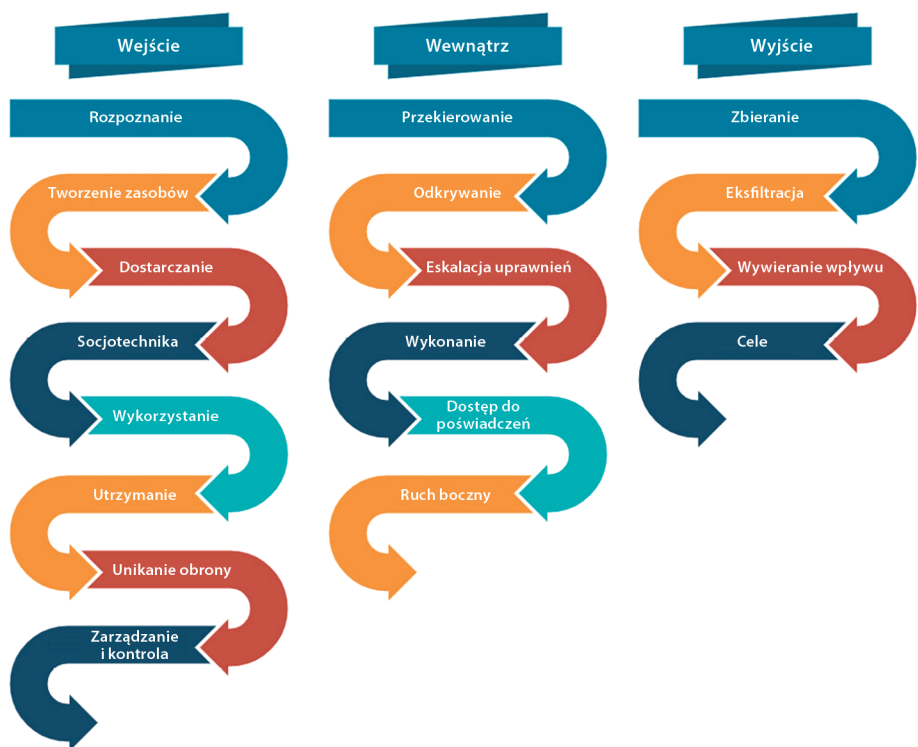
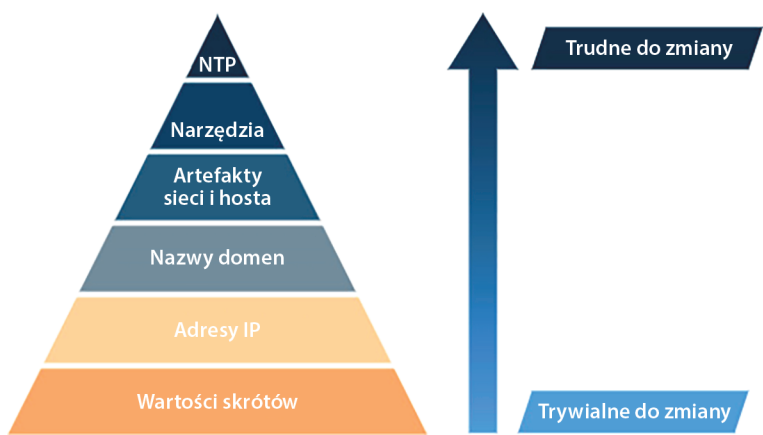


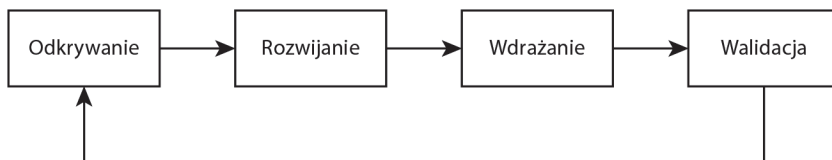
# Rozdział 1. Podstawy inżynierii detekcji



Rysunek 1.1. Model Unified Kill Chain

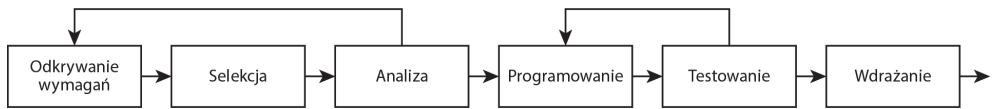


Rysunek 1.2. Model piramidy bólu Davida Bianco

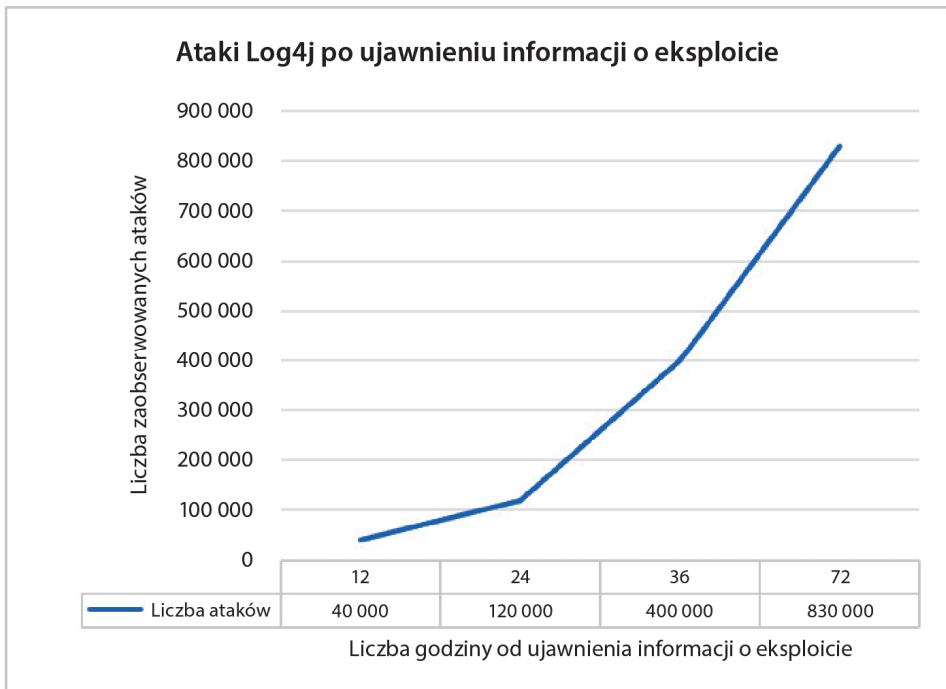


**Rysunek 1.3. Procesy wchodzące w skład inżynierii detekcji**

## Rozdział 2. Cykl życia inżynierii detekcji

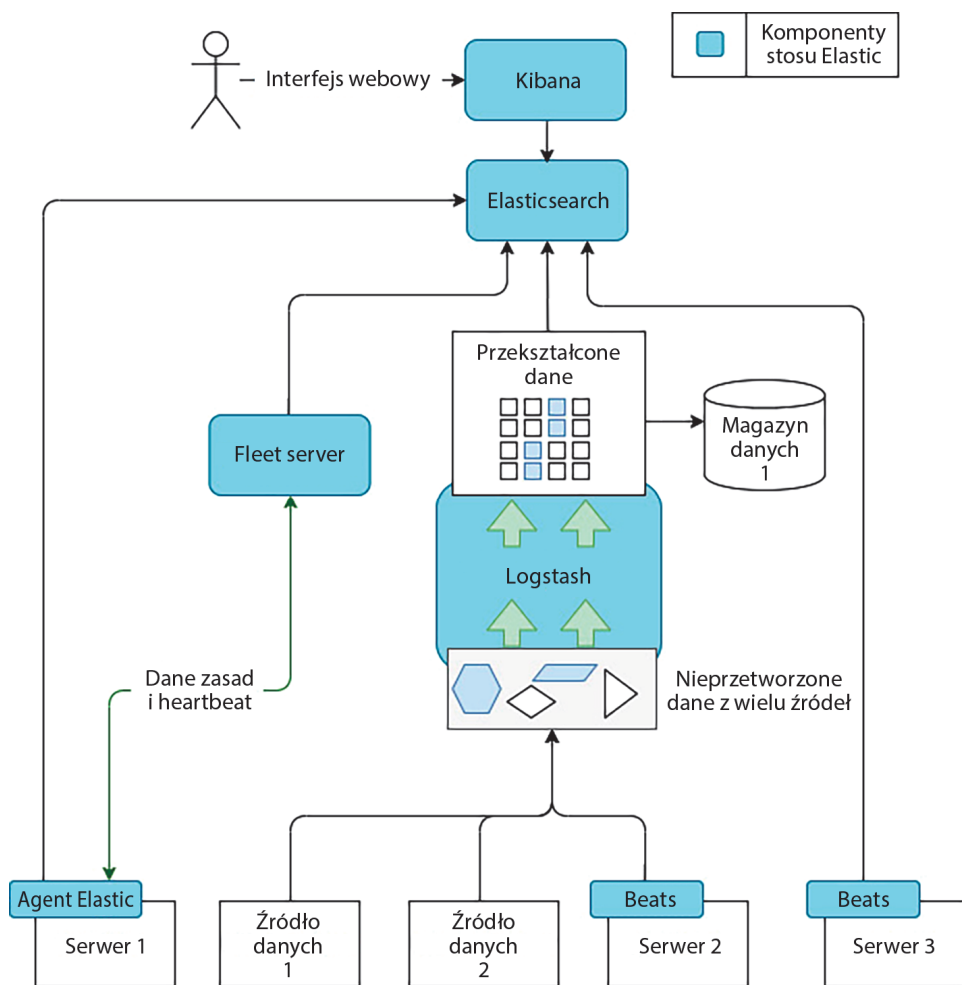


Rysunek 2.1. Cykl życia inżynierii detekcji



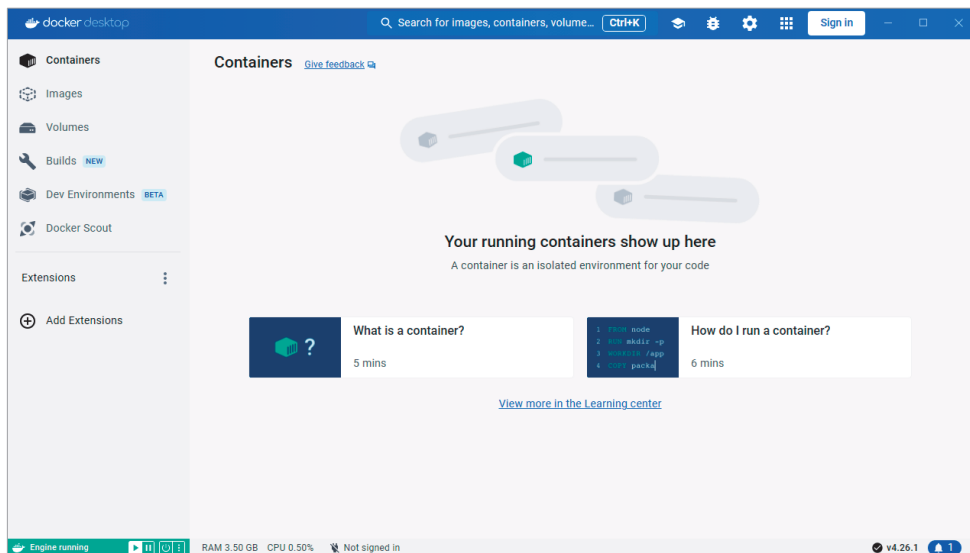
Rysunek 2.2. Statystyki exploitów Log4j. Źródło danych:  
<https://blog.checkpoint.com/security/the-numbers-behind-a-cyber-pandemic-detailed-dive/>

## Rozdział 3. Budowa laboratorium testowego inżynierii detekcji



Rysunek 3.1. Przykład wdrożenia Elasticsearch





Rysunek 3.2. Docker Desktop w systemie Windows

```
examiner@datasrv02:~$ docker --help

Usage: docker [OPTIONS] COMMAND

A self-sufficient runtime for containers

Options:
  --config string      Location of client config files (default "/home/
  -c, --context string  Name of the context to use to connect to the dae
                        "docker context use")
  -D, --debug          Enable debug mode
  -H, --host list       Daemon socket(s) to connect to
  -l, --log-level string Set the logging level ("debug"|"info"|"warn"|"er
                        --tls          Use TLS; implied by --tlsverify
                        --tlscacert string Trust certs signed only by this CA (default "/ho
                        --tlscert string  Path to TLS certificate file (default "/home/exa
                        --tlskey string   Path to TLS key file (default "/home/examiner/.d
                        --tlsverify      Use TLS and verify the remote
  -v, --version        Print version information and quit

Management Commands:
  builder      Manage builds
  compose*     Docker Compose (Docker Inc., v2.7.0)
  config       Manage Docker configs
  container    Manage containers
```

Rysunek 3.3. Pomoc systemu Docker

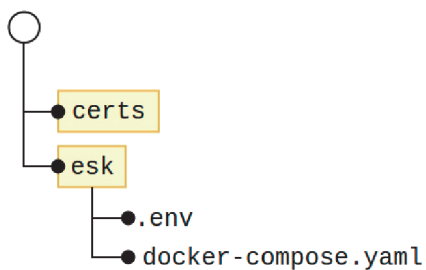
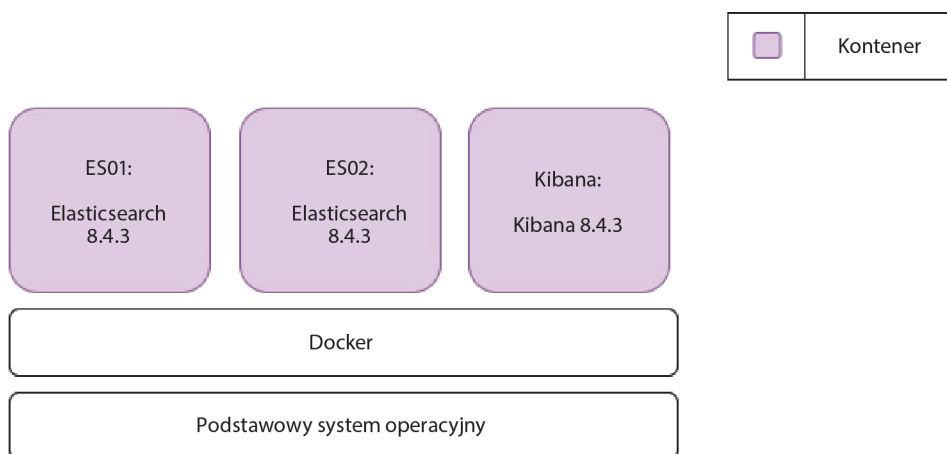
```
C:\Windows\system32>wsl -l
Podsystem Windows dla dystrybucji systemu Linux:
Ubuntu (domyślnie)
docker-desktop-data
docker-desktop
```

**Rysunek 3.4. Lista dystrybucji wsl**

```
C:\Windows\system32>wsl -d docker-desktop
EwelaRewela:/mnt/host/c/Windows/system32# sysctl -w vm.max_map_count=262144
vm.max_map_count = 262144
EwelaRewela:/mnt/host/c/Windows/system32#
```

**Rysunek 3.5. Konfigurowanie pamięci wirtualnej Docker Desktop**

Główny katalog projektu

**Rysunek 3.6. Struktura folderów projektu Elastic Stack****Rysunek 3.7. Wdrożenie platformy Docker**

```
examiner@datasrv02:~/dev/delab/esk$ sudo docker compose ps
NAME                COMMAND                  SERVICE    STATUS    PORTS
esk-es01-1          "/bin/tini -- /usr/l..." es01       running (healthy) 0.0.0.0:9200→9200/tcp, :::9200→9200/tcp, 9300/tcp
esk-es02-1          "/bin/tini -- /usr/l..." es02       running (healthy) 9200/tcp, 9300/tcp
esk-kibana-1        "/bin/tini -- /usr/l..." kibana     running (healthy) 0.0.0.0:5601→5601/tcp, :::5601→5601/tcp
esk-setup-1         "/bin/tini -- /usr/l..." setup      exited (0)
```

