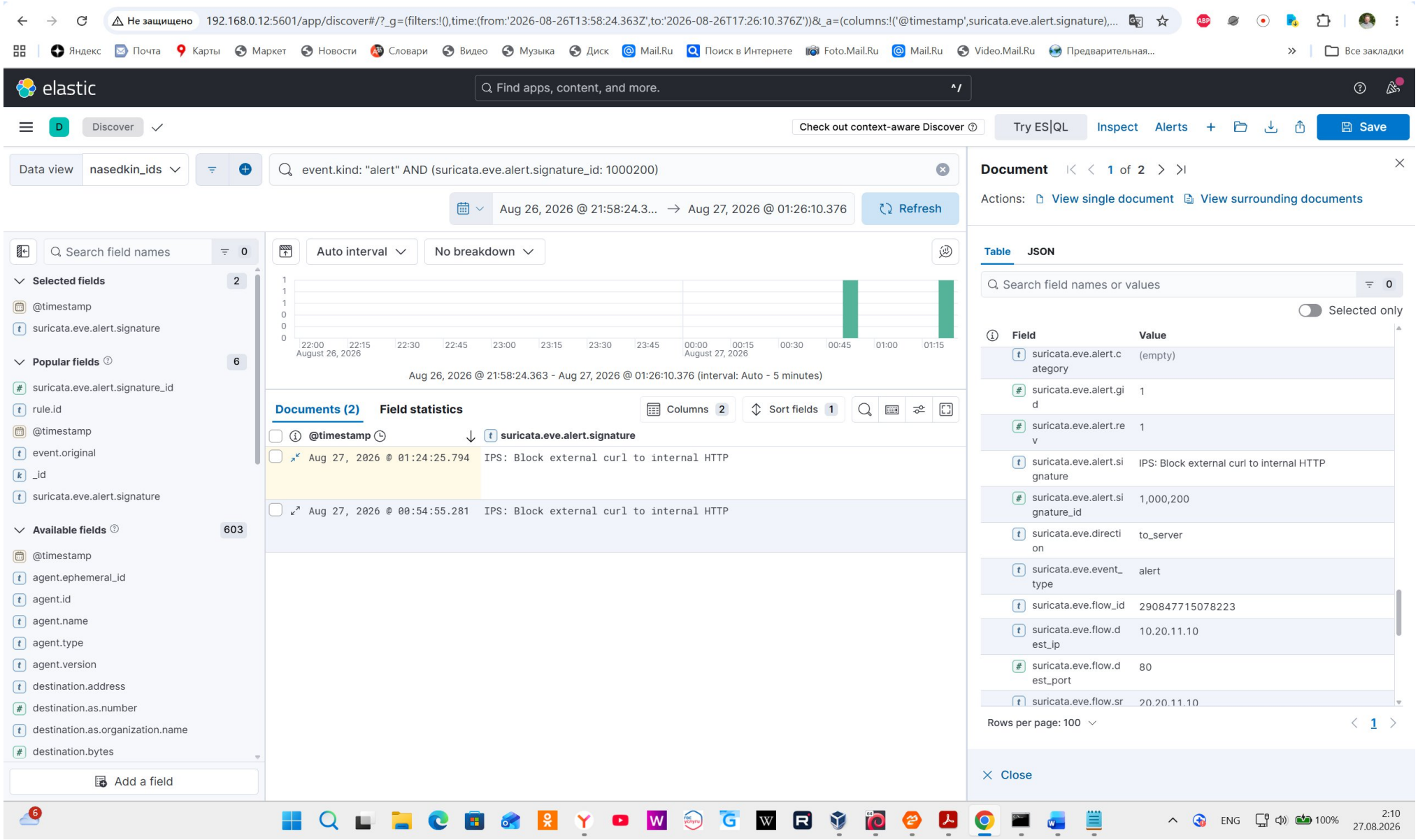
Field	Value
source.geo.location.lon	-97.822
source.ip	20.20.11.10
source.packets	3
source.port	58,970
suricata.eve.alert.category	(empty)
suricata.eve.alert.gid	1
suricata.eve.alert.rev	1
suricata.eve.alert.signature	IPS: Block external curl to internal HTTP
suricata.eve.alert.signature_id	1,000,200
suricata.eve.direction	to_server
suricata.eve.event_type	alert

Rows per page: 100 | 1

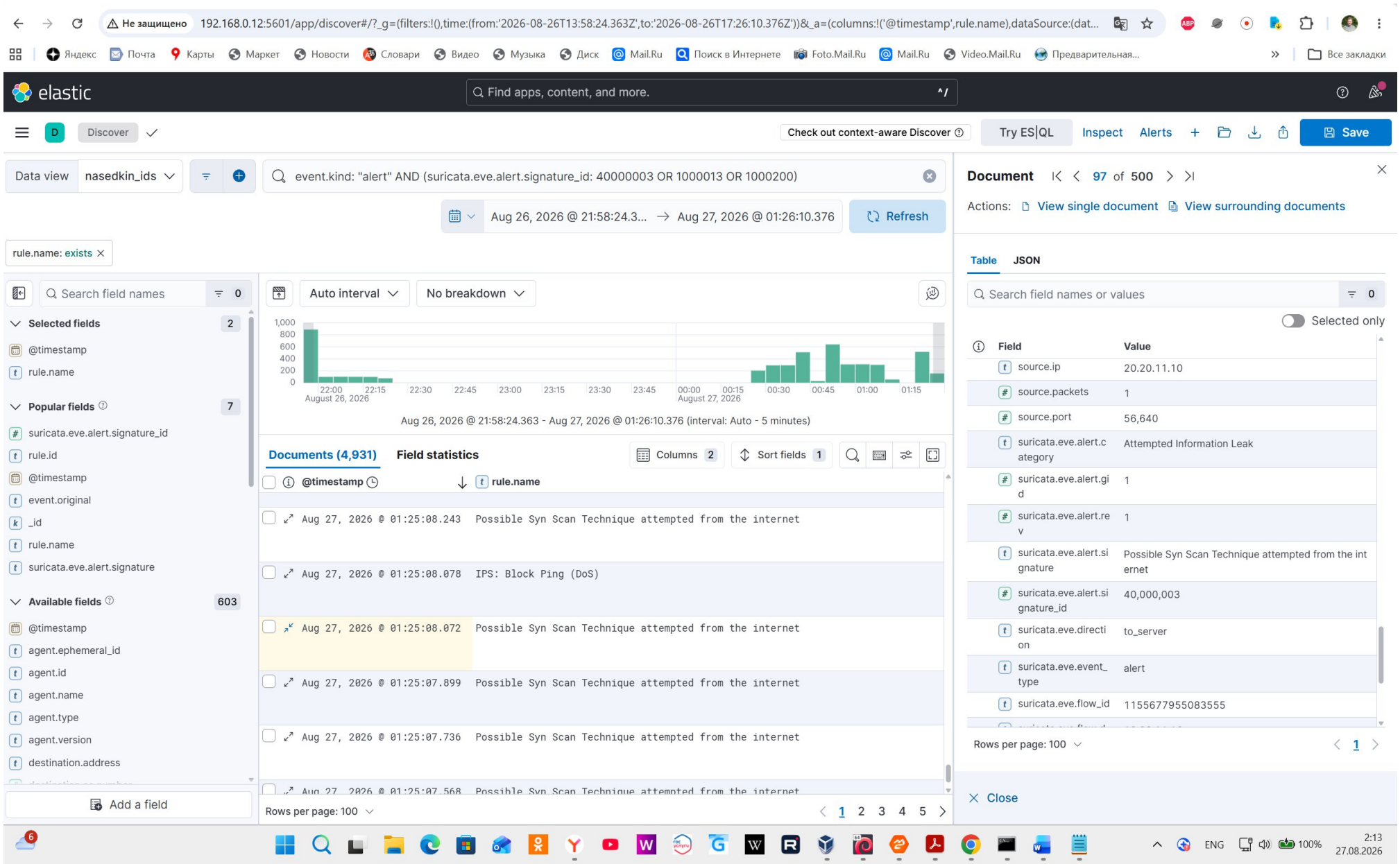
Close

ENG 100% 1:49 27.08.2026

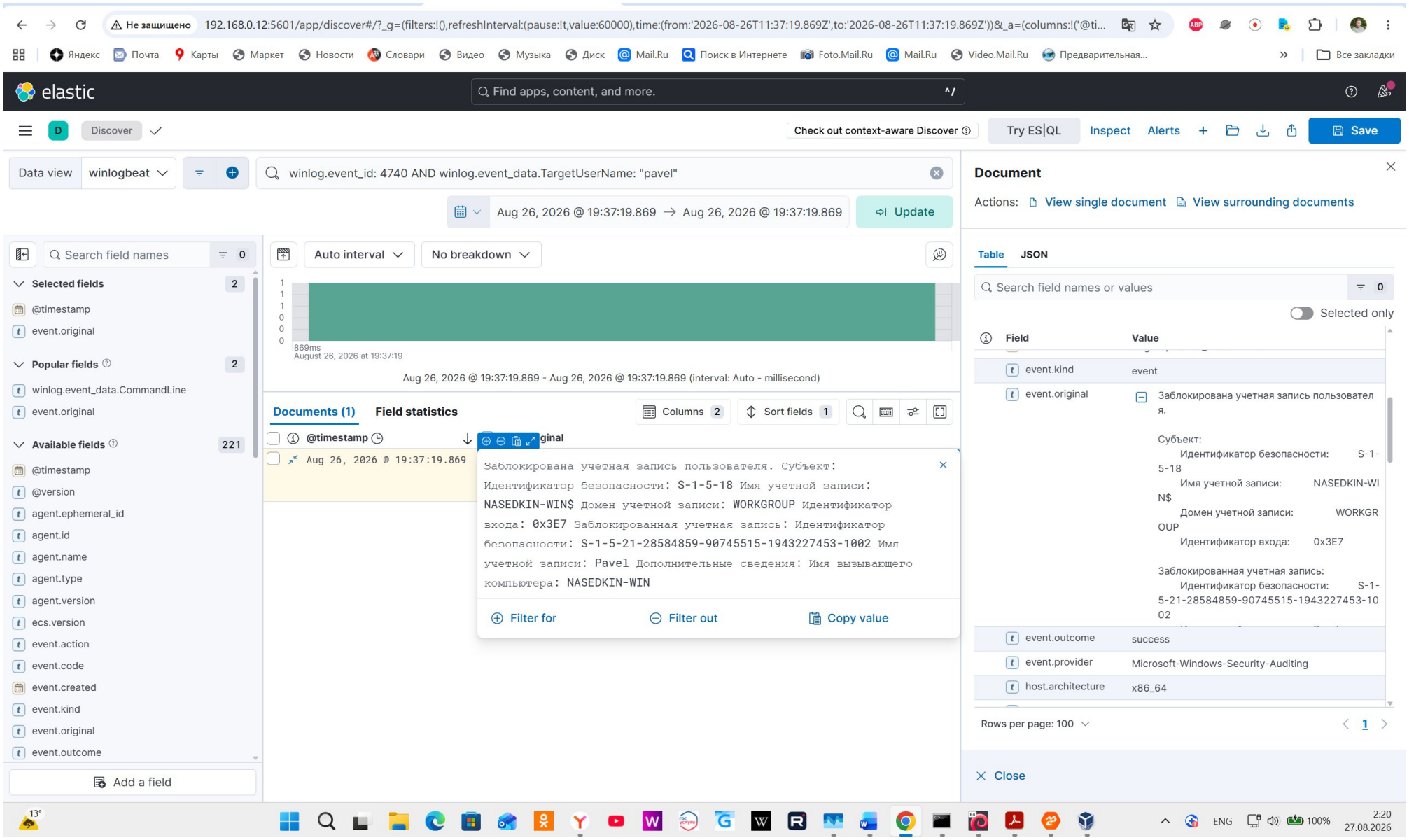
Скриншот №9 – ELK: сигнатура Suricata «1000200» (часть 1)



Скриншот №10 – ELK: сигнатура Suricata «1000200» (часть 2)



Скриншот №11 – ELK: сигнатура Suricata «40000003»



Скриншот №12 – Событие 4740, блокировка Name / pavel

Не защищено 192.168.0.12:5601/app/discover#/?_g=(time:(from:'2026-08-26T11:25:25.746Z',to:'2026-08-26T13:25:27.442Z'))&_a=(columns:!('@timestamp',winlog.event_data.CommandLine),d...

elastic | Find apps, content, and more. | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | Save

Data view: winlogbeat

winlog.event_id: 1 AND winlog.event_data.User: "nasedkin-win\pavel2"

Aug 26, 2026 @ 19:25:25.7... → Aug 26, 2026 @ 21:25:27.442 | Refresh

Search field names

Selected fields 2
- @timestamp
- winlog.event_data.CommandLine

Popular fields 2
- winlog.event_data.CommandLine
- event.original

Available fields 221
- @timestamp
- @version
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- ecs.version
- event.action
- event.code
- event.created
- event.kind
- event.original
- event.outcome

Add a field

Auto interval | No breakdown

Aug 26, 2026 @ 19:25:25.746 - Aug 26, 2026 @ 21:25:27.442 (interval: Auto - minute)

Documents (60) | Field statistics | Columns 2 | Sort fields 1

@timestamp	winlog.event_data.CommandLine
Aug 26, 2026 @ 19:49:42.639	"C:\Windows\system32\mmc.exe" "C:\Windows\system32\eventvwr.msc" /s
Aug 26, 2026 @ 19:47:22.594	ssh user@10.20.11.10
Aug 26, 2026 @ 19:47:01.768	whoami
Aug 26, 2026 @ 19:46:54.924	ipconfig
Aug 26, 2026 @ 19:46:34.736	ping 10.20.11.10
Aug 26, 2026 @ 19:46:25.704	ping ping 10.20.11.10

Rows per page: 100 | 1

Document 3 of 60

Actions: View single document | View surrounding documents

Table | JSON

com | Selected only

Field	Value
event.original	Process Create: RuleName: - UtcTime: 2026-08-26 13:02:15.809 ProcessGuid: {821b00f7-e3d7-6a8e-5f04-000000000e00} ProcessId: 1768

Close

Скриншот №13 – Создание процессов Name2 / pavel2, Sysmon Event ID 1

Заключение

В ходе выполнения домашней работы №1 была успешно развёрнута и настроена комплексная система мониторинга и защиты сетевой инфраструктуры на базе Suricata IDS/IPS и ELK Stack, а также организована централизованная регистрация событий безопасности с Windows-хоста.

В соответствии с заданием были выполнены следующие этапы:

- Собрана сетевая топология из пяти узлов (SRV, ELK, IDS, HACK, WIN) с двумя изолированными подсетями (10.20.11.0/24 и 20.20.11.0/24) и настроена маршрутизация через IDS.
- На сервере SRV установлены и настроены службы SSH и HTTP.
- На сервере ELK развёрнут ELK Stack (Elasticsearch, Logstash, Kibana) и настроен Metricbeat для мониторинга Elasticsearch.
- На IDS установлена и настроена Suricata в режиме IPS с использованием NFQUEUE. Добавлены три кастомные сигнатуры: детектирование SYN-сканирования, ICMP-запросов с пакетами >1000 байт и HTTP-запросов с User-Agent curl.
- На IDS установлен Filebeat, настроенный на отправку событий Suricata в Elasticsearch.
- На Windows-машине WIN созданы пользователи Pavel и Pavel2. Смоделированы инциденты: блокировка учётной записи Pavel после трёх неудачных попыток входа (событие 4740) и запуск команд ipconfig, whoami, ping, ssh пользователем Pavel2.
- На WIN установлены Sysmon (с конфигурацией SwiftOnSecurity) и Winlogbeat, настроенные на отправку событий Security и Sysmon в ELK через Logstash.
- Проведено тестирование с атакующей машины HACK (nmap -sS, ping -s 1024, curl). Все три кастомные сигнатуры Suricata сработали в режиме IPS (действие drop).
- В Kibana созданы Data Views и выполнены запросы по событиям Suricata, Security (4740) и Sysmon (Event ID 1), что подтверждает корректную работу всей системы.

Все скриншоты, подтверждающие выполнение задания, собраны и подписаны в отчёте. Таким образом, цели и задачи работы полностью достигнуты. Полученные

навыки могут быть применены при построении систем мониторинга и защиты корпоративных сетей с централизованным сбором событий безопасности.

Список использованных источников

1. Официальная документация Suricata. — URL: https://suricata.io/documentation/ (дата обращения: 25.08.2026).
2. Официальная документация Elastic Stack (Elasticsearch, Logstash, Kibana, Metricbeat, Filebeat). — URL: https://www.elastic.co/guide/index.html (дата обращения: 25.08.2026).
3. Документация по настройке rsyslog. — URL: https://www.rsyslog.com/doc/ (дата обращения: 25.08.2026).
4. Руководство по iptables (netfilter). — URL: https://www.netfilter.org/documentation/ (дата обращения: 25.08.2026).
5. Официальный сайт nmap. — URL: https://nmap.org/docs.html (дата обращения: 25.08.2026).
6. Sysinternals Sysmon. — URL: https://learn.microsoft.com/ru-ru/sysinternals/downloads/sysmon (дата обращения: 25.08.2026).
7. Конфигурация Sysmon от SwiftOnSecurity. — URL: https://github.com/SwiftOnSecurity/sysmon-config (дата обращения: 25.08.2026).
8. Шабалин А.М. Материалы лекций и методические указания по курсу «Администрирование СЗИ». — ОАНО ДПО «ВЫШТЕХ», 2026.
9. Домашнее задание №1 (файл lab1.pdf), предоставленное преподавателем. — 2026.

Дата составления отчёта: «27» августа 2026 г.

