ENERGY MONITOR

ENERGY SOAR

ENERGY LOGSERVER

SIEM i SOAR – Jak przekształcić regulacyjne wymagania w przewagę biznesową?

Agenda

- O Energy słów kilka
- Jak SIEM i SOAR pomagają spełnić wymogi regulacyjne i jednocześnie zwiększyć bezpieczeństwo?
- Szybsza reakcja na incydenty – jak automatyzacja poprawia skuteczność ochrony organizacji
- Jak SIEM i SOAR zwiększają zaufanie klientów i partnerów?

O Energy

ENERGY LOGSERVER

#Cyber Made InPoland

OWASP TOP10

Information Security Management System ISO 27001 Certified

Referencje

ENERGY LOGSERVER

Referencje

ENERGY LOGSERVER

Portfolio

ENERGY LOGSERVER

- Log Management
- SIEM
- AI
- EDR
- UEBA
- NDR
- Netflow
- Vulnerability scanning
- FIM

ENERGY SOAR

- Automatyzacja procesu obsługi incydentu
- Workflow
- Integracja z 3rd party

ENERGY MONITOR

- Monitoring infrastruktury
- Monitoring sieci
- Monitoring usług biznesowych

ENERGY MONITOR

ENERGY SOAR

ENERGY LOGSERVER

SIEM i SOAR w cyberbezpiecznej organizacji

SIEM i SOAR w dyrektywie NIS2

ENERGY LOGSERVER

- Centralizacja danych
- Zarządzanie logami
- Zgodność z przepisami
- Wykrywanie zagrożeń i alerty

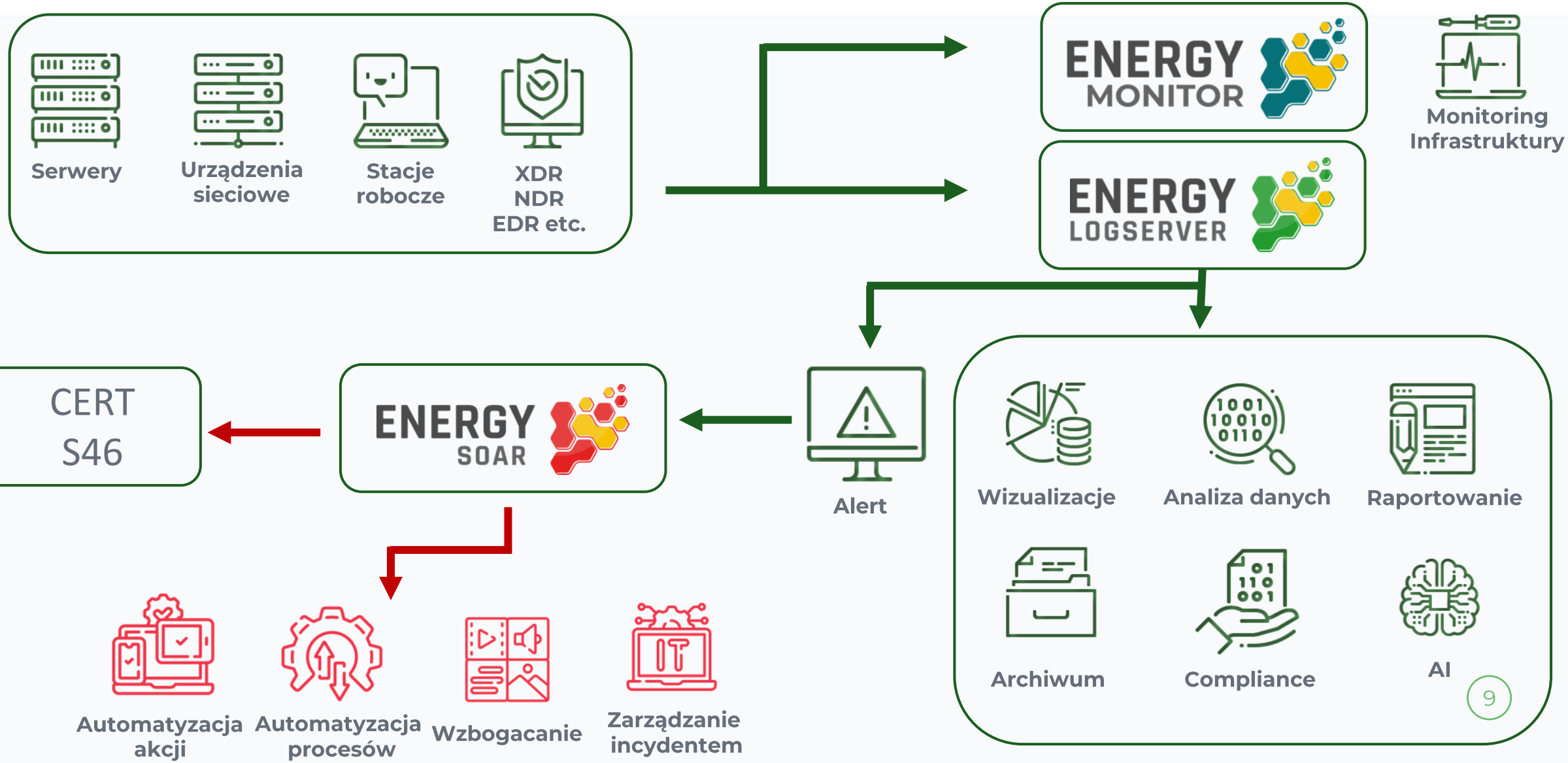
ENERGY SOAR

- Orkiestracja i automatyzacja
- Zarządzanie incydentami
- Raportowanie i analiza