Rysunek 3.8. Status kontenera wyświetlany w terminalu

Containers [Give feedback](#)

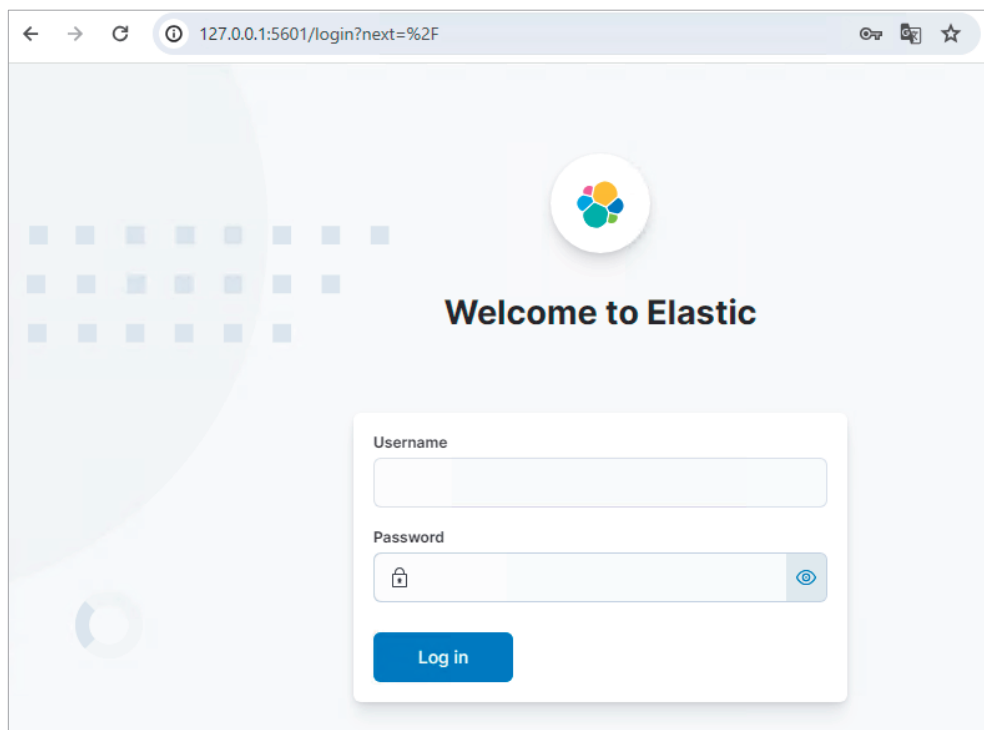
Container CPU usage ⓘ Container memory usage ⓘ [Show charts](#) ▾

Data unavailable at this time Data unavailable at this time

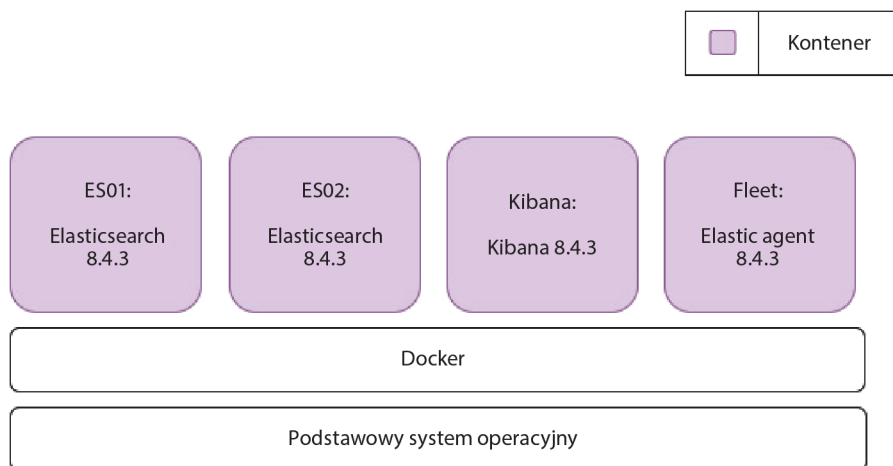
Search  Only show running containers Delete ▶ ⏸ ⌵

	Name	Image	Status	CPU (%)	Port(s)	Last started	Actions
<input type="checkbox"/>	> fleet		Running (1/1)	N/A		1 minute ago	<span>■</span> <span>:</span> <span>🗑</span>
<input type="checkbox"/>	▼ esk		Running (3/4)	N/A		7 seconds ago	<span>■</span> <span>:</span> <span>🗑</span>
<input type="checkbox"/>	kibana-1 8c309e11c	<a href="https://docker.elastic.co/kibana">docker.elastic.co/kibana</a>		N/A	5601:5601 <a href="#">🔗</a>	2 days ago	<span>▶</span> <span>:</span> <span>🗑</span>
<input checked="" type="checkbox"/>	es02-1 2506ad341	<a href="https://docker.elastic.co/elasticsearch">docker.elastic.co/elasticsearch</a>	Running	N/A		7 seconds ago	<span>■</span> <span>:</span> <span>🗑</span>
<input type="checkbox"/>	es01-1 08294d51b	<a href="https://docker.elastic.co/elasticsearch">docker.elastic.co/elasticsearch</a>	Running	N/A	9200:9200 <a href="#">🔗</a>	8 seconds ago	<span>■</span> <span>:</span> <span>🗑</span>
<input type="checkbox"/>	setup-1 7f7cef96bc	<a href="https://docker.elastic.co/elasticsearch">docker.elastic.co/elasticsearch</a>	Running	N/A		10 seconds ago	<span>■</span> <span>:</span> <span>🗑</span>

Rysunek 3.9. Status kontenerów w środowisku Docker Desktop

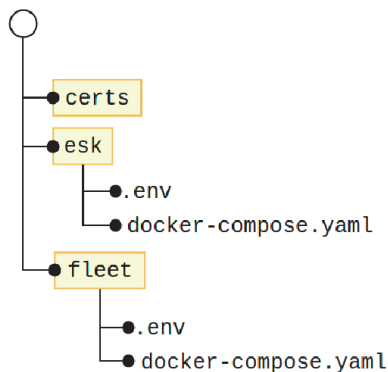


**Rysunek 3.10. Strona logowania do systemu Elastic**



**Rysunek 3.11. Wdrożenie platformy Docker z komponentem Fleet Server**

## Główny katalog projektu



Rysunek 3.12. Struktura folderów projektu z komponentem Fleet

Add a Fleet Server

A Fleet Server is required before you can enroll agents with Fleet. Follow the instructions below to set up a Fleet Server. For more information, see the [Fleet and Elastic Agent Guide](#)

Quick Start

Advanced

1

Get started with Fleet Server

First, set the public IP or host name and port that agents will use to reach Fleet Server. It uses port **8220** by default. We'll then generate a policy for you automatically.

Fleet Server host

https://127.0.0.1:8220

▼

Generate Fleet Server policy

Rysunek 3.13. Ekran konfiguracji komponentu Fleet Server (krok 1.)



## Edit output

Type

Elasticsearch

Hosts

http://localhost:9200

⊕ Add row

Elasticsearch CA trusted fingerprint (optional)

Specify Elasticsearch CA trusted fingerprint

Advanced YAML configuration

ssl.verification\_mode: none

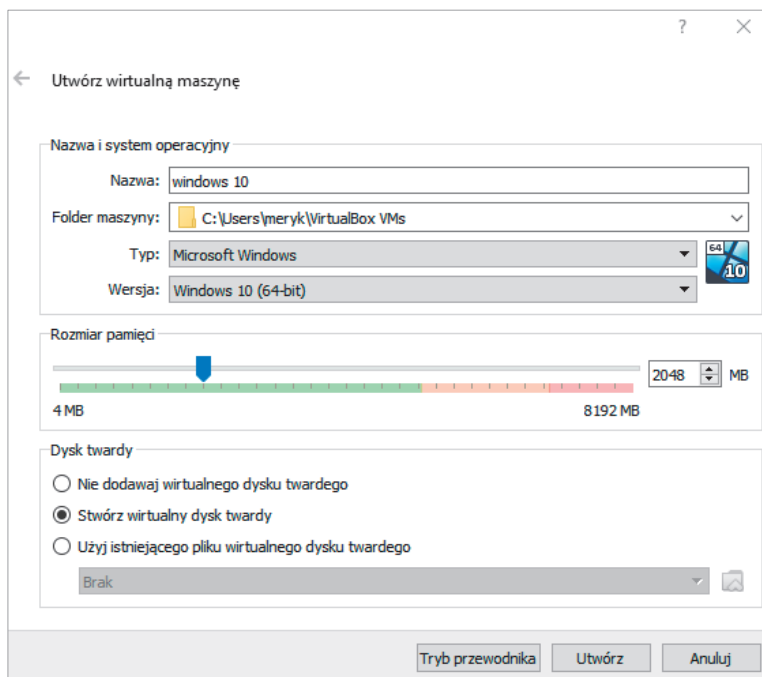
☒ Make this output the default for **agent integrations**.

☒ Make this output the default for **agent monitoring**.

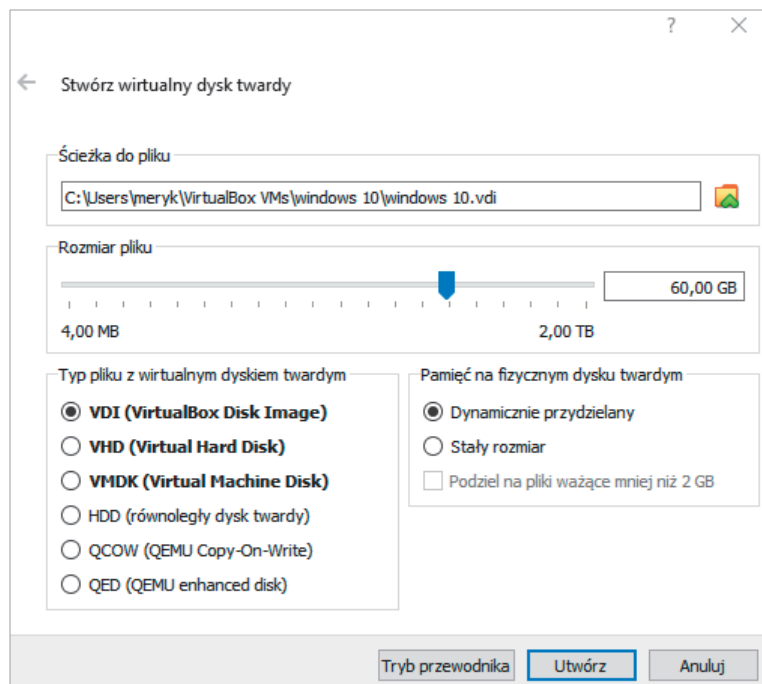
Cancel

Save and apply settings

Rysunek 3.16. Konfiguracja wyjścia komponentu Fleet Server

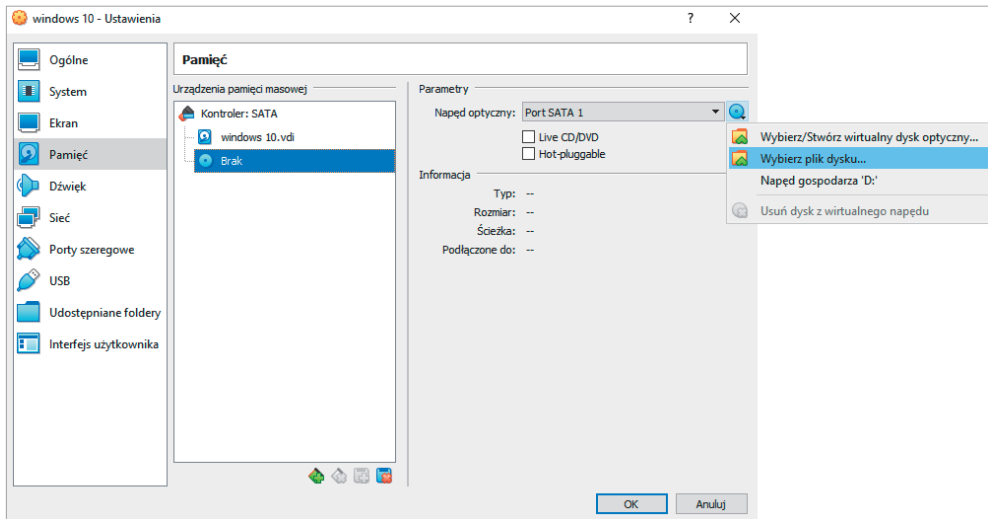


Rysunek 3.17. Obszar Create Virtual Machine w środowisku VirtualBox

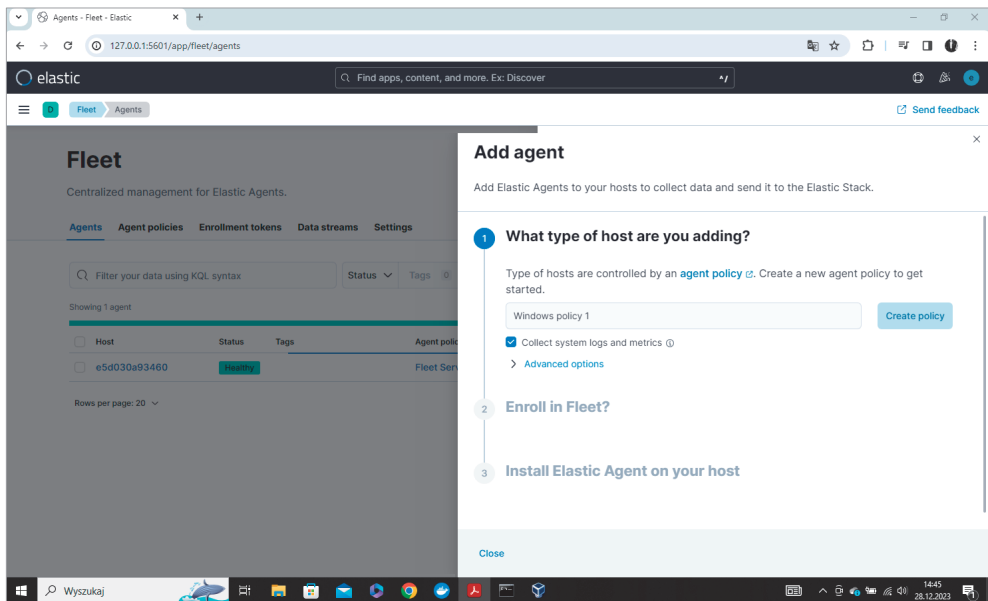


Rysunek 3.18. Obszar Create Virtual Hard Disk w środowisku VirtualBox





Rysunek 3.19. Ustawienia maszyny wirtualnej w środowisku VirtualBox



Rysunek 3.20. Dodawanie agenta

### 3 Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). For additional guidance, see our [installation docs](#).

Linux Tar Mac **Windows** RPM DEB Kubernetes

```
$ProgressPreference = 'SilentlyContinue'  
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent-8.4.3-windows-x86_64.zip -DestinationPath  
cd elastic-agent-8.4.3-windows-x86_64  
.\elastic-agent.exe install --url=https://127.0.0.1:8220 --enrollment-token
```

Rysunek 3.21. Skrypt instalacyjny Elastic Agent

### ✓ Agent enrollment confirmed

✓ 1 agent has been enrolled.

