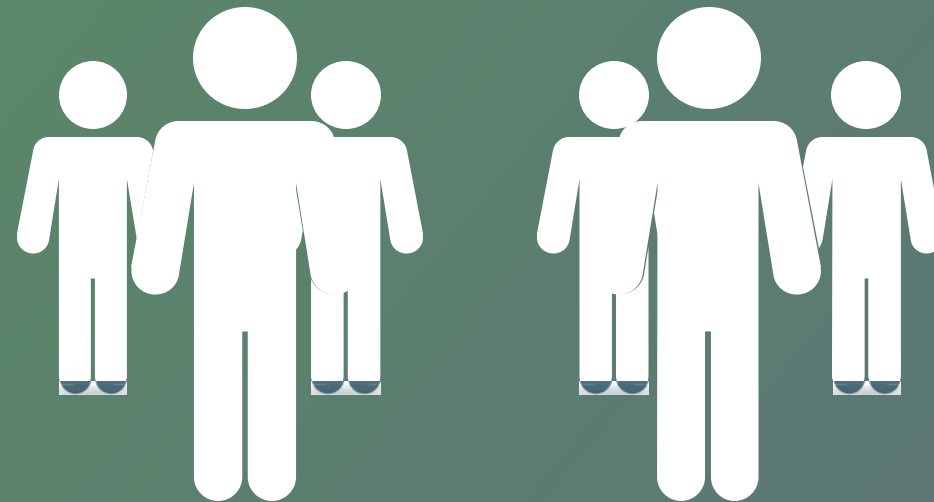




# A day in the life of an “Energized” SOC Team



# How our tools comes together for efficient Cyber Security



# Overall Objectives

Use SIEM and SOAR technologies to maximize efficiency, improve SLAs, reduce manpower and save money

## Proactively hunt for (and mitigate) cyber threats

SOC team members actively identify vulnerabilities and counteract cyber risk.

They help prevent costly security breaches, improve operational efficiency, ensure compliance, and protect the organization's reputation..



## Use Energy SIEM to correlate logs and events

Consolidates data for efficient threat visibility

Provides real-time analysis of security alerts and logs generated by applications and network hardware.



## Automate response with SOAR-defined playbooks

Automation enables rapid and accurate threat response.

SOAR automates and orchestrating responses to security events, making it easier to manage and remediate threats..



## Ensure compliance with regulatory frameworks

Improving operational efficiency and ensuring compliance to protect the organization's reputation, is a core responsibility

While the initial investment may be substantial, the long-term savings and benefits typically justify the expenditure.



# Starting the day

Morning Routine

START

Understand the threats identified during non-business hours  
Focus on High-risk alerts first to ensure efficient resource allocation



8:00 AM  
**NEW ALERTS**  
Review overnight alerts and incidents



Using Energy Empowered AI to identify anomalies  
Visualize and prioritize evolving risks

Analyze feeds for emerging risks and incorporate intelligence to preempt potential threats. Query MISP and bring events into Energy SOAR:  
<https://energysoar.com/many-faces-of-energy-soar-and-misp-integration/>

