



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?



Energy





Referencje

CUI Centrum Usług Informatycznych
we Wrocławiu



Kalmar kommun



MINISTERSTWO
INWESTYCJI
I ROZWOJU



OŚWIĘCIM
MIASTO POKOJU



Ministry
of Education
and Science



MAŁOPOLSKA



Kraków



Rybnik



POLSKI
INSTYTUT
SZTUKI
FILMOWEJ



SWEDISH NATIONAL HERITAGE BOARD
RIKSANTIKVARIÉÄMBETET



VÄRMDÖ
KOMMUN



Urząd Ochrony Konkurencji i Konsumentów



SCANIA
Scania Polska S.A.



SZKOŁA GŁÓWNA
GOSPODARSTWA
WIEJSKIEGO



MIASTO
TORUŃ



Poczta Polska



Zabrze
w sercu Śląska



Referencje





Portfolio



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



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



- Monitoring infrastruktury
- Monitoring sieci
- Monitoring usług biznesowych



SIEM i SOAR w cyberbezpiecznej organizacji

🕒 SIEM i SOAR w dyrektywie NIS2



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

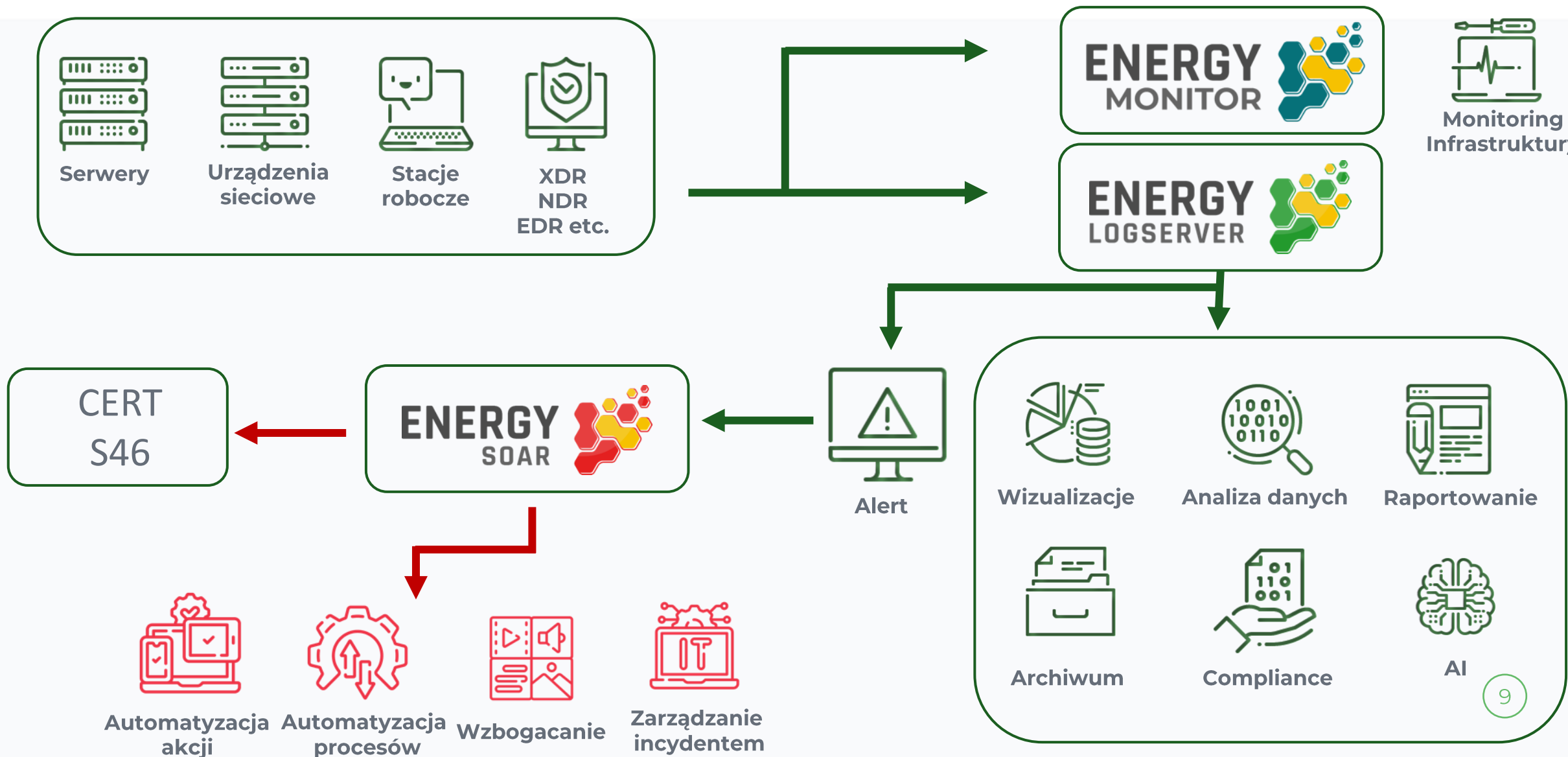


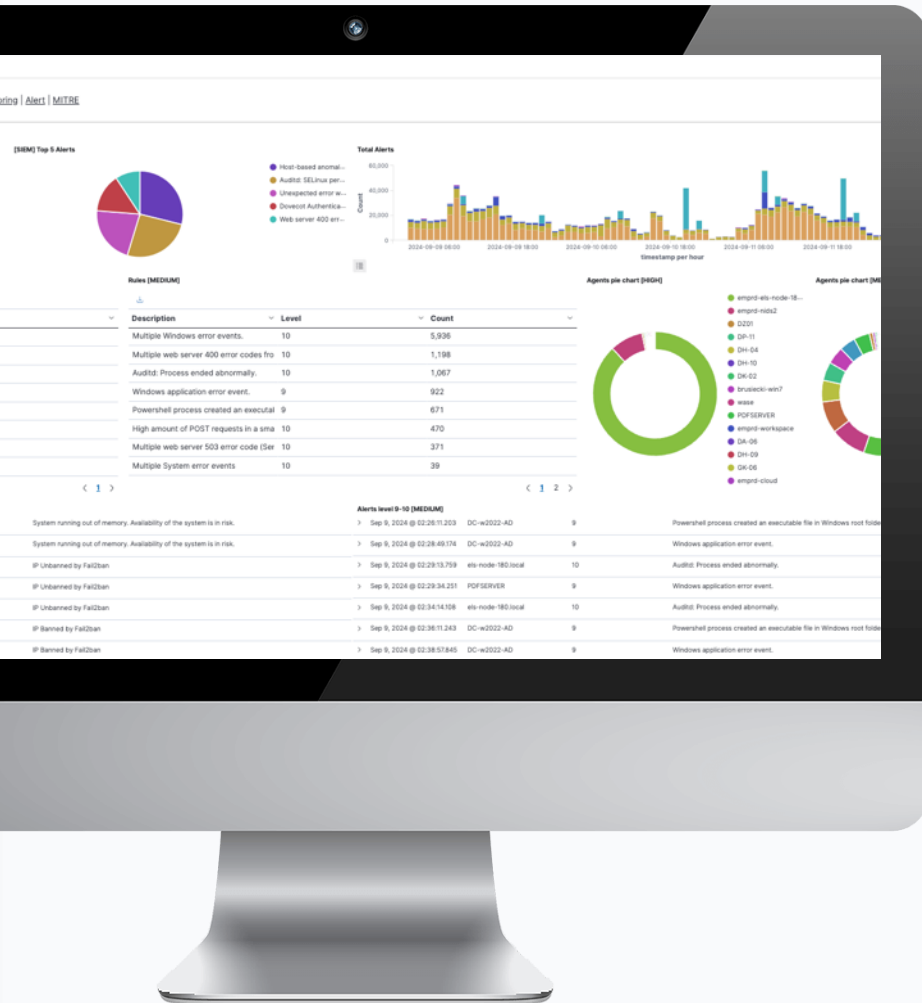
- Orkiestracja i automatyzacja
- Zarządzanie incydentami
- Raportowanie i analiza