[View enrolled agents](#)

### ✓ Incoming data confirmed

✓ Incoming data received from 1 of 1 recently enrolled agent.


[Close](#)

Rysunek 3.22. Potwierdzenie rejestracji agenta



### Rysunek 3.24. Zasady działania komponentu Elastic Agent

[< Cancel](#)



## Edit System integration

Agent policy  
**Windows policy**

Modify integration settings and deploy changes to the selected agent policy.

---

**Integration settings**  
Choose a name and description to help identify how this integration will be used.

Integration name

system-2

Description

Optional

[> Advanced options](#)

---

☒ **Collect logs from System instances**

Change defaults [v](#)

---

☒ **Collect events from the Windows event log**

Change defaults [v](#)

---

☒ **Collect metrics from System instances**

Change defaults [v](#)

---

☐ **Collect logs from third-party REST API (experimental)**

Change defaults [v](#)

---

Rysunek 3.25. Integracja edycji systemu (Edit system)

**Collect events from the Windows event log** [Change defaults](#)

☒ **Application**  
Collect Windows application logs

**Preserve original event**  
☐ ☒ X  
Preserves a raw copy of the original XML event, added to the field `event.original`  
[Advanced options](#)

☒ **Security**  
Security channel

**Preserve original event**  
☐ ☒ X  
Preserves a raw copy of the original XML event, added to the field `event.original`  
[Advanced options](#)

☒ **System**  
Collect Windows system logs

**Preserve original event**  
☐ ☒ X  
Preserves a raw copy of the original XML event, added to the field `event.original`  
[Advanced options](#)

Rysunek 3.26. Ustawienia zbierania logów zdarzeń systemu Windows

**Source**  
Use Kibana [Data Views](#) or specify individual [Index patterns](#) as your rule's data source to be searched.

☒ **Index Patterns** ☐ **Data View**

apm-\*transaction-\* X auditbeat-\* X endgame-\* X filebeat-\* X logs-\* X packetbeat-\* X traces-apm\* X  
winlogbeat-\* X \*-elastic-cloud-logs-\* X

Enter the pattern of Elasticsearch indices where you would like this rule to run. By default, these will include index patterns defined in Security Solution advanced settings.

**Custom query** [Import query from saved timeline](#)

**Group by**  
All results

**Threshold**  
>= 4

Select fields to group by. Fields are joined together with 'AND'

**Count**  
All results

**Unique values**  
>=

Select a field to check cardinality

**Timeline template**  
None

Select which timeline to use when investigating generated alerts.

Rysunek 3.27. Konfiguracja nowej reguły

2

About rule

Name

failed logon threshold met

Description

the number of failed logons has risen over a defined threshold

Default severity

Select a severity level for all alerts generated by this rule.

Low

☐ Severity override

Use source event values to override the default severity.

Default risk score

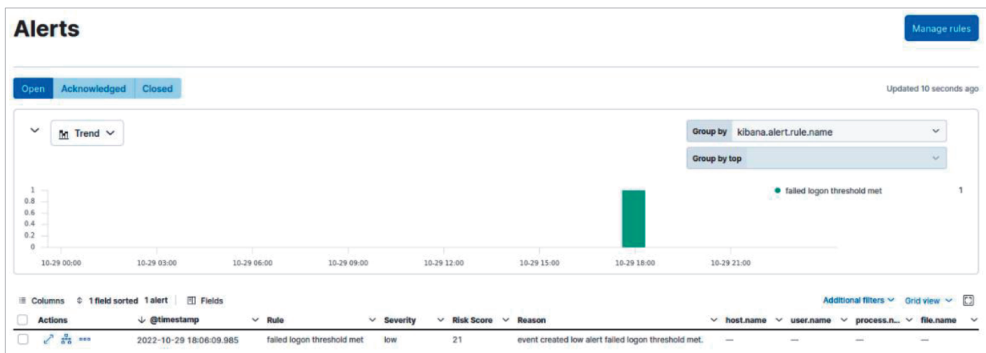
Select a risk score for all alerts generated by this rule.

0255075100

21

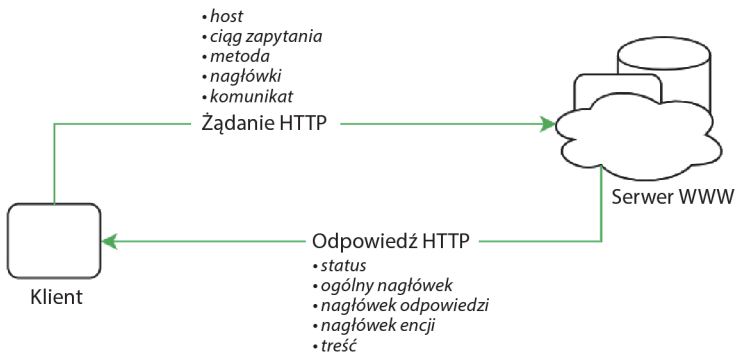
☐ Risk score override

Rysunek 3.28. Szczegółowe dane nowej reguły

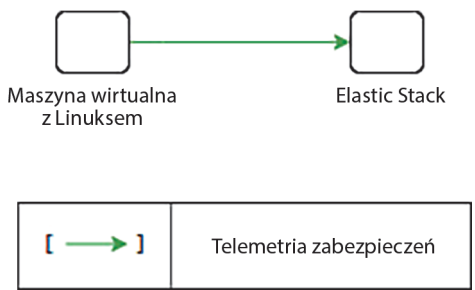


Rysunek 3.29. Pomyślne wykrycie zagrożenia przez mechanizm detekcji

# Rozdział 4. Źródła danych inżynierii detekcji



Rysunek 4.1. Przegląd ruchu na serwerze WWW



Rysunek 4.2. Instalacja z serwerem WWW

×

## Create agent policy

Agent policies are used to manage settings across a group of agents. You can add integrations to your agent policy to specify what data your agents collect. When you edit an agent policy, you can use Fleet to deploy updates to a specified group of agents.

Name

Apache Web Server Policy

☒ Collect system logs and metrics ⓘ

▼ Advanced options

Description

Add a description of how this policy will be used.


Optional description

Default namespace

Namespaces are a user-configurable arbitrary grouping that makes it easier to search for data and manage user permissions. A policy namespace is used to name its integration's data streams. [Learn more](#) ↗.

default ×

Agent monitoring

Collecting monitoring logs and metrics will also create an  Elastic Agent integration. Monitoring data will be written to the default namespace specified above.

☒ Collect agent logs ⓘ  
☒ Collect agent metrics ⓘ

Unenrollment timeout

An optional timeout in seconds. If provided, an agent will automatically unenroll after

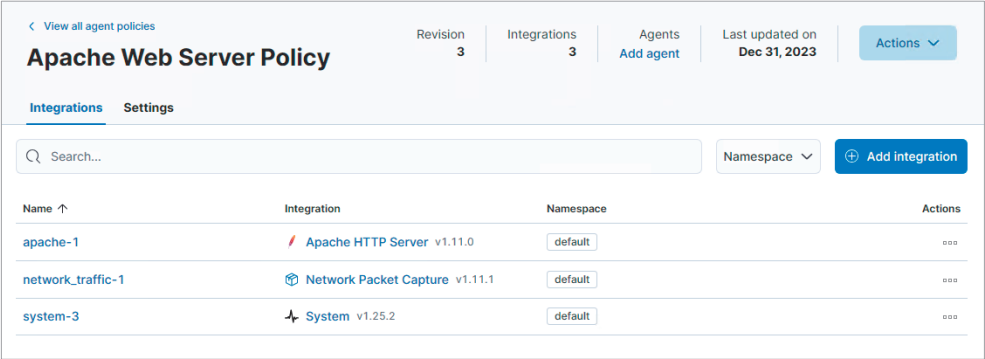
Cancel

Preview API request

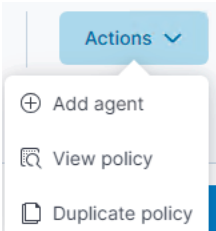
Create agent policy

Rysunek 4.3. Tworzenie zasady agenta

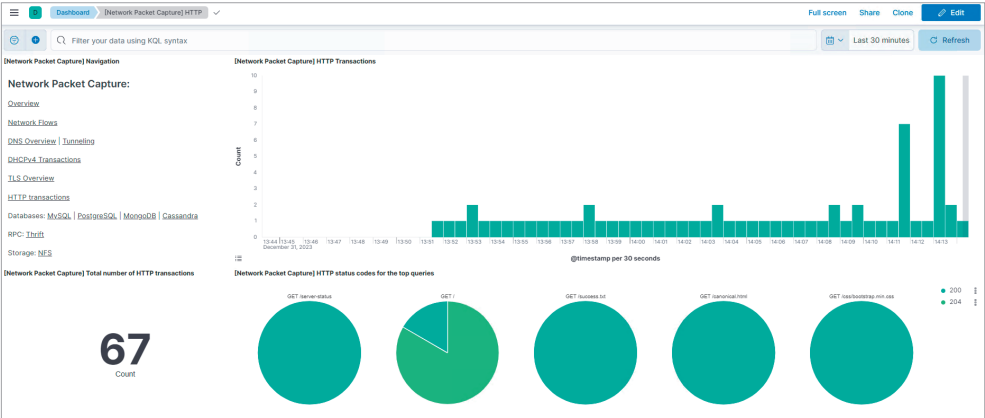




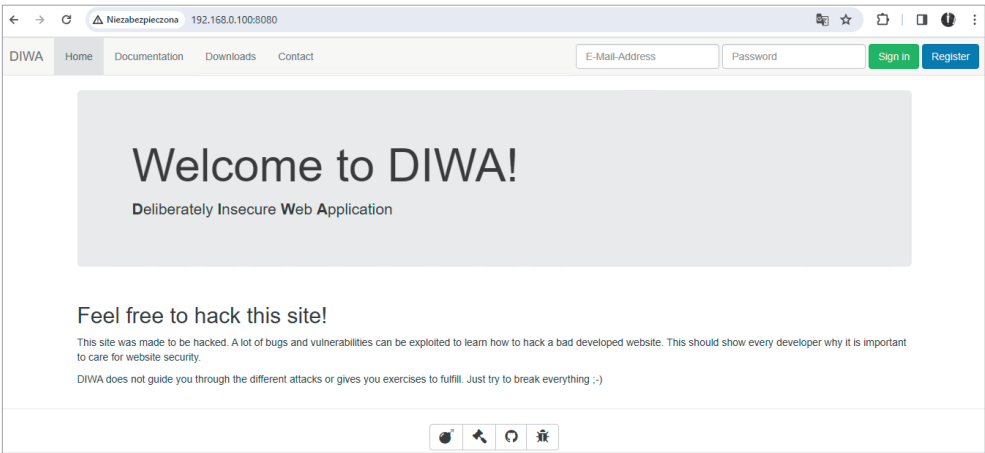
Rysunek 4.4. Zasady serwera WWW Apache



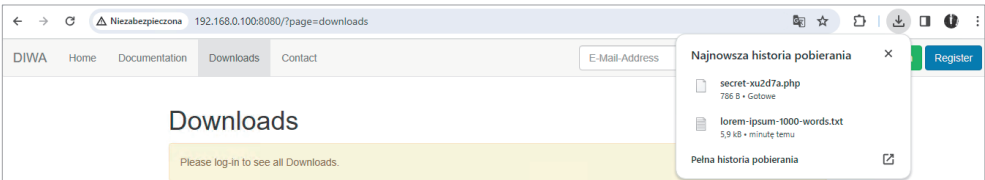
Rysunek 4.5. Dodawanie agenta Elastic



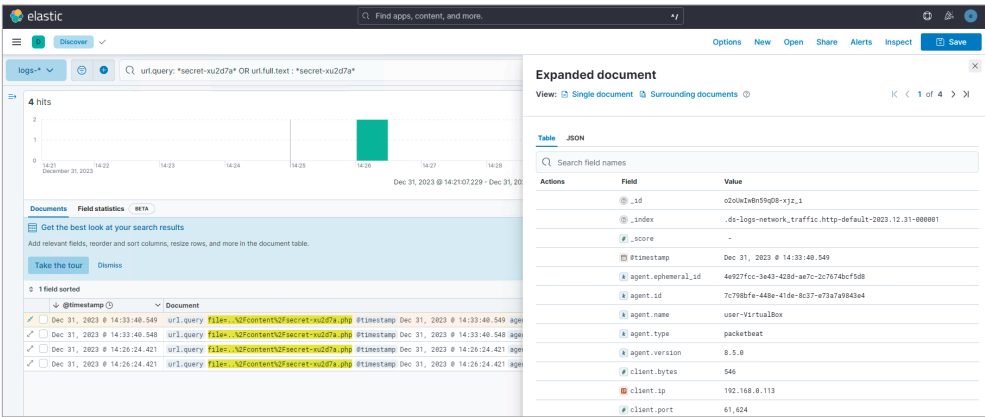
Rysunek 4.6. Pulpit nawigacyjny Network Packet Capture HTTP



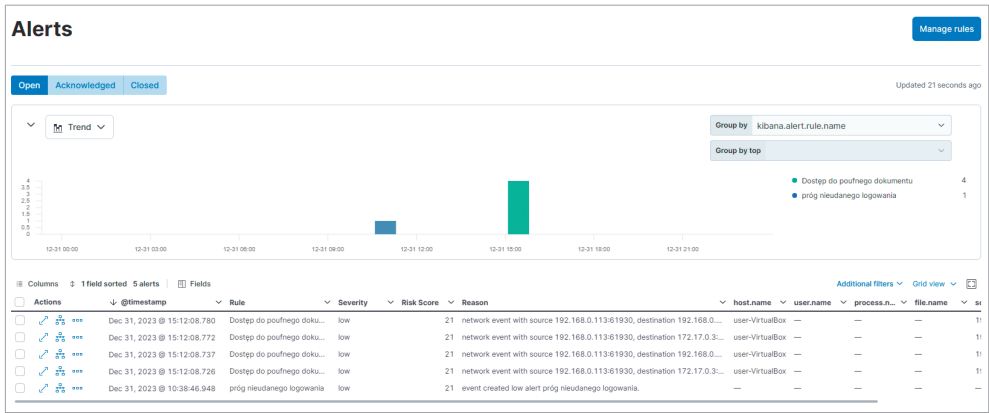
Rysunek 4.7. Główna strona aplikacji DIWA



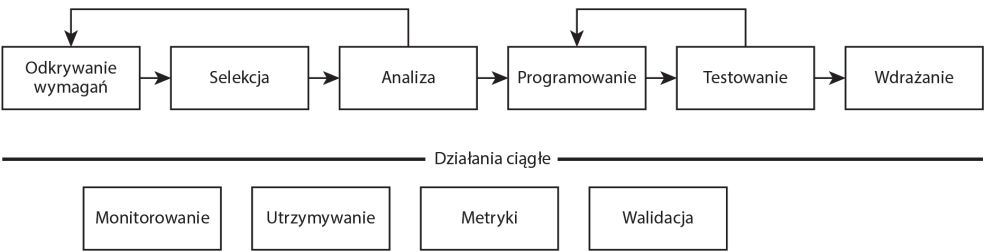
Rysunek 4.8. Pobieranie pliku DIWA



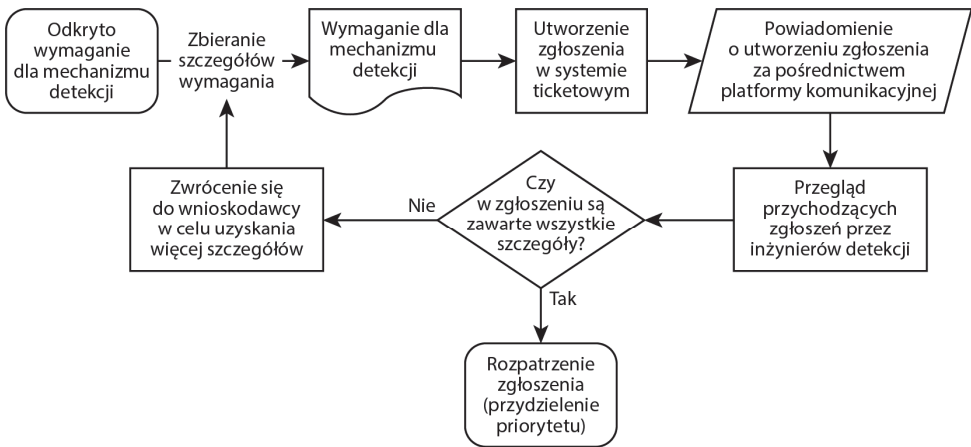
Rysunek 4.9. Rozszerzony widok dokumentu



# Rozdział 5. Analiza wymagań dla mechanizmów detekcji



Rysunek 5.1. Cykl życia mechanizmu detekcji



Rysunek 5.2. Przebieg fazy odkrywania wymagań

$$\text{Dotkliwość zagrożenia} + \text{Dopasowanie mechanizmu detekcji zagrożenia do organizacji} + \text{Pokrycie wymagań} + \left( \text{Aktywne eksploity} \left( \text{Trafność} + \text{Częstość występowania} \right) \right)$$

Rysunek 5.3. Wzór na obliczanie priorytetu

## Rozdział 6. Tworzenie mechanizmów detekcji przy użyciu wskaźników naruszeń zabezpieczeń

☒ Custom Windows event logs

☒ Windows Event Logs

Collect Windows event logs from a custom channel

Channel Name


Microsoft-Windows-Sysmon/Operational

Name of Windows event log channel (eg. Microsoft-Windows-PowerShell/Operational)

Dataset name

winlog.sysmon

Dataset to write data to. Changing the dataset will send the data to a different index. You can't use - in the name of a dataset and only valid characters for [Elasticsearch index names](#).

