

Wykrywanie zagrożeń i reakcja na incydenty

Laboratorium 7

Tomasz Jarząbek 272279
Wiktoria Migasiewicz 272177

20.05.2025

Spis treści

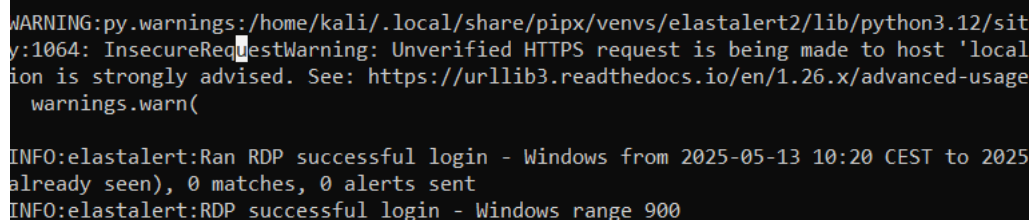
1	Rozwiązanie	3
1.1	Elastalert	3
1.2	Reguły	3
1.2.1	FTP	3
1.2.2	SSH - Linux	7
1.3	Dashboardy	11

1 Rozwiązanie

1.1 Elastalert

Przygotowano środowisko z poprzednich laboratoriów numer 6 - Elastalert z Kibaną i Logstash na Ubuntu, Alma Linux z Filebeat oraz Windows z Winlogbeat oraz obie maszyny z Heartbeat, Packetbeat, Metricbeat oraz Auditbeat. Zainstalowano na Ubuntu aplikację Elastalert2 w wirtualnym środowisku Venv, zmieniono plik `Proszę` zmodyfikować plik konfiguracyjny, by spełniał pewne warunki wskazane w instrukcji do laboratorium (np. folder z zasadami ustawiony jako folder *rules*). Po instalacji, uruchamia się go komendą:

```
1 source ~/elastalert-env/bin/activate
2 python -m elastalert.elastalert --verbose
```



```
WARNING:py.warnings:/home/kali/.local/share/pipx/venvs/elastalert2/lib/python3.12/site-packages/urllib3/util/ssl_.py:1064: InsecureRequestWarning: Unverified HTTPS request is being made to host 'localhost'. This request is strongly advised. See: https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warnings.warn()
INFO:elastalert:Ran RDP successful login - Windows from 2025-05-13 10:20 CEST to 2025-05-13 10:20 CEST (0 matches already seen), 0 matches, 0 alerts sent
INFO:elastalert:RDP successful login - Windows range 900
```

Rysunek 1: Zainstalowany Elastalert.

Następnie stworzono w Kibanie widok Data View dla Elastalert: **elastalert-***.

1.2 Reguły

1.2.1 FTP

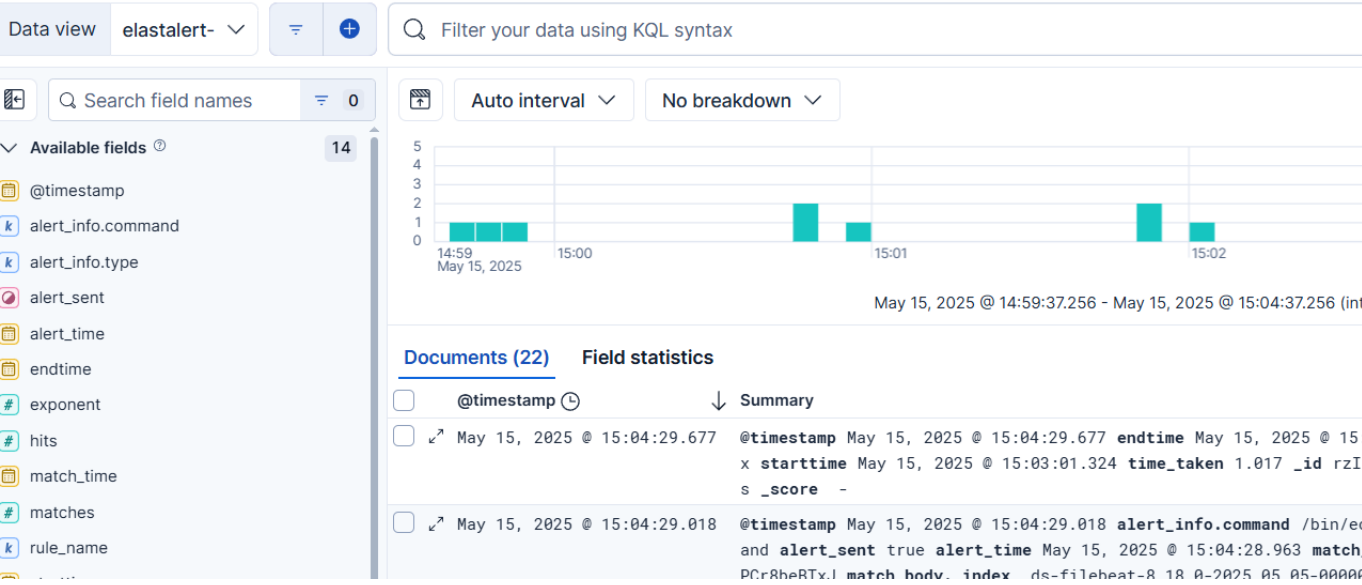
Sprawdzono nmap-em czy port 21 jest otwarty na Almie, co potwierdzono. Przystąpiono do ataku bruteforce na FTP.

```
(kali@kalisledczka)-[/usr/share/wordlists]
$ hydra -l test -P /usr/share/wordlists/rockyou.txt ftp://10.0.3.9
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-13 04:
43:20
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking ftp://10.0.3.9:21/
[STATUS] 230.00 tries/min, 230 tries in 00:01h, 14344169 to do in 1039:26h, 1
6 active
```

Rysunek 2: Atak na port 21 (FTP) na Alinę Linux w Kalim.

Następnie sprawdzono w Data View Elastalert, czy zostały wykryte jakieś logi Filebeata.



Rysunek 3: Logi FTP w Data View Kibany.

W logach Elastalert czytamy np.:

```
1 @timestampMay 13, 2025 @ 10:48:13.486endtimeMay 13, 2025 @ 10:48:13.249
  ↳ hits65matches12rule_nameFTP login failed - LinuxstarttimeMay 13, 2025
  ↳ @ 10:33:13.249time_taken0.237_idpgXUyJYB9XrJA4Rmhlux_ignored -
  ↳ _indexelastalert_status_status_score -
```

FTP login failed - niepowodzenie ataku brute force. Przeprowadzono również prawidłowy login w celu sprawdzenia działania reguły.

```
(kali@kalisledczka)-[/usr/share/wordlists]
$ ftp 10.0.3.9
Connected to 10.0.3.9.
220 (vsFTPD 3.0.5)
Name (10.0.3.9:kali): alma
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||48968|)
150 Here comes the directory listing.
drwxr-xr-x  2 1000      1000                6 Apr 29 14:41 Dokumenty
drwxr-xr-x  2 1000      1000                6 Apr 29 14:41 Muzyka
drwxr-xr-x  2 1000      1000           98 May 05 21:09 Obrazy
drwxr-xr-x  2 1000      1000                6 Apr 29 14:41 Pobrane
drwxr-xr-x  2 1000      1000                6 Apr 29 14:41 Publiczny
drwxr-xr-x  2 1000      1000                6 Apr 29 14:41 Pulpit
drwxr-xr-x  2 1000      1000                6 Apr 29 14:41 Szablony
drwxr-xr-x  2 1000      1000                6 Apr 29 14:41 Wideo
-rw-r--r--  1 0         0                9704 May 05 21:33 filebeat.yml
```

Rysunek 4: Poprawne logowanie FTP na Alnę.

```
hits 2 matches 0 rule_name FTP login successful - Li
8behlyq _ignored - _index elasticsearch_status_statu
```

Rysunek 5: Logi FTP w Data View Kibany - sukces.

```
291 hits 290 matches 289 rule_name FTP Brute-force attempt d
id CThS1JYBBYPCr8beg6uT _ignored - _index elasticsearch_
```

Rysunek 6: Logi FTP w Data View Kibana - cardinality.

Konstrukcja reguł FTP Linux:

```
1   name: "FTP login failed - Linux"
2 type: frequency
3 index: filebeat-*
4 num_events: 5
5 timeframe:
6   minutes: 30
7 filter:
8   - query:
9     query_string:
10      query: "message:\"FAIL LOGIN\""
11 alert:
12   - command
13 command: ["/bin/echo", "ALERT: Multiple FTP login failures on Linux"]
```

```
1   index: filebeat-*
2 name: "FTP login successful - Linux"
3 type: frequency
4 num_events: 1
5 timeframe:
6   minutes: 1
7 filter:
8   - query:
9     query_string:
10      query: "message:\"230 Login successful.\""
11 alert:
12   - command
```

```
13 command: ["/bin/echo", "ALERT: FTP LOGIN SUCCESS"]
```

```
1   name: "FTP Brute-force attempt detected - Linux"
2 type: cardinality
3 index: filebeat-*
4 cardinality_field: message
5 max_cardinality: 1
6 timeframe:
7   minutes: 5
8 filter:
9   - query:
10     query_string:
11       query: "message:(\"FAIL LOGIN\" OR \"230 Login successful.\")"
12 alert:
13   - command
14 command: ["/bin/echo", "ALERT: Possible FTP brute-force detected on Linux"]
```

1.2.2 SSH - Linux

Przeprowadzono następnie atak brute-force na SSH z Kali Linux na Almę Linux (jej port jest otwarty):

```
(kali@kalisledczka)-[~]
$ hydra -l test -P /usr/share/wordlists/rockyou.txt ssh://10.0.3.9
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not
  military or secret service organizations, or for illegal purposes (this
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-
43:49
[WARNING] Many SSH configurations limit the number of parallel tasks, i
ecommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to
waiting)) from a previous session found, to prevent overwriting, ./hyd
tore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries
/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.0.3.9:22/
[STATUS] 200.00 tries/min, 200 tries in 00:01h, 14344204 to do in 1195:
1 active
[STATUS] 171.33 tries/min, 514 tries in 00:03h, 14343892 to do in 1395:
active
```

Rysunek 7: Atak na SSH w Alma z Kali Linux.

```
5 hits 15 matches 3 rule_name SSH login failed - Linu
r8be6ZxD _ignored - _index elasticsearch_status_statu
```

Rysunek 8: Logi SSH w Data View Kibany - Failure dla SSH.