Подпись студента: _____ (Наседкин П.Н.)

Наседкин Павел Николаевич

Подписано цифровой подписью: Наседкин Павел Николаевич
DN: c=RU, st=Иркутская область, l=Иркутск, o=ФГБОУ ВО ИрГУПС, ou=126714, cn=Наседкин Павел Николаевич
Дата: 2026.08.27 05:43:49 +08'00'

ПРИЛОЖЕНИЕ А

ВЫПОЛНЕНИЕ ЗАДАНИЯ

ЭТАП 1. СОЗДАНИЕ И НАСТРОЙКА ВИРТУАЛЬНЫХ МАШИН

VirtualBox: создаём5 ВМ (Debian 12 – для SRV, ELK, IDS; Kali – для HACK; Windows 10/11 – для WIN).

Настраиваем адаптеры для IDS:

- intnet1 – 10.20.11.1/24 (без DHCP)
- intnet2 – 20.20.11.1/24 (без DHCP)

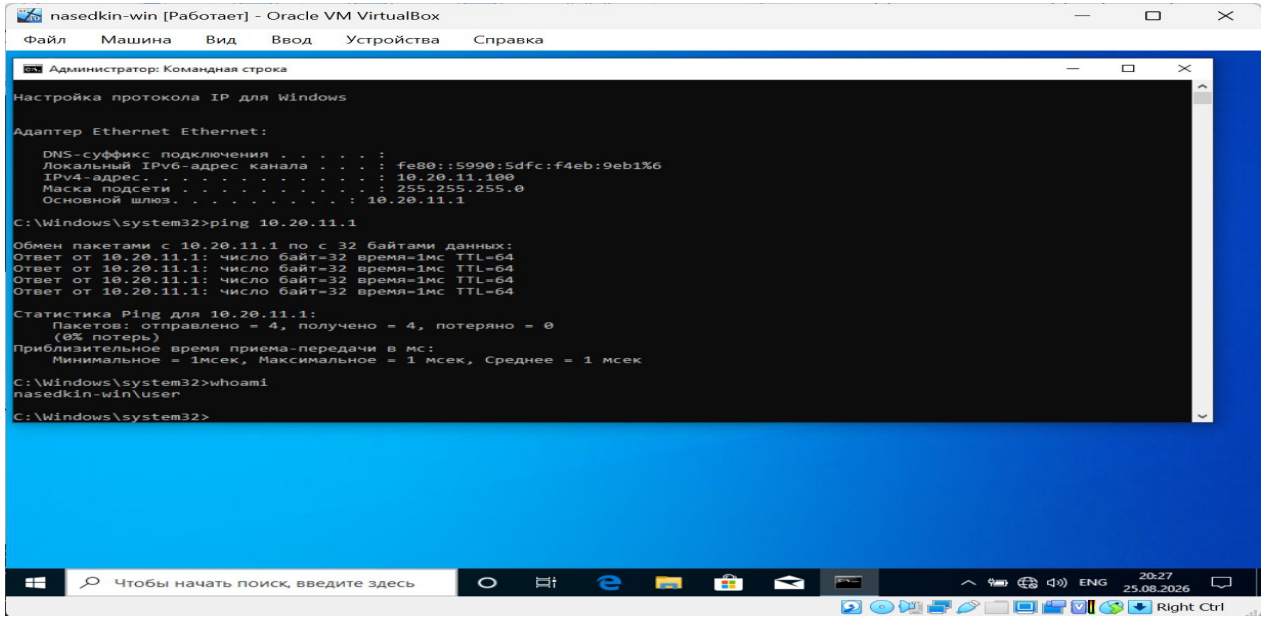
На всех Linux-ВМ назначим статические IP через /etc/network/interfaces (пример для IDS):

```
user@nasedkin-IDS: ~
  GNU nano 7.2                                  /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto enp0s3
iface enp0s3 inet static
address 10.20.11.1/24

auto enp0s8
iface enp0s8 inet static
address 20.20.11.1/24

auto enp0s9
iface enp0s9 inet dhcp

auto enp0s10
iface enp0s10 inet dhcp
```

```
user@nasedkin-elk: ~
  GNU nano 7.2                          /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto enp0s3
iface enp0s3 inet static
address 10.20.11.20/24
gateway 10.20.11.1

auto enp0s8
iface enp0s8 inet dhcp

auto enp0s9
iface enp0s9 inet dhcp
```

```
user@nasedkin-srv: ~
  GNU nano 8.4                                  /etc/network/interfaces
# This file describes the network interfaces available on your system and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
 iface lo inet loopback

# The primary network interface
auto enp0s3
 iface enp0s3 inet static
    address 10.20.11.10
    netmask 255.255.255.0
    gateway 10.20.11.1
    up ip route add 20.20.11.0/24 via 10.20.11.1 dev enp0s3


# This is an autoconfigured IPv6 interface
 iface enp0s3 inet6 auto


auto enp0s8
 iface enp0s8 inet dhcp
    dns-nameservers 8.8.8.8 1.1.1.1


auto enp0s9
 iface enp0s9 inet static
    address 192.168.0.21
    netmask 255.255.255.0
```

На Windows настроим IP 10.20.11.100/24, шлюз 10.20.11.1, DNS можно не указывать.



На IDS включим IP-форвардинг:

bash

sudo sysctl -w net.ipv4.ip_forward=1

echo "net.ipv4.ip_forward=1" | sudo tee -a /etc/sysctl.conf

user@nasedkin-IDS: ~

```
root@nasedkin-IDS:~# nano /etc/network/interfaces
root@nasedkin-IDS:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@nasedkin-IDS:~# echo "net.ipv4.ip_forward=1" | sudo tee -a /etc/sysctl.conf
-bash: sudo: command not found
root@nasedkin-IDS:~# echo "net.ipv4.ip_forward=1" | tee -a /etc/sysctl.conf
net.ipv4.ip_forward=1
root@nasedkin-IDS:~#
```

Проверка: с HACK (20.20.11.10) выполните ping 10.20.11.10 – должен проходить.

nasedkin-hak [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

1 2 3 4 9:04

kali@nasedkin-hak: ~

Session Actions Edit View Help

```
┌──(kali㉿nasedkin-hak)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:63:b0:05 brd ff:ff:ff:ff:ff:ff
    inet 20.20.11.10/24 brd 20.20.11.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe63:b005/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:82:11:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.55/24 brd 192.168.0.255 scope global dynamic noprefixroute eth1
       valid_lft 86376sec preferred_lft 75576sec
    inet6 fe80::9c3c:d20c:a06a:7a4a/64 scope link
       valid_lft forever preferred_lft forever

┌──(kali㉿nasedkin-hak)-[~]
└─$ ping 10.20.11.10
PING 10.20.11.10 (10.20.11.10) 56(84) bytes of data.
64 bytes from 10.20.11.10: icmp_seq=1 ttl=63 time=5.42 ms
64 bytes from 10.20.11.10: icmp_seq=2 ttl=63 time=5.49 ms
64 bytes from 10.20.11.10: icmp_seq=3 ttl=63 time=2.64 ms
64 bytes from 10.20.11.10: icmp_seq=4 ttl=63 time=2.86 ms
64 bytes from 10.20.11.10: icmp_seq=5 ttl=63 time=2.69 ms
64 bytes from 10.20.11.10: icmp_seq=6 ttl=63 time=3.68 ms
64 bytes from 10.20.11.10: icmp_seq=7 ttl=63 time=3.38 ms
64 bytes from 10.20.11.10: icmp_seq=8 ttl=63 time=7.09 ms
64 bytes from 10.20.11.10: icmp_seq=9 ttl=63 time=3.95 ms
64 bytes from 10.20.11.10: icmp_seq=10 ttl=63 time=4.18 ms
64 bytes from 10.20.11.10: icmp_seq=11 ttl=63 time=5.00 ms
64 bytes from 10.20.11.10: icmp_seq=12 ttl=63 time=5.71 ms
^C
--- 10.20.11.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11017ms
rtt min/avg/max/mdev = 2.638/4.339/7.093/1.345 ms

┌──(kali㉿nasedkin-hak)-[~]
└─$
```

Right Ctrl

Проверка связанности:

```
user@nasedkin-IDS: ~
root@nasedkin-IDS:~# ping -c 4 10.20.11.10
PING 10.20.11.10 (10.20.11.10) 56(84) bytes of data.
64 bytes from 10.20.11.10: icmp_seq=1 ttl=64 time=1.71 ms
64 bytes from 10.20.11.10: icmp_seq=2 ttl=64 time=1.46 ms
64 bytes from 10.20.11.10: icmp_seq=3 ttl=64 time=1.56 ms
64 bytes from 10.20.11.10: icmp_seq=4 ttl=64 time=2.96 ms

--- 10.20.11.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3027ms
rtt min/avg/max/mdev = 1.459/1.921/2.962/0.607 ms
root@nasedkin-IDS:~# ping -c 4 10.20.11.20
PING 10.20.11.20 (10.20.11.20) 56(84) bytes of data.
64 bytes from 10.20.11.20: icmp_seq=1 ttl=64 time=2.57 ms
64 bytes from 10.20.11.20: icmp_seq=2 ttl=64 time=2.12 ms
64 bytes from 10.20.11.20: icmp_seq=3 ttl=64 time=1.71 ms
64 bytes from 10.20.11.20: icmp_seq=4 ttl=64 time=2.39 ms

--- 10.20.11.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3096ms
rtt min/avg/max/mdev = 1.714/2.198/2.572/0.322 ms
root@nasedkin-IDS:~# ping -c 4 10.20.11.100
PING 10.20.11.100 (10.20.11.100) 56(84) bytes of data.
64 bytes from 10.20.11.100: icmp_seq=1 ttl=128 time=2.85 ms
64 bytes from 10.20.11.100: icmp_seq=2 ttl=128 time=8.73 ms
64 bytes from 10.20.11.100: icmp_seq=3 ttl=128 time=2.29 ms
64 bytes from 10.20.11.100: icmp_seq=4 ttl=128 time=1.83 ms

--- 10.20.11.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3025ms
rtt min/avg/max/mdev = 1.826/3.923/8.726/2.796 ms
root@nasedkin-IDS:~# ping -c 4 20.20.11.10
PING 20.20.11.10 (20.20.11.10) 56(84) bytes of data.
64 bytes from 20.20.11.10: icmp_seq=1 ttl=64 time=2.44 ms
64 bytes from 20.20.11.10: icmp_seq=2 ttl=64 time=1.27 ms
64 bytes from 20.20.11.10: icmp_seq=3 ttl=64 time=1.62 ms
64 bytes from 20.20.11.10: icmp_seq=4 ttl=64 time=2.08 ms

--- 20.20.11.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3030ms
rtt min/avg/max/mdev = 1.267/1.849/2.437/0.443 ms
root@nasedkin-IDS:~#
```

ЭТАП 2. НАСТРОЙКА СЕРВЕРА SRV (SSH + HTTP)

На nasedkin-srv (10.20.11.10):

bash

sudo apt update

sudo apt install openssh-server apache2 -y

sudo systemctl enable --now ssh apache2

```
root@nasedkin-srv:~# systemctl start apache2
root@nasedkin-srv:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Tue 2026-08-25 21:35:03 +08; 34s ago
 Invocation: b367a2bd43494fc4ae151fd69800a79a
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 1783 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 1786 (apache2)
      Tasks: 55 (limit: 1093)
     Memory: 5M (peak: 5.3M)
        CPU: 76ms
     CGroup: /system.slice/apache2.service
             ├─1786 /usr/sbin/apache2 -k start
             ├─1788 /usr/sbin/apache2 -k start
             └─1789 /usr/sbin/apache2 -k start

Aug 25 21:35:03 nasedkin-srv systemd[1]: Starting apache2.service - The Apache HTTP Server...
Aug 25 21:35:03 nasedkin-srv apachectl[1785]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, us>
Aug 25 21:35:03 nasedkin-srv systemd[1]: Started apache2.service - The Apache HTTP Server.

root@nasedkin-srv:~#
```

Проверка: curl http://10.20.11.10 должен отдать страницу Apache2.

```
root@nasedkin-srv:~# curl http://10.20.11.10
<h1>WEB2 - Nasedkin (10.20.11.30)</h1>
root@nasedkin-srv:~#
```

ЭТАП 3. НАСТРОЙКА ELK STACK + METRICBEAT

На nasedkin-elk (10.20.11.20):

3.1. Установка Elasticsearch, Logstash, Kibana

bash

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list
sudo apt update
sudo apt install elasticsearch logstash kibana -y
```

3.2. Запуск служб

bash

```
sudo systemctl enable --now elasticsearch
sudo systemctl enable --now kibana
```

3.3. Проверка Elasticsearch

bash

```
curl -X GET "localhost:9200"   # должна прийти JSON-информация
```

user@nasedkin-elk: ~

```
root@nasedkin-elk:~# curl -X GET "localhost:9200"
{
  "name" : "nasedkin-elk",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "ofYUEPYAQ8q4UNsimnNdGA",
  "version" : {
    "number" : "8.19.19",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "0b6bd198d583b8566336c0db61afb70b346c6882",
    "build_date" : "2026-07-15T22:15:58.852563788Z",
    "build_snapshot" : false,
    "lucene_version" : "9.12.2",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
root@nasedkin-elk:~# sudo systemctl status elasticsearch
-bash: sudo: command not found
root@nasedkin-elk:~# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)
     Active: active (running) since Tue 2026-08-25 17:49:42 +05; 51min ago
       Docs: https://www.elastic.co
   Main PID: 647 (java)
      Tasks: 96 (limit: 3513)
     Memory: 1.0G
        CPU: 5min 28.739s
     CGroup: /system.slice/elasticsearch.service
             ├─647 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli>
             ├─726 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des>
             └─751 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/contro>

Aug 25 17:48:07 nasedkin-elk systemd[1]: Starting elasticsearch.service - Elasticsearch...
Aug 25 17:49:42 nasedkin-elk systemd[1]: Started elasticsearch.service - Elasticsearch.
lines 1-15/15 (END)
```

```
root@nasedkin-elk:~# systemctl sta
start   status
root@nasedkin-elk:~# systemctl status kibana.service
● kibana.service - Kibana
     Loaded: loaded (/lib/systemd/system/kibana.service; enabled; preset: enabled)
     Active: active (running) since Tue 2026-08-25 17:48:07 +05; 1h 1min ago
       Docs: https://www.elastic.co
   Main PID: 648 (MainThread)
      Tasks: 11 (limit: 3513)
     Memory: 623.6M
        CPU: 2min 58.888s
     CGroup: /system.slice/kibana.service
             └─648 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/bin/../>

Aug 25 18:46:11 nasedkin-elk kibana[648]:     at Timeout._onTimeout (/usr/share/kibana/node_m>
Aug 25 18:46:11 nasedkin-elk kibana[648]:     at listOnTimeout (node:internal/timers:605:17)
Aug 25 18:46:11 nasedkin-elk kibana[648]:     at processTimers (node:internal/timers:541:7)
Aug 25 18:46:11 nasedkin-elk kibana[648]:     at Axios.request (/usr/share/kibana/node_module>
Aug 25 18:46:11 nasedkin-elk kibana[648]:     at processTicksAndRejections (node:internal/pro>
Aug 25 18:46:11 nasedkin-elk kibana[648]:     at TelemetryEventsSender.isTelemetryServicesRea>
Aug 25 18:46:11 nasedkin-elk kibana[648]:     at SecurityTelemetryTask.runTask (/usr/share/ki>
Aug 25 18:46:11 nasedkin-elk kibana[648]:     at Object.run (/usr/share/kibana/node_modules/@>
Aug 25 18:46:11 nasedkin-elk kibana[648]:     at TaskManagerRunner.run (/usr/share/kibana/nod>
Aug 25 18:46:11 nasedkin-elk kibana[648]: [2026-08-25T18:46:11.334+05:00][INFO ][plugins.secu>
lines 1-21/21 (END)
```

user@nasedkin-elk: ~

```
root@nasedkin-elk:~# systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/lib/systemd/system/logstash.service; enabled; preset: enabled)
     Active: active (running) since Tue 2026-08-25 17:48:01 +05; 1h 16min ago
   Main PID: 356 (java)
      Tasks: 44 (limit: 3513)
     Memory: 994.9M
        CPU: 5min 14.322s
     CGroup: /system.slice/logstash.service
             └─356 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.headless=true >

Aug 25 17:52:02 nasedkin-elk logstash[356]: {
Aug 25 17:52:02 nasedkin-elk logstash[356]:       "@version" => "1",
Aug 25 17:52:02 nasedkin-elk logstash[356]:     "@timestamp" => 2026-08-25T12:51:56.8523152>
Aug 25 17:52:02 nasedkin-elk logstash[356]:           "host" => {
Aug 25 17:52:02 nasedkin-elk logstash[356]:         "name" => "nasedkin-elk"
Aug 25 17:52:02 nasedkin-elk logstash[356]:     },
Aug 25 17:52:02 nasedkin-elk logstash[356]:            "log" => {
Aug 25 17:52:02 nasedkin-elk logstash[356]:         "file" => {
Aug 25 17:52:02 nasedkin-elk logstash[356]:             "path" => "/var/log/suricata/nasedk>
Aug 25 17:52:02 nasedkin-elk logstash[356]:         }
lines 1-20/20 (END)
```

3.4. Установка Metricbeat

1. Установка правильной таймзоны (Иркутск, UTC+8)

bash

timedatectl set-timezone Asia/Irkutsk

timedatectl status # *проверить, что Local time теперь +08*

2. Принудительная синхронизация времени (NTP)

bash

timedatectl set-ntp true

systemctl restart systemd-timesyncd # *перезапустить синхронизацию, если активна*

timedatectl status # *убедиться, что System clock synchronized: yes*

3. Установка gnupg (если отсутствует)

bash

apt install gnupg -y

4. Удаление старого GPG-ключа Elastic (если был)

bash

rm -f /usr/share/keyrings/elastic-keyring.gpg

5. Скачивание и импорт свежего GPG-ключа

bash

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | gpg --dearmor -o /usr/share/keyrings/elastic-keyring.gpg

6. Проверка, что ключ создан

bash

ls -l /usr/share/keyrings/elastic-keyring.gpg

7. Создание/правка файла репозитория Elastic

bash

echo "deb [signed-by=/usr/share/keyrings/elastic-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" > /etc/apt/sources.list.d/elastic-8.x.list

8. Обновление списка пакетов

bash

apt update

Если ошибка 403 сохраняется – временно замените https:// на http:// в файле выше и повторите apt update.

Шаг 1. Установка Metricbeat

bash

sudo apt install metricbeat -y

sudo metricbeat modules enable elasticsearch-xpack

sudo systemctl enable --now metricbeat