ENERGY MONITOR

- Monitorowanie infrastruktury
- Ciągłość procesów biznesowych

SIEM i SOAR w organizacji



SIEM

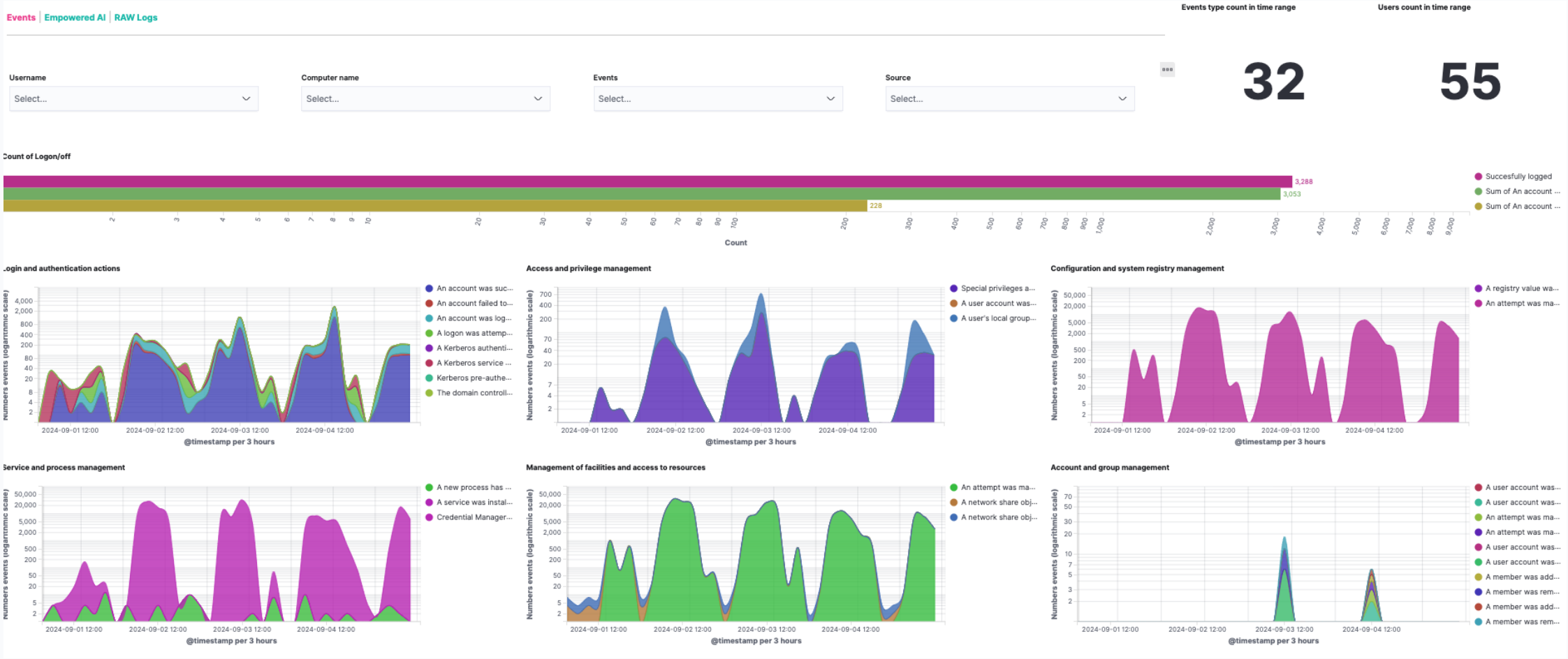
ENERGY LOGSERVER

- Setki gotowych reguł korelacyjnych
- Integracja z MISP
- MITRE ATT&CK
- Zarządzanie ryzykiem
- Zarządzanie incydentem
- Sztuczna inteligencja