Jak widać, atak się nie powiódł, ale został wykryty z Filebeat i wyświetlony w Elastalert. Następnie przeprowadzono poprawne logowanie SSH do Almy.


```
(kali@kalisledczka)-[~]  
$ ssh alma@10.0.3.9  
alma@10.0.3.9's password:  
Activate the web console with: system  
  
Last failed login: Thu May 15 18:08:  
There were 3 failed login attempts s  
Last login: Thu May 15 18:08:23 2025  
[alma@localhost ~]$ exit  
wylogowanie  
Connection to 10.0.3.9 closed.
```

Rysunek 9: Poprawne logowanie SSH do Almy.

```
2 matches 2 rule_name SSH login successful - Linux  
PmT _ignored - _index elasticsearch_status
```

Rysunek 10: Wykryte poprawne logowanie w Elastalert.

Wykryte zostały dwa poprawne logowania do SSH na Almę.

Elastalert również wykrył regułę typu cardinality i wykrył podejrzenie ataku brute force.

```
10 hits 27 matches 0 rule_name SSH Brute-force attempt dete  
rzpp1JYBBYPCr8beE6Kp _ignored - _index elasticsearch_status
```

Rysunek 11: Reguła typu cardinality dla SSH w Elastalert.

```
1 name: "SSH login successful - Linux"  
2 type: frequency  
3 index: filebeat-*  
4 num_events: 1  
5 timeframe:  
6   minutes: 1
```

```
7 filter:
8   - query:
9       query_string:
10         query: "message:\"session opened for\""
11 alert:
12   - command
13 command: ["/bin/echo", "ALERT: SSH login SUCCESS"]
```

```
1 name: "SSH login failed - Linux"
2 type: frequency
3 index: filebeat-*
4 num_events: 5
5 timeframe:
6   minutes: 5
7 filter:
8   - query:
9       query_string:
10         query: "message:(\"Failed password\" OR \"Invalid user\") AND system.auth"
11 alert:
12   - command
13 command: ["/bin/echo", "ALERT: Multiple SSH login FAILURES"]
```

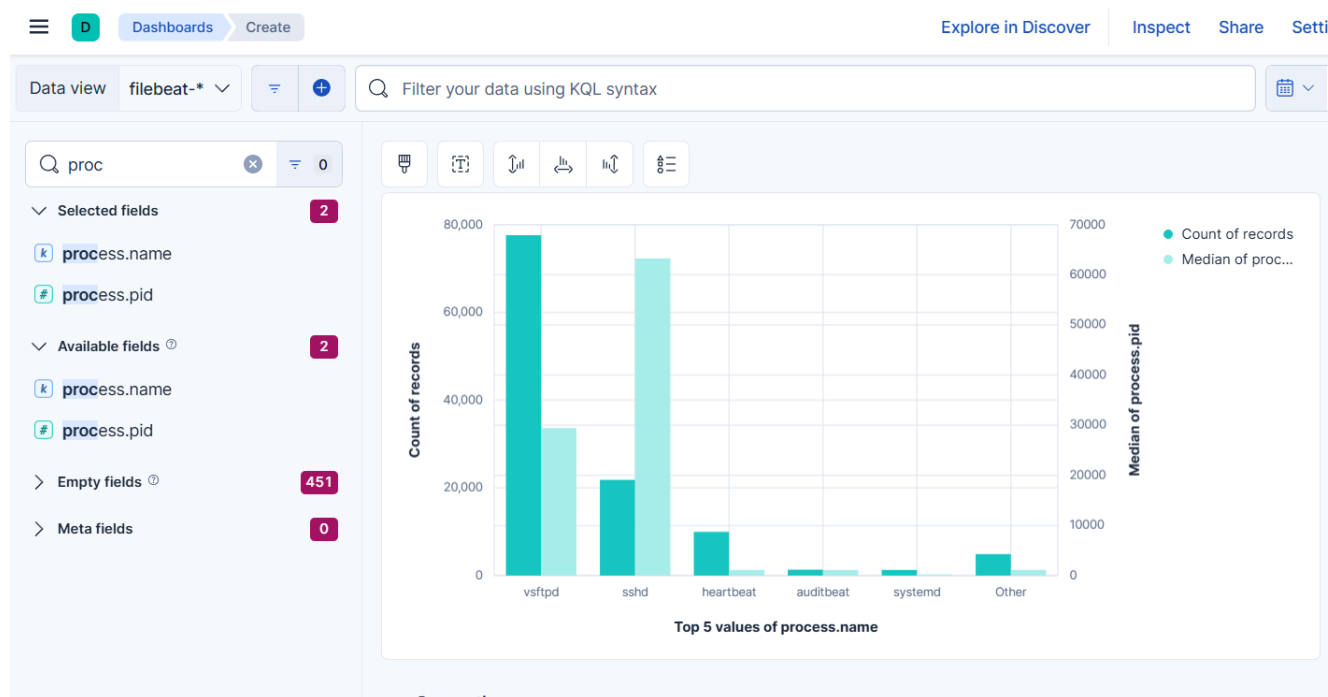
```
1 name: "SSH Brute-force attempt detected - Linux"
2 type: cardinality
3 index: filebeat-*
4 cardinality_field: ssh.user
5 max_cardinality: 3
6 timeframe:
7   minutes: 5
8 filter:
9   - query:
10       query_string:
11         query: "message:(\"Failed password\" OR \"Invalid user\") AND system.auth"
12 alert:
13   - command
14 command: ["/bin/echo", "ALERT: Possible SSH brute-force detected on Linux"]
```

1.3 Dashboardy

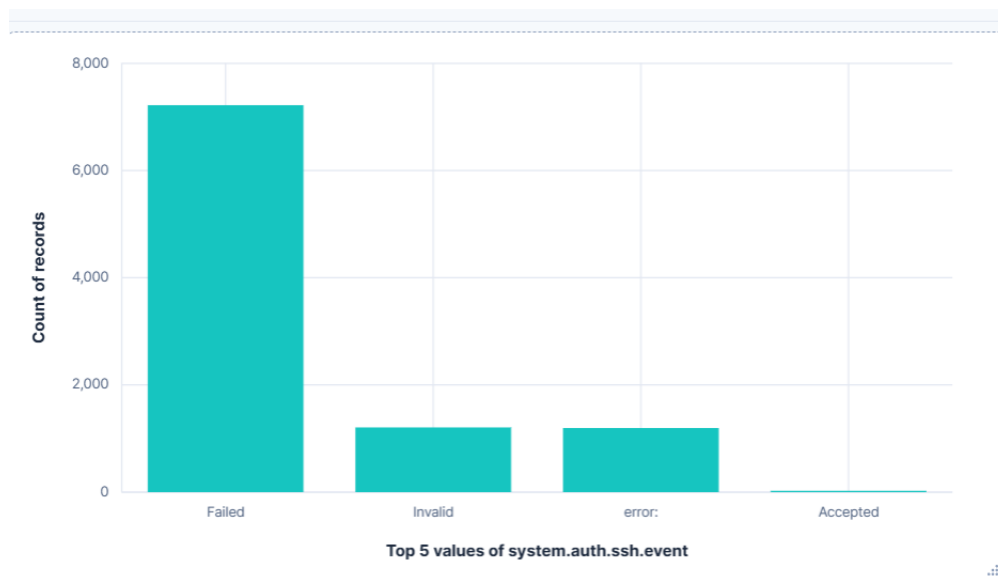
W GUI Kibany stworzono konkretne dashboardy lub znaleziono je (w zależności od konkretnego dashboardu).

Dla **Filebeat** są to:

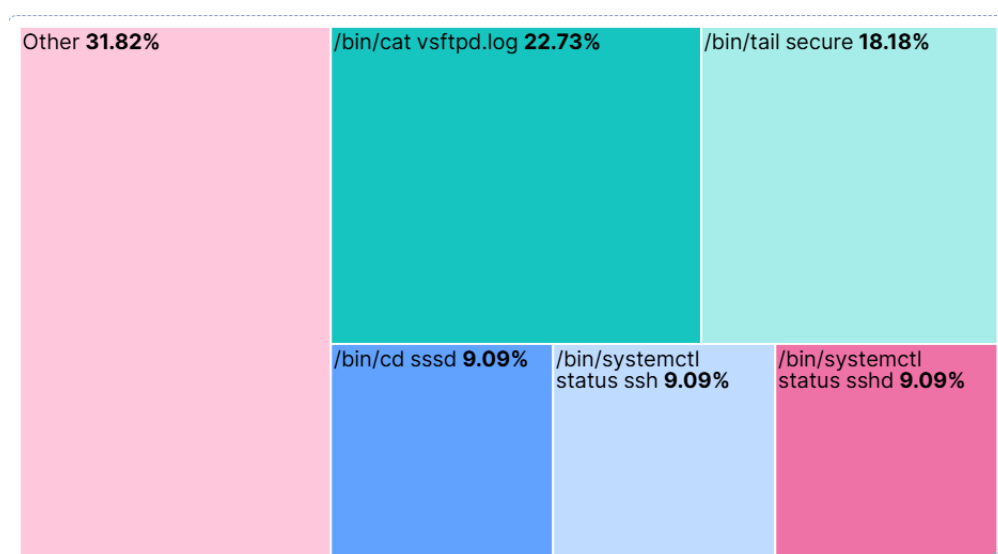
- Wykres przedstawiający listę procesów
- Lista komend wykonanych z uprawnieniami sudo
- Wykres słupkowy poprawnych oraz niepoprawnych logowań do usługi SSH
- Wykres słupkowy poprawnych oraz niepoprawnych logowań do usługi FTP



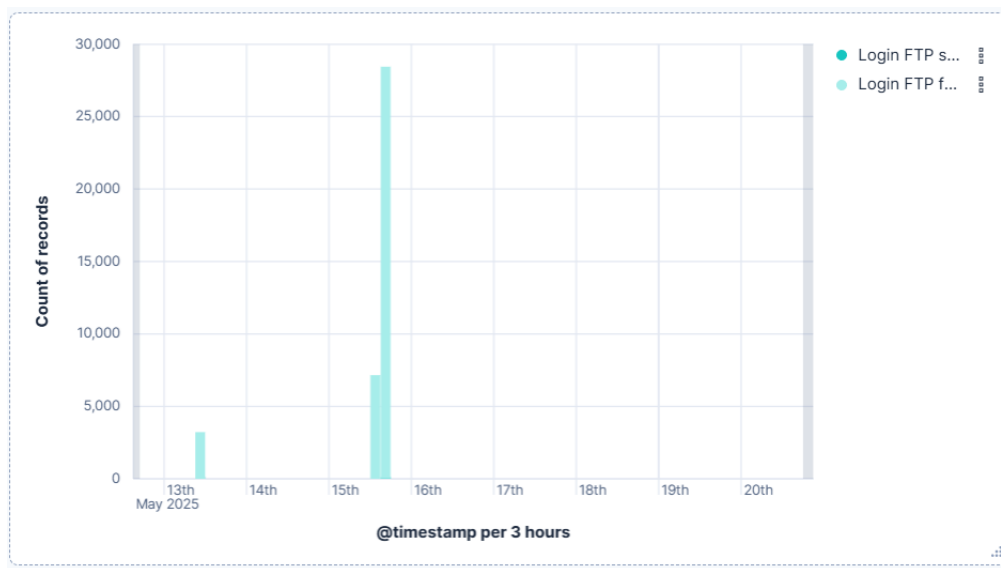
Rysunek 12: Dashboard Kibany Filebeat - Wykres przedstawiający listę procesów.