☐ 

Preserve original event

Preserves a raw copy of the original XML event, added to the field event.original

[Advanced options](#)

Change defaults ^

Rysunek 6.1. Dodawanie integracji Sysmon

Expanded document

View: [Single document](#) [Surrounding documents](#)

< 4 of 36 >

input.type	winlog
log.level	informacje
message	<div>Process Create: RuleName: - UtcTime: 2023-12-31 14:28:00.103 ProcessGuid: {3394ff7e-7a70-6591-9006-00000004400} ProcessId: 9068 Image: C:\Windows\System32\SearchFilterHost.exe FileVersion: 7.0.19041.3758 (WinBuild.160101.0800) Description: Microsoft Windows Search Filter Host Product: Windows Search Company: Microsoft Corporation OriginalFileName: SearchFilterHost.exe CommandLine: "C:\Windows\system32\SearchFilterHost.exe" 0 804 80 8 816 8192 812 788 CurrentDirectory: C:\Windows\system32\ User: ZARZĄDZANIE NT\SYSTEM LogonGuid: {3394ff7e-109c-6591-e703-000000000000} LogonId: 0x3E7 TerminalSessionId: 0 IntegrityLevel: Medium Hashes: SHA256=08500481DC54125715DE3A0997052F781BF7674DC108520C8 DFD38B731BC59DF ParentProcessGuid: {3394ff7e-1110-6591-4901-00000004400} ParentProcessId: 10668 ParentImage: C:\Windows\System32\SearchIndexer.exe ParentCommandLine: C:\Windows\system32\SearchIndexer.exe /Embedding ParentUser: ZARZĄDZANIE NT\SYSTEM</div>

Rysunek 6.2. Przykładowe zdarzenie o identyfikatorze 1

Expanded document

View: [Single document](#) [Surrounding documents](#)

< 1 of 52 >

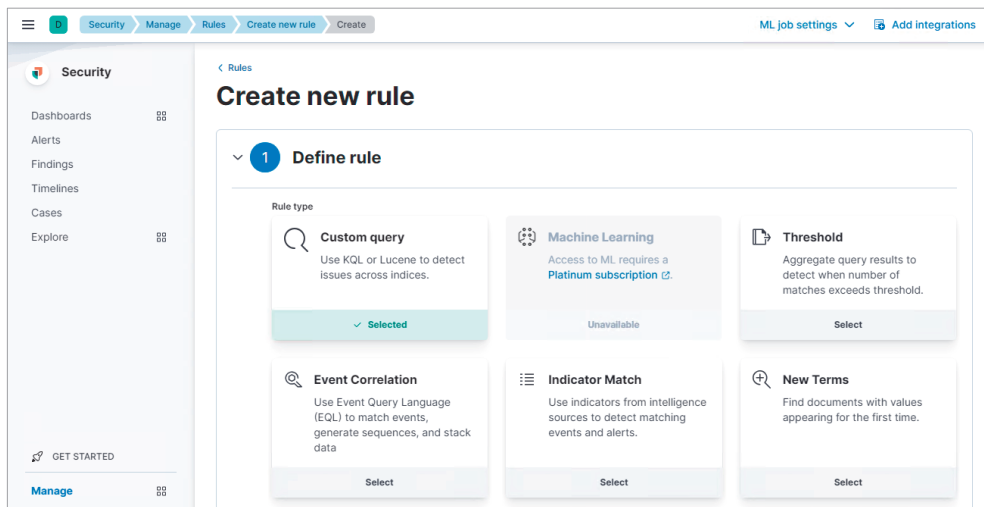
Table JSON

Hash

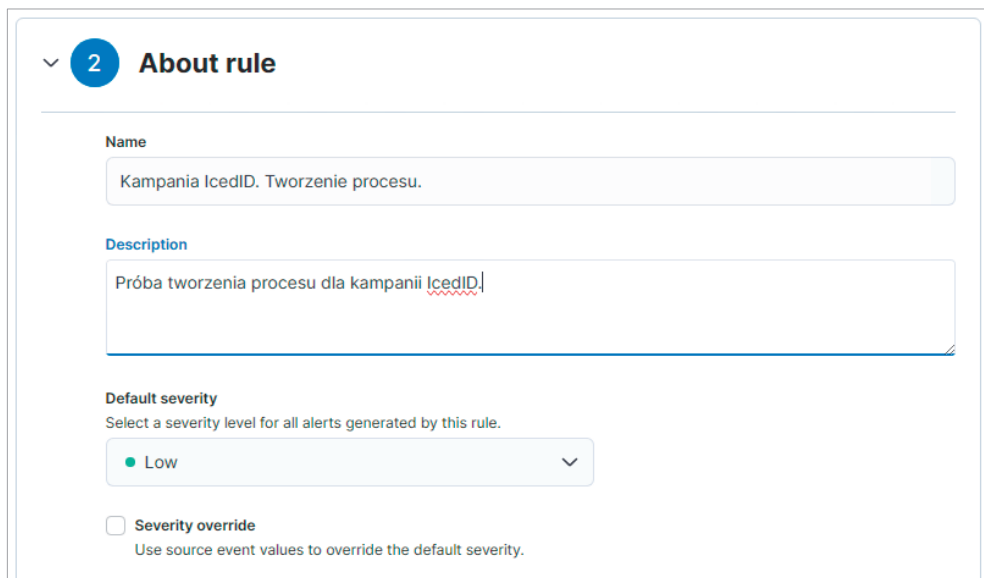
Actions	Field	Value
	winlog.event_data.Hashes	SHA256=F13DE58416738D210DAB465B242E9C949F80A0245EEF45B07C381F0C6C8A43C3

Rows per page: 25 < 1 >

Rysunek 6.3. Pola zawierające skróty dla zdarzenia o identyfikatorze 1



Rysunek 6.4. Konfiguracja nowej reguły



Rysunek 6.5. Konfiguracja reguły About rule

Expanded document

View: [Single document](#) [Surrounding documents](#)

<< < 1 of 4 > >>

host.os.type	windows
host.os.version	10.0
input.type	winlog
log.level	informacje
message	<div>Network connection detected: RuleName: Network connection over port 80 or 443 or 8080 UtcTime: 2023-12-31 14:40:17.601 ProcessGuid: {3394ff7e-117a-6591-6901-000000004400} ProcessId: 3492 Image: C:\Program Files\Google\Chrome\Application\chrome.exe User: DESKTOP-3ADGNTT\PC Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.0.106 SourceHostname: host.docker.internal SourcePort: 63544 SourcePortName: - DestinationIsIpv6: false DestinationIp: 15.197.153.132 DestinationHostname: ae6bee98fe393bd2a.awsglobalaccelerator.com DestinationPort: 443 DestinationPortName: https</div>
winlog.api	wineventlog
winlog.channel	Microsoft-Windows-Sysmon/Operational

Rysunek 6.6. Przykładowe zdarzenie o identyfikatorze 3

Expanded document

View: [Single document](#) [Surrounding documents](#)

<< < 1 of 4 > >>

Table JSON

Dest

Actions	Field	Value
	winlog.event_data.DestinationHostName	ae6bee98fe393bd2a.awsglobalaccelerator.com
	winlog.event_data.DestinationIp	15.197.153.132
	winlog.event_data.DestinationIsIPv6	false
	winlog.event_data.DestinationPort	443
	winlog.event_data.DestinationPortName	https

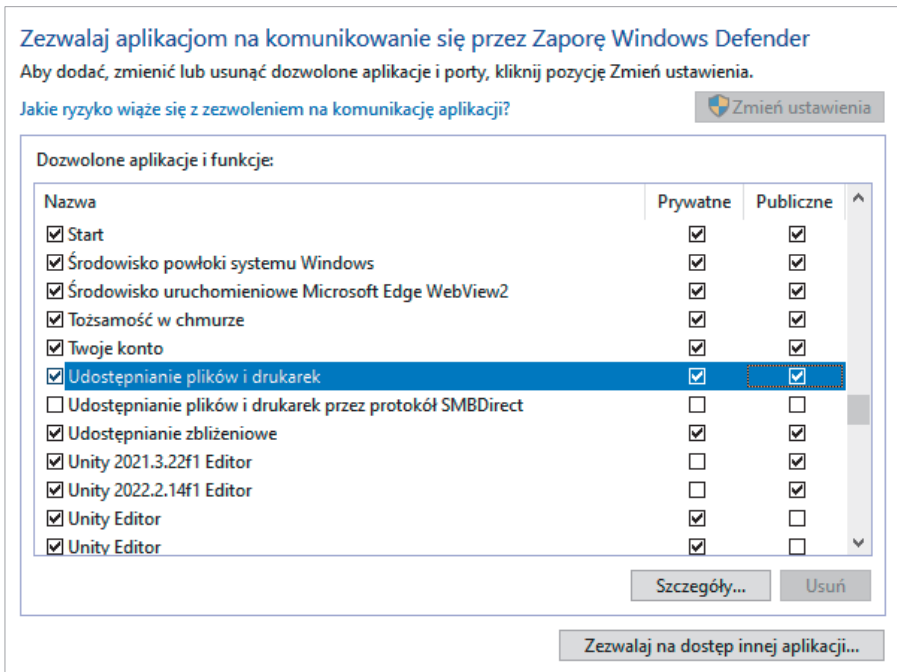
Rows per page: 25

< 1 >

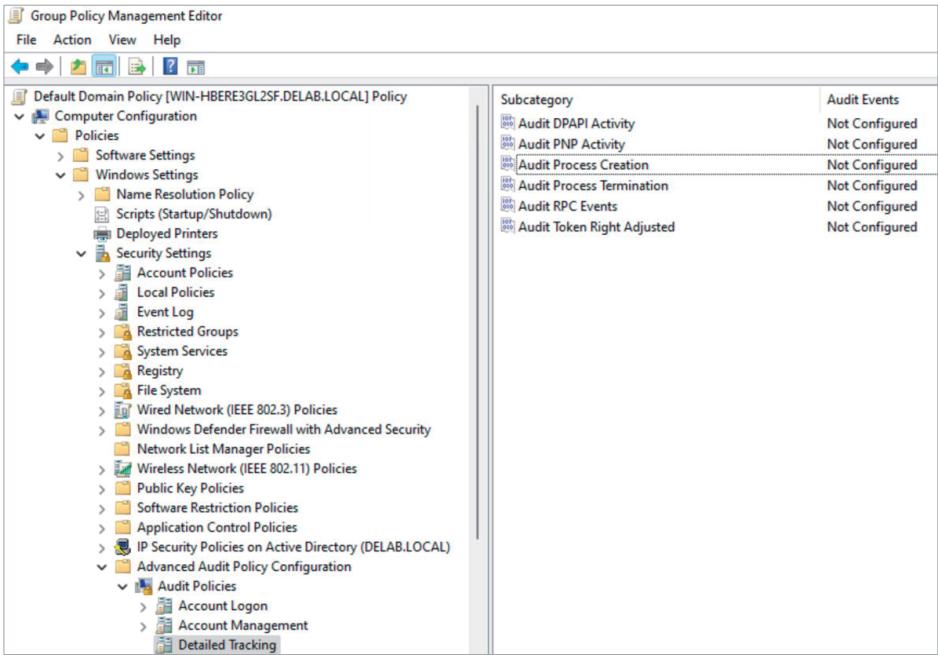
Rysunek 6.7. Pola opisujące docelowy ruch dla zdarzenia o identyfikatorze 3



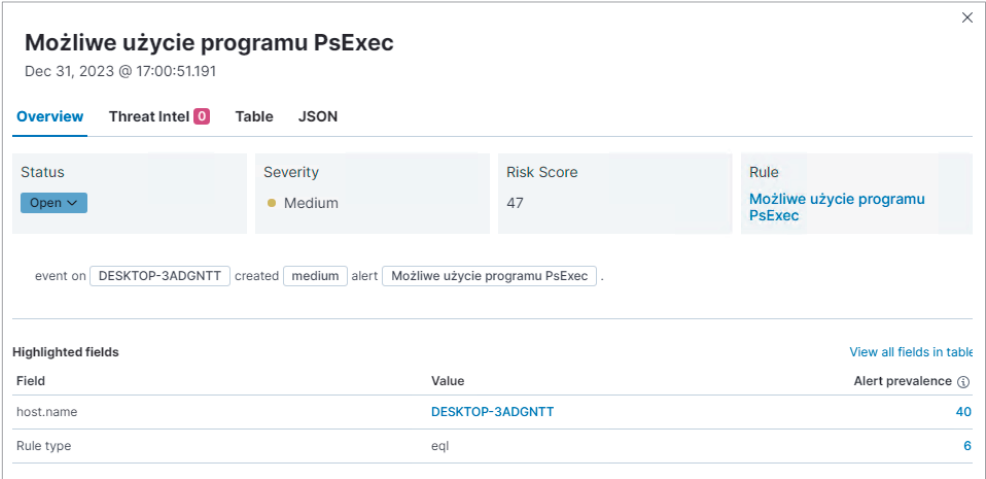
## Rozdział 7. Opracowywanie mechanizmów detekcji opartych na wskaźnikach behawioralnych



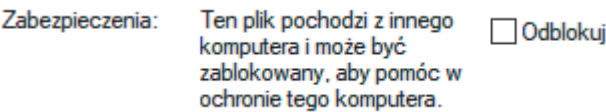
Rysunek 7.1. Zezwalanie na udostępnianie plików i drukarek