```
Full Text Search... Done
metricbeat/stable 8.19.19 amd64
  Metricbeat is a lightweight shipper for metrics.

metricbeat-fips/stable 8.19.19 amd64
  Metricbeat is a lightweight shipper for metrics.

root@nasedkin-elk:~#
```

```
root@nasedkin-elk:~#  timedatectl set-timezone Asia/Irkutsk
root@nasedkin-elk:~# timedatectl status
               Local time: Wed 2026-08-26 11:33:03 +08
           Universal time: Wed 2026-08-26 03:33:03 UTC
                 RTC time: Wed 2026-08-26 03:33:04
                Time zone: Asia/Irkutsk (+08, +0800)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
root@nasedkin-elk:~#
```

Шаг 2. Настройка подключения к Elasticsearch

Отредактируем конфигурационный файл /etc/metricbeat/metricbeat.yml, чтобы указать адрес Elasticsearch.

Способ А (через sed **— быстро и надёжно):**

bash

```
sudo sed -i 's#output.elasticsearch:#output.elasticsearch:\n  hosts: ["localhost:9200"]#' /etc/metricbeat/metricbeat.yml
```

Способ Б (вручную через редактор):

bash

```
sudo nano /etc/metricbeat/metricbeat.yml
```

Найдём строку #output.elasticsearch: и заменим её на:

yaml

```
output.elasticsearch:
```

hosts: ["localhost:9200"]

Сохраните файл (Ctrl+O, затем Ctrl+X).

Важно: Если наш Elasticsearch слушает на другом IP-адресе (например, если мы настраиваем Metricbeat на отдельной машине), заменим localhost на реальный IP. В нашей топологии Metricbeat и Elasticsearch находятся на одной ВМ (nasedkin-elk), поэтому localhost подходит идеально.

```
user@nasedkin-elk: ~
  GNU nano 7.2                    /etc/metricbeat/metricbeat.yml
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

# ================================= Outputs =================================

# Configure what output to use when sending the data collected by the beat.

# ---------------------------- Elasticsearch Output ----------------------------
output.elasticsearch:
  hosts: ["localhost:9200"]
  # Array of hosts to connect to.
 # hosts: ["localhost:9200"]

  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom".
  preset: balanced

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"

# ------------------------------ Logstash Output -------------------------------
#output.logstash:
  # The Logstash hosts
  #hosts: ["localhost:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"
```

Шаг 3. Включение модуля для мониторинга Elasticsearch

bash

sudo metricbeat modules enable elasticsearch-xpack

```
user@nasedkin-elk: ~
root@nasedkin-elk:~# nano /etc/metricbeat/metricbeat.yml
root@nasedkin-elk:~# metricbeat modules enable elasticsearch-xpack
Enabled elasticsearch-xpack
root@nasedkin-elk:~#
```

Шаг 4. Настройка дашбордов в Kibana (опционально, но рекомендуется)

bash

sudo metricbeat setup --dashboards

```
root@nasedkin-elk:~# unset http_proxy
metricbeat setup --dashboards -E setup.kibana.host=http://127.0.0.1:5601
Loading dashboards (Kibana must be running and reachable)
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
-bash: syntax error near unexpected token `('
root@nasedkin-elk:~# unset http_proxy
```

Шаг 3.5. Настройка Logstash (приём от Winlogbeat)

На сервере nasedkin-elk (10.20.11.20) выполним следующие команды.

1. Убедимся, что Logstash установлен

bash

systemctl status logstash

Если не установлен — установим (он уже должен быть, т.к. мы ставили ELK Stack). Если не активен — запустим позже.

```
root@nasedkin-elk:~# systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/lib/systemd/system/logstash.service; enabled; preset: enabled)
     Active: active (running) since Tue 2026-08-25 20:48:01 +08; 16h ago
   Main PID: 356 (java)
      Tasks: 44 (limit: 3513)
     Memory: 705.8M
        CPU: 12min 44.749s
     CGroup: /system.slice/logstash.service
             └─356 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.headless=true -D>

Aug 25 20:52:02 nasedkin-elk logstash[356]: {
Aug 25 20:52:02 nasedkin-elk logstash[356]:       "@version" => "1",
Aug 25 20:52:02 nasedkin-elk logstash[356]:     "@timestamp" => 2026-08-25T12:51:56.852315276>
Aug 25 20:52:02 nasedkin-elk logstash[356]:           "host" => {
Aug 25 20:52:02 nasedkin-elk logstash[356]:         "name" => "nasedkin-elk"
Aug 25 20:52:02 nasedkin-elk logstash[356]:     },
Aug 25 20:52:02 nasedkin-elk logstash[356]:            "log" => {
Aug 25 20:52:02 nasedkin-elk logstash[356]:         "file" => {
Aug 25 20:52:02 nasedkin-elk logstash[356]:             "path" => "/var/log/suricata/nasedkin>
Aug 25 20:52:02 nasedkin-elk logstash[356]:         }
lines 1-20/20 (END)
```

2. Создадим конфигурационный файл для приёма от Winlogbeat

Создадим файл /etc/logstash/conf.d/03-winlogbeat-tag.conf со следующим содержимым (используем nano или vim):

bash
```
sudo nano /etc/logstash/conf.d/03-winlogbeat-tag.conf
```

Вставьте:

text
```
input {
  beats {
    port => 5044
  }
}

output {
  if "winagent" in [tags] {
    elasticsearch {
      hosts => ["http://localhost:9200"]
      index => "tag-winlogbeat-%{+YYYY.MM.dd}"
    }
  }
}
```

Сохраним файл (Ctrl+O, Enter, Ctrl+X).

3. Проверим синтаксис конфигурации Logstash

bash
```
sudo -u logstash /usr/share/logstash/bin/logstash --config.test_and_exit -f /etc/logstash/conf.d/
```
либо
```
root@nasedkin-elk:~# /usr/share/logstash/bin/logstash --config.test_and_exit -f /etc/logstash/conf.d/
Using bundled JDK: /usr/share/logstash/jdk
```

Должно быть сообщение об успешной проверке (без ошибок).

```
Выбрать user@nasedkin-elk: ~
ity.
[WARN ] 2026-08-26 14:01:22.176 [main] runner - 'pipeline.buffer.type' setting is not explicit
ly defined.Before moving to 9.x set it to 'heap' and tune heap size upward, or set it to 'dire
ct' to maintain existing behavior.
[INFO ] 2026-08-26 14:01:22.179 [main] runner - Starting Logstash {"logstash.version"=>"8.19.1
9", "jruby.version"=>"jruby 9.4.15.0 (3.1.7) 2026-06-08 6114208a31 OpenJDK 64-Bit Server VM 21
.0.11+10-LTS on 21.0.11+10-LTS +indy +jit [x86_64-linux]"}
[INFO ] 2026-08-26 14:01:22.194 [main] runner - JVM bootstrap flags: [-Xms1g, -Xmx1g, -Djava.a
wt.headless=true, -Dfile.encoding=UTF-8, -Djruby.compile.invokedynamic=true, -XX:+HeapDumpOnOu
tOfMemoryError, -Djava.security.egd=file:/dev/urandom, -Dlog4j2.isThreadContextMapInheritable=
true, -Djruby.regexp.interruptible=true, -Djdk.io.File.enableADS=true, --add-exports=jdk.compi
ler/com.sun.tools.javac.api=ALL-UNNAMED, --add-exports=jdk.compiler/com.sun.tools.javac.file=A
LL-UNNAMED, --add-exports=jdk.compiler/com.sun.tools.javac.parser=ALL-UNNAMED, --add-exports=j
dk.compiler/com.sun.tools.javac.tree=ALL-UNNAMED, --add-exports=jdk.compiler/com.sun.tools.jav
ac.util=ALL-UNNAMED, --add-opens=java.base/java.security=ALL-UNNAMED, --add-opens=java.base/ja
va.io=ALL-UNNAMED, --add-opens=java.base/java.nio.channels=ALL-UNNAMED, --add-opens=java.base/
sun.nio.ch=ALL-UNNAMED, --add-opens=java.management/sun.management=ALL-UNNAMED, -Dio.netty.all
ocator.maxOrder=11]
[INFO ] 2026-08-26 14:01:22.511 [main] StreamReadConstraintsUtil - Jackson default value overr
ide `logstash.jackson.stream-read-constraints.max-string-length` configured to `200000000` (lo
gstash default)
[INFO ] 2026-08-26 14:01:22.511 [main] StreamReadConstraintsUtil - Jackson default value overr
ide `logstash.jackson.stream-read-constraints.max-number-length` configured to `10000` (logsta
sh default)
[INFO ] 2026-08-26 14:01:22.512 [main] StreamReadConstraintsUtil - Jackson default value overr
ide `logstash.jackson.stream-read-constraints.max-nesting-depth` configured to `1000` (logstas
h default)
[WARN ] 2026-08-26 14:01:23.214 [LogStash::Runner] multilocal - Ignoring the 'pipelines.yml' f
ile because modules or command line options are specified
[INFO ] 2026-08-26 14:01:25.103 [LogStash::Runner] Reflections - Reflections took 423 ms to sc
an 1 urls, producing 150 keys and 530 values
[INFO ] 2026-08-26 14:01:27.494 [LogStash::Runner] javapipeline - Pipeline `main` is configure
d with `pipeline.ecs_compatibility: v8` setting. All plugins in this pipeline will default to
 ecs_compatibility => v8` unless explicitly configured otherwise.
Configuration OK
[INFO ] 2026-08-26 14:01:27.498 [LogStash::Runner] runner - Using config.test_and_exit mode. C
onfig Validation Result: OK. Exiting Logstash
root@nasedkin-elk:~# _
```

Скриншоты № …. – в Kibana → Dashboard → [Metricbeat] Elasticsearch.

ЭТАП 4. НАСТРОЙКА SURICATA В РЕЖИМЕ IPS (НА СЕРВЕРЕ IDS)

Выполняется на сервере nasedkin-ids **(10.20.11.1 / 20.20.11.1)**

Шаг 4.1. Установка Suricata

bash
sudo apt update
sudo apt install suricata -y

Проверьте версию:

bash
suricata -V

1. Проверьте, установлена ли Suricata

```
user@nasedkin-IDS:~$ su -
Password:
root@nasedkin-IDS:~# which suricata
/usr/bin/suricata
root@nasedkin-IDS:~# suricata -V
This is Suricata version 7.0.10 RELEASE
root@nasedkin-IDS:~#
```

2. Проверьте статус службы (если запущена как сервис)

```
root@nasedkin-IDS:~# systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/etc/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Wed 2026-08-26 11:55:58 +05; 1min 45s ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
   Main PID: 625 (Suricata-Main)
      Tasks: 10 (limit: 1096)
     Memory: 85.3M
        CPU: 2.750s
     CGroup: /system.slice/suricata.service
             └─625 /usr/bin/suricata -c /etc/suricata/suricata.yaml -q 0 --simulate-ips

Aug 26 11:55:58 nasedkin-IDS systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
Aug 26 11:55:58 nasedkin-IDS suricata[625]: Info: suricata: Setting IPS mode
Aug 26 11:55:58 nasedkin-IDS suricata[625]: i: suricata: This is Suricata version 7.0.10 RELEA>
Aug 26 11:55:59 nasedkin-IDS suricata[625]: i: threads: Threads created -> RX: 1 W: 2 TX: 1 FM>
lines 1-17/17 (END)
```

3. Проверьте, запущен ли процесс Suricata

```
root@nasedkin-IDS:~# ps aux | grep suricata | grep -v grep
root         625  2.3  8.5 696696 83920 ?        Ssl  11:55   0:03 /usr/bin/suricata -c /etc/su
ricata/suricata.yaml -q 0 --simulate-ips
root         672  0.0  0.6  16448  6080 pts/0    T    11:57   0:00 systemctl status suricata
root@nasedkin-IDS:~#
```

Мы уже проверили, что Suricata установлена и запущена, но в режиме `--simulate-ips`, который **не блокирует** трафик. Нам нужно перевести её в полноценный IPS с блокировкой. Для этого выполним дополнительные шаги в рамках **этапа 4**.

Шаг 4.2. Остановка текущего процесса Suricata

Остановим работающий процесс:

bash
```
sudo pkill -f suricata
```

Или через сервис (если он используется):

bash
```
sudo systemctl stop suricata
```

Убедимся, что процесс завершён:

bash
```
ps aux | grep suricata | grep -v grep
```

Если ничего не вывелось — процесс остановлен.

Шаг 4.9. Проверка и настройка iptables для NFQUEUE

Suricata в режиме IPS использует **NFQUEUE** для перехвата трафика из одной сети в другую.

 # Очищаем всё

iptables -F

iptables -t nat -F

 # Единственное правило для IPS

iptables -I FORWARD -j NFQUEUE --queue-num 0

 # Проверяем

iptables -L -nv | grep NFQUEUE

Этап 5. УСТАНОВКА И НАСТРОЙКА FILEBEAT НА IDS

Мы настраиваем Filebeat на сервере IDS (nasedkin-IDS), чтобы он читал логи Suricata (eve.json) и отправлял их в Elasticsearch на сервере ELK (10.20.11.20:9200). Это позволит нам видеть события Suricata в Kibana.

Шаг 5.1. Установка Filebeat

Что делаем: Устанавливаем Filebeat версии 8.10.3 из репозитория Elastic (через Yandex-зеркало, как указано в методичке).

Команды:

bash

echo "deb [trusted=yes] https://mirror.yandex.ru/mirrors/elastic/8/ stable main" | tee /etc/apt/sources.list.d/elastic-8.x.list

apt update

apt install -y filebeat=8.10.3

Почему: Это обеспечивает совместимость с нашим Elasticsearch 8.x и соответствует заданию.

Шаг 5.2. Включение модуля Suricata

Что делаем: Включаем встроенный модуль Filebeat для чтения логов Suricata.

Команда:

bash

filebeat modules enable suricata

Почему: Модуль уже содержит готовую конфигурацию для парсинга eve.json и преобразования событий в формат, понятный Elasticsearch.

Шаг 5.3. Настройка модуля Suricata

Что делаем: Указываем точный путь к файлу eve.json, который генерирует Suricata.

Откроем файл /etc/filebeat/modules.d/suricata.yml:

bash

```
nano /etc/filebeat/modules.d/suricata.yml
```

Приводим содержимое к такому виду:

yaml

```
- module: suricata
  eve:
    enabled: true
    var.paths: ["/var/log/suricata/eve.json"]
```

Почему: Filebeat должен знать, где искать логи. В нашем случае они лежат в стандартной директории Suricata.

Шаг 5.4. Настройка вывода в Elasticsearch

Что делаем: Указываем Filebeat, куда отправлять данные (адрес Elasticsearch на сервере ELK) и какое имя индекса использовать.

Отредактируем файл /etc/filebeat/filebeat.yml:

bash

```
nano /etc/filebeat/filebeat.yml
```

Найдём секцию output.elasticsearch: и настроим:

yaml

```
output.elasticsearch:
  hosts: ["http://10.20.11.20:9200"]
  indices:
    - index: "nasedkin_ids-%{+yyyy.MM.dd}"
```

Если в файле есть другие настройки вывода (например, output.logstash), закомментируем их (поставим # в начале строк).

Почему: События будут отправляться на сервер ELK (порт 9200) и сохраняться в индексы с именем nasedkin_ids-дата. Это соответствует нашему заданию (фамилия + _ids).

Шаг 5.5. Загрузка дашбордов в Kibana (опционально, но рекомендовано)

Что делаем: Загружаем готовые дашборды Filebeat для Suricata, чтобы в Kibana сразу были визуализации.

Команда:

bash

```
filebeat setup --dashboards -E setup.kibana.host=10.20.11.20:5601
```

Почему: Это упростит анализ событий в Kibana. Если дашборды не загрузятся — не страшно, можно будет работать через Discover.