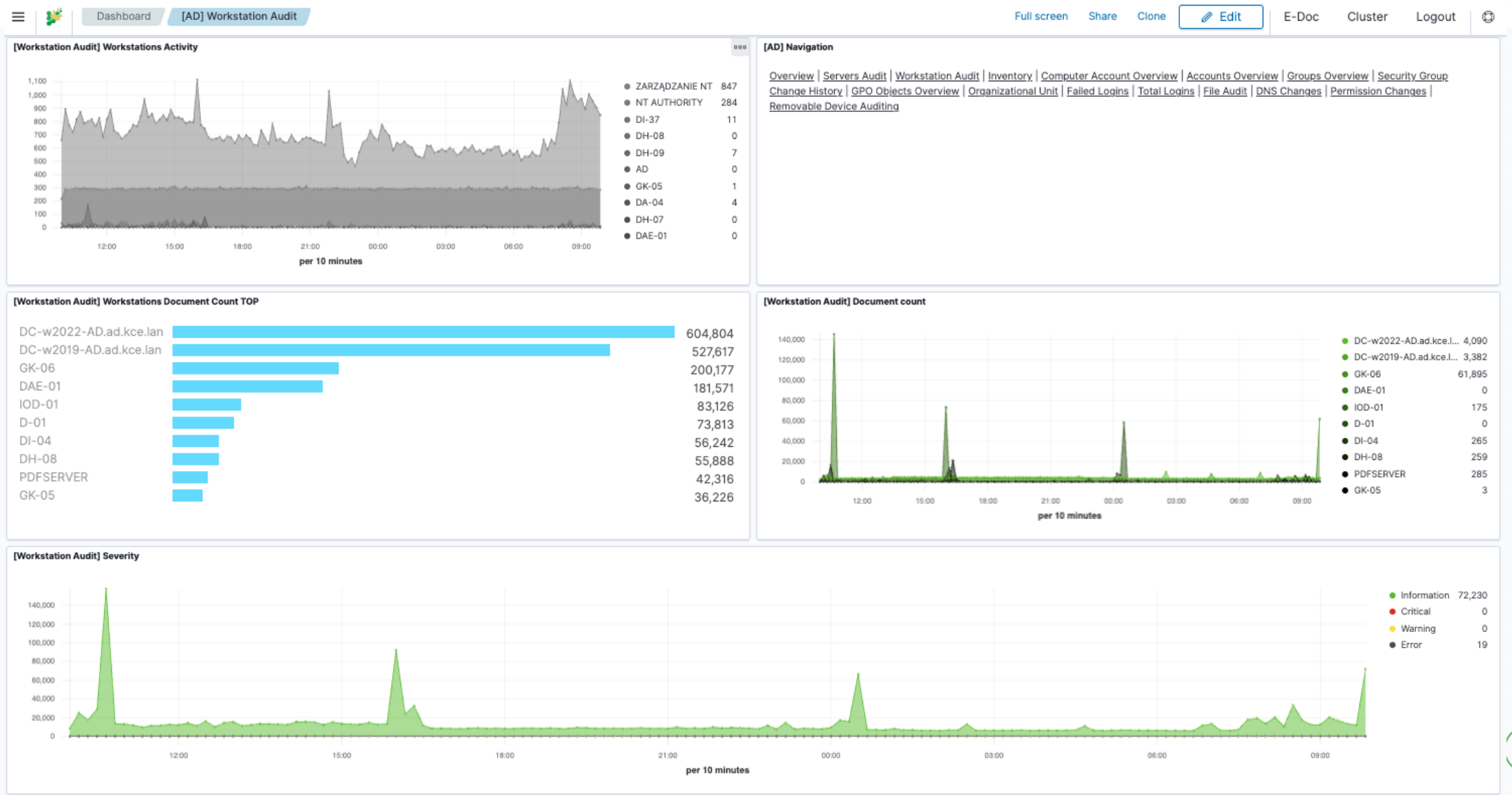
ATT&CK®

MISP Threat Sharing

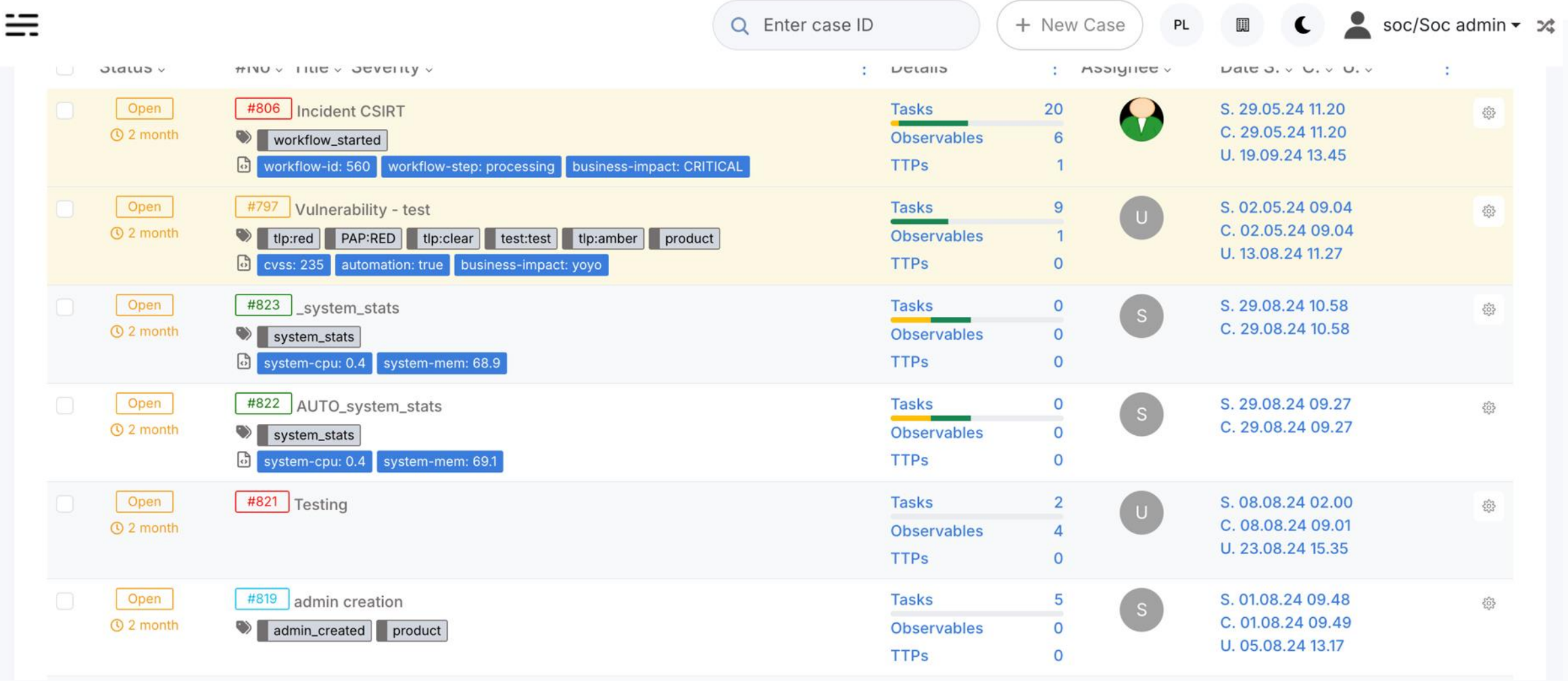
UEBA


Events | Empowered AI | RAW Logs
Events type count in time range
32
Users count in time range
55
Username
Select...
Computer name
Select...
Events
Select...
Source
Select...
Count of Logon/off
3,288
3,053
228
Succesfully logged
Sum of An account ...
Sum of An account ...
Count
Login and authentication actions
An account was suc...
An account failed to...
An account was log...
A logon was attemp...
A Kerberos authenti...
A Kerberos service ...
Kerberos pre-authe...
The domain controll...
Numbers events (logarithmic scale)
2024-09-01 12:00
2024-09-02 12:00
2024-09-03 12:00
2024-09-04 12:00
@timestamp per 3 hours
Access and privilege management
Special privileges a...
A user account was...
A user's local group...
Configuration and system registry management
A registry value wa...
An attempt was ma...
Service and process management
A new process has ...
A service was instal...
Credential Manager...
Management of facilities and access to resources
An attempt was ma...
A network share obj...
A network share obj...
Account and group management
A user account was...
A user account was...
An attempt was ma...
An attempt was ma...
A user account was...
A user account was...
A member was add...
A member was rem...
A member was add...
A member was rem...