Rysunek 13: Dashboard Kibany Filebeat - Wykres słupkowy poprawnych oraz niepoprawnych logowań do usługi SSH.

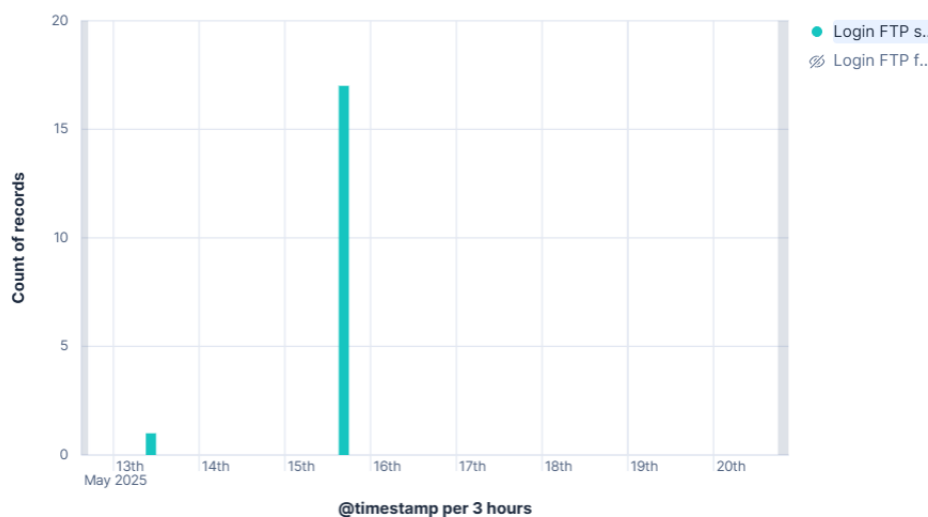


Rysunek 14: Dashboard Kibany Filebeat - Lista komend wykonanych z uprawnieniami sudo.



Rysunek 15: Dashboard Kibany Filebeat - Wykres słupkowy poprawnych oraz niepoprawnych logowań do usługi FTP.

Nie widać praktycznie wykresów dla poprawnych zalogowań do SSH i FTP, dlatego że ich proporcje są w skali kilku tysięcy do kilkunastu. Po naciśnięciu w dashboardzie na konkretną zmienną na legendzie, natomiast, wartości te skalują się i widać poprawnie wszystkie zalogowania.

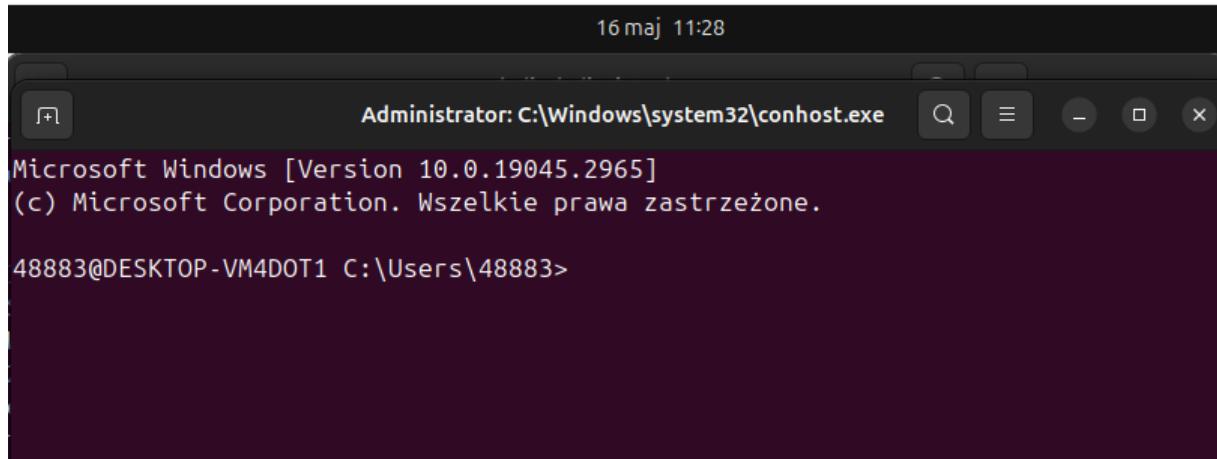


Rysunek 16: Dashboard Kibany Filebeat - Wykres słupkowy wyłącznie poprawnych logowań do usługi FTP.

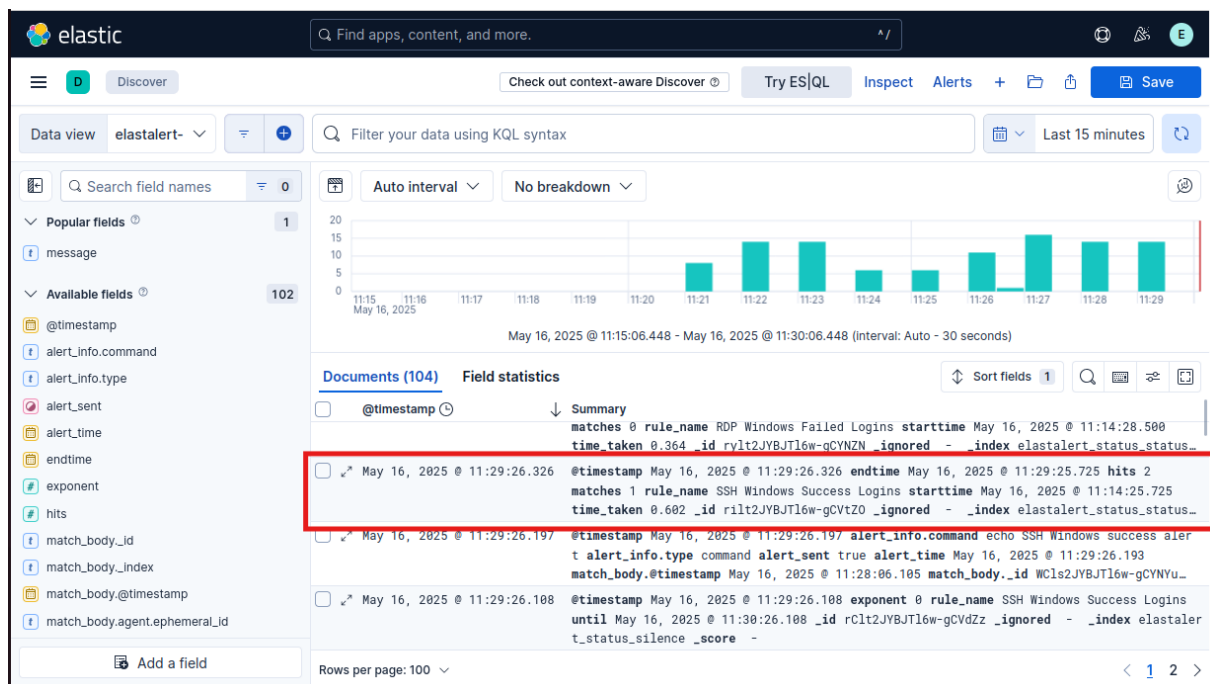
Reguły:

Bruteforce SSH na Windows:

Poprawne logowanie:



Rysunek 1. Poprawna próba logowania przez SSH



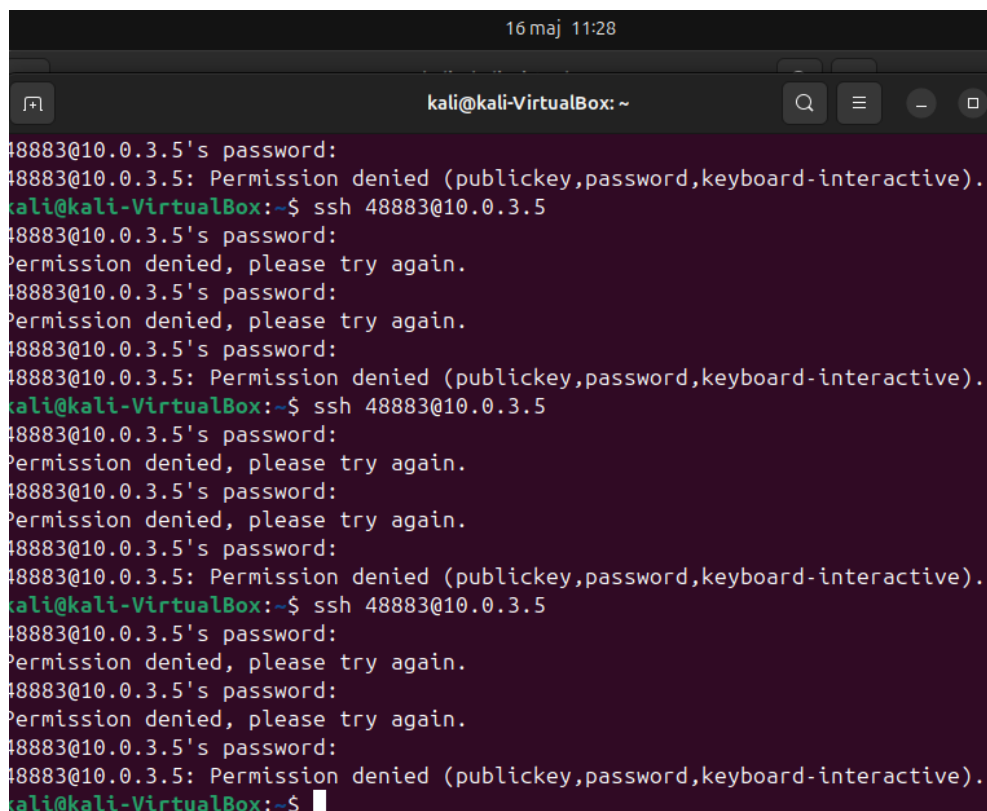
Rysunek 2. Log z widocznym alertem o poprawnym logowaniu

```
kali@kali-VirtualBox:~/rules$ cat ssh_windows_successful.yaml
name: "SSH Windows Success Logins"
type: frequency
index: winlogbeat-*
num_events: 1
timeframe:
  minutes: 5
filter:
  - term:
      winlog.event_data.LogonType: 8
  - query:
      query_string:
        query: 'message: "Logowanie do konta zakończyło się pomyślnie"'
alert:
  - command

command: "echo SSH Windows success alert"
kali@kali-VirtualBox:~/rules$
```