```
systemctl enable --now filebeat
```

ЭТАП 6: НАСТРОЙКА WINDOWS (WIN)

Выполняется на виртуальной машине nasedkin-win (IP: 10.20.11.100) от имени **администратора**.

6.1. Создание пользователей

Откройте **PowerShell от имени администратора** и выполните:

powershell

net user Nasedkin /add

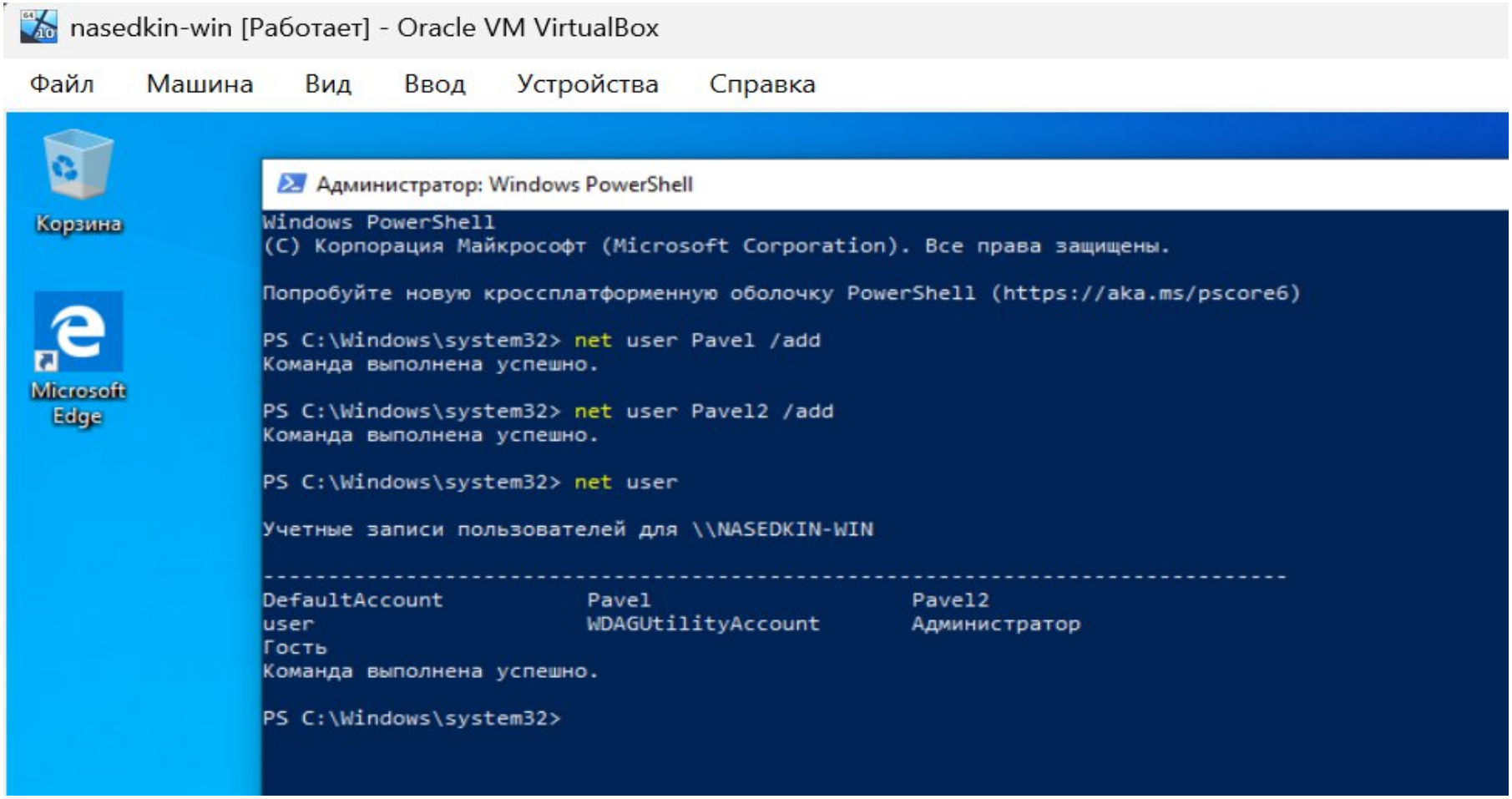
net user Pavel /add

Проверка:

powershell

net user

В списке должны быть Nasedkin и Pavel.



Установка и запуск Winlogbeat (команды из методички)

powershell

cd "C:\Program Files\winlogbeat"

PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-winlogbeat.ps1

Set-Service -Name "winlogbeat" -StartupType automatic

Start-Service -Name "winlogbeat"

Установка Sysmon

В PowerShell (администратор) выполните:

powershell
cd C:\Sysmon
.\Sysmon64.exe -accepteula -i sysmonconfig-export.xml

Проверка:

```
PS C:\Program Files\winlogbeat> Get-Service -Name Sysmon*

Status   Name               DisplayName
------   ----               -----------
Running  Sysmon64           Sysmon64


PS C:\Program Files\winlogbeat> Get-Service -Name winlogbeat

Status   Name               DisplayName
------   ----               -----------
Stopped  winlogbeat         winlogbeat


PS C:\Program Files\winlogbeat>
```

Конфигурация Winlogbeat (winlogbeat.yml) — исправленный вариант

Создал файл C:\Program Files\winlogbeat\winlogbeat.yml с содержимым:

powershell

```
# Создаём резервную копию старого файла
Copy-Item "C:\Program Files\winlogbeat\winlogbeat.yml" "C:\Program Files\winlogbeat\winlogbeat.yml.bak"

# Записываем новый корректный конфиг
@"
######################### Winlogbeat Configuration ##########################

winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h
  - name: System
  - name: Security
    event_id: 4624, 4625, 4688, 4740
  - name: Microsoft-Windows-Sysmon/Operational
    event_id: 1
  - name: Windows PowerShell
    event_id: 400, 403, 600, 800
  - name: Microsoft-Windows-PowerShell/Operational
    event_id: 4103, 4104, 4105, 4106
```

```
tags: ["winagent"]

output.logstash:
  hosts: ["10.20.11.20:5044"]

logging.level: info
logging.to_files: true
logging.files:
  path: C:/Program Files/winlogbeat/logs
  name: winlogbeat
  keepfiles: 150
  permissions: 0644

processors:
  - add_host_metadata:
      when.not.contains.tags: forwarded
"@ | Out-File -FilePath "C:\Program Files\winlogbeat\winlogbeat.yml" -Encoding utf8
```

Проверка синтаксиса;

```
PS C:\Program Files\winlogbeat> .\winlogbeat.exe test config -c winlogbeat.yml
Config OK
```

Проверка подключение к Logstash

powershell

.\winlogbeat.exe test output -c winlogbeat.yml

```
PS C:\Program Files\winlogbeat> cd "C:\Program Files\winlogbeat"
PS C:\Program Files\winlogbeat> .\winlogbeat.exe test config -c winlogbeat.yml
Config OK
PS C:\Program Files\winlogbeat> .\winlogbeat.exe test output -c winlogbeat.yml
logstash: 10.20.11.20:5044...
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 10.20.11.20
    dial up... OK
  TLS... WARN secure connection disabled
  talk to server... OK
PS C:\Program Files\winlogbeat> .\winlogbeat.exe test config -c winlogbeat.yml
Config OK
PS C:\Program Files\winlogbeat> .\winlogbeat.exe test output -c winlogbeat.yml
logstash: 10.20.11.20:5044...
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 10.20.11.20
    dial up... OK
  TLS... WARN secure connection disabled
  talk to server... OK
PS C:\Program Files\winlogbeat>
```

Запуск службы:

```
PS C:\Program Files\winlogbeat> Start-Service winlogbeat
PS C:\Program Files\winlogbeat> Get-Service winlogbeat

Status   Name               DisplayName
------   ----               -----------
Running  winlogbeat         winlogbeat


PS C:\Program Files\winlogbeat>
```

Логи Winlogbeat создаются

```
PS C:\Program Files\winlogbeat> New-Item -ItemType Directory -Force -Path "C:\Program Files\winlogbeat\logs"


    Каталог: C:\Program Files\winlogbeat


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        26.08.2026     18:51                logs


PS C:\Program Files\winlogbeat> Restart-Service winlogbeat
PS C:\Program Files\winlogbeat> Get-ChildItem "C:\Program Files\winlogbeat\logs"


    Каталог: C:\Program Files\winlogbeat\logs


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        26.08.2026     18:47            770 winlogbeat-20260826-1.ndjson
-a----        26.08.2026     18:48           7187 winlogbeat-20260826-2.ndjson
-a----        26.08.2026     18:50            770 winlogbeat-20260826-3.ndjson
-a----        26.08.2026     18:55          28794 winlogbeat-20260826-4.ndjson
-a----        26.08.2026     18:55              0 winlogbeat-20260826-5.ndjson
-a----        26.08.2026     18:46           7187 winlogbeat-20260826.ndjson


PS C:\Program Files\winlogbeat>
```

Просмотр последних записей лога

powershell

Get-Content "C:\Program Files\winlogbeat\logs\winlogbeat-20260826-4.ndjson" -Tail 20

Обратим внимание на строки с "level":"error" или "error" в сообщении. Если таких нет — Winlogbeat работает без ошибок.

nasedkin-win [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

```
PS C:\Program Files\winlogbeat> Restart-Service winlogbeat
PS C:\Program Files\winlogbeat> Get-ChildItem "C:\Program Files\winlogbeat\logs"


    Каталог: C:\Program Files\winlogbeat\logs


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        26.08.2026     18:47            770 winlogbeat-20260826-1.ndjson
-a----        26.08.2026     18:48           7187 winlogbeat-20260826-2.ndjson
-a----        26.08.2026     18:50            770 winlogbeat-20260826-3.ndjson
-a----        26.08.2026     18:55          28794 winlogbeat-20260826-4.ndjson
-a----        26.08.2026     18:55              0 winlogbeat-20260826-5.ndjson
-a----        26.08.2026     18:46           7187 winlogbeat-20260826.ndjson


PS C:\Program Files\winlogbeat> Get-Content "C:\Program Files\winlogbeat\logs\winlogbeat-20260826-4.ndjson" -Tail 20
{"log.level":"info","@timestamp":"2026-08-26T18:55:18.800+0800","log.logger":"service_windows","log.origin":{"function":"github.com/elastic/elastic-agent-libs/ser
cute","file.name":"service/service_windows.go","file.line":77},"message":"received state change 'svc.Stop' from windows service manager","service.name":"winlogbea
"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:18.809+0800","log.logger":"service_windows","log.origin":{"function":"github.com/elastic/elastic-agent-libs/ser
cute","file.name":"service/service_windows.go","file.line":91},"message":"changed windows service state to svc.StopPending, invoking stopCallback","service.name":
on":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:18.809+0800","log.logger":"service","log.origin":{"function":"github.com/elastic/elastic-agent-libs/service.Han
.name":"service/service.go","file.line":59},"message":"Received Windows SVC stop/shutdown request","service.name":"winlogbeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:19.819+0800","log.logger":"winlogbeat","log.origin":{"function":"github.com/elastic/beats/v7/winlogbeat/beater.
le.name":"beater/winlogbeat.go","file.line":204},"message":"Stopping Winlogbeat","service.name":"winlogbeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.165+0800","log.logger":"winlogbeat","log.origin":{"function":"github.com/elastic/beats/v7/winlogbeat/beater.
3","file.name":"beater/eventlogger.go","file.line":126},"message":"Stop processing.","service.name":"winlogbeat","id":"Microsoft-Windows-Sysmon/Operational","ecs.
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.176+0800","log.logger":"metric_registry","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monit
Registry.func1","file.name":"inputmon/input.go","file.line":70},"message":"unregistering","service.name":"winlogbeat","input_type":"winlog","id":"Microsoft-Window
key":"Microsoft-Windows-Sysmon/Operational","uuid":"4d5714dc-f941-40c8-b043-9eb41703dc4e","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.589+0800","log.logger":"winlogbeat","log.origin":{"function":"github.com/elastic/beats/v7/winlogbeat/beater.
3","file.name":"beater/eventlogger.go","file.line":126},"message":"Stop processing.","service.name":"winlogbeat","id":"Application","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.589+0800","log.logger":"metric_registry","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monit
Registry.func1","file.name":"inputmon/input.go","file.line":70},"message":"unregistering","service.name":"winlogbeat","input_type":"winlog","id":"Application","ke
:"fdd19f25-b3e3-4e96-96da-e21e35de6f90","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.596+0800","log.logger":"winlogbeat","log.origin":{"function":"github.com/elastic/beats/v7/winlogbeat/beater.
3","file.name":"beater/eventlogger.go","file.line":126},"message":"Stop processing.","service.name":"winlogbeat","id":"Windows PowerShell","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.596+0800","log.logger":"metric_registry","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monit
Registry.func1","file.name":"inputmon/input.go","file.line":70},"message":"unregistering","service.name":"winlogbeat","input_type":"winlog","id":"Windows PowerShe
rShell","uuid":"3b16dca9-498d-4294-a89e-523d5027d38a","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.760+0800","log.logger":"winlogbeat","log.origin":{"function":"github.com/elastic/beats/v7/winlogbeat/beater.
3","file.name":"beater/eventlogger.go","file.line":126},"message":"Stop processing.","service.name":"winlogbeat","id":"Security","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.760+0800","log.logger":"metric_registry","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monit
Registry.func1","file.name":"inputmon/input.go","file.line":70},"message":"unregistering","service.name":"winlogbeat","input_type":"winlog","id":"Security","key":
cf3d-91ba-4013-8630-7928e214657c","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.766+0800","log.logger":"winlogbeat","log.origin":{"function":"github.com/elastic/beats/v7/winlogbeat/beater.
3","file.name":"beater/eventlogger.go","file.line":126},"message":"Stop processing.","service.name":"winlogbeat","id":"Microsoft-Windows-PowerShell/Operational","
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.766+0800","log.logger":"metric_registry","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monit
Registry.func1","file.name":"inputmon/input.go","file.line":70},"message":"unregistering","service.name":"winlogbeat","input_type":"winlog","id":"Microsoft-Window
l","key":"Microsoft-Windows-PowerShell/Operational","uuid":"7a9c2a3f-2949-4ba1-bab0-6b795cb6dcaa","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.766+0800","log.logger":"winlogbeat","log.origin":{"function":"github.com/elastic/beats/v7/winlogbeat/beater.
3","file.name":"beater/eventlogger.go","file.line":126},"message":"Stop processing.","service.name":"winlogbeat","id":"System","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.766+0800","log.logger":"metric_registry","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monit
Registry.func1","file.name":"inputmon/input.go","file.line":70},"message":"unregistering","service.name":"winlogbeat","input_type":"winlog","id":"System","key":"S
-0d36-4108-89c3-8b129e00a60d","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.778+0800","log.logger":"monitoring","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monitoring
.logTotals","file.name":"log/log.go","file.line":200},"message":"Total metrics","service.name":"winlogbeat","monitoring":{"metrics":{"beat":{"cpu":{"system":{"tic
968}},"total":{"ticks":10733,"time":{"ms":10733},"value":10733},"user":{"ticks":1765,"time":{"ms":1765}}},"info":{"ephemeral_id":"74f1971-9177-4468-8050-b950fcdf
t","uptime":{"ms":259007},"version":"8.15.2"},"memstats":{"gc_next":57100216,"memory_alloc":27882296,"memory_sys":61556984,"memory_total":139774944,"rss":84664320
s":18}},"libbeat":{"config":{"module":{"running":0,"starts":0,"stops":0},"reloads":0,"scans":0},"output":{"batches":{"split":0},"events":{"acked":1811,"active":0,
r":0,"dropped":0,"duplicates":0,"failed":418,"toomany":0,"total":2229},"read":{"bytes":168,"errors":1},"type":"logstash","write":{"bytes":534302,"errors":0,"laten
t":0,"max":0,"mean":0,"median":0,"min":0,"p75":0,"p95":0,"p99":0,"p999":0,"stddev":0}}}}},"processor":{"add_host_metadata":{"fqdn_lookup_failed":0}},"system":{"cp
":{"open":224}}},"ecs.version":"1.6.0"}}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.778+0800","log.logger":"monitoring","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monitoring
.logTotals","file.name":"log/log.go","file.line":201},"message":"Uptime: 4m18.99507s","service.name":"winlogbeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.778+0800","log.logger":"monitoring","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monitoring
.snapshotLoop","file.name":"log/log.go","file.line":168},"message":"Stopping metrics logging.","service.name":"winlogbeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2026-08-26T18:55:20.782+0800","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/cmd/instance.(*Beat).launch","file.n
,"file.line":549},"message":"winlogbeat stopped.","service.name":"winlogbeat","ecs.version":"1.6.0"}
PS C:\Program Files\winlogbeat>
```

Моделирование инцидентов — это Этап 6.4 (завершающая часть настройки Windows)

Сейчас мы находимся на **этапе 6.4. Моделирование инцидентов на Windows**.

Ранее уже:

- ✅ Созданы пользователи Pavel и Pavel2.
- ✅ Установлены Sysmon с конфигурацией SwiftOnSecurity.
- ✅ Установил и настроил Winlogbeat (он работает и отправляет данные в Logstash).

Теперь выполняем **моделирование инцидентов**, чтобы сгенерировать события, которые Winlogbeat отправит в ELK, и затем сможем их увидеть в Kibana.

Шаг 1. Блокировка пользователя Pavel2 (событие Security 4740)

1. Нажмём Ctrl+Alt+Del → **Сменить пользователя** или выйдем из системы.
2. На экране входа вводим имя пользователя Pavel2.
3. **Трижды** вводим **неверный пароль** (например, wrong).
4. После третьей неудачной попытки учётная запись будет заблокирована.

Что произойдёт:

В журнале **Security** появится событие с ID **4740** (блокировка учётной записи). Winlogbeat его отправит → индексы tag-winlogbeat-* в Elasticsearch.

Шаг 1. Включим политику блокировки учётных записей

В PowerShell (администратор):

powershell

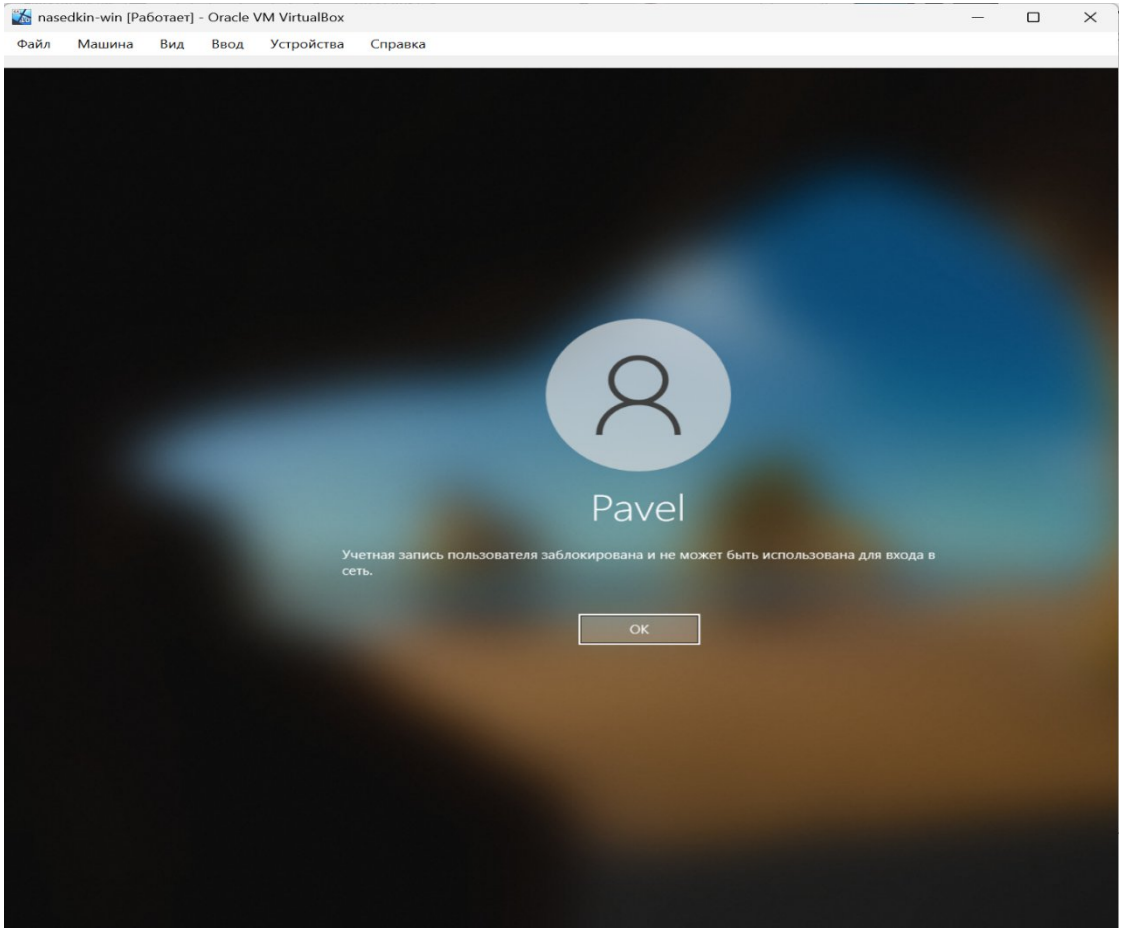
```
# Установить порог блокировки = 3 попытки
net accounts /lockoutthreshold:3
# Время до сброса счётчика (минуты)
net accounts /lockoutwindow:5
# Длительность блокировки (минуты)
net accounts /lockoutduration:5
```