Rysunek 7.2. Edytor Group Policy Management



Rysunek 7.3. Wyzwolony alert możliwego użycia PsExec

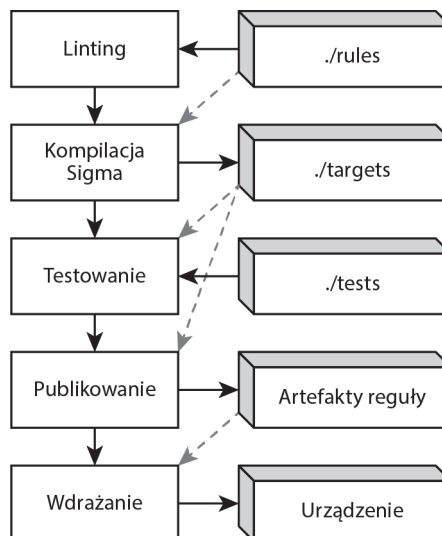


Rysunek 7.4. Znacznik sieciowy w systemie Windows

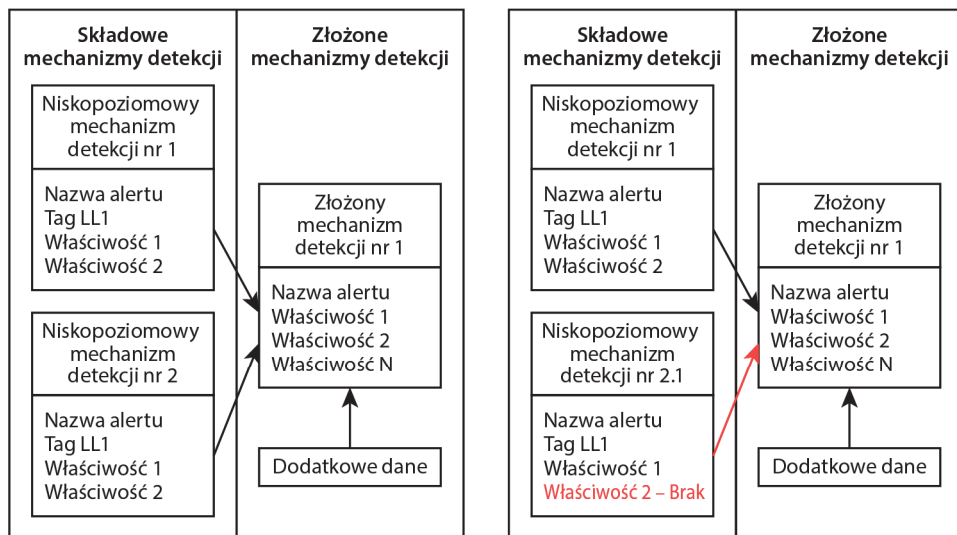
## Rozdział 8. Tworzenie dokumentacji i potoki mechanizmów detekcji

```
detection_rules
README.md
rules
  windows
  macos
  linux
  network
...
tests
  general
  windows
  macos
  linux
  network
...
targets
  qradar
  elasticsearch
...
```

Rysunek 8.1. Układ repozytorium mechanizmów detekcji



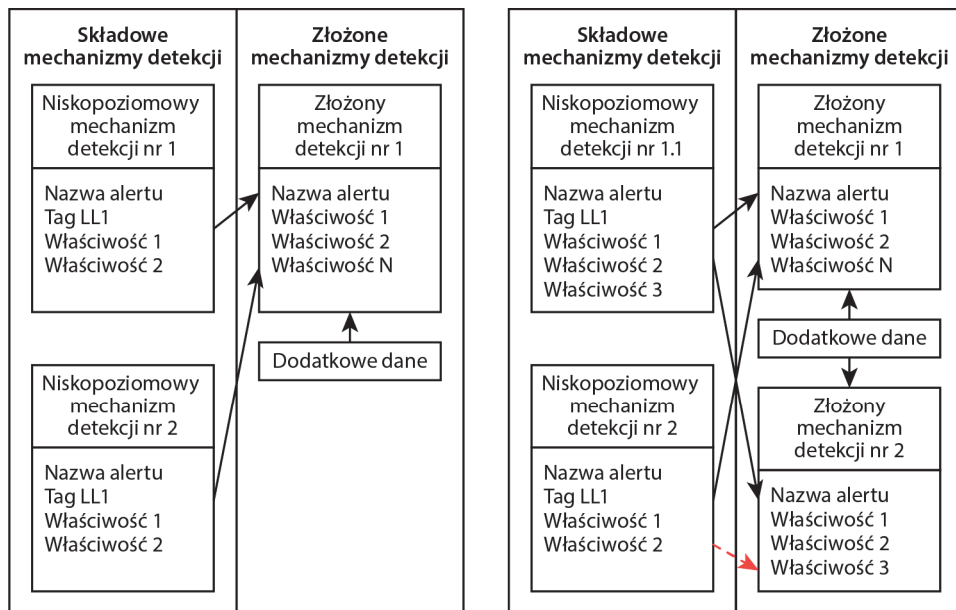
Rysunek 8.2. Potok ciągłego wdrażania dla reguł Sigma



Złożony mechanizm detekcji nr 1 jest generowany w oparciu o alerty oznaczone znacznikiem LL1, które mogły zostać wygenerowane za pomocą niskopoziomowych mechanizmów detekcji nr 1 i nr 2 i wymagają do uaktywnienia właściwości 1 i 2

Niskopoziomowy mechanizm detekcji nr 2 został zaktualizowany do wersji 2.1, a właściwość 2 nie jest już uwzględniona w alertach lub jest nieprawidłowo sformatowana. Złożony mechanizm detekcji nr 1 nadal się uaktywnia, ale tylko dla niskopoziomowego mechanizmu detekcji nr 1. Zespół SOC nadal widzi alerty złożonego mechanizmu detekcji nr 1, nie zdając sobie sprawy, że brakuje niektórych alertów

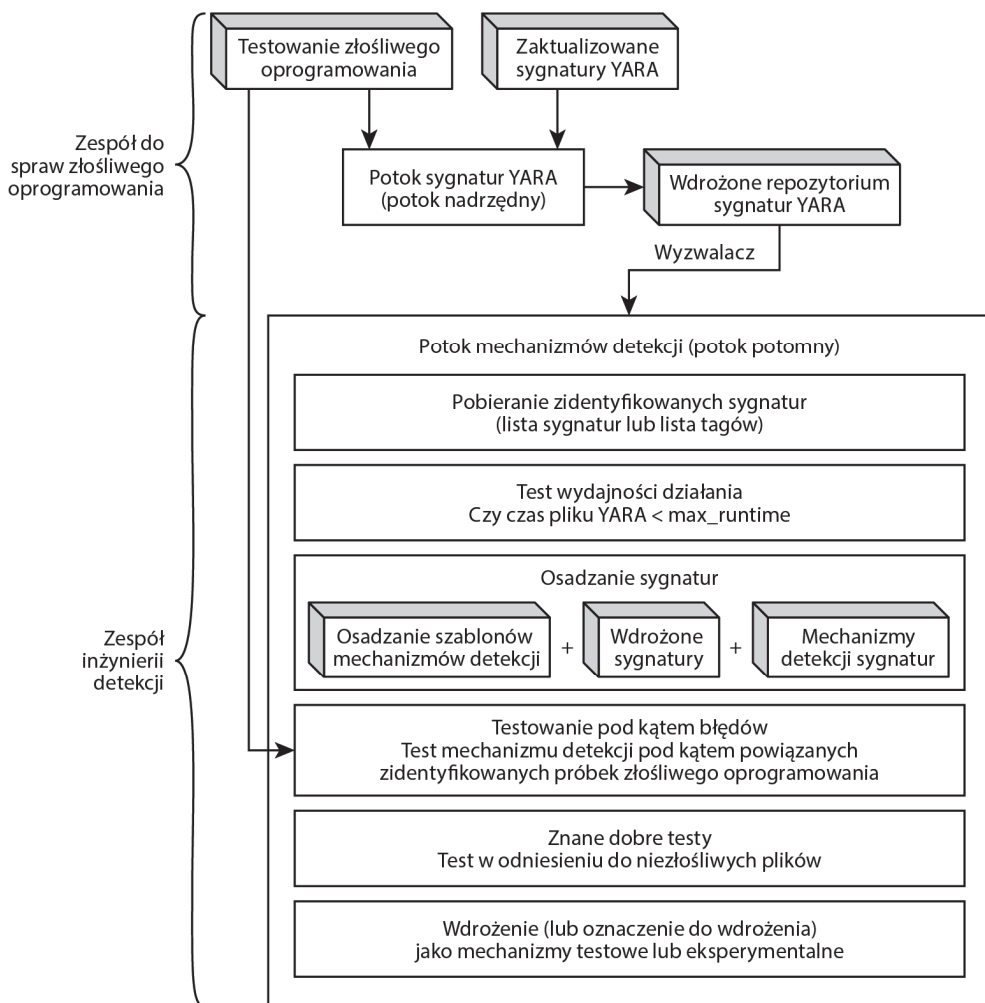
**Rysunek 8.3. Składowe mechanizmy detekcji i mechanizmy złożone — przykład nr 1**



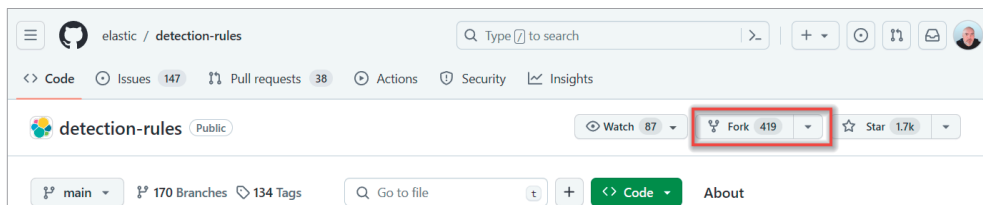
Złożony mechanizm detekcji nr 1 jest generowany w oparciu o alerty oznaczone znacznikiem LL1, które mogły zostać wygenerowane za pomocą niskopoziomowych mechanizmów detekcji nr 1 i nr 2 i wymagają do uaktywnienia właściwości 1 i 2

Niskopoziomowy mechanizm detekcji nr 1 został zaktualizowany do wersji 1.1 i dodano właściwość 3 w celu obsługi złożonego mechanizmu detekcji nr 2, ale analityk zapomniał zaktualizować również niskopoziomowy mechanizm detekcji nr 2, przez co nie wszystkie niskopoziomowe mechanizmy detekcji dostarczają informacji pozwalających na poprawne uaktywnienie złożonego mechanizmu detekcji nr 2

**Rysunek 8.4. Składowe mechanizmy detekcji i mechanizmy złożone — przykład nr 2**



**Rysunek 8.5. Przykładowy potok mechanizmu detekcji jako kodu z osadzaniem sygnatur YARA**



**Rysunek 8.6. Tworzenie forka repozytorium detection-rules**

```
(env) D:\gitrepo\detection_rules>python -m detection_rules --help

DETECTION RULES

Usage: detection_rules [OPTIONS] COMMAND [ARGS]...

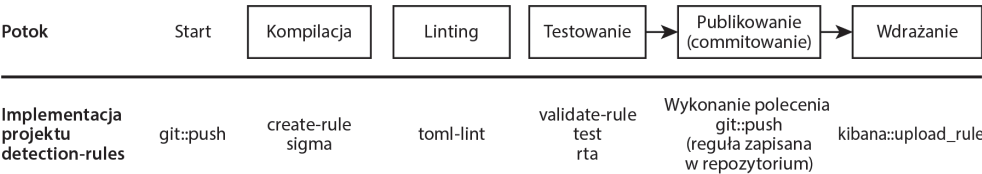
  Commands for detection-rules repository.

Options:
  -D, --debug / -N, --no-debug  Print full exception stacktrace on errors
  -h, --help                    Show this message and exit.

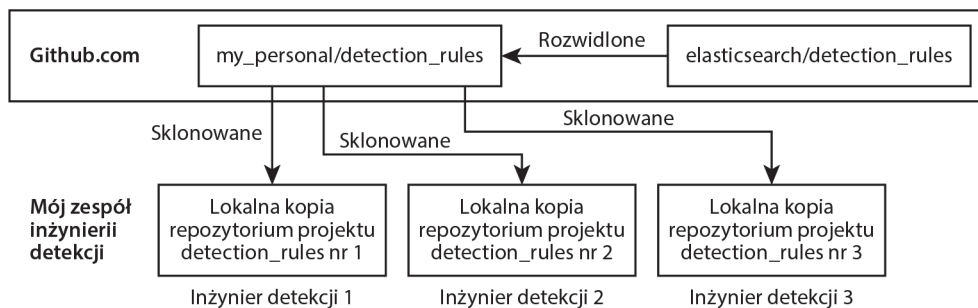
Commands:
  build-limited-rules  Import rules from json, toml, or Kibana...
  build-threat-map-entry  Build a threat map entry.
  create-rule          Create a detection rule.
  dev                  Commands related to the Elastic Stack rules...
  es                   Commands for integrating with Elasticsearch.
  export-rules         Export rule(s) into an importable ndjson file.
  generate-rules-index  Generate enriched indexes of rules, based on a...
  import-rules          Import rules from json, toml, yaml, or Kibana...
  kibana               Commands for integrating with Kibana.
  mass-update           Update multiple rules based on eql results.
  normalize-data         Normalize Elasticsearch data timestamps and sort.
  rta                   Commands related to Red Team Automation (RTA)...
  rule-search           Use KQL or EQL to find matching rules.
  test                 Run unit tests over all of the rules.
  toml-lint             Cleanup files with some simple toml formatting.
  typosquat             Commands for generating typosquat detections.
  validate-all         Check if all rules validates against a schema.
  validate-rule         Check if a rule staged in rules dir validates...
  view-rule            View an internal rule or specified rule file.

(env) D:\gitrepo\detection_rules>
```

Rysunek 8.7. Ekran pomocy projektu detection-rules



Rysunek 8.8. Potok z implementacją projektu detection-rules

**Rysunek 8.9. Potok z implementacją projektu detection-rules**

```
eql.errors.EqlSchemaError: Error at line:1,column:89
Field not recognized
any where event.code=="1" and winlog.channel=="Microsoft-Windows-VHDMP-Operational" and winlog.event_data.VhdFileName like~ ("*Temp*", "*.zip*", "*.iso")
stack: 8.9.0, beats: 8.9.0, ecs: 8.9.0, endgame: 8.4.0
```

**Rysunek 8.10. Błąd EqlSchemaError**

```
(env) D:\gitrepo\detection_rules>python -m detection_rules import-rules ./rules/windows/defense_evasion_iso_mounted_from_zip_temp_directory.toml
```

## DETECTION RULES


```
[+] Building rule for D:\gitrepo\detection_rules\rules\obraz_iso_zamontowany_z_tymczasowego_folderu_zip.toml
```

**Rysunek 8.11. Wynik działania polecenia import-rules**



# Rozdział 9. Walidacja mechanizmów detekcji

[Back to integrations](#)



## Elastic Defend

Elastic Agent

Version 8.5.0 | Agent policies 0 | [Add Elastic Defend](#)

[Overview](#) | [Integration policies](#) | [Assets](#) | [Settings](#) | [Advanced](#)

### Elastic Defend Integration

This integration sets up templates and index patterns required for Elastic Defend.

**Compatibility**

For compatibility information view our [documentation](#).

**Logs**

The log type of documents are stored in the `logs-endpoint.*` indices. The following sections define the mapped fields sent by the endpoint.