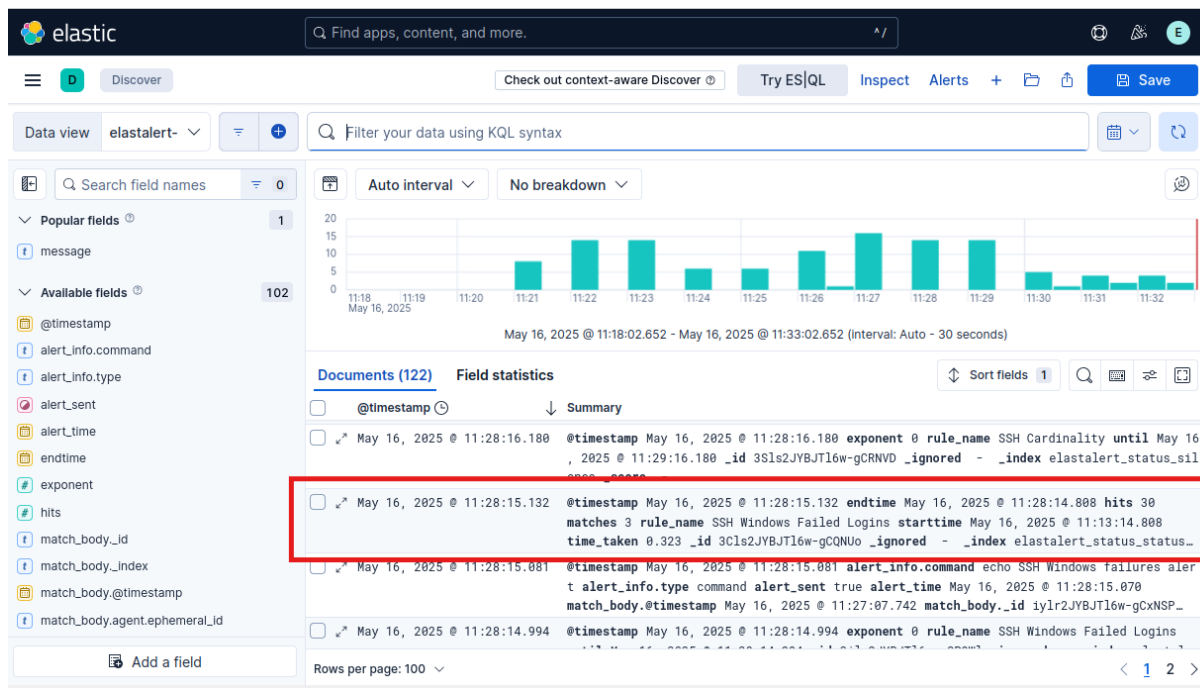
Rysunek 3. Treść reguły z pozytywnym logowaniem przez SSH

Wiele niepoprawnych logowań:



```
16 maj 11:28
kali@kali-VirtualBox: ~
48883@10.0.3.5's password:
48883@10.0.3.5: Permission denied (publickey,password,keyboard-interactive).
kali@kali-VirtualBox:~$ ssh 48883@10.0.3.5
48883@10.0.3.5's password:
Permission denied, please try again.
48883@10.0.3.5's password:
Permission denied, please try again.
48883@10.0.3.5's password:
48883@10.0.3.5: Permission denied (publickey,password,keyboard-interactive).
kali@kali-VirtualBox:~$ ssh 48883@10.0.3.5
48883@10.0.3.5's password:
Permission denied, please try again.
48883@10.0.3.5's password:
Permission denied, please try again.
48883@10.0.3.5's password:
48883@10.0.3.5: Permission denied (publickey,password,keyboard-interactive).
kali@kali-VirtualBox:~$ ssh 48883@10.0.3.5
48883@10.0.3.5's password:
Permission denied, please try again.
48883@10.0.3.5's password:
Permission denied, please try again.
48883@10.0.3.5's password:
48883@10.0.3.5: Permission denied (publickey,password,keyboard-interactive).
kali@kali-VirtualBox:~$
```

Rysunek 4. Niepoprawna próba logowania przez SSH



Rysunek 5. Log z widocznym alertem o niepoprawnym logowaniu

```
kali@kali-VirtualBox:~/rules$ cat ssh_windows_unsuccessful.yaml
name: "SSH Windows Failed Logins"
type: frequency
index: winlogbeat-*
num_events: 5
timeframe:
  minutes: 5
filter:
  - term:
      winlog.event_data.LogonType: 8
  - query:
      query_string:
        query: 'message: "Logowanie na koncie nie powiodło się"'
alert:
  - command
command: "echo SSH Windows failures alert"
kali@kali-VirtualBox:~/rules$
```

Rysunek 6. Treść reguły z negatywnym logowaniem przez SSH

The screenshot shows the Elastic Kibana interface. At the top, there's a search bar with the text "Find apps, content, and more." Below it, the "Discover" tab is active. The left sidebar shows the "Data view" section with a filter "elastalert-". The main area displays a KQL filter "Filter your data using KQL syntax" and a bar chart showing data over time. Below the chart, the "Documents (104)" section is visible, showing a list of documents. A red box highlights a document entry with the following details:

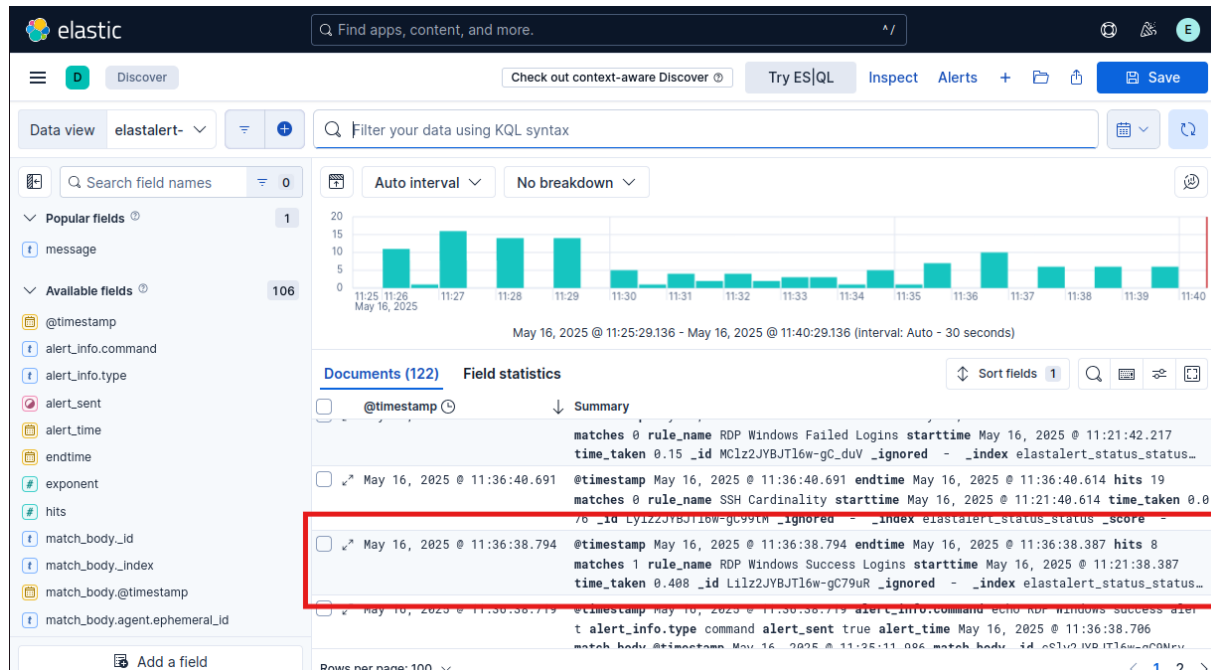
- ☐ ☒ May 16, 2025 @ 11:29:19.841
- @timestamp** May 16, 2025 @ 11:29:19.841
- endtime** May 16, 2025 @ 11:29:18.361
- hits** 35
- matches** 4
- rule_name** SSH Cardinality
- starttime** May 16, 2025 @ 11:14:18.361
- time_taken** 1.48
- _id** qylt2JYBJTl6w-gCPNbq_ignored
- _index** elastalert_status_score
- _score** -

```
kali@kali-VirtualBox:~/rules$ cat ssh_windows_cardinality.yaml
index: winlogbeat-*
cardinality_field: message
name: "SSH Cardinality"
type: cardinality
max_cardinality: 1
timeframe:
  minutes: 5
filter:
  - term:
      winlog.event_data.LogonType: 8
  - query:
      query_string:
        query: 'message: "Logowanie na koncie nie powiodło się" OR "Logowanie do
konta zakończyło się pomyślnie"'
alert:
  - command
command: "echo SSH Windows Bruteforce detected"

kali@kali-VirtualBox:~/rules$
```

Bruteforce RDP na Windows

Poprawne logowanie:

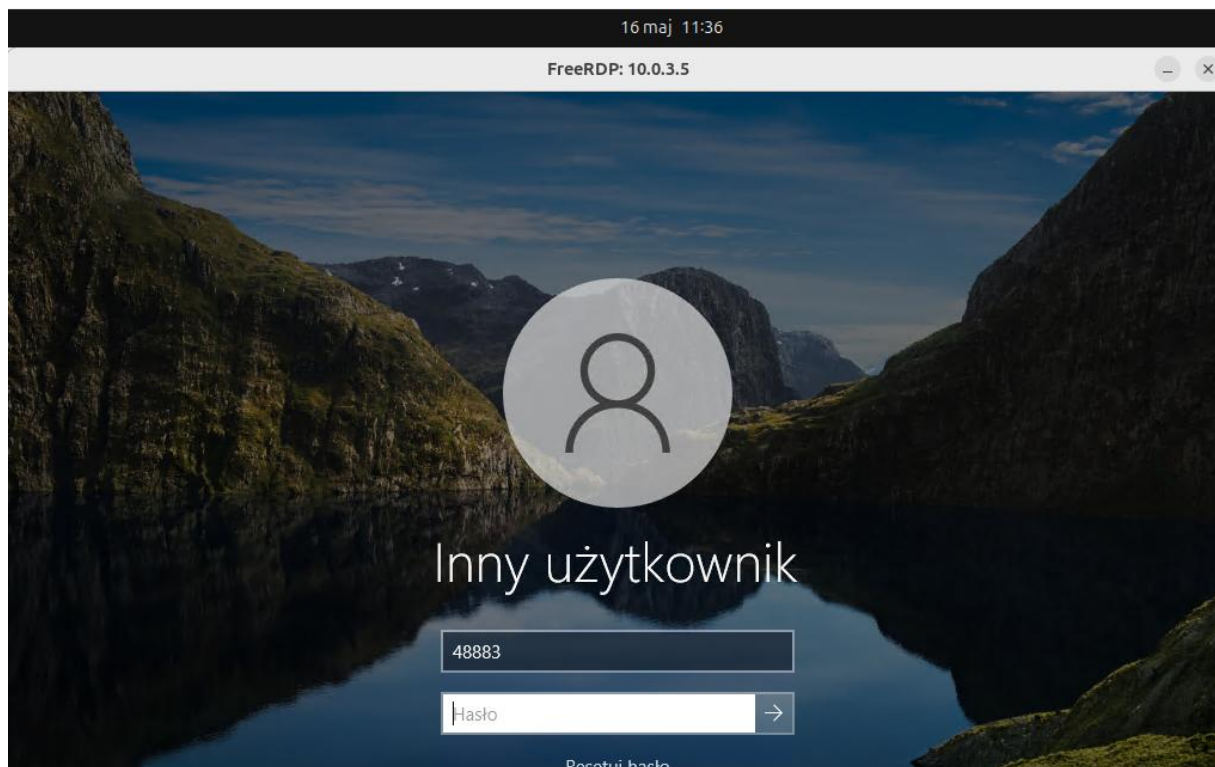


Rysunek 9. Alert o poprawnym logowaniu przez RDP

```
kali@kali-VirtualBox:~/rules$ cat rdp_windows_successful.yaml
name: "RDP Windows Success Logins"
type: frequency
index: winlogbeat-*
num_events: 1
timeframe:
  minutes: 5
filter:
  - term:
      winlog.event_data.LogonType: 3
  - query:
      query_string:
        query: 'message: "Logowanie do konta zakończyło się pomyślnie"'
alert:
  - command

command: "echo RDP Windows success alert"
kali@kali-VirtualBox:~/rules$
```

Rysunek 10. Treść reguły o poprawnym logowaniu przez RDP



Rysunek 11. Poprawne zalogowanie przez RDP

Wiele niepopranych logowań:

```
kali@kali-VirtualBox:~/rules$ cat rdp_windows_unsuccessful.yaml
name: "RDP Windows Failed Logins"
type: frequency
index: winlogbeat-*
num_events: 5
timeframe:
  minutes: 5

filter:
  - term:
      winlog.event_data.LogonType: 3
  - query:
      query_string:
        query: 'message: "Logowanie na koncie nie powiodło się"'

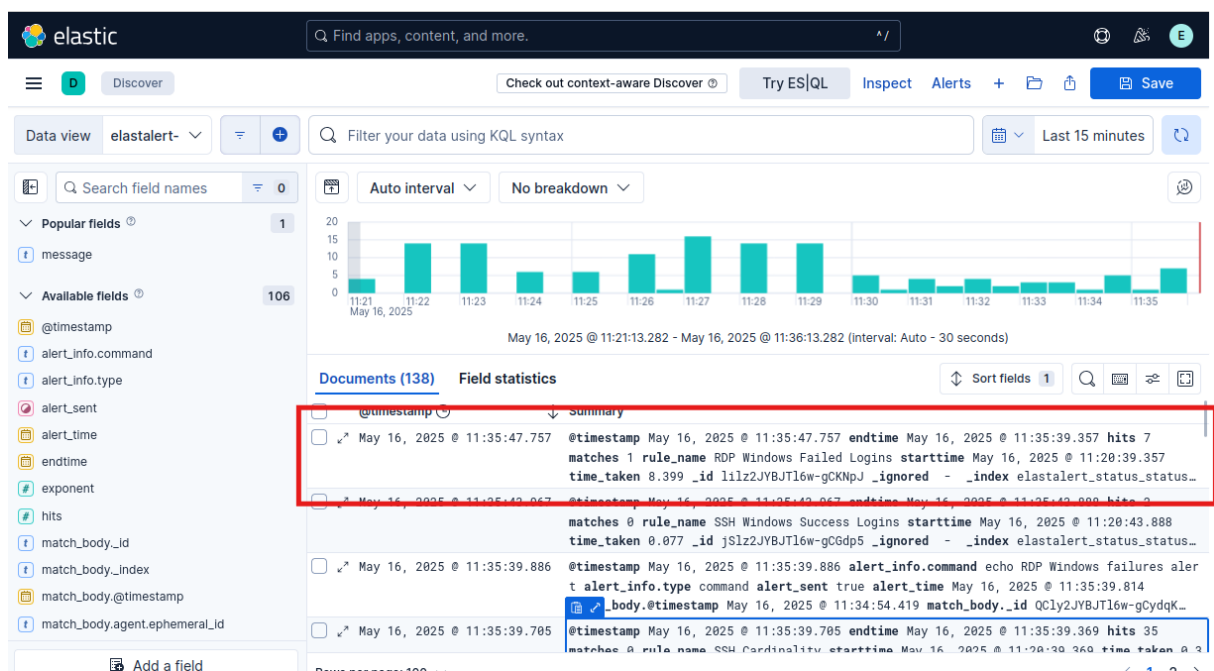
alert:
  - command

command: "echo RDP Windows failures alert"
kali@kali-VirtualBox:~/rules$
```

Rysunek 12. Treść reguły o niepoprawnym zalogowaniu przez RDP

```
16 maj 11:34
kali@kali-VirtualBox: ~
[11:34:49:238] [7490:7491] [WARN][com.freerdp.crypto] - CN = DESKTOP-VM4DOT1
Password:
[11:34:51:734] [7490:7491] [WARN][com.freerdp.core.nla] - SPNEGO received NTSTAT
US: STATUS_LOGON_FAILURE [0xC000006D] from server
[11:34:51:735] [7490:7491] [ERROR][com.freerdp.core] - nla_rcv_pdu:freerdp_set_
last_error_ex ERRCONNECT_LOGON_FAILURE [0x00020014]
[11:34:51:735] [7490:7491] [ERROR][com.freerdp.core.rdp] - rdp_rcv_callback: CO
NNECTION_STATE_NLA - nla_rcv_pdu() fail
[11:34:51:735] [7490:7491] [ERROR][com.freerdp.core.transport] - transport_check
_fds: transport->ReceiveCallback() - -1
kali@kali-VirtualBox:~$ xfreerdp /u:48883 /v:10.0.3.5
[11:34:53:790] [7505:7506] [WARN][com.freerdp.crypto] - Certificate verification
failure 'self-signed certificate (18)' at stack position 0
[11:34:53:791] [7505:7506] [WARN][com.freerdp.crypto] - CN = DESKTOP-VM4DOT1
Password:
[11:34:55:689] [7505:7506] [WARN][com.freerdp.core.nla] - SPNEGO received NTSTAT
US: STATUS_LOGON_FAILURE [0xC000006D] from server
[11:34:55:694] [7505:7506] [ERROR][com.freerdp.core] - nla_rcv_pdu:freerdp_set_
last_error_ex ERRCONNECT_LOGON_FAILURE [0x00020014]
[11:34:55:696] [7505:7506] [ERROR][com.freerdp.core.rdp] - rdp_rcv_callback: CO
NNECTION_STATE_NLA - nla_rcv_pdu() fail
[11:34:55:696] [7505:7506] [ERROR][com.freerdp.core.transport] - transport_check
_fds: transport->ReceiveCallback() - -1
kali@kali-VirtualBox:~$
```

Rysunek 13. Niepoprawne próby zalogowania przez RDP



Rysunek 14. Alert o niepoprawnym logowaniu przez RDP

The screenshot shows the Elastic Kibana interface. At the top, there's a search bar with the text "Find apps, content, and more." Below it, the "Discover" tab is active, showing a KQL search for "elastalert-". The interface includes a sidebar with "Popular fields" and "Available fields", a main search bar, a bar chart visualization, and a table of search results. A red box highlights the first result row.

Popular fields

- message

Available fields

- @timestamp
- alert_info.command
- alert_info.type
- alert_sent
- alert_time
- endtime
- exponent
- hits
- match_body_id
- match_body_index
- match_body.@timestamp
- match_body.agent.ephemeral_id

Search Results

Timestamp	Summary
May 16, 2025 @ 11:36:36.577	@timestamp May 16, 2025 @ 11:36:36.577 endtime May 16, 2025 @ 11:36:36.289 hits 15 matches 1 rule_name RDP Cardinality starttime May 16, 2025 @ 11:21:36.289 time_taken 0.288 _id Kylz2JYBJTl6w-gC6dsM _ignored - _index elastalert_status_status _score -
May 16, 2025 @ 11:36:36.534	@timestamp May 16, 2025 @ 11:36:36.534 alert_info.command echo RDP Windows Bruteforce detected alert_info.type command alert_sent true alert_time May 16, 2025 @ 11:36:36.528 match_body.@timestamp May 16, 2025 @ 11:35:11.986 match_body._id cSly2JYBJTl6w-gC9Nr_v
May 16, 2025 @ 11:36:36.470	@timestamp May 16, 2025 @ 11:36:36.470 exponent 0 rule_name RDP Cardinality until May 16, 2025 @ 11:37:36.470 _id KSLz2JYBJTl6w-gC5tt7 _ignored - _index elastalert_status_silence _score -
May 16, 2025 @ 11:36:31.453	@timestamp May 16, 2025 @ 11:36:31.453 endtime May 16, 2025 @ 11:36:31.338 hits 18 matches 1 rule_name SSH Windows Failed Login starttime May 16, 2025 @ 11:31:31.298