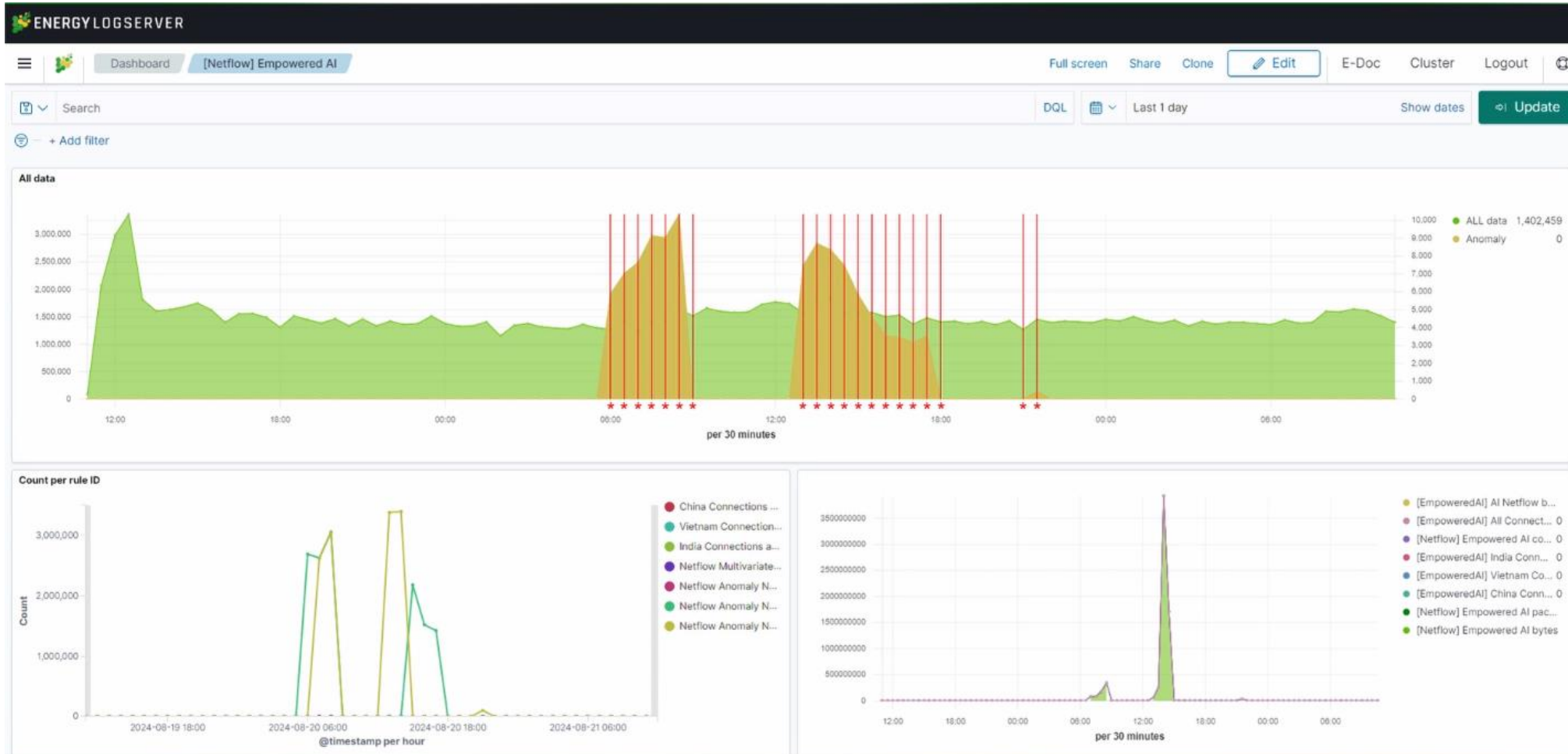


9:00 AM  
**MISP Events**  
Analyze threat intelligence feeds

# Energy Empowered AI detects rare words, numbers and vectors

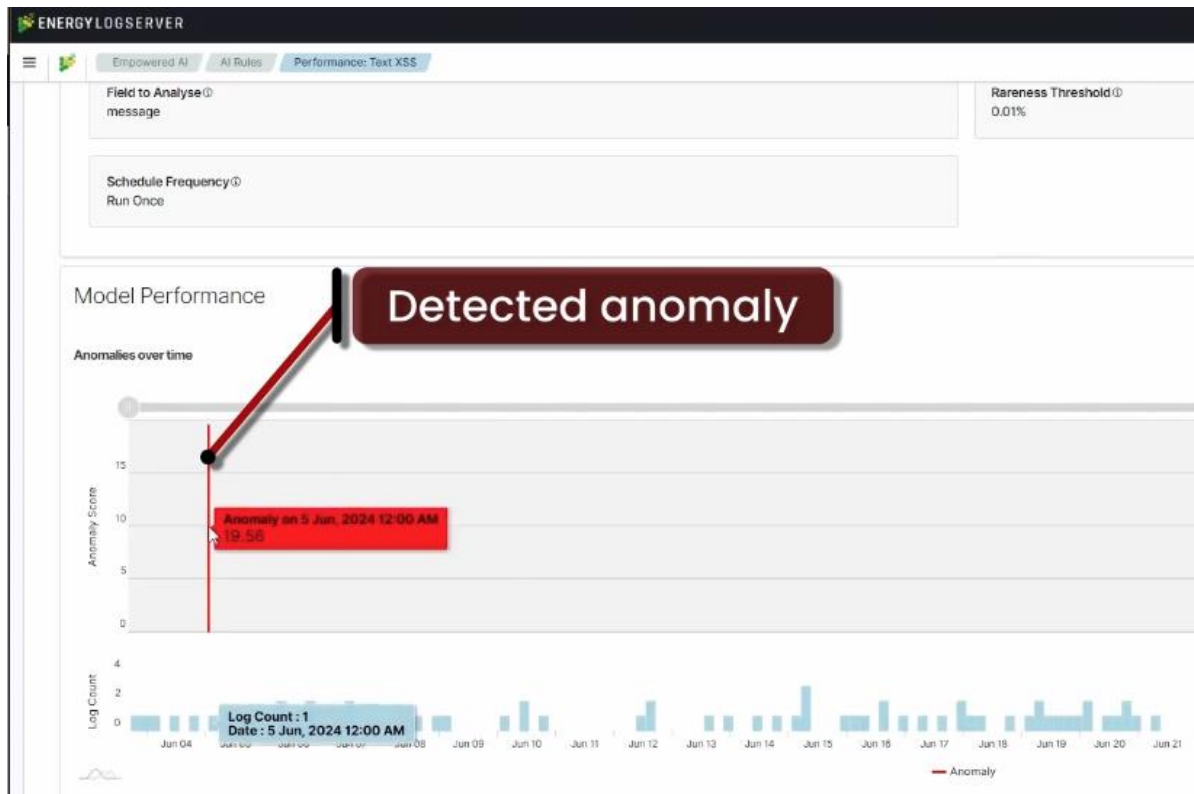


Using Energy Empowered AI to catch anomalies in the network



# Energy Empowered AI detects rare words, numbers and vectors

A rare word occurs in the logs



Example steps:

- SQL/XSS Injection detected by AI
- Attack fingerprint created by SOC team
- Playbook in SOAR created/updated for that attack
- Evaluate the scope of attack

# Reviewing Incidents and Threats



## SOAR and MISP Integration

ENERGY SOAR + New Case My tasks 0 Waiting tasks 711 Alerts 2934 Dashboards Reports Workflows

Alert Preview New

List of alerts (1000+ of 2990)

No event selected Quick Filters Sort by

1 filter(s) applied: type: misp Clear filters

First Previous 1 2

Severity	Read	Title
<input type="checkbox"/>	<span>L</span> Unread	#206189 Daily Incremental ThreatFox Import - 2024-01-16