AD & M365 monitoring



Centralizacja zdarzeń



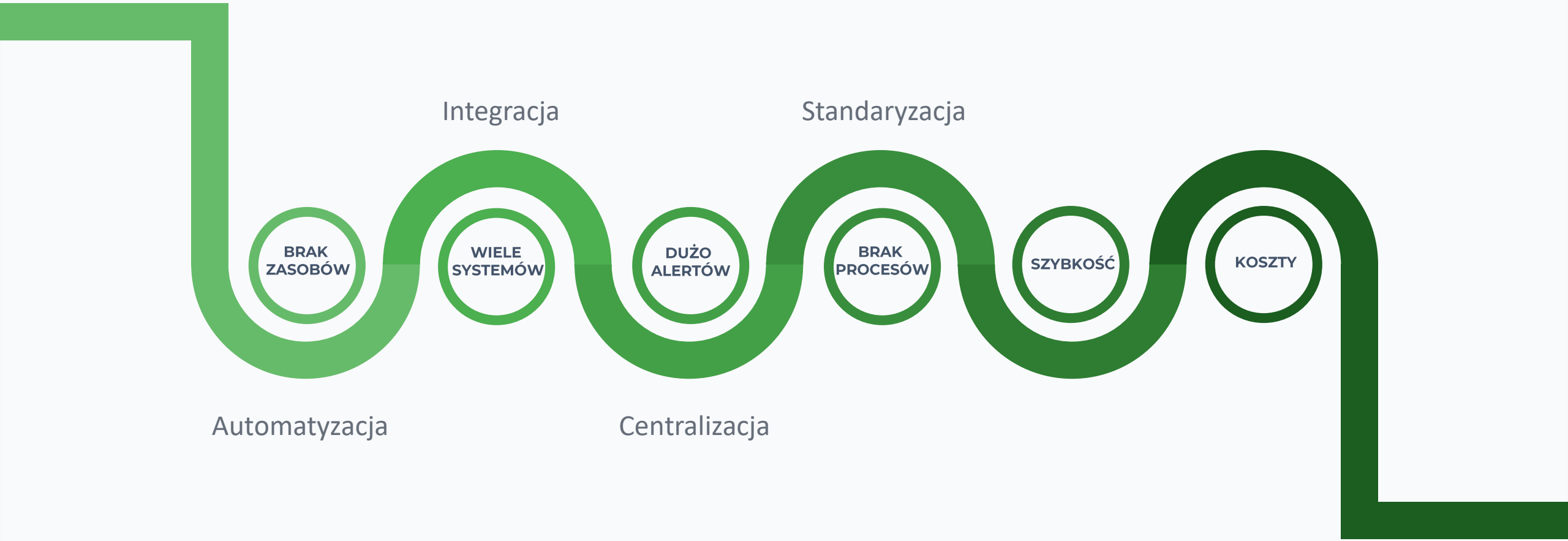
ENERGY MONITOR

ENERGY SOAR

ENERGY LOGSERVER

Szybsza reakcja na incydenty – jak automatyzacja poprawia skuteczność ochrony organizacji

Problemy życia codziennego



Phishing use case

Subject: Nowe zamówienie nr ZZ-135/02/25/Z_CNG
From: "Paula Bednarczyk (CERRAD Sp. z o.o.)" <elena.pana@cocor.ro>
Date: 13.02.2025, 12:16
To: sales@falk-ross.eu

Dzień dobry,

Proszę podać nam najlepszą ofertę (ceny i dostawa) na załączoną listę zamówień.

Dziękujemy za uprzejmą odpowiedź.

Pozdrawiam,

Pozdrawiam,

Paula Bednarczyk
Specjalista ds. Zakupów

mob.: 691 191 177
tel.: 41 276 31 94
e-mail: p.bednarczyk@cerrad.com

CERRAD

ULTIME CERRAD NowaGala CERAMIKA CeramikaGres

CERRAD Sp. z o.o. 27-200 Starachowice ul. Radomska 49b
Sąd Rejonowy w Kielcach X Wydział Gospodarczy Krajowego Rejestru Sądowego KRS: 0000064429
NIP: 796-101-26-11 REGON: 670754817 Kapitał zakładowy: 51.000,00 PLN Nr rejestrowy BDO:000012331
Posiada status dużego przedsiębiorcy

2 attachments 2.0 MB Save All

Nowe zamówienie nr ZZ-135/02/25/Z_CNG.eml 2.0 MB ZAMÓWIENIE-ZZ-135.02.25.Z_CNG.IMG 1.4 MB

Phishing use case

ENERGY LOGSERVER

Processes

C:\Users\Admin\AppData\Local\Temp\Zamówienia_G1.13.02.25._005623900883.exe

PID:3068

```
"C:\Users\Admin\AppData\Local\Temp\Zamówienia_G1.13.02.25._005623900883.exe"
```

C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

PID:1848

```
powershell.exe -windowstyle hidden "$Cruncher=gc -raw 'C:\Users\Admin\AppData\Roaming\mortens
gss\Breddeminut\Tankrensningsanlggene\Bverunge.Per';$Rangemen=$Cruncher.SubString(55581,
3);.$Rangemen($Cruncher) "
```