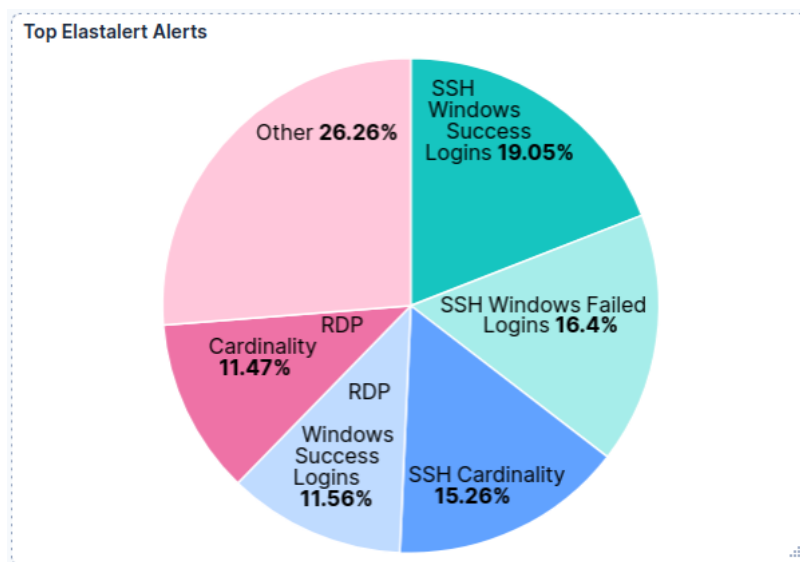
```
kali@kali-VirtualBox:~/rules$ cat rdp_windows_cardinality.yaml
index: winlogbeat-*
cardinality_field: message
name: "RDP Cardinality"
type: cardinality
max_cardinality: 1
timeframe:
  minutes: 5
filter:
  - term:
      winlog.event_data.LogonType: 3
  - query:
      query_string:
        query: 'message: "Logowanie na koncie nie powiodło się" OR "Logowanie do
konta zakończyło się pomyślnie"'
alert:
  - command
command: "echo RDP Windows Bruteforce detected"

kali@kali-VirtualBox:~/rules$
```

Dashboard

Elastalert

- Wykres kołowy najczęściej wznieczanych alertów



Rysunek 17. Wykres kołowy najczęściej wznieczanych alertów

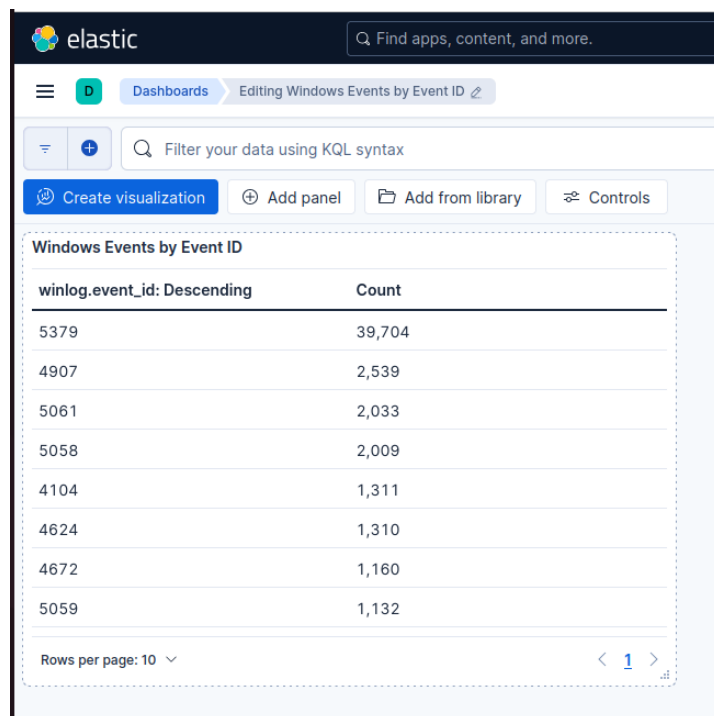
- Listę najnowszych alertów

Latest Elastalert LAerts		
1,063 documents		
<div>Columns 2Sort fields 1</div>		
<input type="checkbox"/>	@timestamp	rule_name
<input type="checkbox"/>	May 16, 2025 @ 13:13:39.604	SSH Windows Failed Logins
<input type="checkbox"/>	May 16, 2025 @ 13:13:33.791	SSH Cardinality
<input type="checkbox"/>	May 16, 2025 @ 13:13:24.110	RDP Cardinality
<input type="checkbox"/>	May 16, 2025 @ 13:13:07.421	SSH Windows Success Logins
<input type="checkbox"/>	May 16, 2025 @ 13:13:07.380	RDP Windows Success Logins
Rows per page: 100		
<div>< 1 2 3 4 5 ></div>		

Rysunek 18. Lista najnowszych alertów

Winlogbeat

- Tabela podsumowująca liczbę zdarzeń w systemie Windows, jednocześnie wskazując na ich identyfikator

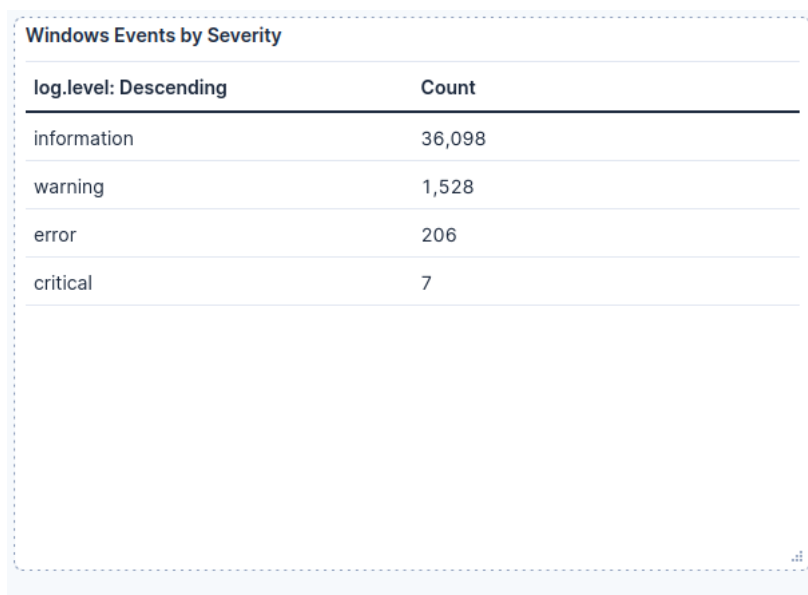


The screenshot shows the Elastic dashboard interface. At the top, there's a search bar with the text "Find apps, content, and more." Below it, the dashboard title is "Editing Windows Events by Event ID". A search bar for KQL syntax is present. The main visualization is a table titled "Windows Events by Event ID". The table has two columns: "winlog.event_id: Descending" and "Count". The data is sorted by event ID in descending order. The table shows 10 rows of data. At the bottom, there's a pagination control showing "Rows per page: 10" and a page number "1".

winlog.event_id: Descending	Count
5379	39,704
4907	2,539
5061	2,033
5058	2,009
4104	1,311
4624	1,310
4672	1,160
5059	1,132

Rysunek 19. Tabela podsumowująca liczbę zdarzeń w systemie Windows

- Tabela podsumowująca liczbę zdarzeń w systemie Windows wskazując na ich poziom krytyczności



The screenshot shows a table titled "Windows Events by Severity". The table has two columns: "log.level: Descending" and "Count". The data is sorted by log level in descending order. The table shows 4 rows of data. The log levels are information, warning, error, and critical.

log.level: Descending	Count
information	36,098
warning	1,528
error	206
critical	7

Rysunek 20. Tabela podsumowująca liczbę zdarzeń w systemie Windows wskazując na ich poziom krytyczności

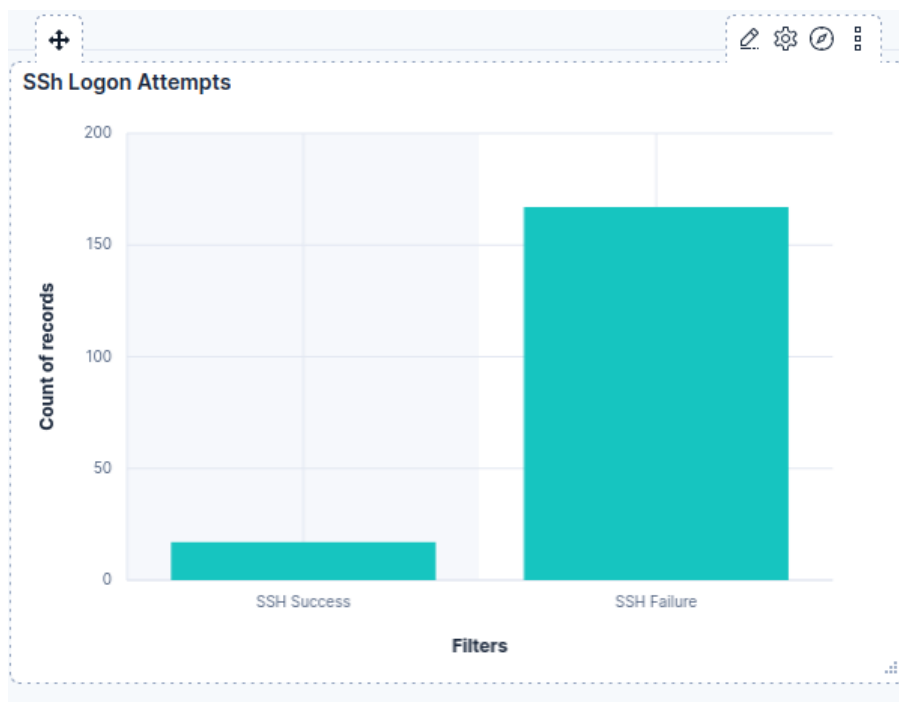
- **Wykres słupkowy poprawnych oraz niepoprawnych logowań do usługi RDP**

Zerowa liczebność poprawnych połączeń RDP wynika z kolejności realizacji zadań. Reguła RDP została wdrożona po stworzeniu wykresu.