**alerts**

EXPORTED FIELDS

Details	
Version	8.5.0
Category	Cloud, Security
Elasticsearch assets	Index templates 2
	Transforms 2
	Ingest pipelines 13
Features	logs, metrics
Subscription	basic

Rysunek 9.1. Integracja Elastic Defend

1

## Configure integration

### Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name

Description Optional

[Advanced options](#)

Rysunek 9.2. Krok nr 1 kreatora dodawania integracji

2

## Where to add this integration?

New hosts | Existing hosts

### Agent policy

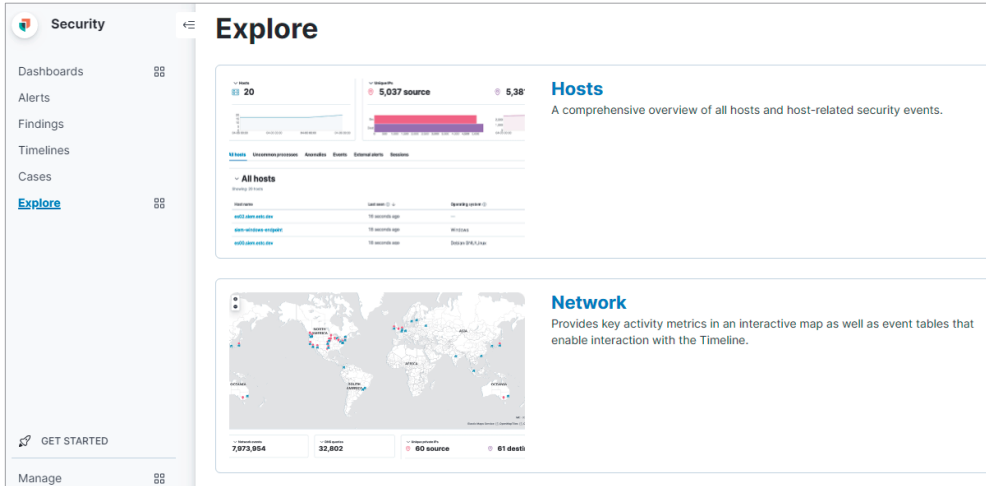
Agent policies are used to manage a group of integrations across a set of agents.

Agent policy

Windows policy

1 agent is enrolled with the selected agent policy.

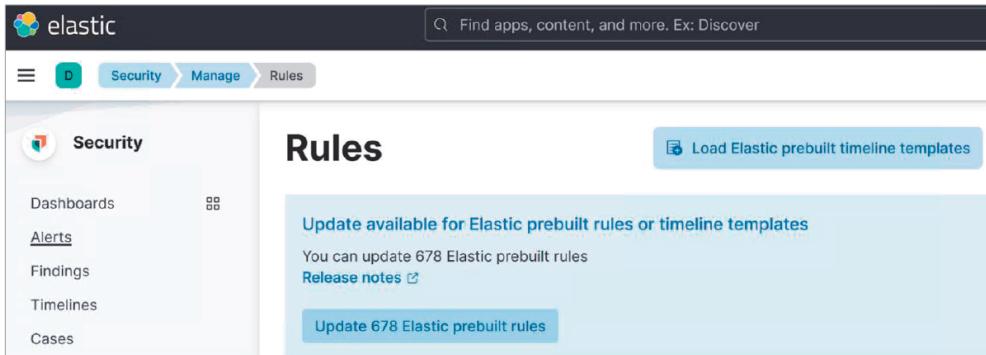
Rysunek 9.3. Krok nr 2 kreatora dodawania integracji



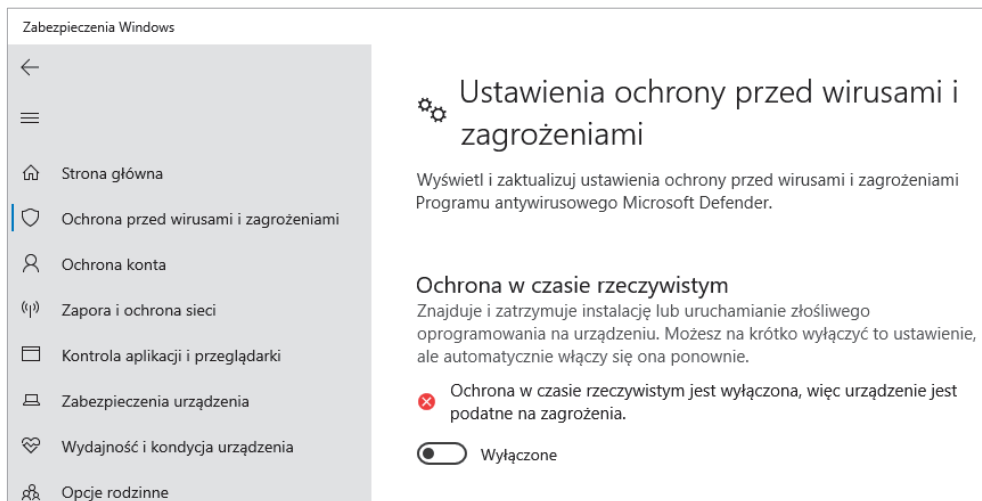
Rysunek 9.4. Aplikacja Elastic Security



Rysunek 9.5. Widok Events w aplikacji Elastic Security



Rysunek 9.6. Zarządzanie regułami Kibana Security



Rysunek 9.7. Wyłączanie ochrony w czasie rzeczywistym w usłudze Windows Defender

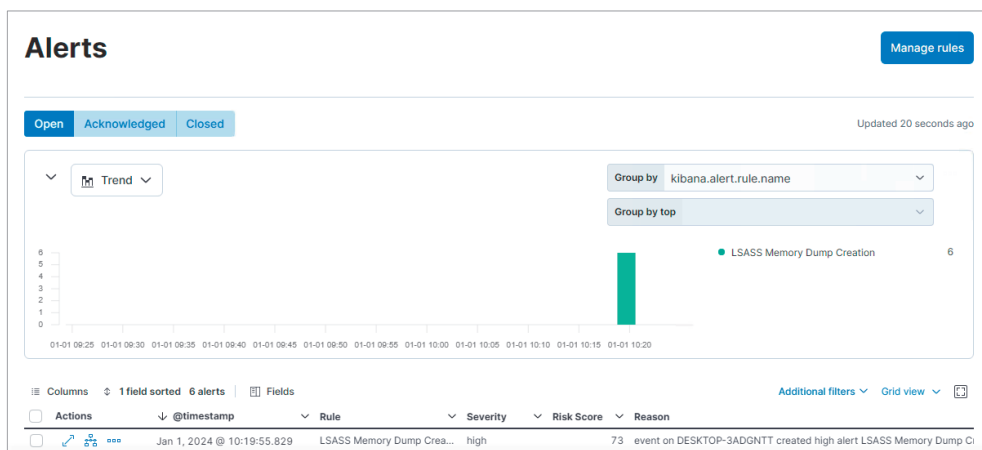
```
PS C:\procdump> ./procdump.exe -accepteula -ma lsass.exe c:\windows\temp\lsass_dump.dmp

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[09:00:53] Dump 1 initiated: c:\windows\temp\lsass_dump.dmp
[09:01:00] Dump 1 writing: Estimated dump file size is 61 MB.
[09:01:01] Dump 1 complete: 62 MB written in 7.6 seconds
[09:01:01] Dump count reached.

PS C:\procdump>
```

Rysunek 9.8. Uruchomienie testu Atomic Red Team



Rysunek 9.9. Alerty w aplikacji Elastic Security

LSASS Memory Dump Creation

Jan 1, 2024 @ 10:19:55.829

Overview

Threat Intel

Table

JSON

Status

Open

Severity

High

Risk Score

73

Rule

LSASS Memory Dump Creation

event on DESKTOP-3ADGNTT created high alert LSASS Memory Dump Creation

Highlighted fields

View all fields in table

Field	Value	Alert prevalence
host.name	DESKTOP-3ADGNTT	6
Rule type	query	6

Rysunek 9.10. Alarm tworzenia zrzutu pamięci LSASS

Rules

Rules

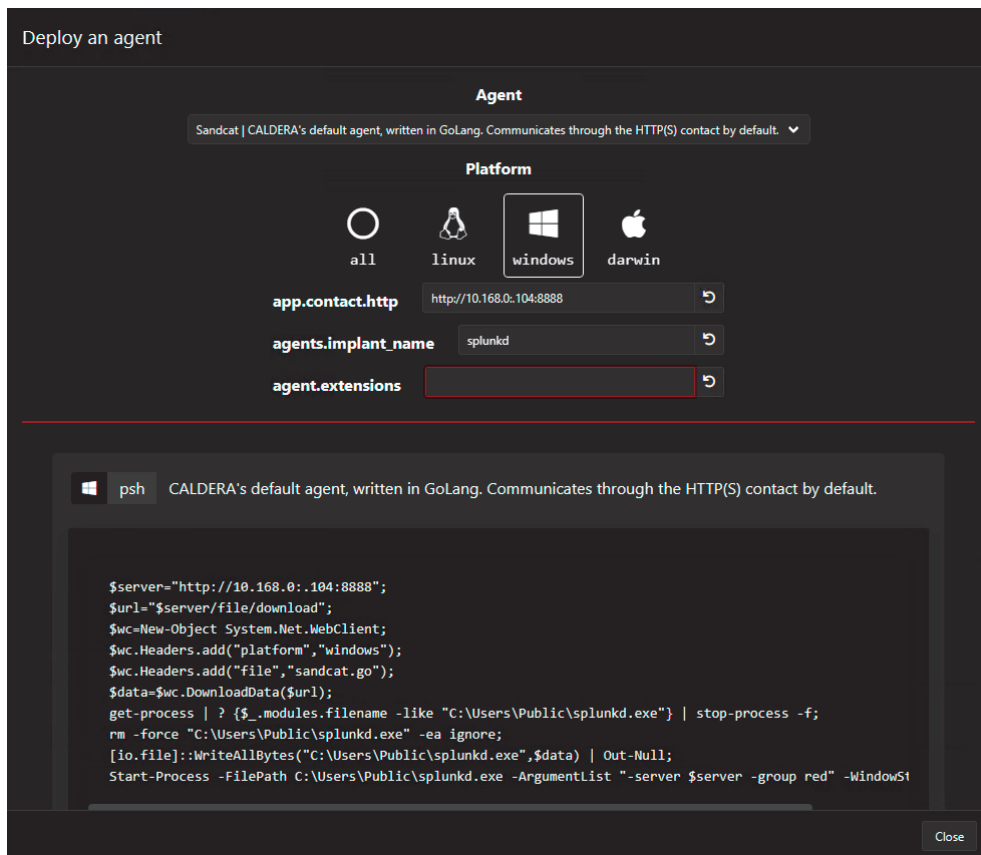
Rule Monitoring

Rule name, index pattern (e.g., "filebeat-\*"), or MITRE ATT&CK™ tactic or technique (e.g., "Defense Evasion" or "TA0005")

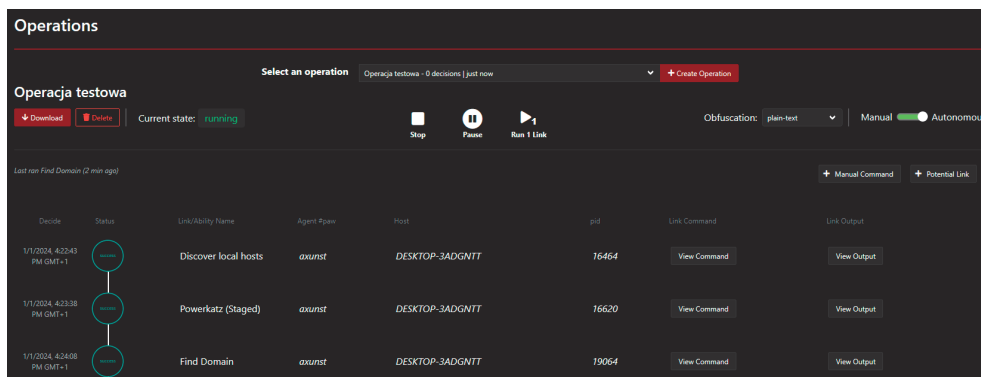
Showing 1-19 of 19 rules | Selected 19 rules | Select all 19 rules | Bulk actions | Refresh | Refresh settings

Rule		Risk score	Severity
Whoami Process Activity	1/3 integrations 6	21	Low
Account Discovery Command via SYSTEM Account	0/2 integrations 5	21	Low

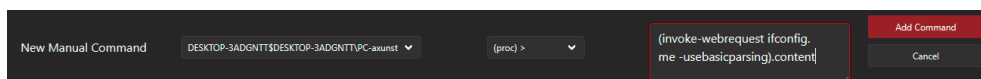
Rysunek 9.11. Reguły Windows i Discovery



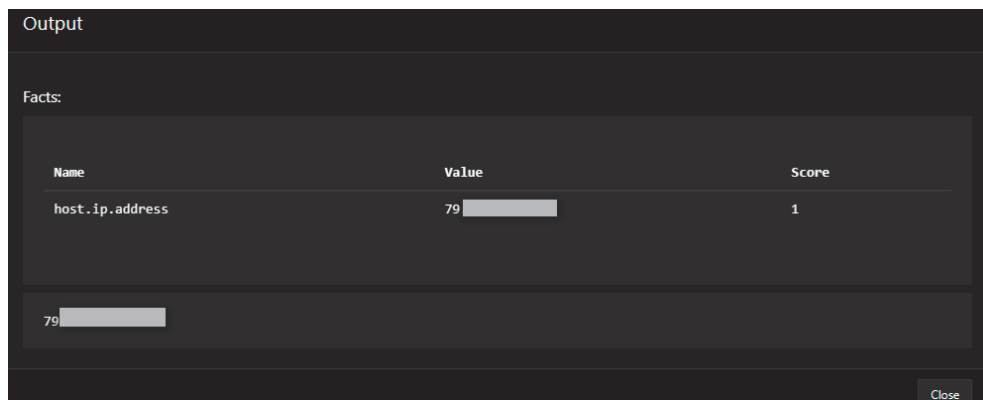
Rysunek 9.12. Instalacja agenta CALDERA



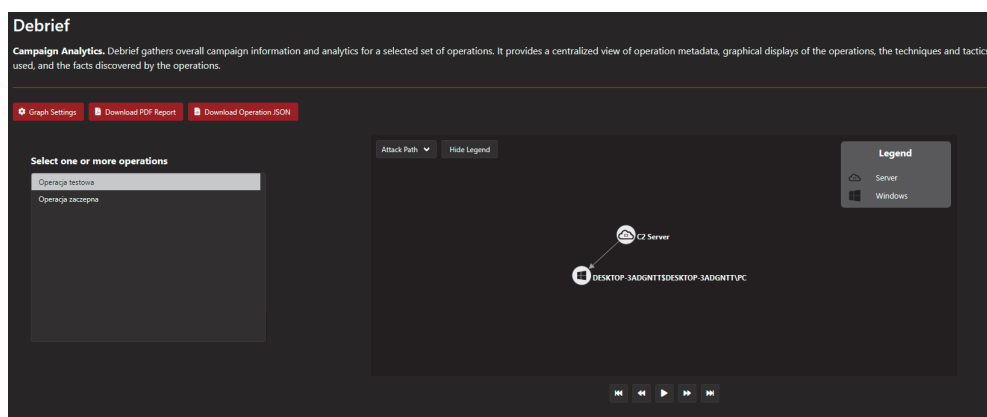
Rysunek 9.13. Operacje w systemie CALDERA



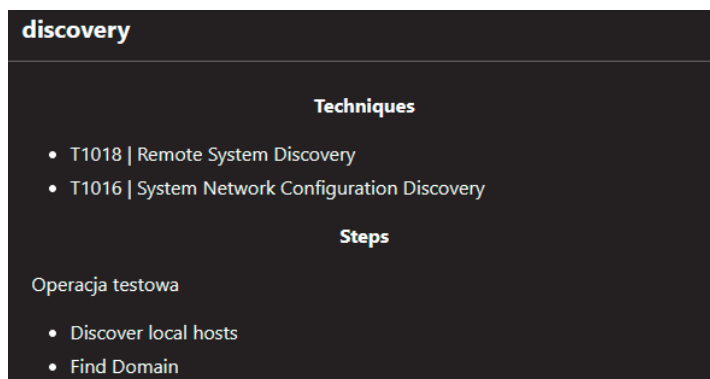
Rysunek 9.14. Ręczne polecenia w systemie CALDERA