C:\Users\Admin\AppData\Local\Temp\Rebemire.exe

PID:3768

```
"C:\Users\Admin\AppData\Local\Temp\Rebemire.exe"
```

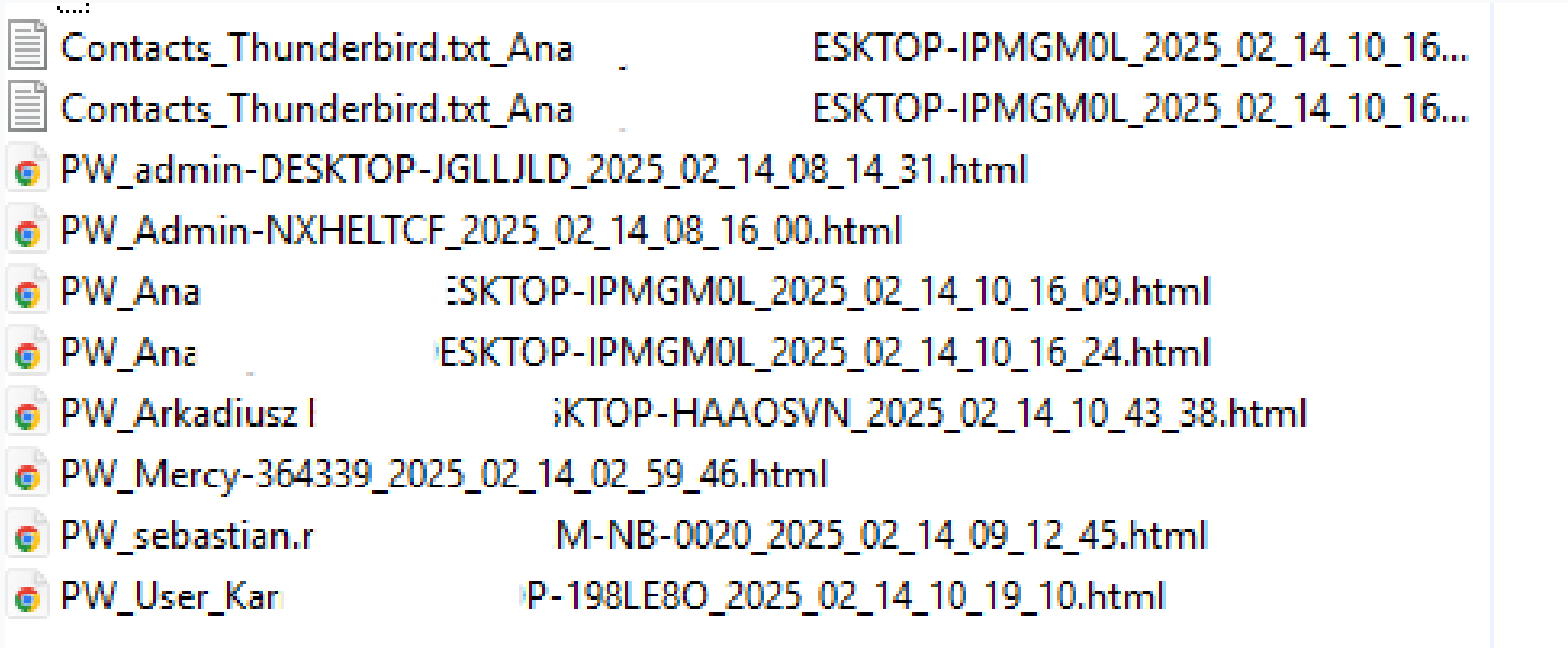
Phishing use case

Malware Config

Extracted

Family	agenttesla
Credentials	**Protocol:** ftp
	Host: ftp://ftp.carbognin.it
	Port: 21
	Username: server@carbognin.it
	Password: 59Cif8wZUH#X

Phishing use case



Phishing use case

Discover Index Pattern:

windows-winlogbeat-* [id: a740f980-0a0c-11ea-...

Target address:

https://hqelsclient01

From (minutes):

1

To: (minutes)

0

Alert Method

None

Example

Show example

Rule Definition

```
filter:
  - query_string:
      query: "winlog.event_id:1 AND winlog.event_data.CommandLine:*powershell* AND winlog.event_data.CommandLine:(*Hidden* OR *hidden*) AND NOT winlog.event_data.CommandLine:*IsHidden*"
```

AI Netflow Anomaly

ENERGY LOGSERVER

Alert Rule: AI Netflow Anomaly Text country

Alert Method

Energy SOAR

Title

AI Netflow Anomaly Text country

Alert type: Alert

Follow (Active on update)