Rysunek 21. Wykres słupkowy poprawnych oraz niepoprawnych logowań do usługi RDP

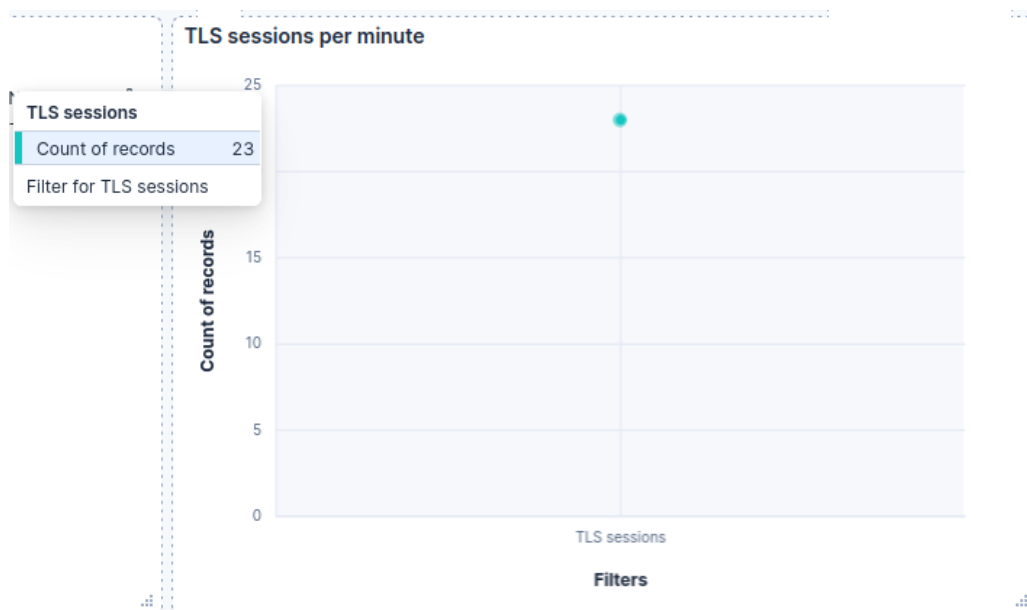
- **Wykres słupkowy poprawnych oraz niepoprawnych logowań do usługi SSH**



Rysunek 22. Wykres słupkowy poprawnych oraz niepoprawnych logowań do usługi SSH

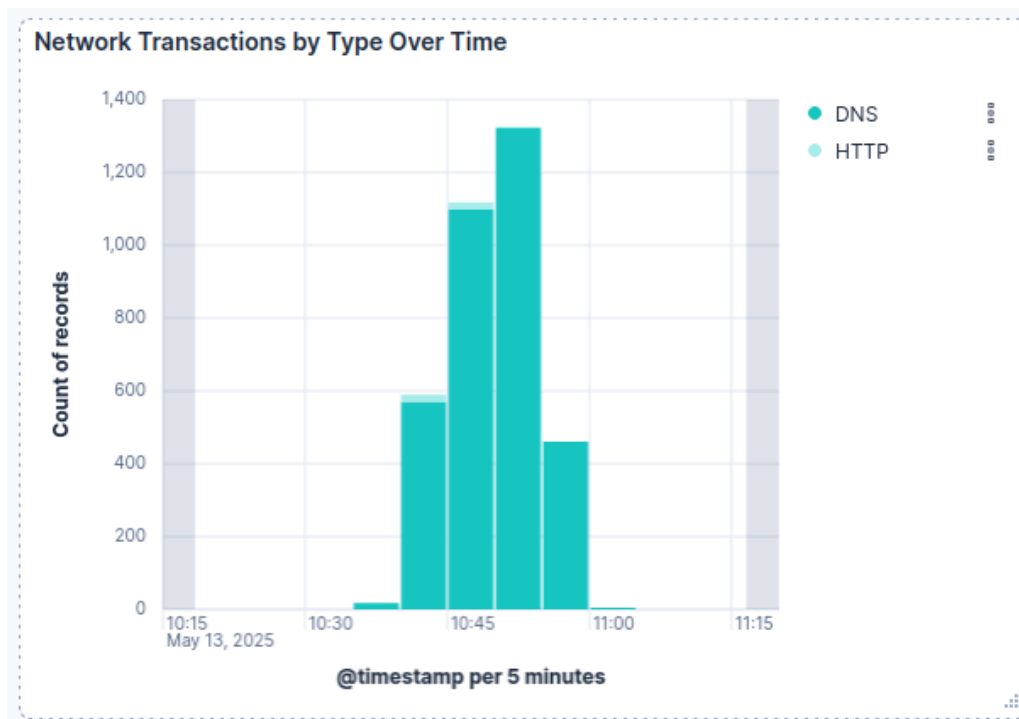
Packetbeat

- Podsumowanie liczby sesji TLS na minutę



Rysunek 23. Podsumowanie liczby sesji TLS na minutę

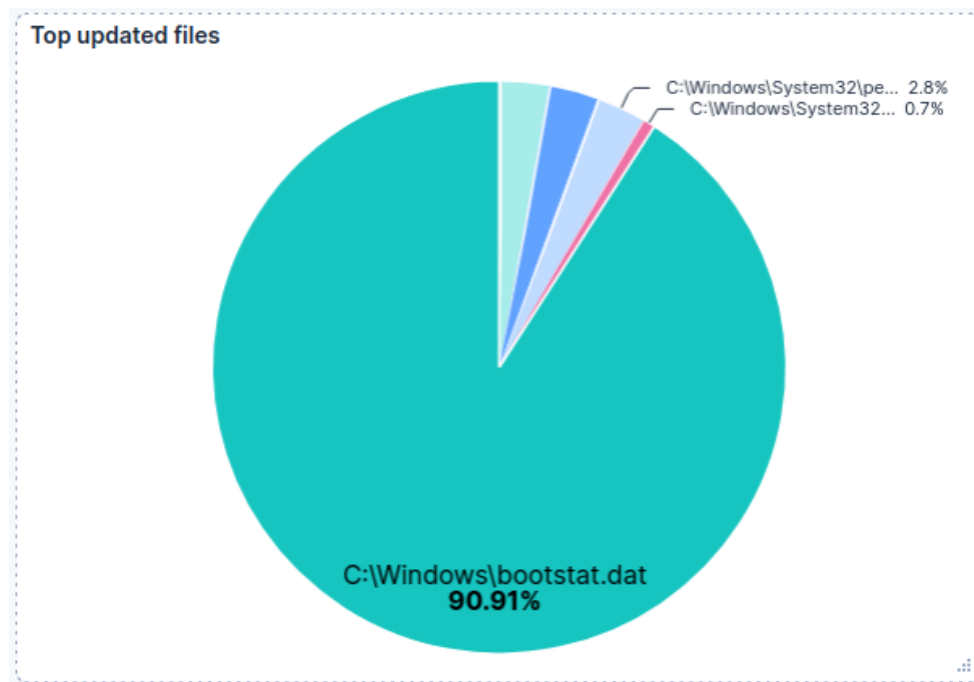
- Podsumowanie transakcji sieciowych w oparciu o ich typ na jednostkę czasu



Rysunek 24. Podsumowanie transakcji sieciowych w oparciu o ich typ na jednostkę czasu

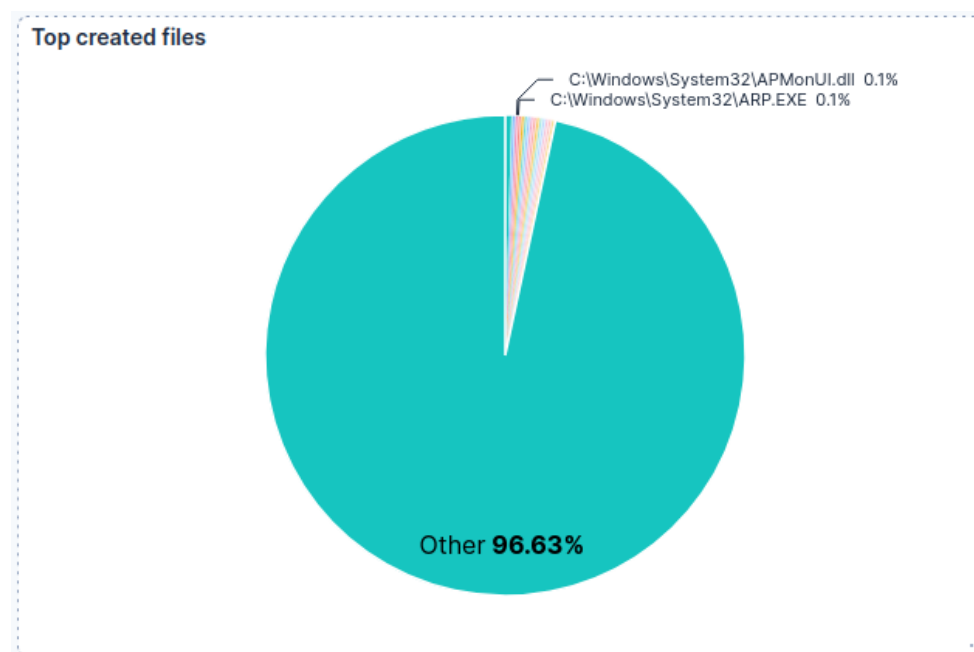
Auditbeat

- Wykres kołowy najczęściej zmienianych plików



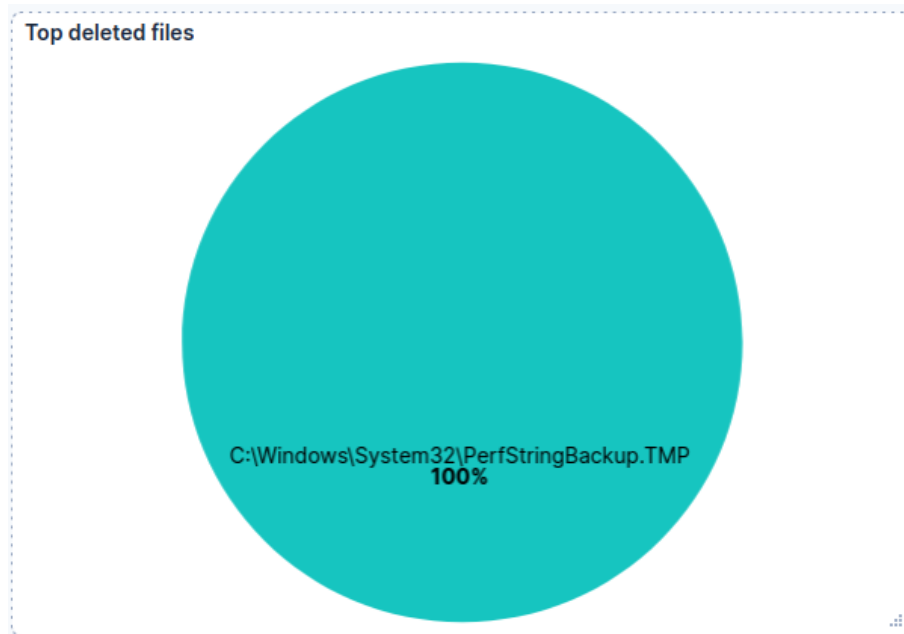
Rysunek 25. Wykres kołowy najczęściej zmienianych plików