Rysunek 9.15. Wynik działania ręcznego polecenia w systemie CALDERA



Rysunek 9.16. Wtyczka Debrief systemu CALDERA



Rysunek 9.17. Techniki wykrywania stosowane w operacji CALDERA

OPERATIONS DEBRIEF

TACTICS AND TECHNIQUES

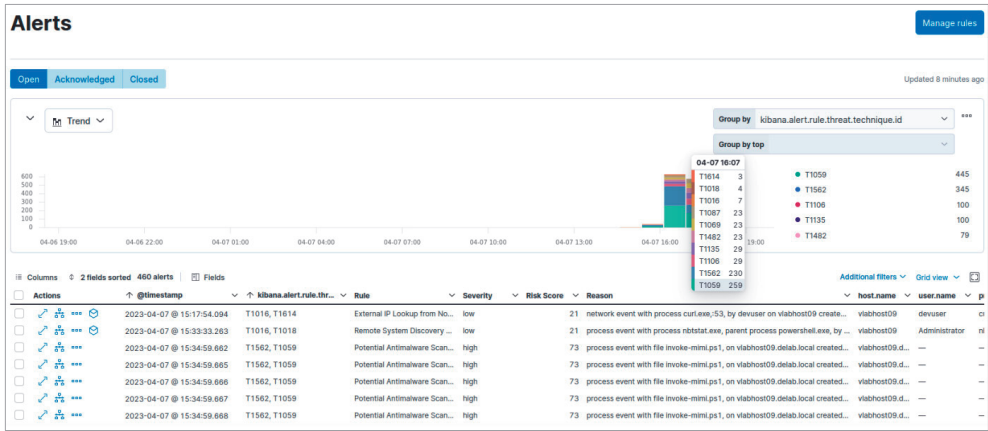
Tactics	Techniques	Abilities
Auto-generated	auto-generated: auto-generated	Operacja testowa Manual Command
Credential-access	T1003.001: OS Credential Dumping: LSASS Memory	Operacja testowa Powercatz (Staged)
Discovery	T1018: Remote System Discovery T1016: System Network Configuration Discovery	Operacja testowa Discover local hosts Find Domain

STEPS IN OPERATION OPERACJA TESTOWA

The table below shows detailed information about the steps taken in an operation and whether the command run discovered any facts.

Time	Status	Agent	Name	Command	Facts
2024-01-01 T15:23:35Z	success	axunst	Discover local hosts	Import-Module 'powersview.ps1';Get-DomainComputer	No
2024-01-01 T15:24:07Z	success	axunst	Powercatz (Staged)	Import-Module 'invoke-mimi.ps1';Invoke-Mimikatz -DumpCreds	No
2024-01-01 T15:25:05Z	success	axunst	Find Domain	nbstatat -n	No
2024-01-01 T15:30:17Z	failure	axunst	Manual Command	(invoke-webrequest ficonfig.me -usebasicsparsing).content	No
2024-01-01 T15:32:18Z	success	axunst	Manual Command	(invoke-webrequest ficonfig.me -usebasicsparsing).content	Yes

Rysunek 9.18. Raport PDF z podsumowania operacji CALDERA



Rysunek 9.19. Zmodyfikowany widok Alerts w systemie Elastic Security

### External IP Lookup from Non-Browser Process

2023-04-07 @ 20:39:40.576

**Overview** Threat Intel 0 Table JSON

Status <a href="#">Open</a>	Severity ● Low	Risk Score 21	Rule <a href="#">External IP Lookup from Non-Browser Process</a>
--------------------------------	-------------------	------------------	---

network event with process powershell.exe;53, by Administrator on vlabhost09 created low alert External IP Lookup from Non-Browser Process.

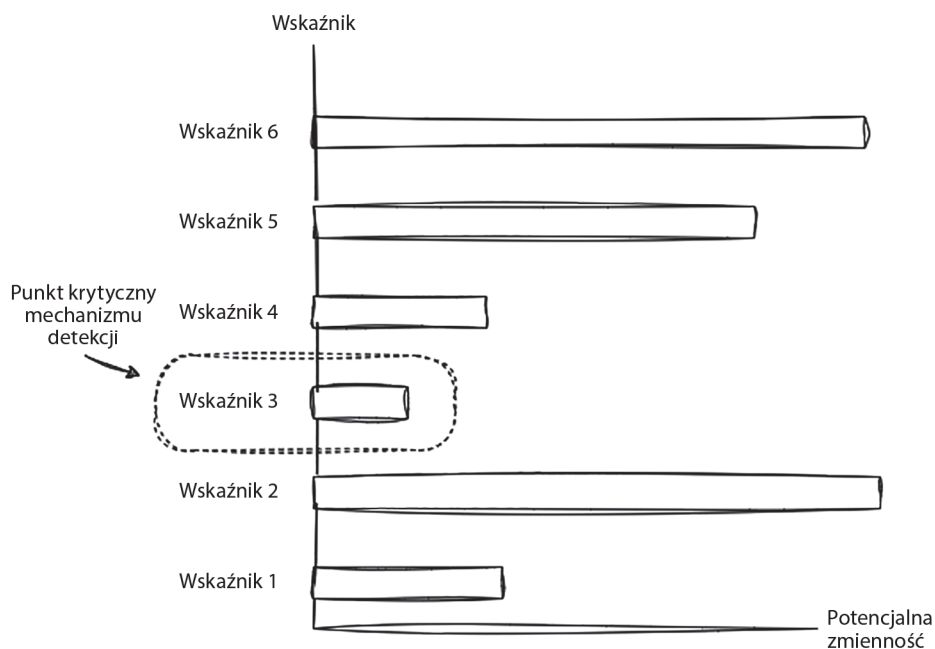
**Highlighted fields** [View all fields in table](#)

Field	Value	Alert prevalence <sup>①</sup>
host.name	vlabhost09	1
Agent status	Healthy	—
user.name	Administrator	1
Rule type	eql	1
destination.port	53 <a href="#">🔗</a>	1
dns.question.name	ifconfig.me	1
process.name	powershell.exe	1

**Insights**

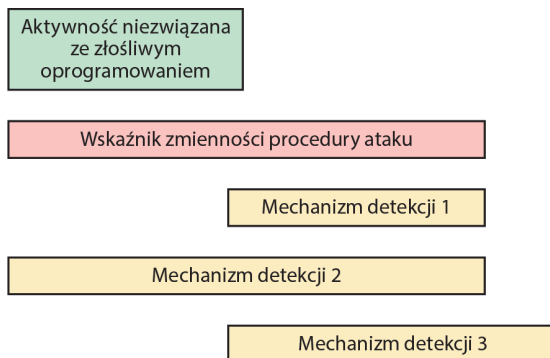
- > 0 cases related to this alert
- > 1 alert related by source event

**Rysunek 9.20. Alert wyszukiwania zewnętrznego adresu IP z procesu spoza przeglądarki**



**Rysunek 9.21. Wskaźniki i potencjalna zmienność**





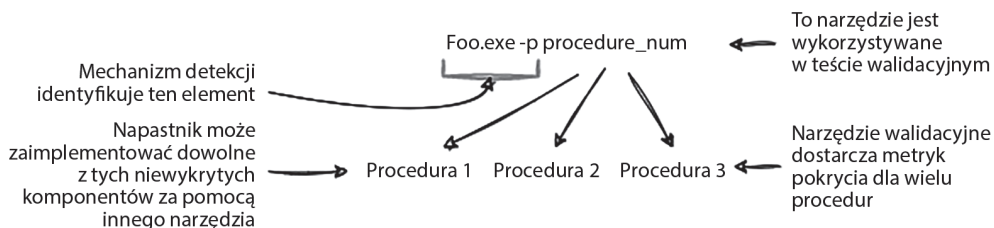
Jednowymiarowy widok przestrzeni ataków i powiązanych z nimi mechanizmów detekcji. Ten widok dodaje wymiar z każdym używanym wskaźnikiem jako warunek „i” w ramach mechanizmu detekcji

**Mechanizm detekcji 1:** brak fałszywych alarmów, ale także brak poprawnych wyników dodatnich

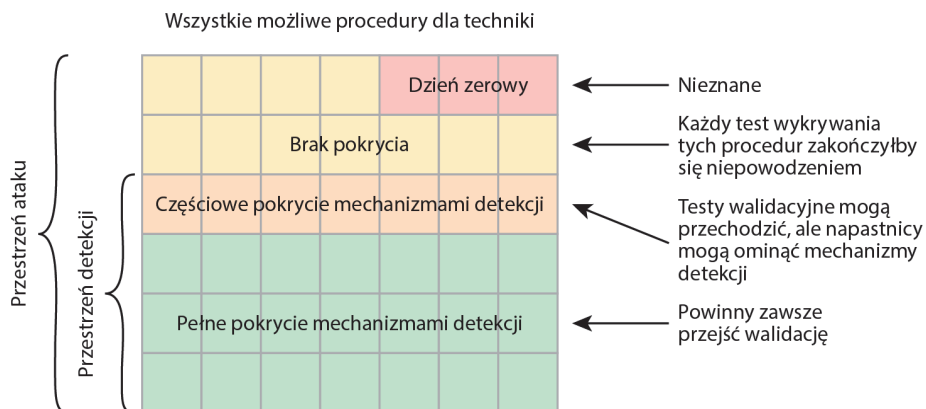
**Mechanizm detekcji 2:** uwzględnia fałszywe alarmy, ale nie pomija poprawnych wyników dodatnich

**Mechanizm detekcji 3:** obejmuje fałszywe alarmy niemożliwe do uzyskania w wyniku działania przeciwnika i obejmuje tylko niektóre wyniki poprawnie dodatnie

**Rysunek 9.22. Przestrzeń mechanizmu detekcji**



**Rysunek 9.23. Narzędzia walidacyjne a procedury**



**Rysunek 9.24. Przestrzenie ataku i detekcji wielu procedur**

# Rozdział 10. Wykorzystanie wiedzy o zagrożeniach

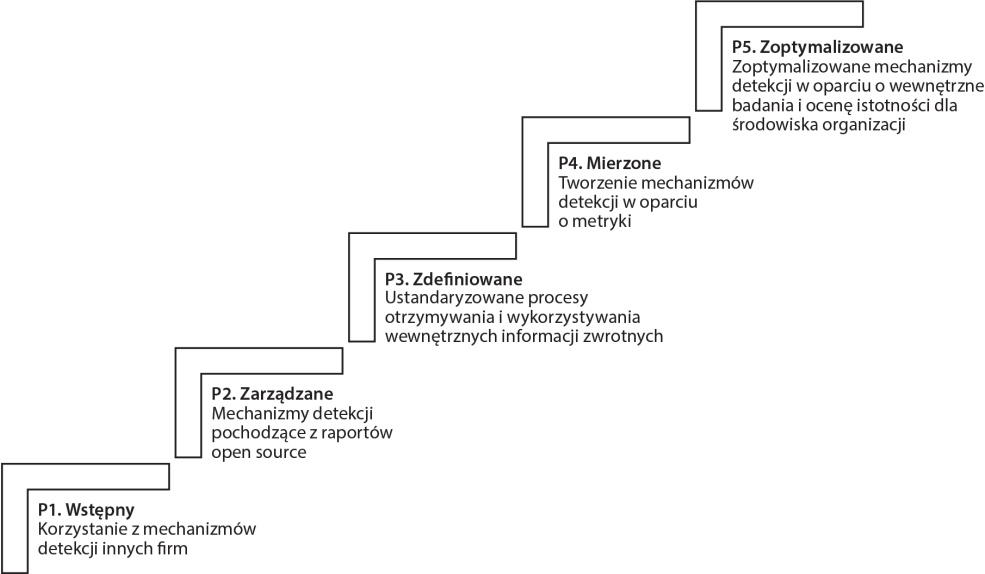
Techniques Used				ATT&CK® Navigator Layers -
Domain	ID	Name	Use	
Enterprise	T1583	.001	Acquire Infrastructure: Domains	Winnti Group has registered domains for C2 that mimicked sites of their intended targets. <sup>[1]</sup>
Enterprise	T1083		File and Directory Discovery	Winnti Group has used a program named ff.exe to search for specific documents on compromised hosts. <sup>[1]</sup>
Enterprise	T1105		Ingress Tool Transfer	Winnti Group has downloaded an auxiliary program named ff.exe to infected machines. <sup>[1]</sup>
Enterprise	T1057		Process Discovery	Winnti Group looked for a specific process running on infected servers. <sup>[1]</sup>
Enterprise	T1014		Rootkit	Winnti Group used a rootkit to modify typical server functionality. <sup>[1]</sup>
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	Winnti Group used stolen certificates to sign its malware. <sup>[1]</sup>

Rysunek 10.1. Winnti Group — wykorzystywane techniki

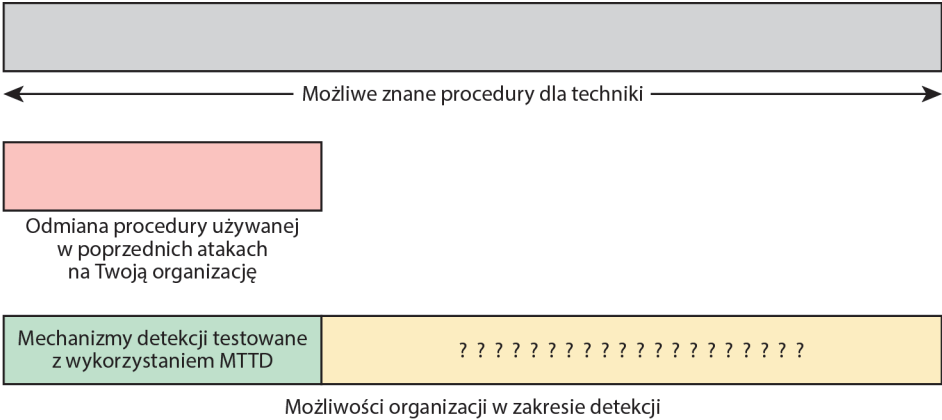
Software			
ID	Name	References	Techniques
S0501	PipeMon	[6]	Abuse Elevation Control Mechanism: Bypass User Account Control, Access Token Manipulation: Create Process with Token, Access Token Manipulation: Parent PID Spoofing, Boot or Logon Autostart Execution: Print Processors, Create or Modify System Process: Windows Service, Deobfuscate/Decode Files or Information, Encrypted Channel: Symmetric Cryptography, Fallback Channels, Ingress Tool Transfer, Masquerading: Match Legitimate Name or Location, Modify Registry, Native API, Non-Application Layer Protocol, Obfuscated Files or Information, Obfuscated Files or Information: Fileless Storage, Process Discovery, Process Injection: Dynamic-link Library Injection, Shared Modules, Software Discovery: Security Software Discovery, Subvert Trust Controls: Code Signing, System Information Discovery, System Network Configuration Discovery, System Time Discovery
S0013	PlugX	[1]	Application Layer Protocol: Web Protocols, Application Layer Protocol: DNS, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, Deobfuscate/Decode Files or Information, Encrypted Channel: Symmetric Cryptography, File and Directory Discovery, Hide Artifacts: Hidden Files and Directories, Hijack Execution Flow: DLL Side-Loading, Hijack Execution Flow: DLL Search Order Hijacking, Ingress Tool Transfer, Input Capture: Keylogging, Masquerading: Masquerade Task or Service, Masquerading: Match Legitimate Name or Location, Modify Registry, Native API, Network Share Discovery, Non-Application Layer Protocol, Obfuscated Files or Information, Process Discovery, Query Registry, Screen Capture, System Network Connections Discovery, Trusted Developer Utilities Proxy Execution: MSBuild, Virtualization/Sandbox Evasion: System Checks, Web Service: Dead Drop Resolver
S0141	Winnti for Windows	[1][2]	Abuse Elevation Control Mechanism: Bypass User Account Control, Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Create or Modify System Process: Windows Service, Deobfuscate/Decode Files or Information, Encrypted Channel: Symmetric Cryptography, Execution Guardrails: Environmental Keying, File and Directory Discovery, Indicator Removal: File Deletion, Indicator Removal: Timestamp, Ingress Tool Transfer, Masquerading: Match Legitimate Name or Location, Native API, Non-Application Layer Protocol, Obfuscated Files or Information, Process Discovery, Proxy: External Proxy, Proxy: Internal Proxy, System Binary Proxy Execution: Rundll32, System Information Discovery, System Services: Service Execution