Type

external

Source

SIEM

Status

New

Severity

2: medium

TLP

2: amber

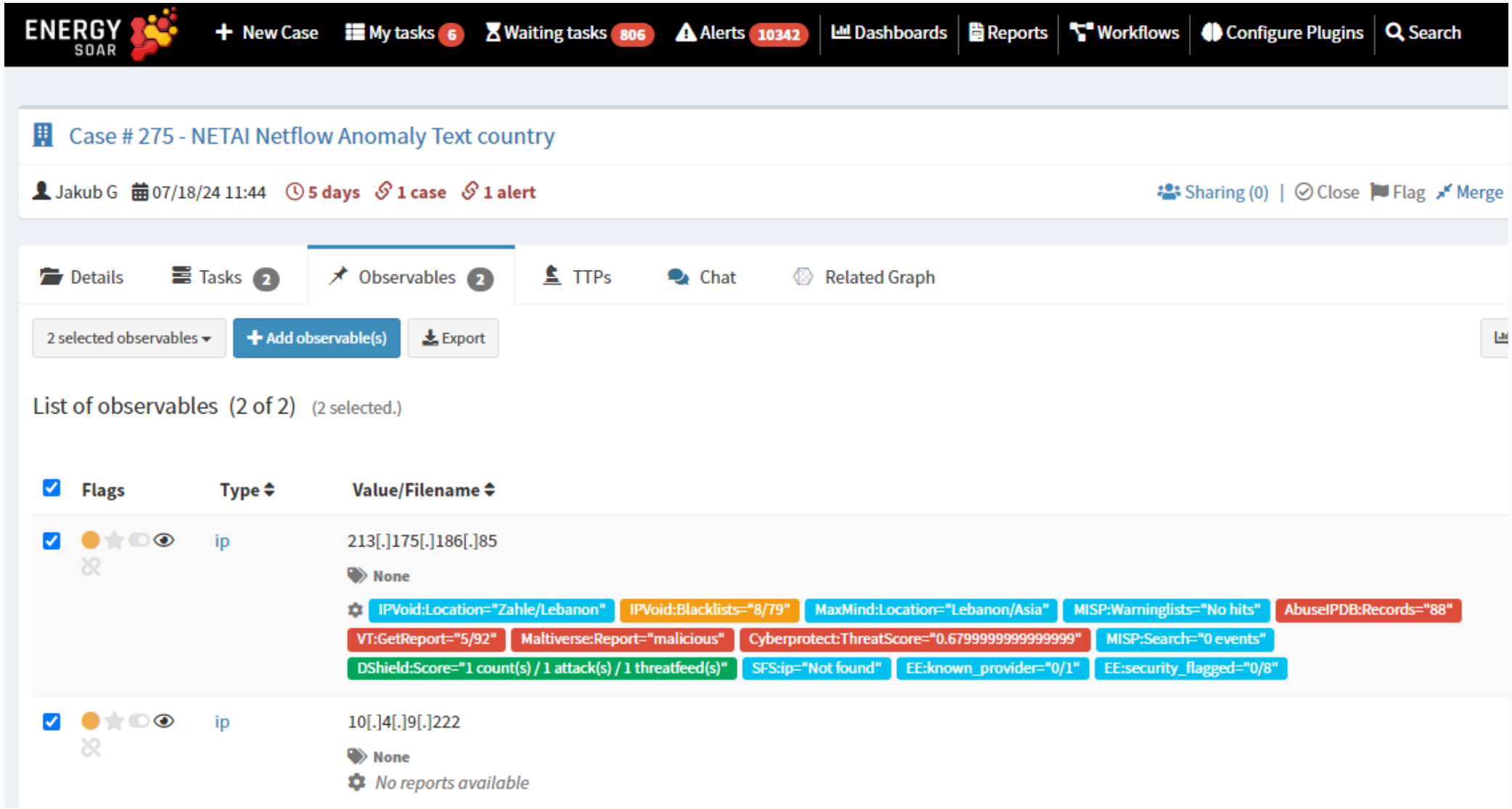
Tags

AI ×