- Monitorowanie infrastruktury
- Ciągłość procesów biznesowych

SIEM i SOAR w organizacji





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

ATT&CK®



Events | Empowered AI | RAW Logs

Events type count in time range

Users count in time range

Username:
 Computer name:
 Events:
 Source:

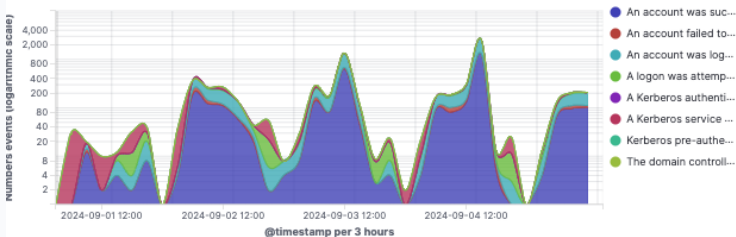
32

55

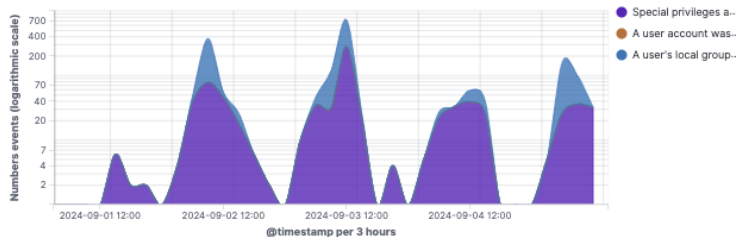
Count of Logon/off



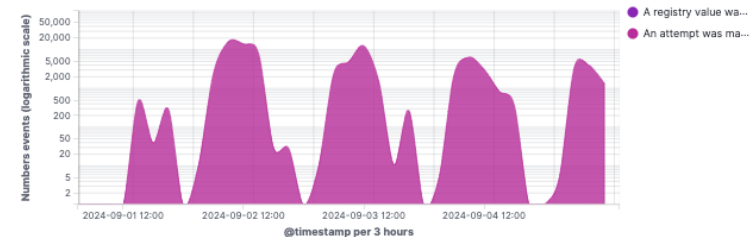
.login and authentication actions



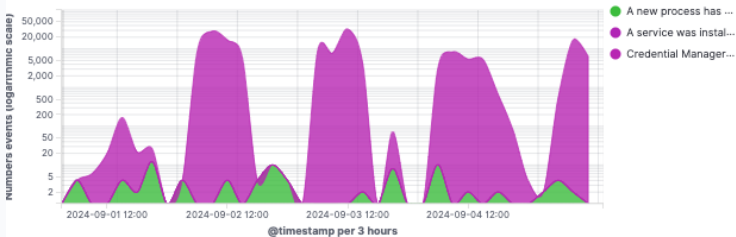
Access and privilege management



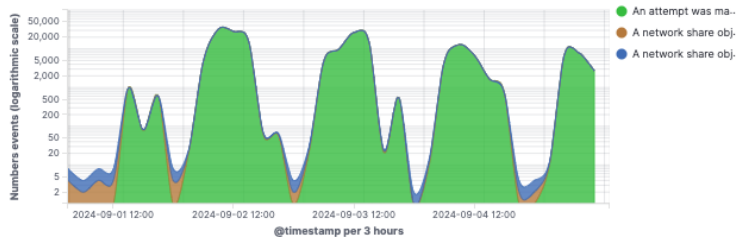
Configuration and system registry management