Rysunek 10.2. Winnti Group — oprogramowanie

# Rozdział 11. Zarządzanie wydajnością



Rysunek 11.1. Model dojrzałości inżynierii detekcji



Rysunek 11.2. Testowanie mechanizmów detekcji za pomocą MTTD

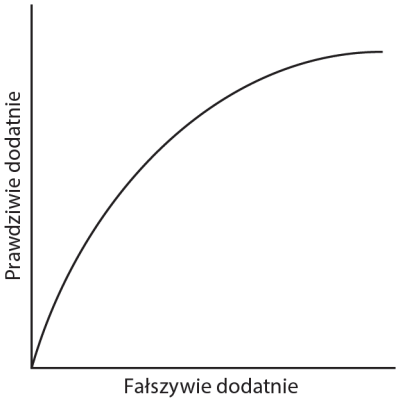
Skuteczność

Metryki	Niski wpływ	Średni/ wysoki	Wysoki wpływ
Wydajność	×	×	×
Trafność i czułość		×	×
Niski poziom wierności		×	×
Automatyczna walidacja		×	×
Wysoki poziom wierności			×

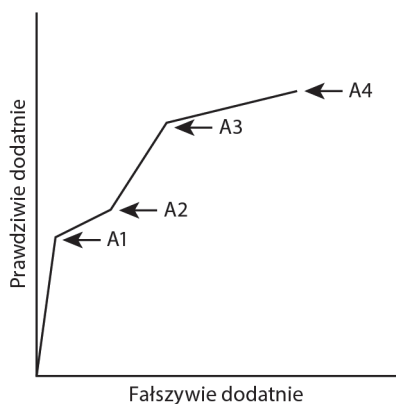
Rysunek 11.3. Metryki według poziomów ważności



Rysunek 11.4. Określanie alertów



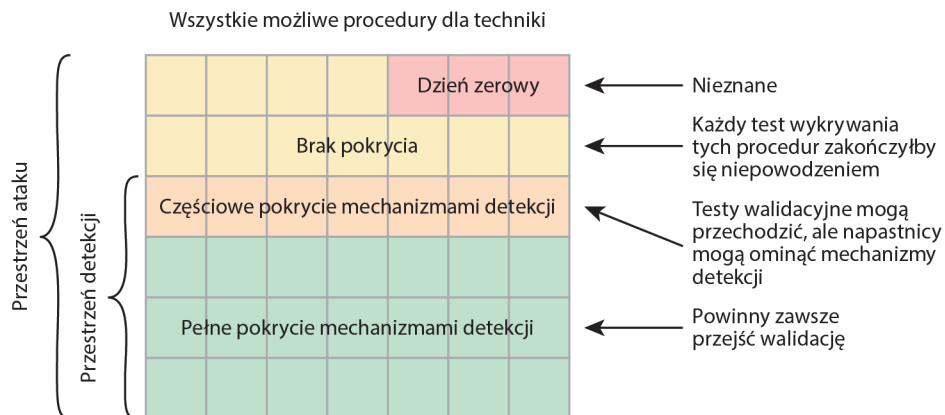
Rysunek 11.5. Standardowa krzywa ROC



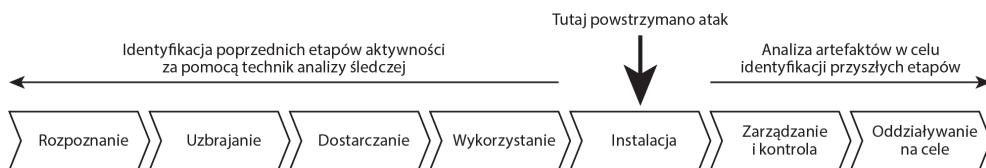
### Rysunek 11.6. Ocena podejść do mechanizmów detekcji z wykorzystaniem krzywej ROC

[illegible]

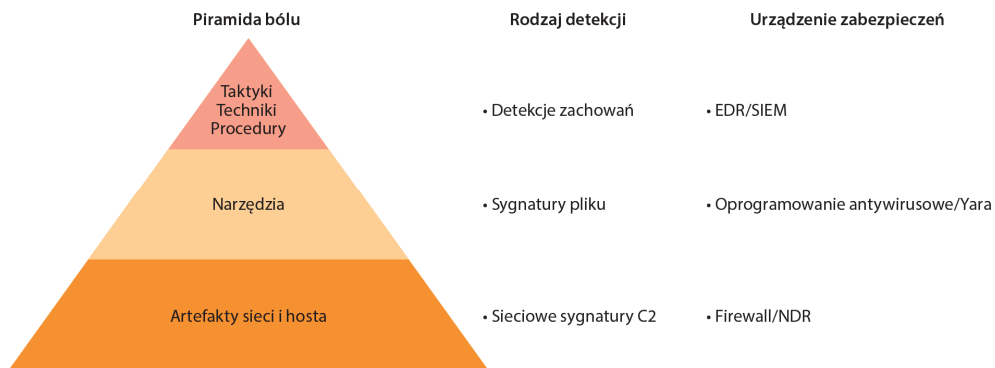
### Rysunek 11.7. Przykład macierzy MITRE ATT&CK



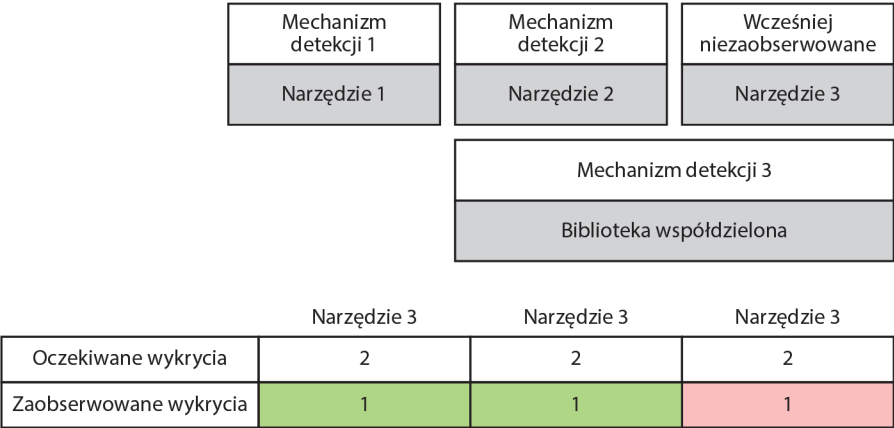
**Rysunek 11.8. Kategorie wyników walidacji mechanizmów detekcji**



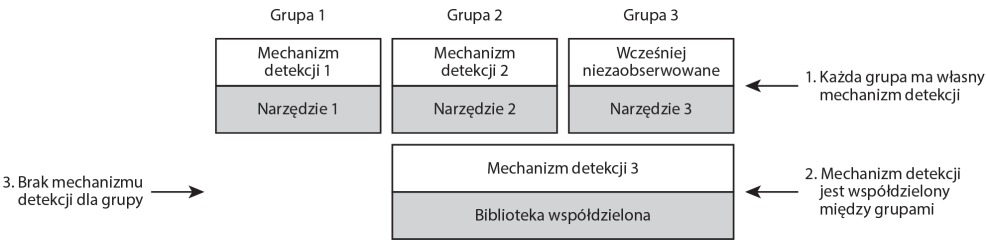
**Rysunek 11.9. Analiza Cyber Kill Chain w celu zidentyfikowania niewykrytych działań napastnika**



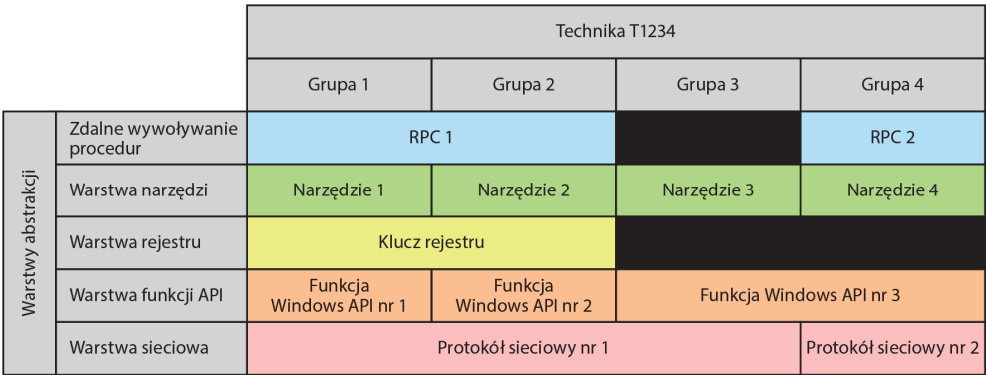
**Rysunek 11.10. Piramida bólu i rodzaje detekcji**



Rysunek 11.11. Dryf mechanizmu detekcji dla wielu narzędzi stosowanych przez atakującego



Rysunek 11.12. Różnice w pokryciu mechanizmów detekcji



Rysunek 11.13. Mapa abstrakcji z pięcioma warstwami

		Grupy możliwości			
		Grupa 1	Grupa 2	Grupa 3	Grupa 4
Warstwy abstrakcji	Warstwa abstrakcji 1	Szczegóły artefaktu			Szczegóły artefaktu
	Warstwa abstrakcji 2	Szczegóły artefaktu	Szczegóły artefaktu	Szczegóły artefaktu	Szczegóły artefaktu
	Warstwa abstrakcji 3	Szczegóły artefaktu			
	Warstwa abstrakcji 4	Szczegóły artefaktu	Szczegóły artefaktu	Szczegóły artefaktu	
	Warstwa abstrakcji 5	Szczegóły artefaktu			Szczegóły artefaktu

Rysunek 11.14. Uogólniona mapa abstrakcji

Mapa abstrakcji ze znacznikami minimalnej liczby detekcji

		Technika T1234			
		Grupa 1	Grupa 2	Grupa 3	Grupa 4
Warstwy abstrakcji	Zdalne wywoływanie procedur	TAG: T1234 MD: 5 RPC 1			TAG: T1234 MD: 4 RPC 2
	Warstwa narzędzi	TAG: T1234 MD: 5 Narzędzie 1	TAG: T1234 MD: 5 Narzędzie 2	TAG: T1234 MD: 3 Narzędzie 3	TAG: T1234 MD: 4 Narzędzie 4
	Warstwa rejestru	TAG: T1234 MD: 5 Klucz rejestru			
	Warstwa funkcji API	TAG: T1234 MD: 5 Funkcja Win API nr 1	TAG: T1234 MD: 5 Funkcja Win API nr 2	TAG: T1234 MD: 3 Funkcja Windows API nr 3	
	Warstwa sieciowa	TAG: T1234 MD: 3 Protokół sieciowy nr 1			TAG: T1234 MD: 4 Protokół sieciowy nr 2

Rysunek 11.15. Przykład oznaczania MD

$$\text{Minimalny dryf mechanizmu detekcji} = \text{Max}(MD_1, MD_2, MD_n) - n$$

Gdzie:  $n$  = liczba alertów

Rysunek 11.16. Wzór na dryf MD

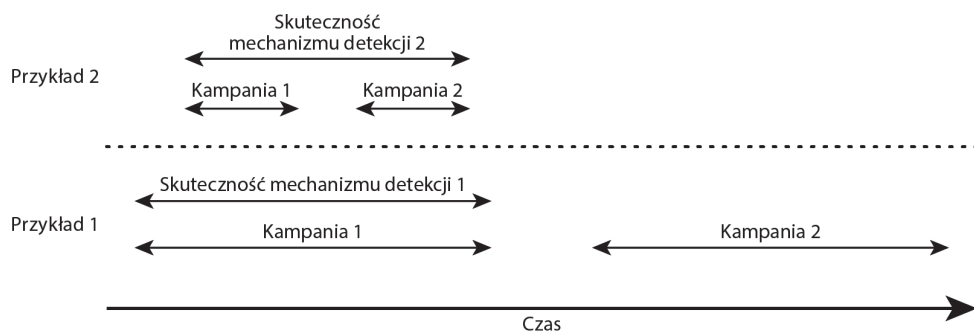
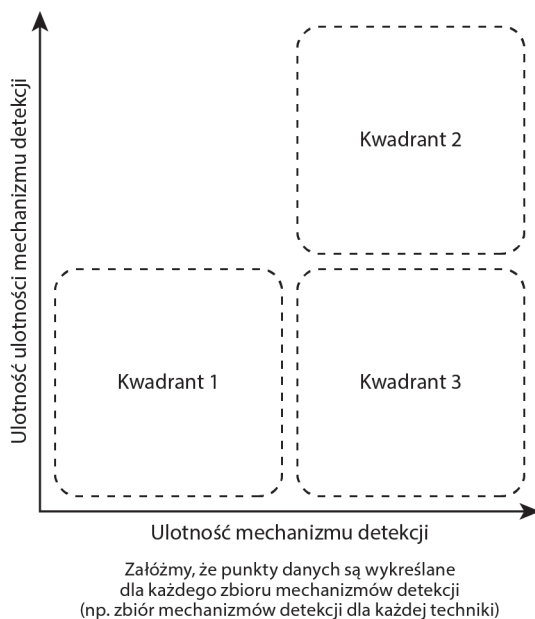
Mapa abstrakcji ze znacznikami minimalnej liczby detekcji i odpowiedzią EDR

EDR zatrzymuje atak, jeśli zostanie wykryty →

		Technika T1234			
		Grupa 1	Grupa 2	Grupa 3	Grupa 4
Warstwy abstrakcji	Zdalne wywoływanie procedur	TAG: T1234 MD: 4 RPC 1			TAG: T1234 MD: 3 RPC 2
	Warstwa narzędzi	TAG: T1234 MD: 4 Narzędzie 1	TAG: T1234 MD: 4 Narzędzie 2	TAG: T1234 MD: 2 Narzędzie 3	TAG: T1234 MD: 3 Narzędzie 4
	Warstwa rejestru	TAG: T1234 MD: 4 Klucz rejestru			
	Warstwa funkcji API	TAG: T1234 MD: 4 Funkcja Win API nr 1	TAG: T1234 MD: 4 Funkcja Win API nr 2	TAG: T1234 MD: 2 Funkcja Windows API nr 3	
	Warstwa sieciowa	TAG: T1234 MD: 3 Protokół sieciowy nr 1			TAG: T1234 MD: 4 Protokół sieciowy nr 2

Rysunek 11.17. Mapa abstrakcji z odpowiedzią EDR



**Rysunek 11.18. Skuteczność mechanizmów detekcji w czasie****Rysunek 11.19. Wykres aspektów ulotności mechanizmów detekcji**