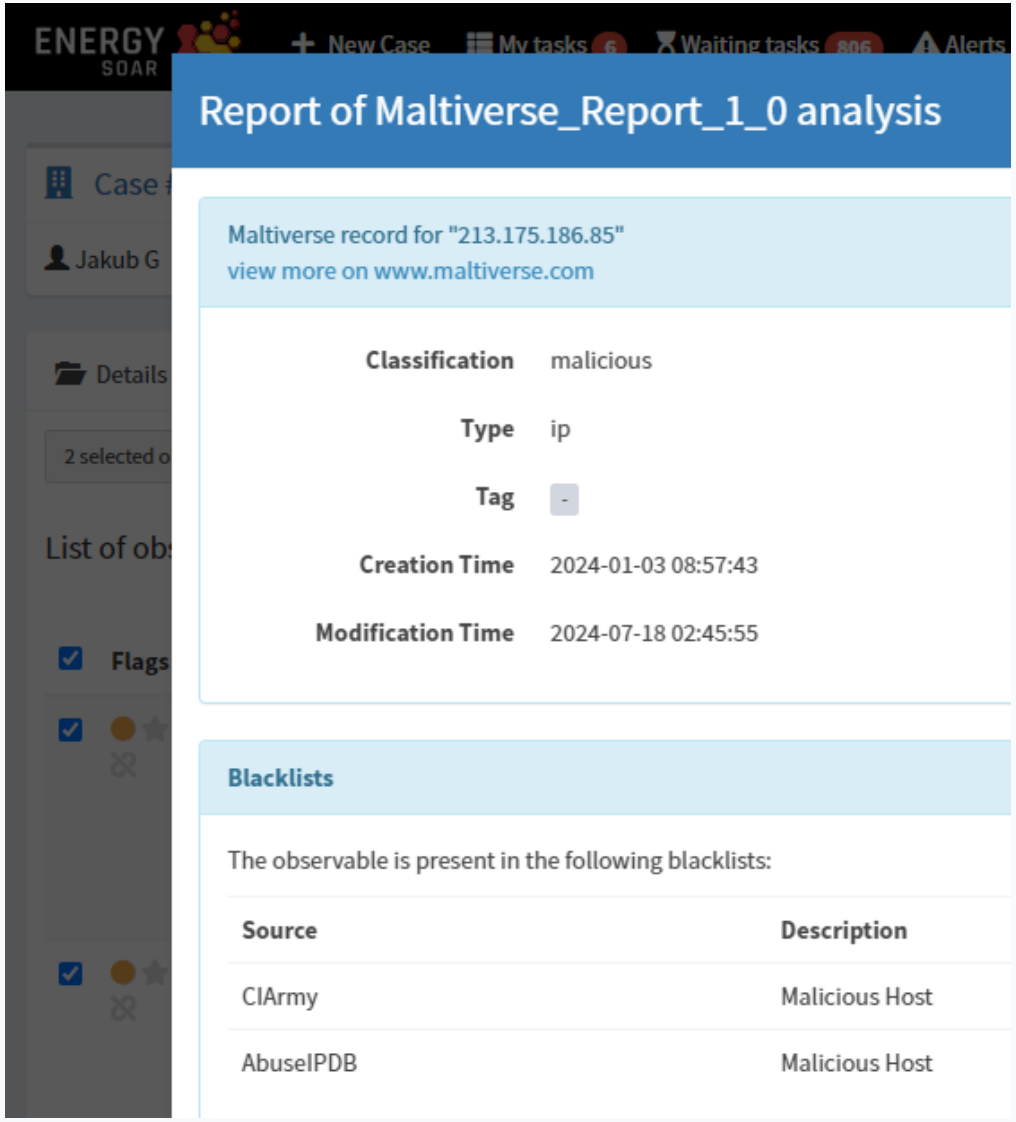
Observable data mapping

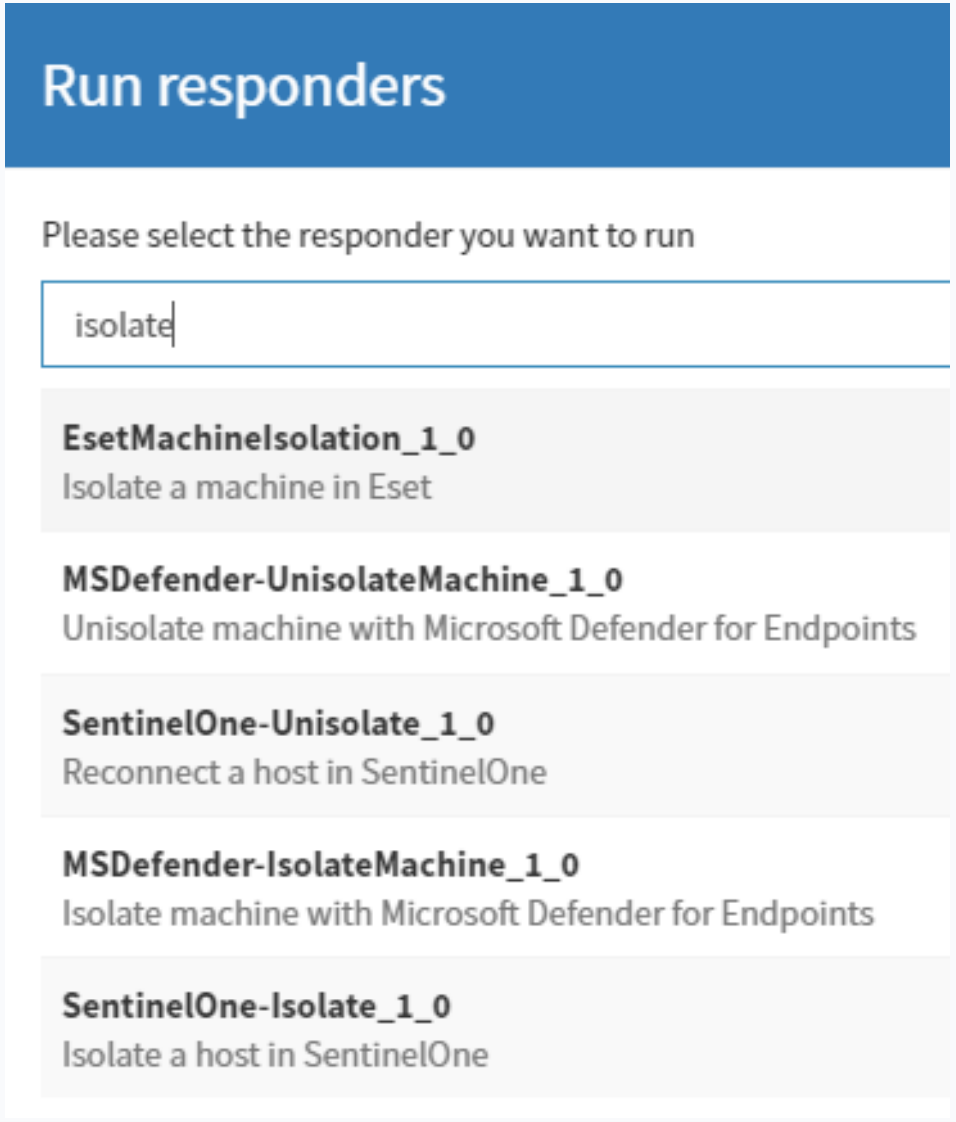
ip	{match[server][ip]}
ip	{match[client][ip]}