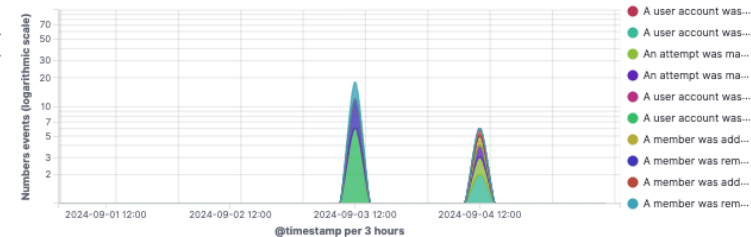
Service and process management



Management of facilities and access to resources

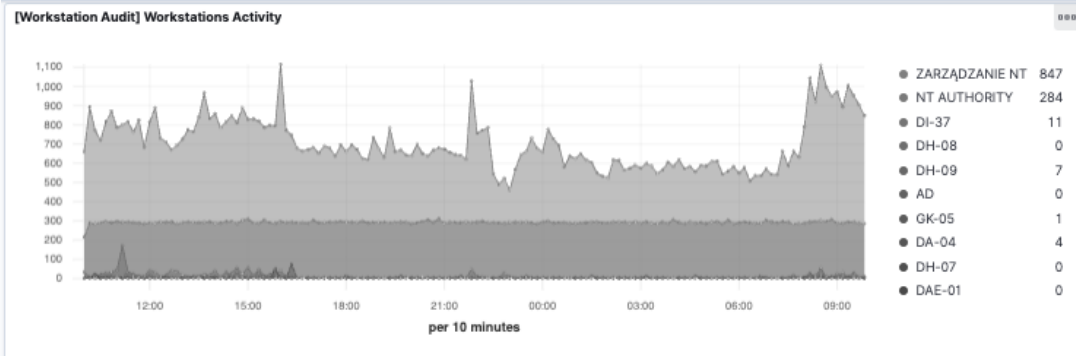


Account and group management



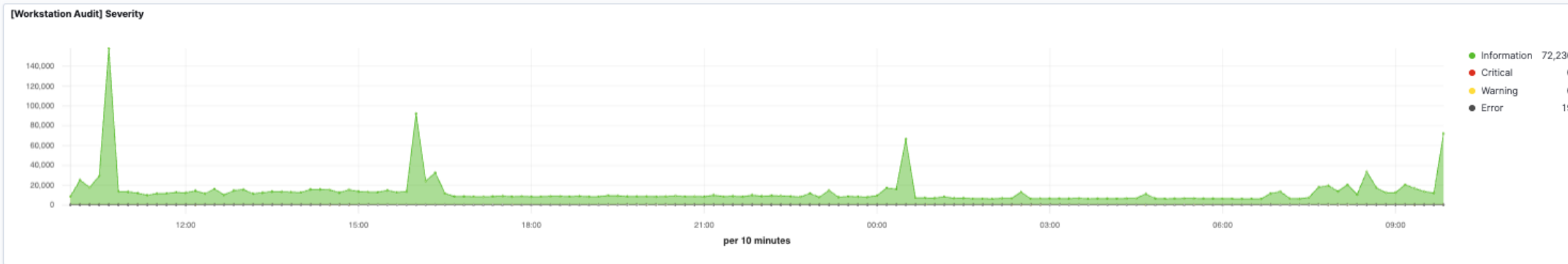
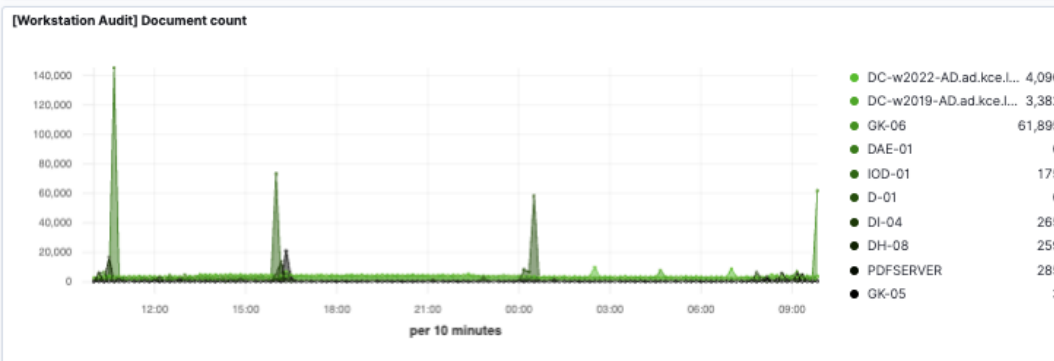
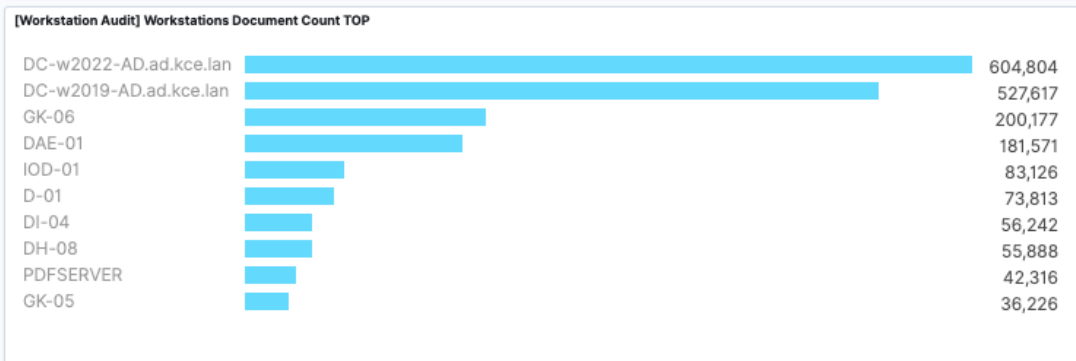