```
PS C:\Program Files\winlogbeat> net accounts /lockoutthreshold:3
Команда выполнена успешно.

PS C:\Program Files\winlogbeat> net accounts /lockoutwindow:5
Команда выполнена успешно.

PS C:\Program Files\winlogbeat> net accounts /lockoutduration:5
Команда выполнена успешно.

PS C:\Program Files\winlogbeat> net accounts
Принудительный выход по истечении времени через:          Никогда
Минимальный срок действия пароля (дней):                  0
Максимальный срок действия пароля (дней):                 42
Минимальная длина пароля:                                 0
Хранение неповторяющихся паролей:                         Нет
Блокировка после ошибок ввода пароля:                     3
Длительность блокировки (минут):                          5
Сброс счетчика блокировок через (минут):                  5
Роль компьютера:                                          РАБОЧАЯ СТАНЦИЯ
Команда выполнена успешно.

PS C:\Program Files\winlogbeat>
```

Шаг 2. Блокировка пользователя Pavel (событие Security 4740)

1. Нажмём Ctrl+Alt+Del → **Сменим пользователя** или выйдем из системы.
2. На экране входа введём имя пользователя Pavel.
3. **Трижды** введём **неверный пароль** (например, wrong).
4. После третьей неудачной попытки учётная запись **Pavel** будет заблокирована.

Результат: в журнале **Security** появится событие **4740** с TargetUserName: "Pavel".



nasedkin-win [Работает] - Oracle VM VirtualBox

Управление компьютером

Файл Действие Вид Справка

Управление компьютером (л
- Служебные программы
  - Планировщик заданий
  - Просмотр событий
    - Настраиваемые пр
      - События управ.
    - Журналы Windows
      - Приложение
      - Безопасность
      - Установка
      - Система
      - Перенаправлен
    - Журналы приложе
    - Подписки
  - Общие папки
  - Локальные пользоват
    - Пользователи
    - Группы
  - Производительность
  - Диспетчер устройств
- Запоминающие устройст
  - Управление дисками
- Службы и приложения

Отфильтровано:Журнал: Security; Источник: ; Код события: 4740Диапазон дат: Последний час. Событий: 2

Ключевые слова	Дата и время	Источник	Код события	Категория за...
Аудит успеха	26.08.2026 19:37:19	Microsoft Wi...	4740	User Account...
Аудит успеха	26.08.2026 19:30:16	Microsoft Wi...	4740	User Account...

Свойства событий - Событие 4740, Microsoft Windows security auditing.

Общие Подробности

Заблокированная учетная запись:
Идентификатор безопасности: NASEDKIN-WIN\Pavel
Имя учетной записи: Pavel

Дополнительные сведения:
Имя вызывающего компьютера: NASEDKIN-WIN

Имя журнала:	Безопасность		
Источник:	Microsoft Windows security	Дата:	26.08.2026 19:37:19
Код	4740	Категория задачи:	User Account Management
Уровень:	Сведения	Ключевые слова:	Аудит успеха
Пользов.:	Н/Д	Компьютер:	nasedkin-win
Код операции:	Сведения		
Подробности:	Справка в Интернете для		

Копировать Закрыть

Событие 4740, Microsoft Windows

Общие Подробности

Понятное представление Режим XML

```
+ System
- EventData
    TargetUserName Pavel
    TargetDomainName NASEDKIN-WIN
    TargetSid S-1-5-21-28584859-90745515-1943227453-1002
    SubjectUserSid S-1-5-18
    SubjectUserName NASEDKIN-WIN$
    SubjectDomainName WORKGROUP
    SubjectLogonId 0x3e7
```

Действия

Безопасность
- Открыть сохраненны...
- Создать настраиваем...
- Импорт настраиваем...
- Очистить журнал...
- Фильтр текущего жур...
- Очистить фильтр
- Свойства
- Найти...
- Сохранить файл отфи...
- Привязать задачу к жу...
- Сохранить фильтр в н...
- Вид
- Обновить
- Справка

Событие 4740, Microsoft W...
- Свойства событий
- Привязать задачу к со...
- Копировать
- Сохранить выбранны...
- Обновить
- Справка

Чтобы начать поиск, введите здесь запрос

ENG 19:40 26.08.2026

Шаг 3. Действия пользователя Pavel2 (события Sysmon ID 1)

1. Войдём в систему под пользователем Pavel2 (используем правильный пароль).
2. Откроем **командную строку** (cmd) от имени этого пользователя.
3. Выполним последовательно:

```
cmd
ipconfig
whoami
ping 10.20.11.10
ssh user@10.20.11.10   # (или любая другая команда, чтобы создать процесс)
```

Результат: Sysmon запишет **Event ID 1** (создание процесса) для каждой команды с User: "Pavel2".

nasedkin-win [Работает] - Oracle VM VirtualBox

user@nasedkin-srv: ~

```
Microsoft Windows [Version 10.0.19041.388]
(c) Корпорация Майкрософт (Microsoft Corporation), 2020. Все права защищены.

C:\Users\Pavel2>ping ping 10.20.11.10
При проверке связи не удалось обнаружить узел ping.
Проверьте имя узла и повторите попытку.

C:\Users\Pavel2>ping 10.20.11.10

Обмен пакетами с 10.20.11.10 по с 32 байтами данных:
Ответ от 10.20.11.10: число байт=32 время=2мс TTL=64
Ответ от 10.20.11.10: число байт=32 время=2мс TTL=64
Ответ от 10.20.11.10: число байт=32 время=1мс TTL=64
Ответ от 10.20.11.10: число байт=32 время=2мс TTL=64

Статистика Ping для 10.20.11.10:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 2 мсек, Среднее = 1 мсек

C:\Users\Pavel2>ipconfig

Настройка протокола IP для Windows


Адаптер Ethernet Ethernet:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::5990:5dfc:f4eb:9eb1%6
   IPv4-адрес. . . . . . . . . . . . : 10.20.11.100
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . . : 10.20.11.1

C:\Users\Pavel2>whoami
nasedkin-win\pavel2

C:\Users\Pavel2>ssh user@10.20.11.10
The authenticity of host '10.20.11.10 (10.20.11.10)' can't be established.
ECDSA key fingerprint is SHA256:2MTDoPOgKSamFj2xpjzuXdksD2jrWC2ZehOEoUu7FbY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.20.11.10' (ECDSA) to the list of known hosts.
user@10.20.11.10's password:
Linux nasedkin-srv 6.12.96+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.96-1 (2026-07-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Aug 26 19:45:46 2026 from 192.168.0.50
user@nasedkin-srv:~$ su -
Password:
root@nasedkin-srv:~#
```

Чтобы начать поиск, введите здесь запрос

ENG 19:47 26.08.2026

nasedkin-win [Работает] - Oracle VM VirtualBox

Просмотр событий

Файл Действие Вид Справка

Свойства событий - Событие 1, Sysmon

Общие Подробности

```
Process Create:
RuleName: -
UtcTime: 2026-08-26 11:46:54.906
ProcessGuid: {821b00f7-d22e-6a8e-f103-000000000e00}
ProcessId: 7552
Image: C:\Windows\System32\ipconfig.exe
FileVersion: 10.0.19041.1 (WinBuild.160101.0800)
Description: IP Configuration Utility
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: ipconfig.exe
CommandLine: ipconfig
CurrentDirectory: C:\Users\Pavel2\
User: NASEDKIN-WIN\Pavel2
LogonGuid: {821b00f7-cd23-6a8e-49f6-4e0000000000}
LogonId: 0x4EF649
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=62F170FB07FDBB79CEB7147101406EB8,SHA256=
53E000F5AA9B3A00934319DB8080BB99CB323BF48FC628A64F75D7847C265606,IMPHASH=
1002D523645A81BC52877D82D9E88417
ParentProcessGuid: {821b00f7-d167-6a8e-d503-000000000e00}
ParentProcessId: 8904
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\system32\cmd.exe"
ParentUser: NASEDKIN-WIN\Pavel2
```

Имя журнала:	Microsoft-Windows-Sysmon/Operational		
Источник:	Sysmon	Дата:	26.08.2026 19:46:54
Код	1	Категория задачи:	Process Create (rule: ProcessCrea
Уровень:	Сведения	Ключевые слова:	
Пользов.:	СИСТЕМА	Компьютер:	nasedkin-win
Код операции:	Сведения		
Подробности:	Справка в Интернете для		

Копировать Закрыть

Чтобы начать поиск, введите здесь запрос

ENG 20:11

nasedkin-win [Работает] - Oracle VM VirtualBox

Просмотр событий

Файл Действие Вид Справка

Operational Событий: 893 (!) Есть новые события

Отфильтровано:Журнал: Microsoft-Windows-Sysmon/Operational; Источник: ; Код события: 1Диапазон дат: Последний час. Событий:

Уровень	Дата и время	Источник	Код события	Категория задачи
Сведения	26.08.2026 19:57:23	Sysmon	1	Process Create (rule:...
			1	Process Create (rule:...
			1	Process Create (rule:...

nasedkin-win [Работает] - Oracle VM VirtualBox

Просмотр событий

Файл Действие Вид Справка

Operational Событий: 893 (!) Есть новые события

Свойства событий - Событие 1, Sysmon

Общие Подробности

```
Process Create:
RuleName: -
UtcTime: 2026-08-26 11:47:22.563
ProcessGuid: {821b00f7-d24a-6a8e-f303-000000000e00}
ProcessId: 8132
Image: C:\Windows\System32\OpenSSH\ssh.exe
FileVersion: 7.7.2.1
Description: -
Product: OpenSSH for Windows
Company: -
OriginalFileName: -
CommandLine: ssh  user@10.20.11.10
CurrentDirectory: C:\Users\Pavel2\
User: NASEDKIN-WIN\Pavel2
LogonGuid: {821b00f7-cd23-6a8e-49f6-4e0000000000}
LogonId: 0x4EF649
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=B664CCD9E064BA9542BCC71A5DED6A1A,SHA256=
0C0E91427A4B0E4CD0B59BDB73054252FB74C0977D13A73AB7423E15528B0485,IMPHASH=
5F959422308AC3D721010D66647E100E
ParentProcessGuid: {821b00f7-d167-6a8e-d503-000000000e00}
ParentProcessId: 8904
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\system32\cmd.exe"
ParentUser: NASEDKIN-WIN\Pavel2
```

Имя журнала:	Microsoft-Windows-Sysmon/Operational		
Источник:	Sysmon	Дата:	26.08.2026 19:47:22
Код	1	Категория задачи:	Process Create (rule: ProcessCrea
Уровень:	Сведения	Ключевые слова:	
Пользов.:	СИСТЕМА	Компьютер:	nasedkin-win
Код операции:	Сведения		
Подробности:	Справка в Интернете для		

Копировать Закрыть

Действия

Operational

Открыть сохраненный журнал...
Создать настраиваемое предст...
Импорт настраиваемого предс...
Очистить журнал...
Фильтр текущего журнала...
Очистить фильтр
Свойства
Отключить журнал
Найти...
Сохранить файл отфильтрован...
Привязать задачу к журналу...
Сохранить фильтр в настраива...
Вид
Обновить
Справка

Событие 1, Sysmon

Свойства событий
Привязать задачу к событию...
Сохранить выбранные событи...
Копировать
Обновить
Справка

Чтобы начать поиск, введите здесь запрос

ENG 20:14 26.08.2026

nasedkin-win [Работает] - Oracle VM VirtualBox

Просмотр событий

Файл Действие Вид Справка

Свойства событий - Событие 1, Sysmon

Общие Подробности

```
Process Create:
RuleName: -
UtcTime: 2026-08-26 11:47:01.742
ProcessGuid: {821b00f7-d235-6a8e-f203-000000000e00}
ProcessId: 8464
Image: C:\Windows\System32\whoami.exe
FileVersion: 10.0.19041.1 (WinBuild.160101.0800)
Description: whoami - displays logged on user information
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: whoami.exe
CommandLine: whoami
CurrentDirectory: C:\Users\Pavel2\
User: NASEDKIN-WIN\Pavel2
LogonGuid: {821b00f7-cd23-6a8e-49f6-4e0000000000}
LogonId: 0x4EF649
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=A4A6924F3EAF97981323703D38FD99C4,SHA256=
1D4902A04D99E8CCBFE7085E63155955FEE397449D386453F6C452AE407B8743,IMPHASH=
7FF0758B766F747CE57DFAC70743FB88
ParentProcessGuid: {821b00f7-d167-6a8e-d503-000000000e00}
ParentProcessId: 8904
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\system32\cmd.exe"
ParentUser: NASEDKIN-WIN\Pavel2
```

Имя журнала:	Microsoft-Windows-Sysmon/Operational		
Источник:	Sysmon	Дата:	26.08.2026 19:47:01
Код	1	Категория задачи:	Process Create (rule: ProcessCrea
Уровень:	Сведения	Ключевые слова:	
Пользов.:	СИСТЕМА	Компьютер:	nasedkin-win
Код операции:	Сведения		
Подробности:	Справка в Интернете для		

Копировать Закрыть

Чтобы начать поиск, введите здесь запрос

ENG 20:15 26.08.2026

Английский (США)
США клавиатура

Для переключения методов ввода нажмите клавиши WINDOWS+ПРОБЕЛ.

Шаг 4. Проверка в Kibana

Шаг 1. Убедимся, что SSH-туннель активен

На нашей Windows-машине должно быть открыто окно командной строки с командой:

cmd