- Wykres kołowy najczęściej tworzonych plików



Rysunek 26. Wykres kołowy najczęściej tworzonych plików

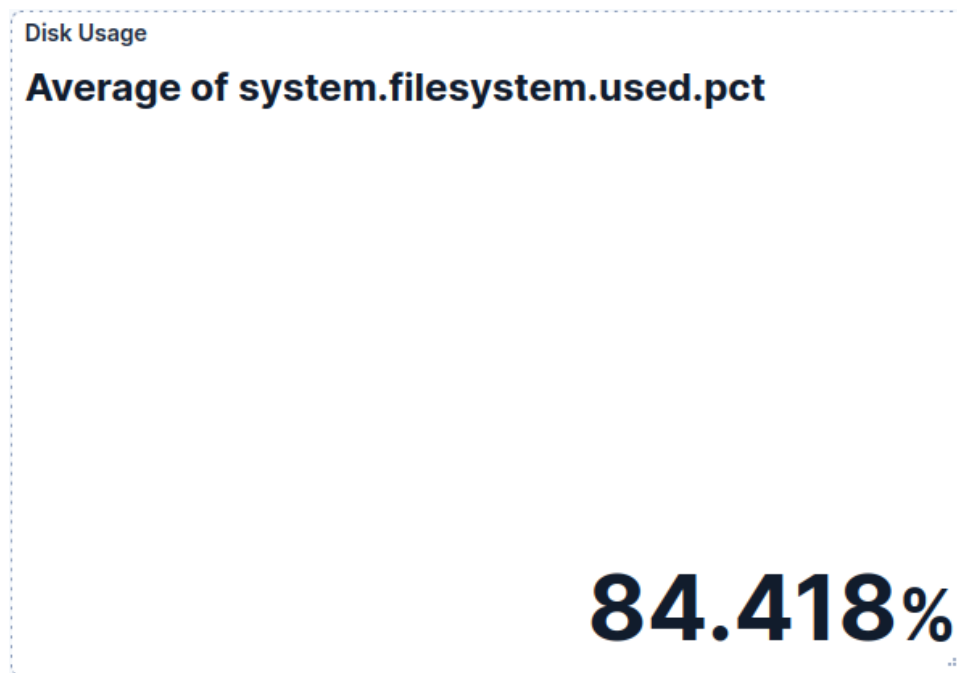
- Wykres kołowy najczęściej usuwanych plików



Rysunek 27. Wykres kołowy najczęściej usuwanych plików

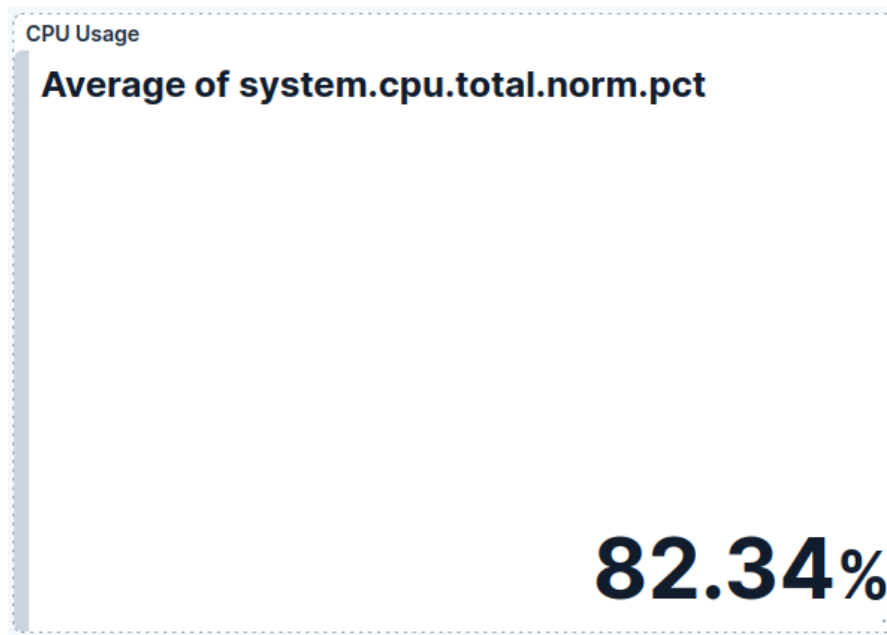
Metricbeat

- Wskaźnik użycia dysku



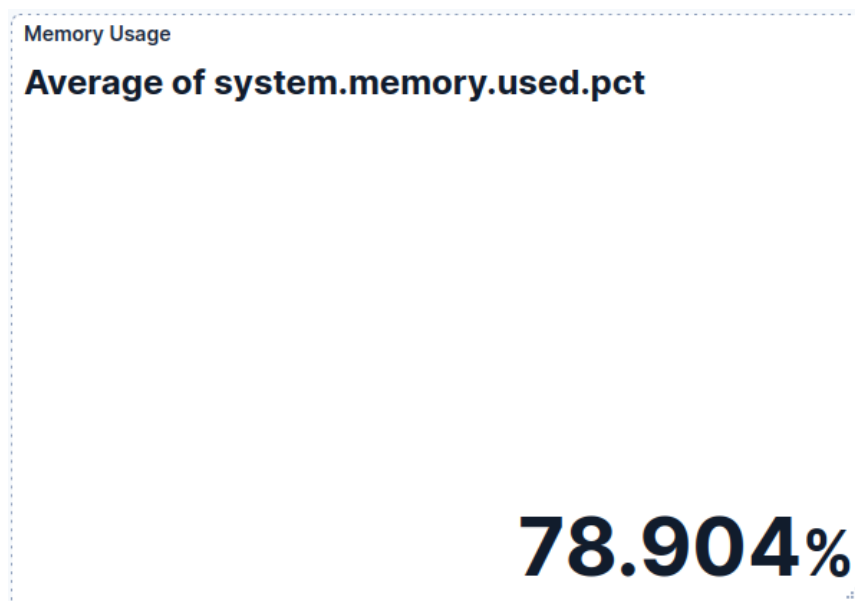
Rysunek 28. Wskaźnik użycia dysku

- Wskaźnik użycia procesora



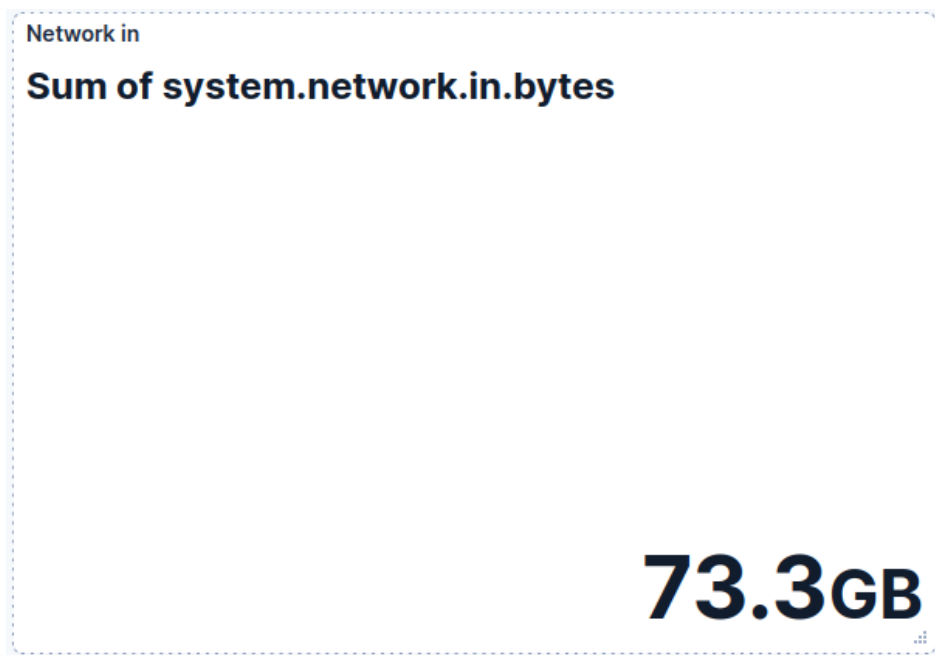
Rysunek 29. Wskaźnik użycia procesora

- Wskaźnik użycia pamięci



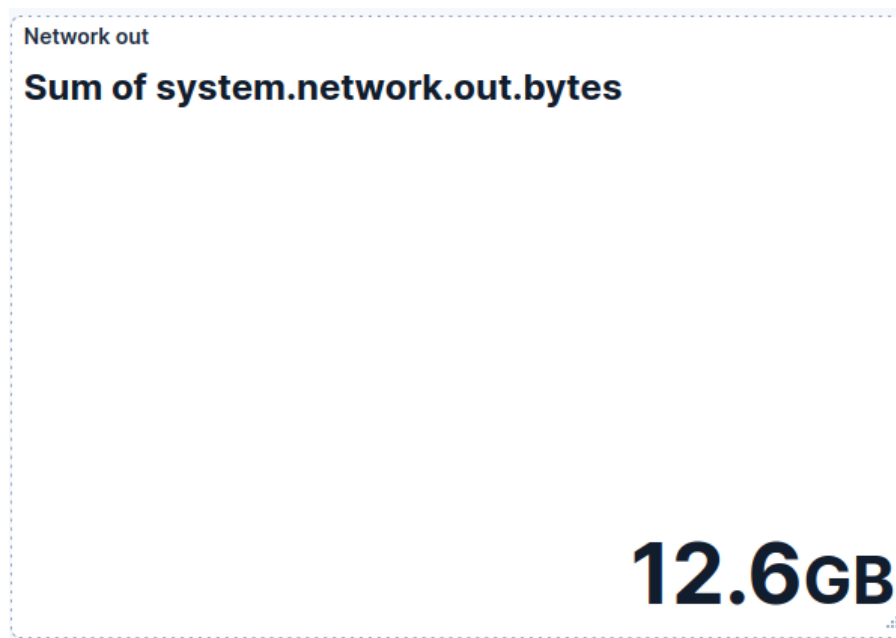
Rysunek 30. Wskaźnik użycia pamięci

- Wskaźnik transferu przychodzącego



Rysunek 31. Wskaźnik transferu przychodzącego

- Wskaźnik transferu wychodzącego

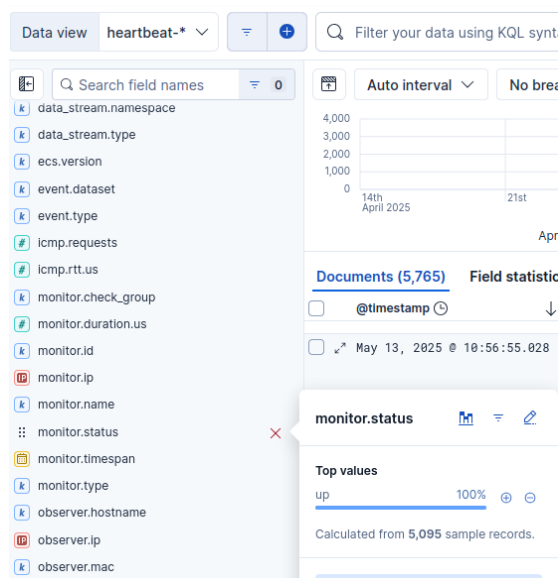


Rysunek 31. Wskaźnik transferu wychodzącego

Heartbeat

- Wykres słupkowy niedostępności hostów

Wszystkie hosty były dostępne przez 100% czasu, dlatego nie udało się wykonać wykresu o niedostępności hostów.



Rysunek 32. Dane o dostępności hostów