AD & M365 monitoring



[AD] Navigation

Overview | Servers Audit | Workstation Audit | Inventory | Computer Account Overview | Accounts Overview | Groups Overview | Security Group Change History | GPO Objects Overview | Organizational Unit | Failed Logins | Total Logins | File Audit | DNS Changes | Permission Changes | Removable Device Auditing





Centralizacja zdarzeń




Enter case ID

+ New Case

PL



soc/Soc admin

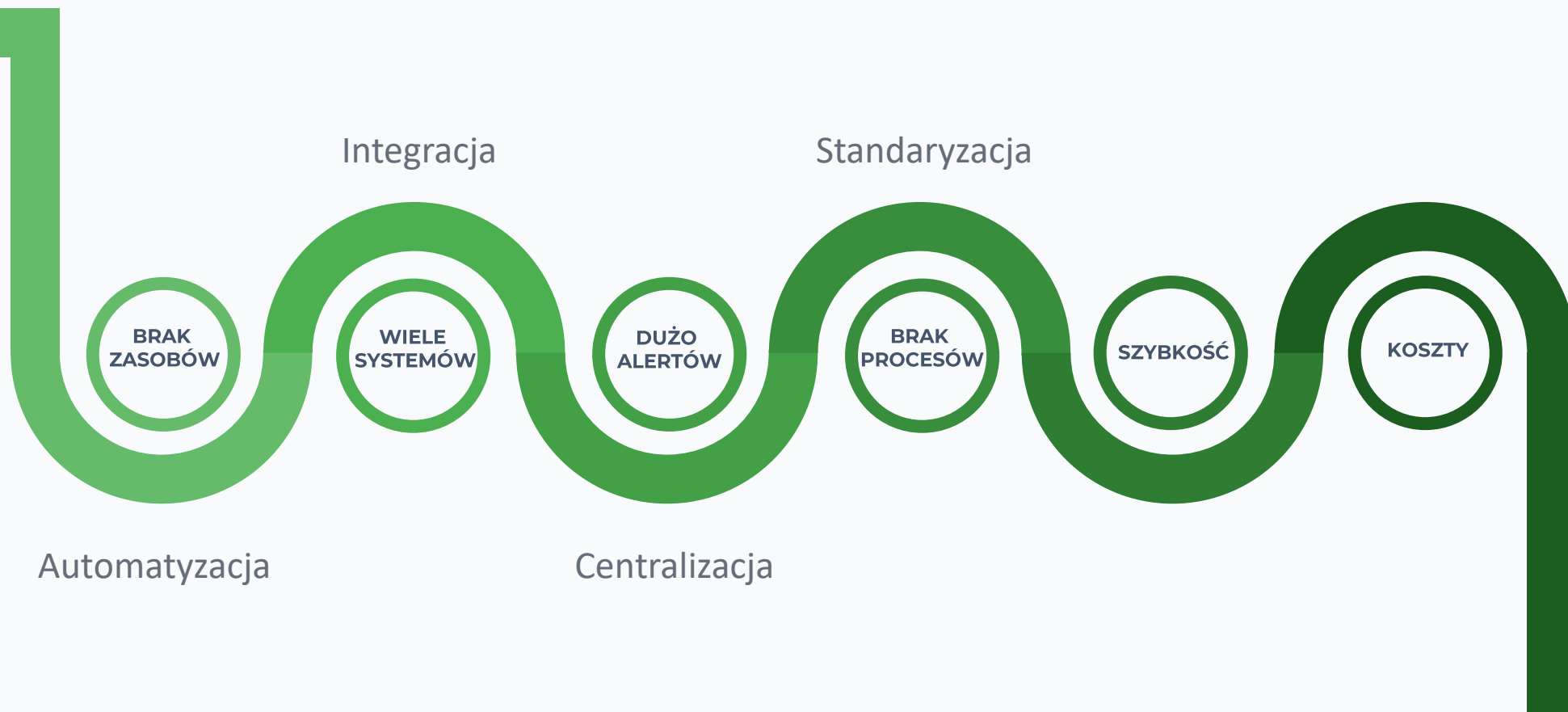
Status	#NO	Title	Severity	Details	Assignee	Date S.	C.	U.
Open 2 month	#806	Incident CSIRT		Tasks: 20 Observables: 6 TTPs: 1 workflow_started workflow-id: 560 workflow-step: processing business-impact: CRITICAL		S. 29.05.24 11.20	C. 29.05.24 11.20	U. 19.09.24 13.45
Open 2 month	#797	Vulnerability - test		Tasks: 9 Observables: 1 TTPs: 0 tlp:red PAP:RED tlp:clear test:test tlp:amber product cvss: 235 automation: true business-impact: yoyo	U	S. 02.05.24 09.04	C. 02.05.24 09.04	U. 13.08.24 11.27
Open 2 month	#823	_system_stats		Tasks: 0 Observables: 0 TTPs: 0 system_stats system-cpu: 0.4 system-mem: 68.9	S	S. 29.08.24 10.58	C. 29.08.24 10.58	
Open 2 month	#822	AUTO_system_stats		Tasks: 0 Observables: 0 TTPs: 0 system_stats system-cpu: 0.4 system-mem: 69.1	S	S. 29.08.24 09.27	C. 29.08.24 09.27	