AI Netflow Anomaly

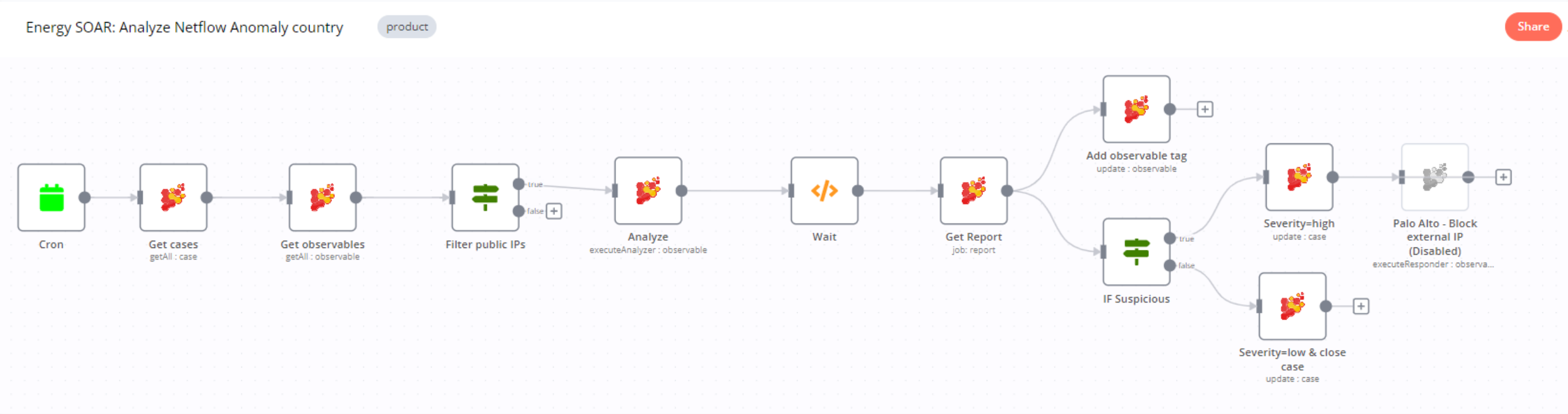


AI Netflow Anomaly





AI Netflow Anomaly



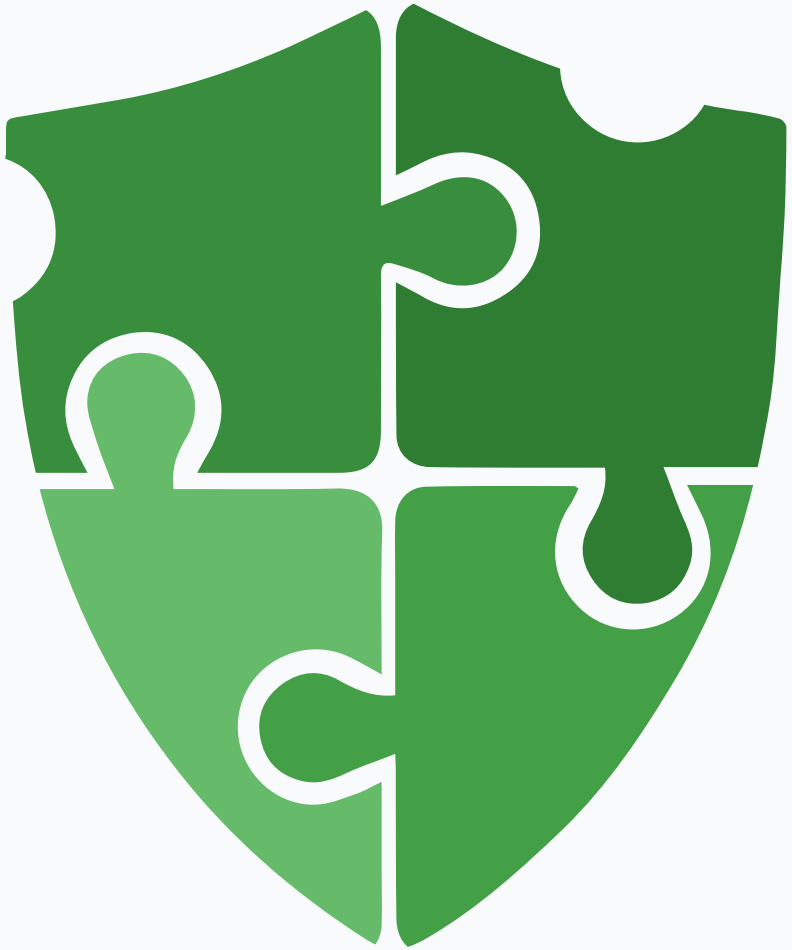
ENERGY MONITOR

ENERGY SOAR

ENERGY LOGSERVER

Jak SIEM i SOAR zwiększają zaufanie klientów i partnerów?

Energy dla Biznesu



Bezpieczeństwo

Optymalizacja kosztów

Zaufanie rynku

Elastyczność

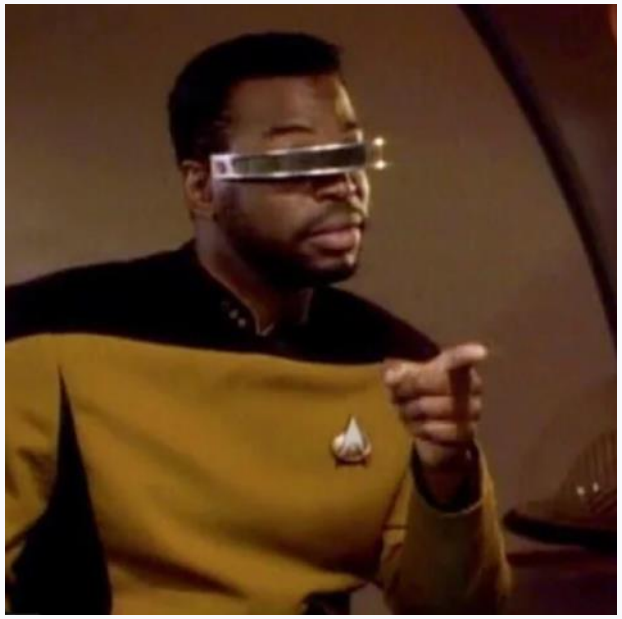
Rozwój to przewaga

Wsparcie producenta

- Dostęp do nowych wersji oprogramowania
- Support online i sesje zdalne
- Support telefoniczny

Managed Support

- Bieżąca administracja systemem
- Tworzenie reguł, widoków i integracji
- Healthcheck
- Rekomendacje rozwoju
- Budowanie kompetencji zespołu



ENERGY LOGSERVER

Licencjonowanie

Wieczyste I Subskrypcja I MSSP

Licencjonowanie

Oferta LITE

Dla organizacji do 100-150 użytkowników
- Do 20 GB danych dziennie
- Ekonomiczne rozwiązanie na start

Oferta Standard

Dla organizacji powyżej 150 użytkowników
- Do 100 GB danych dziennie dla jednej licencji
- Elastyczna licencja bez limitu na źródła, ilość danych...

Dziękuję za uwagę!

Łukasz Nieborek
+48 601 199 639
Lukasz.nieborek@energylogserver.com
sales@energylogserver.com