```
ssh -L 5601:localhost:5601 user@192.168.0.12
```

Если туннель не активен — запустите его.

Шаг 2. Откроем Kibana в браузере

Перейдём по адресу:

`http://localhost:5601`

Шаг 3. Создадим Data View (индексный шаблон) для событий Windows

Создадим Data View для `tag-winlogbeat-*`:

1. В левом меню Kibana нажмём на иконку **"Stack Management"** (шестерёнка) или найдём в меню.
2. Выберем **"Data Views"**.
3. Нажмём **"Create data view"**.
4. В поле **"Name"** введём: `winlogbeat`
5. В поле **"Index pattern"** введём: `tag-winlogbeat-*`
6. Нажмём **"Save data view to Kibana"**.

Mail: Почта, Облако, Календар | Google | Dashboards - Эластичный | winlogbeat - Elastic

Не защищено 192.168.0.12:5601/app/management/kibana/dataViews/dataView/876462c1-211f-4804-9ab2-ac8257f256bd#/?_a=(tab:indexedFields)

Яндекс Почта Карты Маркет Новости Словари Видео Музыка Диск Mail.Ru Поиск в Интернете Foto.Mail.Ru Mail.Ru Video.Mail.Ru Предварительная... Все закладки

elastic | Find apps, content, and more. ^/

D > Stack Management > Data views > winlogbeat

Management

Ingest
- Ingest Pipelines

Data
- Index Management
- Index Lifecycle Policies
- Data Set Quality
- Snapshot and Restore
- Rollup Jobs
- Transforms
- Remote Clusters
- Migrate

Alerts and Insights
- Alerts
- Rules
- Cases
- Connectors
- Reporting
- Machine Learning
- Maintenance Windows

Kibana
- Data Views
- Files
- Saved Objects

winlogbeat

Delete | Set as default | Edit

Index pattern: `tag-winlogbeat-*` Time field: `@timestamp`

Fields (530) | Scripted fields (0) | Field filters (0) | Relationships (0)

Search | Field type 8 | Schema type 2 | Refresh | Add field

Name	Type	Format	Searchable	Aggregatable	Excluded	Actions
@timestamp	date		●	●		
@version	text		●			
@version.keyword	keyword		●	●		
_id	_id		●			
_ignored	_ignored		●	●		
_index	_index		●	●		
_score						
_source	_source					
agent.ephemeral_id	text		●			
agent.ephemeral_id.keyword	keyword		●	●		

Rows per page: 10

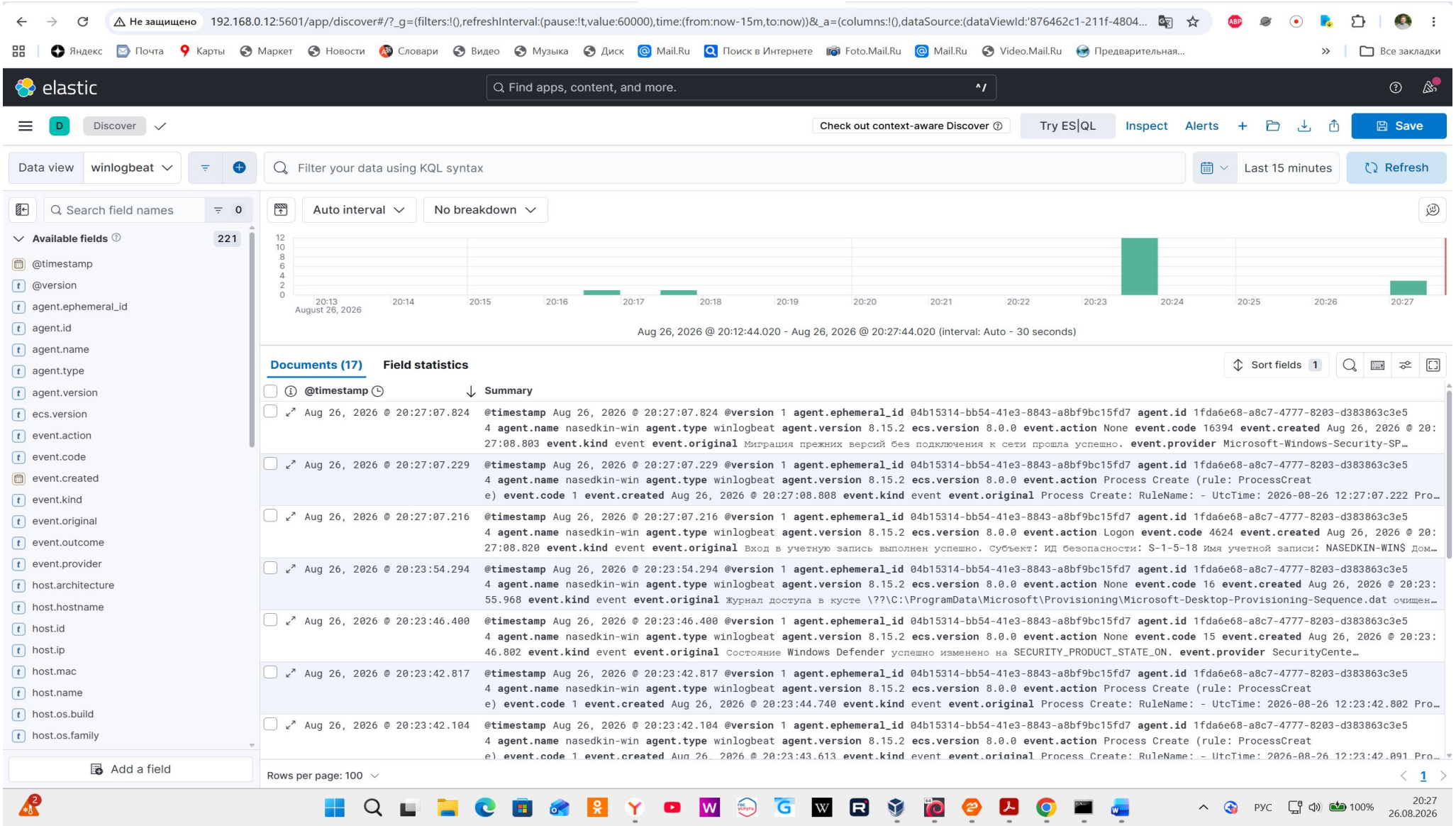
1 2 3 4 5 ... 53

ENG 100% 20:24 26.08.2026

Шаг 4. Перейдём в Discover

В левом меню выберем **"Discover"** (лупа).

В верхнем левом углу выберем созданный Data View winlogbeat.



Шаг 5. Выполним запросы в поле поиска (KQL)

Запрос №1 (блокировка Pavel):

text

winlog.event_id: 4740 AND winlog.event_data.TargetUserName: "Pavel"

Запрос №2 (команды Pavel2, Sysmon ID 1):

text

winlog.event_id: 1 AND winlog.user_name: "nasedkin-win\Pavel2"

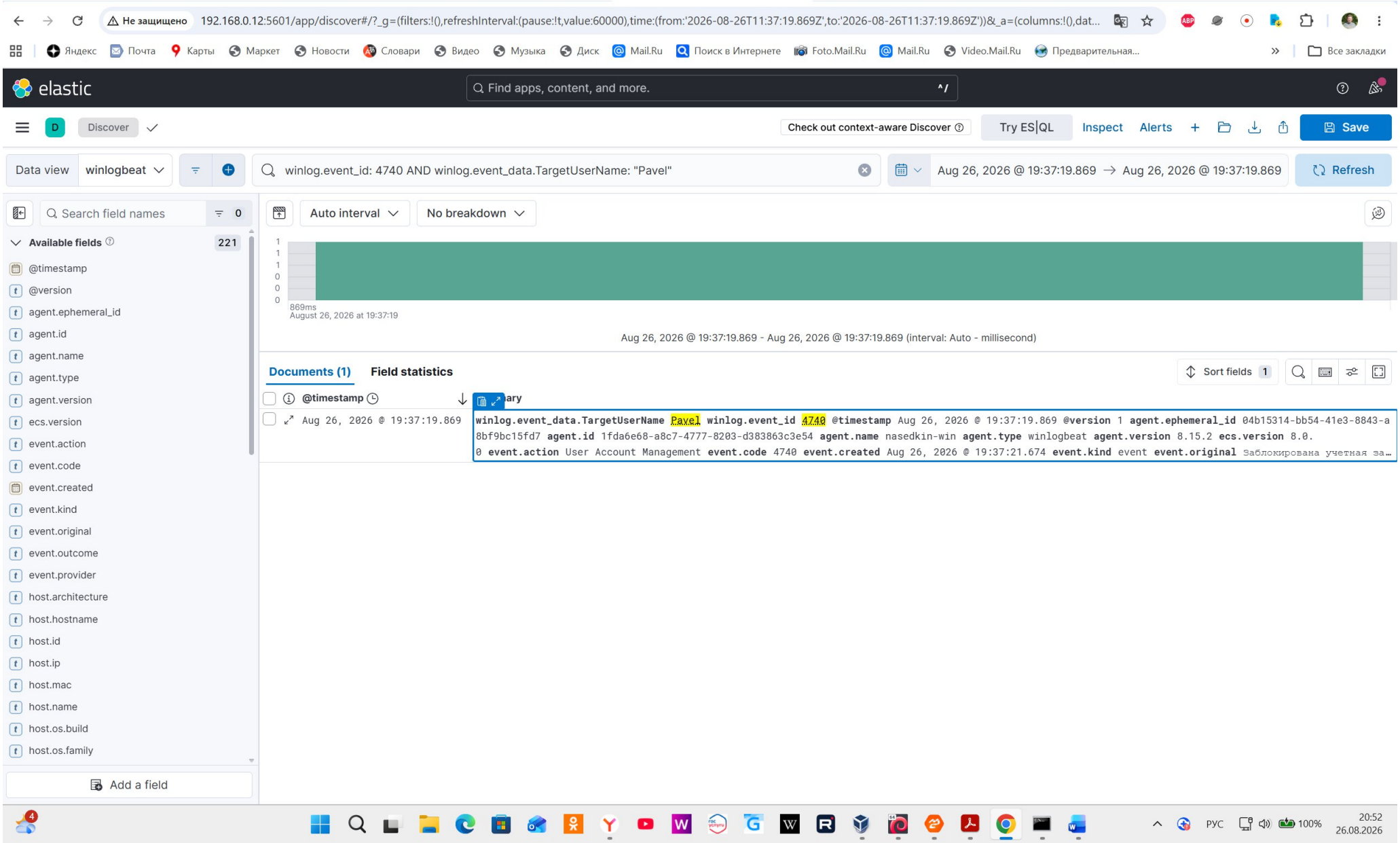
Примечание: Вместо nasedkin-win подставим имя вашего компьютера. Его можно найти в поле winlog.computer_name в любом событии.

Если события есть — они отобразятся в таблице. Сделаем скриншоты для отчёта.

На скриншоте видно, что в Kibana Discover есть документ с:

- winlog.event_data.TargetUserName: Pavel
- winlog.event_id: 4740

Это означает, что **блокировка Pavel зафиксирована** и Winlogbeat доставил событие в ELK.



winlog.event_id: 4740 AND winlog.event_data.TargetUserName: "Pavel"

Убедимся, что Pavel2 выполнил команды

Войдём под пользователем **Pavel2** (используем правильный пароль).

Откроем командную строку и выполним:

cmd

ipconfig

whoami

ping 10.20.11.10

ssh user@10.20.11.10 # (или любую другую команду)

winlog.event_id: 1 AND winlog.event_data.User: "nasedkin-win\pavel2"

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2024-09-18T05:36:30.931Z',to:'2026-08-26T12:57:37.435Z'))&_a=(columns:!(winl...

Яндекс | Почта | Карты | Маркет | Новости | Словари | Видео | Музыка | Диск | Mail.Ru | Поиск в Интернете | Foto.Mail.Ru | Mail.Ru | Video.Mail.Ru | Предварительная... | Все закладки

elastic | Find apps, content, and more. ^/

D | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: winlogbeat

winlog.event_id: 1 AND winlog.event_data.User: "nasedkin-win\pavel2"

Sep 18, 2024 @ 13:36:30.931 → Aug 26, 2026 @ 20:57:37.4... | Refresh

Search field names | 0

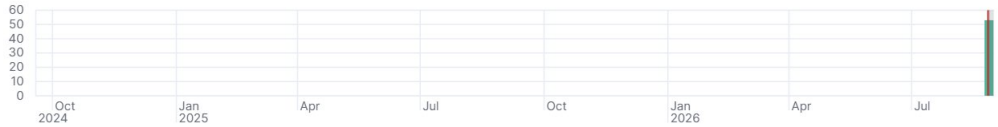
Selected fields 1
- winlog.event_data.CommandLine

Popular fields 1
- winlog.event_data.CommandLine

Available fields 268
- @timestamp
- @version
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- ecs.version
- event.action
- event.code
- event.created
- event.kind
- event.original
- event.outcome
- event.provider
- host.architecture

Add a field

Auto interval | No breakdown



Sep 18, 2024 @ 13:36:30.931 - Aug 26, 2026 @ 20:57:37.435 (interval: Auto - 7 days)

Documents (53) | Field statistics | 5 Selected | Columns 2 | Sort fields 1

@timestamp	winlog.event_data.CommandLine
Aug 26, 2026 @ 19:47:22.594	ssh user@10.20.11.10
Aug 26, 2026 @ 19:47:01.768	whoami
Aug 26, 2026 @ 19:46:54.924	ipconfig
Aug 26, 2026 @ 19:46:34.736	ping 10.20.11.10
Aug 26, 2026 @ 19:46:25.704	ping ping 10.20.11.10
Aug 26, 2026 @ 19:45:07.768	C:\Windows\system32\AppHostRegistrationVerifier.exe

Rows per page: 100 | 1

Document 2 of 53

Actions: View single document | View surrounding documents

Table | JSON

winlog.event_data.CommandLine | 0

Selected only

Field	Value
winlog.event_data.CommandLine	C:\Windows\system32\AppHostRegistrationVerifier.exe

Close

ENG 100% 21:16 26.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2024-09-18T05:36:30.931Z',to:'2026-08-26T12:57:37.435Z'))&_a=(columns:!(),dat...

Яндекс | Почта | Карты | Маркет | Новости | Словари | Видео | Музыка | Диск | Mail.Ru | Поиск в Интернете | Foto.Mail.Ru | Mail.Ru | Video.Mail.Ru | Предварительная... | Все закладки

elastic — Find apps, content, and more. ^/

D Discover ✓ | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: winlogbeat

winlog.event_id: 1 AND winlog.event_data.User: "nasedkin-win\pavel2"

Sep 18, 2024 @ 13:36:30.931 → Aug 26, 2026 @ 20:57:37.4... | Refresh

winlog.event_data.CommandLine: exists ×

Search field names 0

Popular fields 1

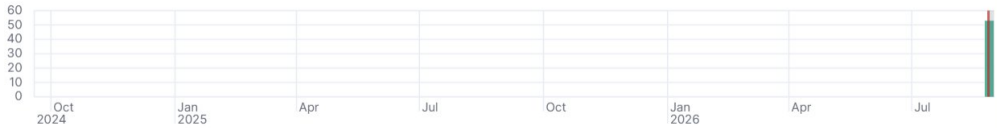
- winlog.event_data.CommandLine

Available fields 221

- @timestamp
- @version
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- ecs.version
- event.action
- event.code
- event.created
- event.kind
- event.original
- event.outcome
- event.provider
- host.architecture
- host.hostname

Add a field

Auto interval | No breakdown



Sep 18, 2024 @ 13:36:30.931 - Aug 26, 2026 @ 20:57:37.435 (interval: Auto - 7 days)

Documents (53) | Field statistics | 5 Selected | Sort fields 1

@timestamp	Summary
Aug 26, 2026 @ 19:47:22.594	c15fd7 agent.id 1fda6e68-a8c7-4777-8203-d383863c3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:47:01.768	nt_id 1 @timestamp Aug 2 04b15314-bb54-41e3-8843-a 3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:46:54.924	nt_id 1 @timestamp Aug 2 04b15314-bb54-41e3-8843-a 3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:46:34.736	nt_id 1 @timestamp Aug 2 04b15314-bb54-41e3-8843-a 3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:46:25.704	nt_id 1 @timestamp Aug 2 6, 2026 @ 19:46:25.704 @version 1 agent.ephemeral_id 04b15314-bb54-41e3-8843-a 8bf9bc15fd7 agent.id 1fda6e68-a8c7-4777-8203-d383863c3e54 agent.name nasedkin…


```
],
"winlog.event_data.CommandLine.keyword":
  [
  "ssh  user@10.20.11.10  "
],
"winlog.version": [
  5
],
"event.original": [
```


Copy value

Rows per page: 100 | 1

Document 2 of 53

Actions: View single document | View surrounding documents

Table | JSON

winlog.event_data.CommandLine 0

Selected only

Field	Value
winlog.event_data.CommandLine	C:\Windows\system32\AppHostRegistrationVerifier.exe

Close

ENG 100% 21:19 26.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2024-09-18T05:36:30.931Z',to:'2026-08-26T12:57:37.435Z'))&_a=(columns:!(),dat...

Яндекс | Почта | Карты | Маркет | Новости | Словари | Видео | Музыка | Диск | Mail.Ru | Поиск в Интернете | Foto.Mail.Ru | Mail.Ru | Video.Mail.Ru | Предварительная... | Все закладки

elastic | Find apps, content, and more. ^/

Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | Save

Data view: winlogbeat

winlog.event_id: 1 AND winlog.event_data.User: "nasedkin-win\pavel2"

Sep 18, 2024 @ 13:36:30.931 → Aug 26, 2026 @ 20:57:37.4... | Refresh

winlog.event_data.CommandLine: exists

Search field names

Popular fields 1

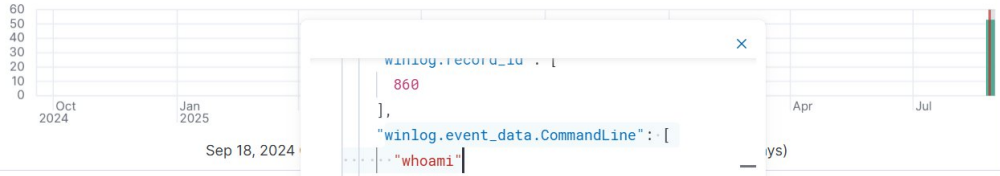
- winlog.event_data.CommandLine

Available fields 221

- @timestamp
- @version
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- ecs.version
- event.action
- event.code
- event.created
- event.kind
- event.original
- event.outcome
- event.provider
- host.architecture
- host.hostname

Add a field

Auto interval | No breakdown



Documents (53) | Field statistics

@timestamp	
Aug 26, 2026 @ 19:47:22.594	3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:47:01.768	winlog.event_data.User NASEDKIN-WIN\Pavel2 winlog.event_id 1 @timestamp Aug 26, 2026 @ 19:47:01.768 @version 1 agent.ephemeral_id 04b15314-bb54-41e3-8843-a8bf9bc15fd7 agent.id 1fda6e68-a8c7-4777-8203-d383863c3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:46:54.924	winlog.event_data.User NASEDKIN-WIN\Pavel2 winlog.event_id 1 @timestamp Aug 26, 2026 @ 19:46:54.924 @version 1 agent.ephemeral_id 04b15314-bb54-41e3-8843-a8bf9bc15fd7 agent.id 1fda6e68-a8c7-4777-8203-d383863c3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:46:34.736	winlog.event_data.User NASEDKIN-WIN\Pavel2 winlog.event_id 1 @timestamp Aug 26, 2026 @ 19:46:34.736 @version 1 agent.ephemeral_id 04b15314-bb54-41e3-8843-a8bf9bc15fd7 agent.id 1fda6e68-a8c7-4777-8203-d383863c3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:46:25.704	winlog.event_data.User NASEDKIN-WIN\Pavel2 winlog.event_id 1 @timestamp Aug 26, 2026 @ 19:46:25.704 @version 1 agent.ephemeral_id 04b15314-bb54-41e3-8843-a8bf9bc15fd7 agent.id 1fda6e68-a8c7-4777-8203-d383863c3e54 agent.name nasedkin…