Open 2 month	#821	Testing		Tasks: 2 Observables: 4 TTPs: 0	U	S. 08.08.24 02.00	C. 08.08.24 09.01	U. 23.08.24 15.35
Open 2 month	#819	admin creation		Tasks: 5 Observables: 0 TTPs: 0 admin_created product	S	S. 01.08.24 09.48	C. 01.08.24 09.49	U. 05.08.24 13.17



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 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

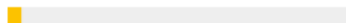
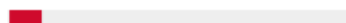

Nowe zamówienie nr ZZ-135/02/25/Z_CNG.eml 2.0 MB ZAMÓWIENIE-ZZ-135.02.25.Z_CNG.IMG 1.4 MB



Phishing use case

Processes



<ul style="list-style-type: none">■ C:\Users\Admin\AppData\Local\Temp\Zamówienia_G1.13.02.25_005623900883.exe "C:\Users\Admin\AppData\Local\Temp\Zamówienia_G1.13.02.25_005623900883.exe"		PID:3068
<ul style="list-style-type: none">■ C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe powershell.exe -windowstyle hidden "\$Cruncher=gc -raw 'C:\Users\Admin\AppData\Roaming\mortensgss\Breddeminut\Tankrensningssanlggene\Bverunge.Per';\$Rangemen=\$Cruncher.SubString(55581,3);.\$Rangemen(\$Cruncher) "		PID:1848
<ul style="list-style-type: none">■ C:\Users\Admin\AppData\Local\Temp\Rebemire.exe "C:\Users\Admin\AppData\Local\Temp\Rebemire.exe"		PID:3768