<code>osint:source-type="block-or-filter-list"</code>		
</> None		
<input type="checkbox"/>	<span>M</span> Unread	#206190 Phishing URL findings
<code>misp-galaxy:mitre-attack-pattern="Input Capture - T1056"</code> <code>src:CERT-EE</code> <code>Phishing</code> <code>misp-galaxy:mitre-attack-pattern="Phishing - T1566"</code> <code>tlp:green</code>		
</> None		

Group	Task
<input type="checkbox"/> Identification	Search DNS logs
<input type="checkbox"/> Identification	Search Mail Server logs

#206165 Phishing email

ID: ~223273176 Date: 01/15/24 00:00 Type: misp Reference: 206165 Source: it.emca.pl

Basic Information

Tags `CSIRT_Social_Engineering` `veris:action:social:variety="Phishing"` `src:Proximus CSIRT` `Phishing Site` `Phishing`

Description

Imported from MISP Event #206165, created at Mon Jan 15 00:00:00 CET 2024

Additional fields Layout

No additional information has been specified

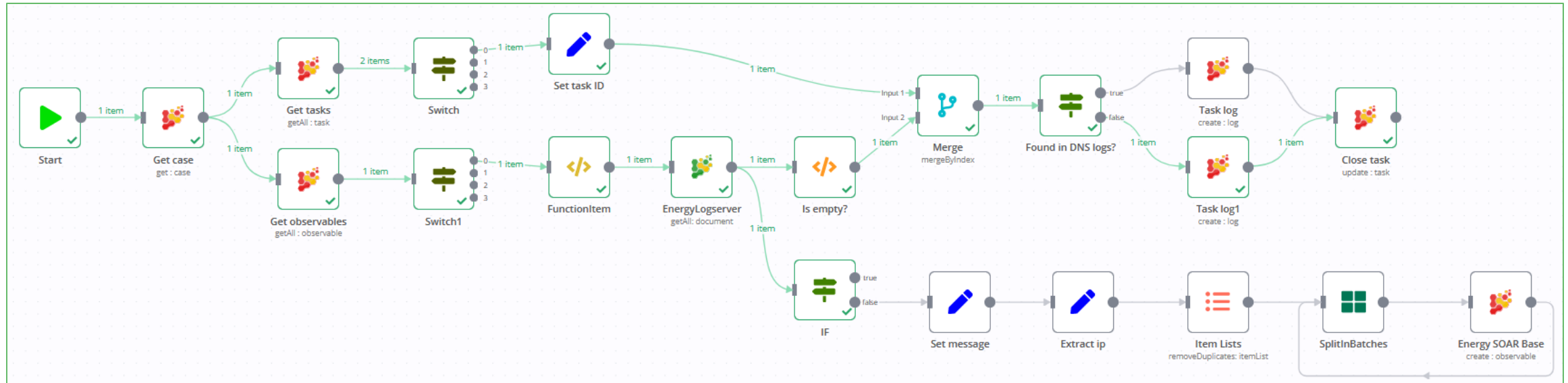
Observables 3 Similar cases 2

List of observables (3 of 3)