```
860
],
"winlog.event_data.CommandLine": [
  "whoami"
],
"winlog.event_data.RuleName.keyword": [
  "-"
],
"event.kind.keyword": [
```

Copy value

Rows per page: 100 | 1

Document 2 of 53

Actions: View single document | View surrounding documents

Table | JSON

winlog.event_data.CommandLine | 0

Selected only

Field	Value
winlog.event_data.CommandLine	C:\Windows\system32\AppHostRegistrationVerifier.exe

Close

ENG 100% 21:22 26.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2024-09-18T05:36:30.931Z',to:'2026-08-26T12:57:37.435Z'))&_a=(columns:!(),dat...

Яндекс Почта Карты Маркет Новости Словари Видео Музыка Диск Mail.Ru Поиск в Интернете Foto.Mail.Ru Mail.Ru Video.Mail.Ru Предварительная... Все закладки

elastic | Find apps, content, and more. ^/

D Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: winlogbeat

winlog.event_id: 1 AND winlog.event_data.User: "nasedkin-win\pavel2"

Sep 18, 2024 @ 13:36:30.931 → Aug 26, 2026 @ 20:57:37.4... | Refresh

winlog.event_data.CommandLine: exists

Search field names 0

Popular fields 1

- winlog.event_data.CommandLine

Available fields 221

- @timestamp
- @version
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- ecs.version
- event.action
- event.code
- event.created
- event.kind
- event.original
- event.outcome
- event.provider
- host.architecture
- host.hostname

Add a field

Auto interval | No breakdown

60 50 40 30 20 10 0

Oct 2024 | Jan 2025 | Apr | Jul

Sep 18, 2024

Documents (53) | Field statistics

@timestamp	
Aug 26, 2026 @ 19:47:22.594	
Aug 26, 2026 @ 19:47:01.768	
Aug 26, 2026 @ 19:46:54.924	winlog.event_data.User NASEDKIN-WIN\Pavel2 winlog.event_id 1 @timestamp Aug 26, 2026 @ 19:46:54.924 @version 1 agent.ephemeral_id 04b15314-bb54-41e3-8843-a8bf9bc15fd7 agent.id 1fda6e68-a8c7-4777-8203-d383863c3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:46:34.736	winlog.event_data.User NASEDKIN-WIN\Pavel2 winlog.event_id 1 @timestamp Aug 26, 2026 @ 19:46:34.736 @version 1 agent.ephemeral_id 04b15314-bb54-41e3-8843-a8bf9bc15fd7 agent.id 1fda6e68-a8c7-4777-8203-d383863c3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:46:25.704	winlog.event_data.User NASEDKIN-WIN\Pavel2 winlog.event_id 1 @timestamp Aug 26, 2026 @ 19:46:25.704 @version 1 agent.ephemeral_id 04b15314-bb54-41e3-8843-a8bf9bc15fd7 agent.id 1fda6e68-a8c7-4777-8203-d383863c3e54 agent.name nasedkin…


```
"host.os.version.keyword": [
  "10.0"
],
"winlog.event_data.CommandLine.keyword":
  [
  "ipconfig"
],
"winlog.version": [
  5
```


Copy value

Rows per page: 100 | 1

Document 2 of 53

Actions: View single document | View surrounding documents

Table | JSON

winlog.event_data.CommandLine 0

Selected only

Field	Value
winlog.event_data.CommandLine	C:\Windows\system32\AppHostRegistrationVerifier.exe

Close

ENG 100% 21:26 26.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2024-09-18T05:36:30.931Z',to:'2026-08-26T12:57:37.435Z'))&_a=(columns:!(),dat...

Яндекс | Почта | Карты | Маркет | Новости | Словари | Видео | Музыка | Диск | Mail.Ru | Поиск в Интернете | Foto.Mail.Ru | Mail.Ru | Video.Mail.Ru | Предварительная... | Все закладки

elastic | Find apps, content, and more. ^/

D | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: winlogbeat

winlog.event_id: 1 AND winlog.event_data.User: "nasedkin-win\pavel2"

Sep 18, 2024 @ 13:36:30.931 → Aug 26, 2026 @ 20:57:37.4... | Refresh

winlog.event_data.CommandLine: exists

Search field names | 0

Popular fields 1

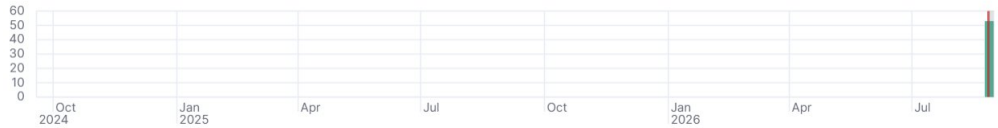
- winlog.event_data.CommandLine

Available fields 221

- @timestamp
- @version
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- ecs.version
- event.action
- event.code
- event.created
- event.kind
- event.original
- event.outcome
- event.provider
- host.architecture
- host.hostname

Add a field

Auto interval | No breakdown



Sep 18, 2024 @ 13:36:30.931 - Aug 26, 2026 @ 20:57:37.435 (interval: Auto - 7 days)

Documents (53) | **Field statistics**

@timestamp	
Aug 26, 2026 @ 19:47:22.594	3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:47:01.768	nt_id 1 @timestamp Aug 2 04b15314-bb54-41e3-8843-a 3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:46:54.924	nt_id 1 @timestamp Aug 2 04b15314-bb54-41e3-8843-a 3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:46:34.736	winlog.event_data.User NASEDKIN-WIN\Pavel2 winlog.event_id 1 @timestamp Aug 26, 2026 @ 19:46:34.736 @version 1 agent.ephemeral_id 04b15314-bb54-41e3-8843-a 8bf9bc15fd7 agent.id 1fda6e68-a8c7-4777-8203-d383863c3e54 agent.name nasedkin…
Aug 26, 2026 @ 19:46:25.704	winlog.event_data.User NASEDKIN-WIN\Pavel2 winlog.event_id 1 @timestamp Aug 26, 2026 @ 19:46:25.704 @version 1 agent.ephemeral_id 04b15314-bb54-41e3-8843-a 8bf9bc15fd7 agent.id 1fda6e68-a8c7-4777-8203-d383863c3e54 agent.name nasedkin…

```
"winlog.record_id": [
  858
],
"winlog.event_data.CommandLine": [
  "ping 10.20.11.10"
],
"winlog.event_data.RuleName.keyword": [
  "-"
],
```

Copy value

Rows per page: 100 | 1

Document 2 of 53

Actions: View single document | View surrounding documents

Table | JSON

winlog.event_data.CommandLine | 0

Selected only

Field	Value
winlog.event_data.CommandLine	C:\Windows\system32\AppHostRegistrationVerifier.exe

Close

13° | ENG | 100% | 21:27 26.08.2026

Тестирование с HACK (Скриншоты №3, 4, 5, 7)

Теперь, когда Windows-инциденты подтверждены в Kibana, переходим к атакам с HACK.

Шаг 5. На HACK (Kali Linux, 20.20.11.10) выполним:

```bash
sudo apt update
sudo apt install nmap curl -y

nmap -sS 10.20.11.10
ping -s 1024 10.20.11.10
curl http://10.20.11.10
```

nasedkin-hak [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

1 2 3 4 12:25

kali@nasedkin-hak: ~

Session Actions Edit View Help

```
Setting up nmap-common (7.99+dfsg-1kali1) ...
Setting up curl (8.21.0-2) ...
Setting up nmap (7.99+dfsg-1kali1) ...
Setcap worked! Adding configuration to environment
Processing triggers for kali-menu (2025.4.3) ...
Processing triggers for libc-bin (2.41-12) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for wordlists (2025.4.0) ...

┌──(kali㉿nasedkin-hak)-[~]
└─$ nmap -sS 10.20.11.10
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-26 09:58 -0400
Stats: 0:01:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.09% done; ETC: 10:07 (0:07:51 remaining)
Stats: 0:01:40 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.39% done; ETC: 10:07 (0:07:55 remaining)
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.35% done; ETC: 10:10 (0:10:14 remaining)
Stats: 0:02:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 15.78% done; ETC: 10:11 (0:10:56 remaining)
Stats: 0:02:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 15.88% done; ETC: 10:11 (0:10:57 remaining)
Stats: 0:02:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.63% done; ETC: 10:12 (0:11:32 remaining)
Stats: 0:02:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.64% done; ETC: 10:12 (0:11:36 remaining)
Stats: 0:02:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.75% done; ETC: 10:12 (0:11:44 remaining)
Stats: 0:03:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.71% done; ETC: 10:13 (0:12:09 remaining)
Stats: 0:03:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 23.64% done; ETC: 10:14 (0:12:39 remaining)
Nmap scan report for 10.20.11.10
Host is up (0.0068s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1512.07 seconds

┌──(kali㉿nasedkin-hak)-[~]
└─$
```

Right Ctrl

nasedkin-hak [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

1 2 3 4 13:25

Home

File System

kali@nasedkin-hak: ~

Session Actions Edit View Help

```
┌──(kali㉿nasedkin-hak)-[~]
└─$ nmap -sS 10.20.11.10
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-26 13:24 -0400
```

kali@nasedkin-hak: ~

Session Actions Edit View Help

```
┌──(kali㉿nasedkin-hak)-[~]
└─$ ping -s 1024 10.20.11.10
ING 10.20.11.10 (10.20.11.10) 1024(1052) bytes of data.
```

kali@nasedkin-hak: ~

Session Actions Edit View Help

```
┌──(kali㉿nasedkin-hak)-[~]
└─$ curl http://10.20.11.10
```

Right Ctrl

Выбрать user@nasedkin-IDS: ~

```
root@nasedkin-IDS:~# cat /var/log/suricata/fast.log | grep 40000003 | head -20
08/26/2026-21:50:35.402190  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10
:143
08/26/2026-21:50:35.402212  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10
:1723
08/26/2026-21:50:35.404250  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10
:21
08/26/2026-21:50:35.402208  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10
:23
08/26/2026-21:50:35.402210  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10
:554
08/26/2026-21:50:35.402219  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10
:3306
08/26/2026-21:50:35.402221  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10
:8080
08/26/2026-21:50:35.402223  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10
:113
08/26/2026-21:50:35.404242  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10
:3389
08/26/2026-21:50:35.404252  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60397 -> 10.20.11.10
:995
08/26/2026-21:50:36.556852  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60399 -> 10.20.11.10
:113
08/26/2026-21:50:36.556854  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60399 -> 10.20.11.10
:8080
08/26/2026-21:50:36.556862  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60399 -> 10.20.11.10
:143
08/26/2026-21:50:36.556594  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60399 -> 10.20.11.10
:21
08/26/2026-21:50:36.556848  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60399 -> 10.20.11.10
:3389
08/26/2026-21:50:36.556855  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60399 -> 10.20.11.10
:3306
08/26/2026-21:50:36.556857  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60399 -> 10.20.11.10
:1723
08/26/2026-21:50:36.556858  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60399 -> 10.20.11.10
:554
08/26/2026-21:50:36.556860  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60399 -> 10.20.11.10
:23
08/26/2026-21:50:37.664888  [Drop] [**] [1:40000003:2] SYN SCAN BLOCKED (TEST) [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 20.20.11.10:60401 -> 10.20.11.10
:1723
root@nasedkin-IDS:~#
```

ENG 100% 1:27 27.08.2026

```
user@nasedkin-IDS: ~
root@nasedkin-IDS:~# cat /var/log/suricata/fast.log | grep 1000013 | head -20
08/26/2026-21:53:17.984439  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:19.125621  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:20.164753  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:21.188540  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:22.217517  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:23.257379  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:24.261464  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:25.289706  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:26.314062  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:27.392031  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:28.426101  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:29.449284  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:30.523785  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:31.529312  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:32.669237  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:33.679489  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:34.709213  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:35.767537  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:36.773135  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
08/26/2026-21:53:37.811562  [Drop] [**] [1:1000013:1] IPS: Block Ping (DoS) [**] [Classification: (null)] [Priority: 3] {ICMP} 20.20.11.10:8 -> 10.20.11.10:0
root@nasedkin-IDS:~#
```