🕒 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

....	
 Contacts_Thunderbird.txt_Ana	ESKTOP-IPMGM0L_2025_02_14_10_16...
 Contacts_Thunderbird.txt_Ana	ESKTOP-IPMGM0L_2025_02_14_10_16...
 PW_admin-DESKTOP-JGLLJLD_2025_02_14_08_14_31.html	
 PW_Admin-NXHELTCF_2025_02_14_08_16_00.html	
 PW_Ana	ESKTOP-IPMGM0L_2025_02_14_10_16_09.html
 PW_Ana	ESKTOP-IPMGM0L_2025_02_14_10_16_24.html
 PW_Arkadiusz I	ESKTOP-HAAOSVN_2025_02_14_10_43_38.html
 PW_Mercy-364339_2025_02_14_02_59_46.html	
 PW_sebastian.r	M-NB-0020_2025_02_14_09_12_45.html
 PW_User_Kar	P-198LE8O_2025_02_14_10_19_10.html



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

```
1 filter:
2   - query_string:
3     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*"
4
```



AI Netflow Anomaly

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

ENERGY SOAR + New Case My tasks 6 Waiting tasks 806 Alerts 10342 Dashboards Reports Workflows Configure Plugins Search

Case # 275 - NETAI Netflow Anomaly Text country

Jakub G 07/18/24 11:44 5 days 1 case 1 alert

Sharing (0) | Close | Flag | Merge

Details **Tasks 2** **Observables 2** TTPs Chat Related Graph

2 selected observables + Add observable(s) Export

List of observables (2 of 2) (2 selected.)

<input checked="" type="checkbox"/>	Flags	Type	Value/Filename
<input checked="" type="checkbox"/>	🟡 ★ 👁️ 🔗	ip	213[.]175[.]186[.]85 None IPVoid:Location="Zahle/Lebanon" IPVoid:Blacklists="8/79" MaxMind:Location="Lebanon/Asia" MISP:Warninglists="No hits" AbuselPDB:Records="88" VT:GetReport="5/92" Maltiverse:Report="malicious" Cyberprotect:ThreatScore="0.6799999999999999" MISP:Search="0 events" DShield:Score="1 count(s) / 1 attack(s) / 1 threatfeed(s)" SFS:ip="Not found" EE:known_provider="0/1" EE:security_flagged="0/8"
<input checked="" type="checkbox"/>	🟡 ★ 👁️ 🔗	ip	10[.]4[.]9[.]222 None No reports available



AI Netflow Anomaly

ENERGY SOAR + New Case My tasks 6 Waiting tasks 806 Alerts

Report of Maltiverse_Report_1_0 analysis

Maltiverse record for "213.175.186.85"
[view more on www.maltiverse.com](http://www.maltiverse.com)

Classification	malicious
Type	ip
Tag	-
Creation Time	2024-01-03 08:57:43
Modification Time	2024-07-18 02:45:55

Blacklists

The observable is present in the following blacklists:

Source	Description
CIArmy	Malicious Host
AbuseIPDB	Malicious Host

Run responders

Please select the responder you want to run

EsetMachineIsolation_1_0

Isolate a machine in Eset

MSDefender-UnisolateMachine_1_0

Unisolate machine with Microsoft Defender for Endpoints

SentinelOne-Unisolate_1_0

Reconnect a host in SentinelOne

MSDefender-IsolateMachine_1_0

Isolate machine with Microsoft Defender for Endpoints

SentinelOne-Isolate_1_0

Isolate a host in SentinelOne

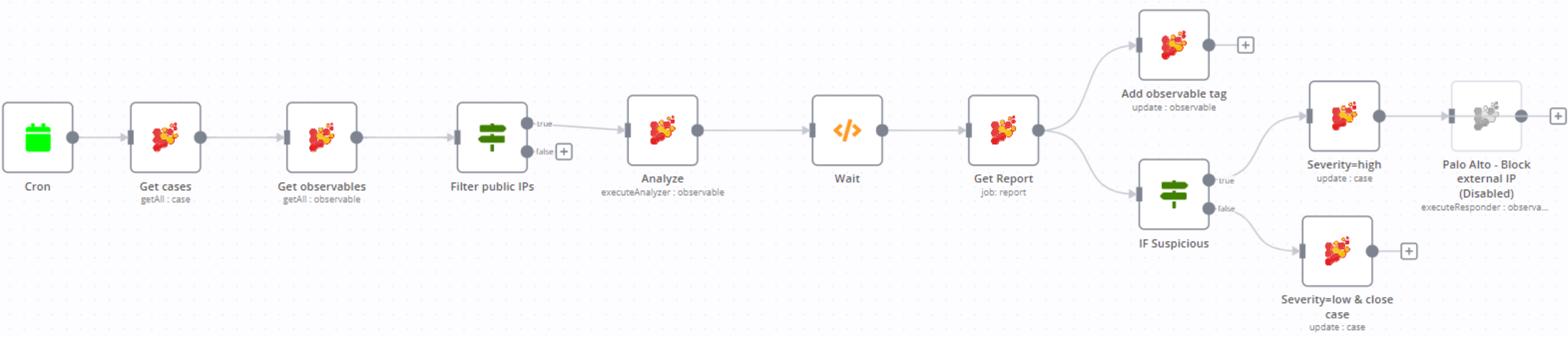


AI Netflow Anomaly

Energy SOAR: Analyze Netflow Anomaly country

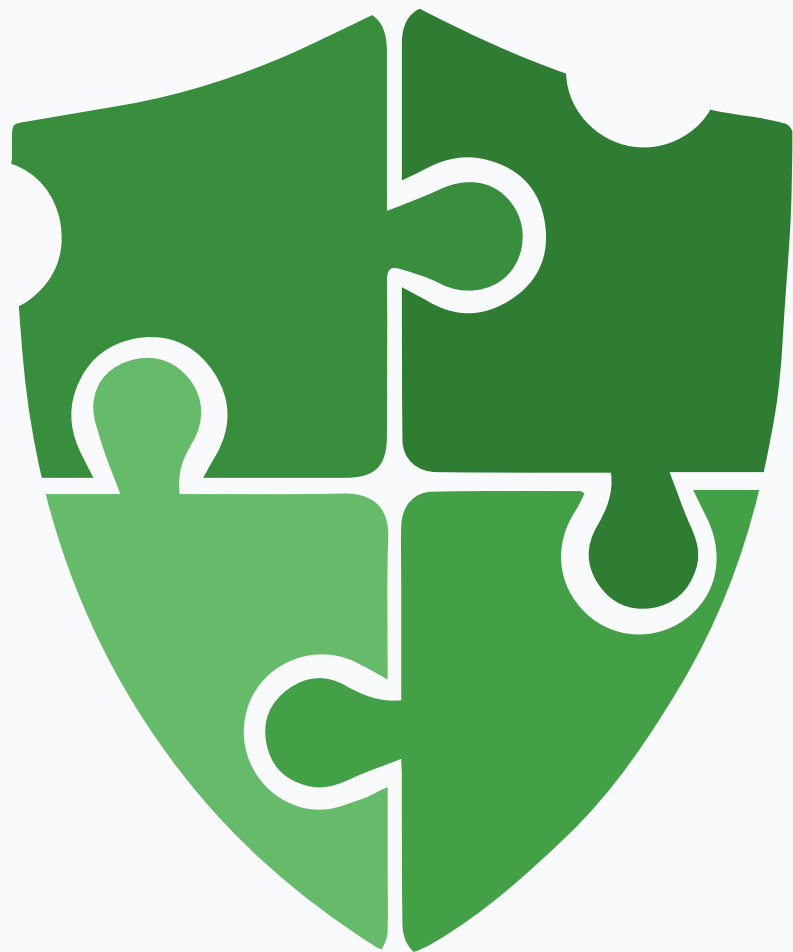
product

Share





Jak SIEM i SOAR zwiększają
zaufanie klientów i partnerów?



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



Licencjonowanie

Wieczyste | Subskrypcja | MSSP

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