```
user@nasedkin-IDS: ~
root@nasedkin-IDS:~# cat /var/log/suricata/fast.log | grep 1000200
08/26/2026-21:54:55.281805  [Drop] [**] [1:1000200:1] IPS: Block external curl to internal HTTP [**] [Classification: (null)] [Priority: 3] {TCP} 20.20.11.10:36044 -> 10.20.11.10:80
08/26/2026-22:24:25.794927  [Drop] [**] [1:1000200:1] IPS: Block external curl to internal HTTP [**] [Classification: (null)] [Priority: 3] {TCP} 20.20.11.10:58970 -> 10.20.11.10:80
root@nasedkin-IDS:~#
```

Шаг *. Проверим Kibana (скриншоты №7, 8, 9)

Если Filebeat доставил события, в Kibana Discover:

- Suricata (индекс nasedkin_ids-*):

text

event.kind: "alert" AND (suricata.eve.alert.signature_id: 40000003 OR 1000013 OR 1000200)

- Событие 4740 (Pavel) (индекс tag-winlogbeat-*):

text

winlog.event_id: 4740 AND winlog.event_data.TargetUserName: "pavel"

- Sysmon ID 1 (Pavel2) (индекс tag-winlogbeat-*):

text

winlog.event_id: 1 AND winlog.user_name: "nasedkin-win\pavel2"

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2026-08-26T13:58:24.363Z',to:'2026-08-26T17:26:10.376Z'))&_a=(columns:!(),dat...

Яндекс | Почта | Карты | Маркет | Новости | Словари | Видео | Музыка | Диск | Mail.Ru | Поиск в Интернете | Foto.Mail.Ru | Mail.Ru | Video.Mail.Ru | Предварительная... | Все закладки

elastic — Find apps, content, and more. ^/

D | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: nasedkin_ids

event.kind: "alert" AND (suricata.eve.alert.signature_id: 40000003 OR 1000013 OR 1000200)

Aug 26, 2026 @ 21:58:24.3... → Aug 27, 2026 @ 01:26:10.376 | Refresh

event.original: exists ×

Search field names | 0

Popular fields 1

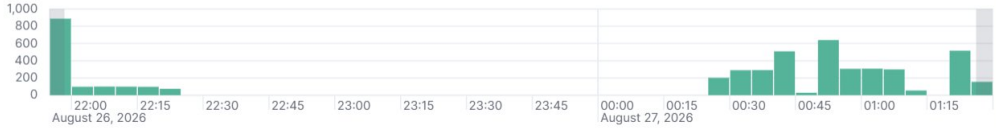
- event.original

Available fields 603

- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- destination.address
- destination.as.number
- destination.as.organization.name
- destination.bytes
- destination.domain
- destination.geo.city_name
- destination.geo.continent_name
- destination.geo.country_iso_code
- destination.geo.country_name
- destination.geo.location.lat
- destination.geo.location.lon

Add a field

Auto interval | No breakdown



Aug 26, 2026 @ 21:58:24.363 - Aug 27, 2026 @ 01:26:10.376 (interval: Auto - 5 minutes)

Documents (4,931) | Field statistics | Sort fields 1

@timestamp	Summary
Aug 27, 2026 @ 01:25:08.404	event.kind alert @timestamp Aug 27, 2026 @ 01:25:08.404 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:25:08.243	event.kind alert @timestamp Aug 27, 2026 @ 01:25:08.243 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:25:08.078	event.kind alert event.original {"timestamp":"2026-08-26T22:25:08.078096+0500","flow_id":635724911925687,"event_type":"alert","src_ip":"20.20.11.10","dest_ip":"10.20.11.10","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire…
Aug 27, 2026 @ 01:25:08.072	event.kind alert @timestamp Aug 27, 2026 @ 01:25:08.072 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:25:07.899	event.kind alert @timestamp Aug 27, 2026 @ 01:25:07.899 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:25:07.736	event.kind alert @timestamp Aug 27, 2026 @ 01:25:07.736 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0

Rows per page: 100 | 1 2 3 4 5

Document 96 of 500

Actions: View single document | View surrounding documents

Table | JSON

event.original | 0

Selected only

Field	Value
_ignored	event.original.keyword
event.original	{"timestamp":"2026-08-26T22:25:08.078096+0500","flow_id":635724911925687,"event_type":"alert","src_ip":"20.20.11.10","dest_ip":"10.20.11.10","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire/pcap","alert":{"action":"blocked","gid":1,"signature_id":1000013,"rev":1,"signa

Close

ENG 100% 1:41 27.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2026-08-26T13:58:24.363Z',to:'2026-08-26T17:26:10.376Z'))&_a=(columns:!(suric...

Яндекс | Почта | Карты | Маркет | Новости | Словари | Видео | Музыка | Диск | Mail.Ru | Поиск в Интернете | Foto.Mail.Ru | Mail.Ru | Video.Mail.Ru | Предварительная... | Все закладки

elastic | Find apps, content, and more. ^/

D | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: nasedkin_ids

event.kind: "alert" AND (suricata.eve.alert.signature_id: 40000003 OR 1000013 OR 1000200)

Aug 26, 2026 @ 21:58:24.3... → Aug 27, 2026 @ 01:26:10.376 | Refresh

Search field names | 0

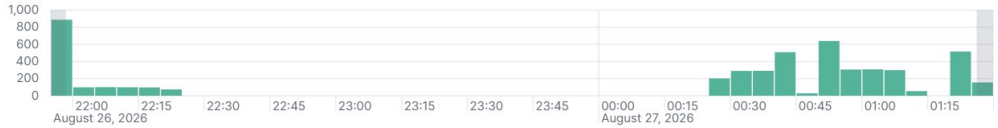
Selected fields 1
- suricata.eve.alert.signature

Popular fields 3
- suricata.eve.alert.signature_id
- event.original
- suricata.eve.alert.signature

Available fields 603
- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- destination.address
- destination.as.number
- destination.as.organization.name
- destination.bytes
- destination.domain
- destination.geo.city_name
- destination.geo.continent_name
- destination.geo.country_iso_code

Add a field

Auto interval | No breakdown



Aug 26, 2026 @ 21:58:24.363 - Aug 27, 2026 @ 01:26:10.376 (interval: Auto - 5 minutes)

Documents (4,931) | Field statistics | Columns 2 | Sort fields 1

@timestamp	suricata.eve.alert.signature
Aug 27, 2026 @ 01:26:10.376	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:26:09.376	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:26:08.372	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:26:07.120	IPS: Block Ping (DoS)
Aug 27, 2026 @ 01:26:06.100	IPS: Block Ping (DoS)
Aug 27, 2026 @ 01:26:05.071	IPS: Block Ping (DoS)

Rows per page: 100 | 1 2 3 4 5

Document 4 of 500

Actions: View single document | View surrounding documents

Table | JSON

Search field names or values | 0

Selected only

Field	Value
suricata.eve.alert.gid	1
suricata.eve.alert.rev	1
suricata.eve.alert.signature	IPS: Block Ping (DoS)
suricata.eve.alert.signature_id	1,000,013
suricata.eve.direction	to_server
suricata.eve.event_type	alert
suricata.eve.flow_id	635724911925687
suricata.eve.flow.dest_ip	10.20.11.10
suricata.eve.flow.src_ip	20.20.11.10
suricata.eve.icmp_code	0

Rows per page: 100 | 1

Close

ENG 100% 1:51 27.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2026-08-26T13:58:24.363Z',to:'2026-08-26T17:26:10.376Z'))&_a=(columns:!(),dat...

Яндекс | Почта | Карты | Маркет | Новости | Словари | Видео | Музыка | Диск | Mail.Ru | Поиск в Интернете | Foto.Mail.Ru | Mail.Ru | Video.Mail.Ru | Предварительная... | Все закладки

elastic | Find apps, content, and more. ^/

Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: nasedkin_ids

event.kind: "alert" AND (suricata.eve.alert.signature_id: 40000003 OR 1000013 OR 1000200)

Aug 26, 2026 @ 21:58:24.3... → Aug 27, 2026 @ 01:26:10.376 | Refresh

Search field names 0

Popular fields 2

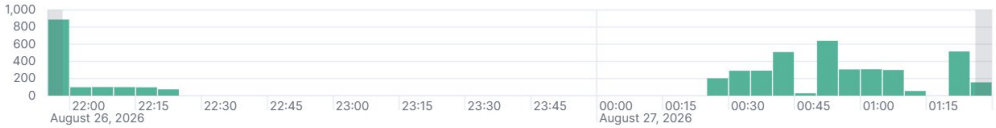
- suricata.eve.alert.signature_id
- event.original

Available fields 603

- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- destination.address
- destination.as.number
- destination.as.organization.name
- destination.bytes
- destination.domain
- destination.geo.city_name
- destination.geo.continent_name
- destination.geo.country_iso_code
- destination.geo.country_name
- destination.geo.location.lat
- destination.geo.location.lon
- destination.geo.region_iso_code

Add a field

Auto interval | No breakdown



Aug 26, 2026 @ 21:58:24.363 - Aug 27, 2026 @ 01:26:10.376 (interval: Auto - 5 minutes)

Documents (4,931) | Field statistics | Sort fields 1

@timestamp	Summary
Aug 27, 2026 @ 01:26:10.376	event.kind alert @timestamp Aug 27, 2026 @ 01:26:10.376 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:26:09.376	event.kind alert @timestamp Aug 27, 2026 @ 01:26:09.376 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:26:08.372	event.kind alert @timestamp Aug 27, 2026 @ 01:26:08.372 agent.ephemeral_id 29fdb47f-0024-4745-83dd-f242bdae878d agent.id 43fa6053-7f04-4e0b-a0c7-e5b3ceca1d0e agent.name nasedkin-IDS agent.type filebeat agent.version 8.10.…
Aug 27, 2026 @ 01:26:07.120	event.kind alert event.original {"timestamp":"2026-08-26T22:26:07.120089+0500","flow_id":635724911925687,"event_type":"alert","src_ip":"20.20.11.10","dest_ip":"10.20.11.10","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire…
Aug 27, 2026 @ 01:26:06.100	event.kind alert event.original {"timestamp":"2026-08-26T22:26:06.100580+0500","flow_id":635724911925687,"event_type":"alert","src_ip":"20.20.11.10","dest_ip":"10.20.11.10","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire…
Aug 27, 2026 @ 01:26:05.071	event.kind alert event.original {"timestamp":"2026-08-26T22:26:05.071238+0500","flow_id":635724911925687,"event_type":"alert","src_ip":"20.20.11.10","dest_ip":"10.20.11.10","proto":"ICMP","icmp_type":8,"icmp_code":0,"pkt_src":"wire…

Rows per page: 100 | 1 2 3 4 5

Document 470 of 500

Actions: View single document | View surrounding documents

Table | JSON

Search field names or values 0

Selected only

Field	Value
source.geo.location.lon	-97.822
source.ip	20.20.11.10
source.packets	3
source.port	58,970
suricata.eve.alert.category	(empty)
suricata.eve.alert.gid	1
suricata.eve.alert.rev	1
suricata.eve.alert.signature	IPS: Block external curl to internal HTTP
suricata.eve.alert.signature_id	1,000,200
suricata.eve.direction	to_server
suricata.eve.event_type	alert

Rows per page: 100 | 1

Close

ENG 100% 1:49 27.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),time:(from:'2026-08-26T13:58:24.363Z',to:'2026-08-26T17:26:10.376Z'))&_a=(columns:!('@timestamp',suricata.eve.alert.signature),...

elastic | Find apps, content, and more. | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | Save

Data view: nasedkin_ids

event.kind: "alert" AND (suricata.eve.alert.signature_id: 1000200)

Aug 26, 2026 @ 21:58:24.3... → Aug 27, 2026 @ 01:26:10.376 | Refresh

Search field names

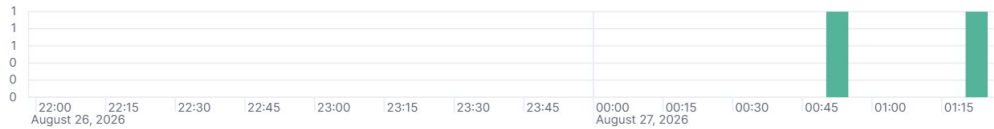
Selected fields 2
- @timestamp
- suricata.eve.alert.signature

Popular fields 6
- suricata.eve.alert.signature_id
- rule.id
- @timestamp
- event.original
- _id
- suricata.eve.alert.signature

Available fields 603
- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- destination.address
- destination.as.number
- destination.as.organization.name
- destination.bytes

Add a field

Auto interval | No breakdown



Aug 26, 2026 @ 21:58:24.363 - Aug 27, 2026 @ 01:26:10.376 (interval: Auto - 5 minutes)

Documents (2) | Field statistics | Columns 2 | Sort fields 1

@timestamp	suricata.eve.alert.signature
Aug 27, 2026 @ 01:24:25.794	IPS: Block external curl to internal HTTP
Aug 27, 2026 @ 00:54:55.281	IPS: Block external curl to internal HTTP

Document 1 of 2

Actions: View single document | View surrounding documents

Table | JSON

Search field names or values

Selected only

Field	Value
suricata.eve.alert.category	(empty)
suricata.eve.alert.gid	1
suricata.eve.alert.rev	1
suricata.eve.alert.signature	IPS: Block external curl to internal HTTP
suricata.eve.alert.signature_id	1,000,200
suricata.eve.direction	to_server
suricata.eve.event_type	alert
suricata.eve.flow_id	290847715078223
suricata.eve.flow.dest_ip	10.20.11.10
suricata.eve.flow.dest_port	80
suricata.eve.flow.sr	20.20.11.10

Rows per page: 100 | 1

Close

ENG 100% 2:10 27.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),time:(from:'2026-08-26T13:58:24.363Z',to:'2026-08-26T17:26:10.376Z'))&_a=(columns:!('@timestamp',rule.name),dataSource:(dat...

Яндекс | Почта | Карты | Маркет | Новости | Словари | Видео | Музыка | Диск | Mail.Ru | Поиск в Интернете | Foto.Mail.Ru | Mail.Ru | Video.Mail.Ru | Предварительная... | Все закладки

elastic — Find apps, content, and more. ^/

Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: nasedkin_ids

event.kind: "alert" AND (suricata.eve.alert.signature_id: 40000003 OR 1000013 OR 1000200)

Aug 26, 2026 @ 21:58:24.3... → Aug 27, 2026 @ 01:26:10.376 | Refresh

rule.name: exists ×

Search field names 0

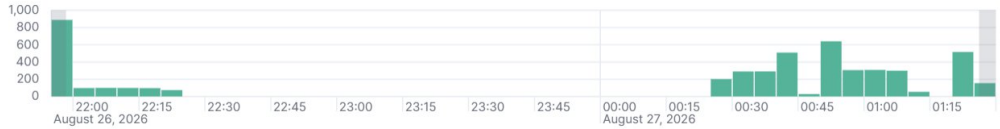
Selected fields 2
- @timestamp
- rule.name

Popular fields 7
- suricata.eve.alert.signature_id
- rule.id
- @timestamp
- event.original
- _id
- rule.name
- suricata.eve.alert.signature

Available fields 603
- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- destination.address

Add a field

Auto interval | No breakdown



Aug 26, 2026 @ 21:58:24.363 - Aug 27, 2026 @ 01:26:10.376 (interval: Auto - 5 minutes)

Documents (4,931) | Field statistics | Columns 2 | Sort fields 1

@timestamp	rule.name
Aug 27, 2026 @ 01:25:08.243	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:25:08.078	IPS: Block Ping (DoS)
Aug 27, 2026 @ 01:25:08.072	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:25:07.899	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:25:07.736	Possible Syn Scan Technique attempted from the internet
Aug 27, 2026 @ 01:25:07.568	Possible Syn Scan Technique attempted from the internet

Rows per page: 100 — 1 2 3 4 5

Document 97 of 500

Actions: View single document | View surrounding documents

Table | JSON

Search field names or values 0

Selected only

Field	Value
source.ip	20.20.11.10
source.packets	1
source.port	56,640
suricata.eve.alert.category	Attempted Information Leak
suricata.eve.alert.gid	1
suricata.eve.alert.rev	1
suricata.eve.alert.signature	Possible Syn Scan Technique attempted from the internet
suricata.eve.alert.signature_id	40,000,003
suricata.eve.direction	to_server
suricata.eve.event_type	alert
suricata.eve.flow_id	1155677955083555

Rows per page: 100 — 1

Close

ENG 100% 2:13 27.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:'2026-08-26T11:37:19.869Z',to:'2026-08-26T11:37:19.869Z'))&_a=(columns:!('@ti...

Яндекс | Почта | Карты | Маркет | Новости | Словари | Видео | Музыка | Диск | Mail.Ru | Поиск в Интернете | Foto.Mail.Ru | Mail.Ru | Video.Mail.Ru | Предварительная... | Все закладки

elastic | Find apps, content, and more. ^/

D | Discover | Check out context-aware Discover | Try ES|QL | Inspect | Alerts | + | Save

Data view: winlogbeat

winlog.event_id: 4740 AND winlog.event_data.TargetUserName: "pavel"

Aug 26, 2026 @ 19:37:19.869 → Aug 26, 2026 @ 19:37:19.869 | Update

Search field names | 0

Selected fields 2
- @timestamp
- event.original

Popular fields 2
- winlog.event_data.CommandLine
- event.original

Available fields 221
- @timestamp
- @version
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- ecs.version
- event.action
- event.code
- event.created
- event.kind
- event.original
- event.outcome

Add a field

Auto interval | No breakdown

Aug 26, 2026 @ 19:37:19.869 - Aug 26, 2026 @ 19:37:19.869 (interval: Auto - millisecond)

Documents (1) | **Field statistics** | Columns 2 | Sort fields 1

@timestamp	ginal
Aug 26, 2026 @ 19:37:19.869	

Заблокирована учетная запись пользователя. Субъект: Идентификатор безопасности: S-1-5-18 Имя учетной записи: NASEDKIN-WIN$ Домен учетной записи: WORKGROUP Идентификатор входа: 0x3E7 Заблокированная учетная запись: Идентификатор безопасности: S-1-5-21-28584859-90745515-1943227453-1002 Имя учетной записи: Pavel Дополнительные сведения: Имя вызывающего компьютера: NASEDKIN-WIN

Filter for | Filter out | Copy value

Document

Actions: View single document | View surrounding documents

Table | JSON

Search field names or values | 0

Selected only

Field	Value
event.kind	event
event.original	Заблокирована учетная запись пользователя. Субъект: Идентификатор безопасности: S-1-5-18 Имя учетной записи: NASEDKIN-WIN$ Домен учетной записи: WORKGROUP Идентификатор входа: 0x3E7 Заблокированная учетная запись: Идентификатор безопасности: S-1-5-21-28584859-90745515-1943227453-1002
event.outcome	success
event.provider	Microsoft-Windows-Security-Auditing
host.architecture	x86_64

Rows per page: 100 | 1

Close

13° | ENG | 100% | 2:20 27.08.2026

Не защищено 192.168.0.12:5601/app/discover#/?_g=(time:(from:'2026-08-26T11:25:25.746Z',to:'2026-08-26T13:25:27.442Z'))&_a=(columns:!('@timestamp',winlog.event_data.CommandLine),d...

Яндекс Почта Карты Маркет Новости Словари Видео Музыка Диск Mail.Ru Поиск в Интернете Foto.Mail.Ru Mail.Ru Video.Mail.Ru Предварительная... Все закладки

elastic Find apps, content, and more. ^/

D Discover Check out context-aware Discover Try ES|QL Inspect Alerts + Save

Data view winlogbeat winlog.event_id: 1 AND winlog.event_data.User: "nasedkin-win\pavel2"

Aug 26, 2026 @ 19:25:25.7... → Aug 26, 2026 @ 21:25:27.442 Refresh

Search field names 0

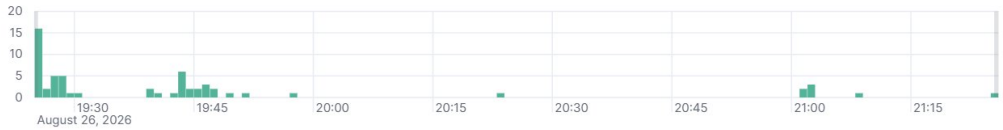
Selected fields 2
- @timestamp
- winlog.event_data.CommandLine

Popular fields 2
- winlog.event_data.CommandLine
- event.original

Available fields 221
- @timestamp
- @version
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- ecs.version
- event.action
- event.code
- event.created
- event.kind
- event.original
- event.outcome

Add a field

Auto interval No breakdown



Aug 26, 2026 @ 19:25:25.746 - Aug 26, 2026 @ 21:25:27.442 (interval: Auto - minute)

Documents (60) Field statistics Columns 2 Sort fields 1

@timestamp	winlog.event_data.CommandLine
Aug 26, 2026 @ 19:49:42.639	"C:\Windows\system32\mmc.exe" "C:\Windows\system32\eventvwr.msc" /s
Aug 26, 2026 @ 19:47:22.594	ssh user@10.20.11.10
Aug 26, 2026 @ 19:47:01.768	whoami
Aug 26, 2026 @ 19:46:54.924	ipconfig
Aug 26, 2026 @ 19:46:34.736	ping 10.20.11.10
Aug 26, 2026 @ 19:46:25.704	ping ping 10.20.11.10

Rows per page: 100 1

Document 3 of 60

Actions: View single document View surrounding documents

Table JSON

com 0

Selected only

Field	Value
event.original	Process Create: RuleName: - UtcTime: 2026-08-26 13:02:15.809 ProcessGuid: {821b00f7-e3d7-6a8e-5f04-000000000e00} ProcessId: 1768

Close

ENG 100% 2:25 27.08.2026