Flags	Type	Data
<input type="radio"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	url	<code>https://jardonabogadosnavia[.]com/argenta</code> <code>misp.category="Payload delivery"</code> <code>misp.type="url"</code>
<input type="radio"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	mail	<code>manager@controlbuild[.]mx</code> <code>misp.category="Payload delivery"</code> <code>misp.type="email-src"</code>

# Reviewing Incidents and Threats

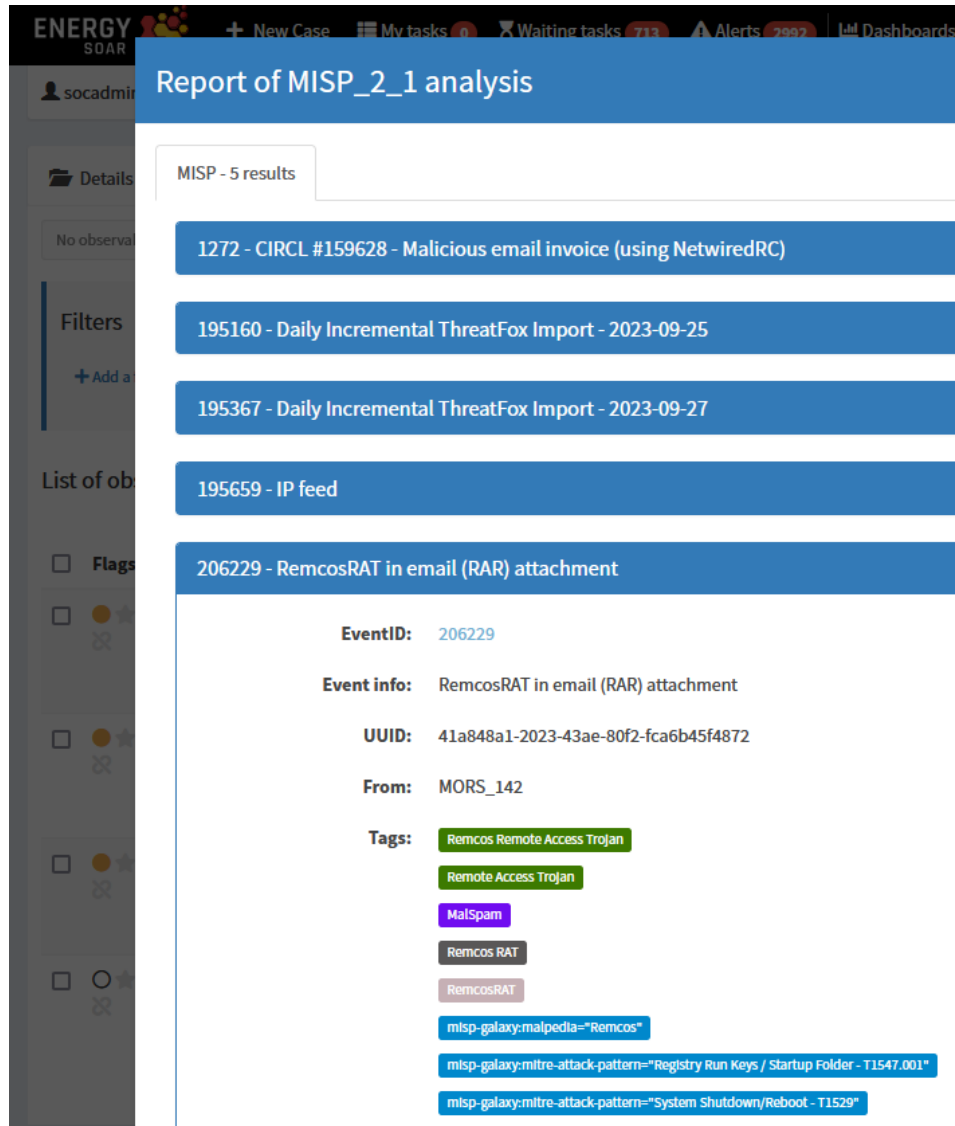
SOAR Workflow to Search DNS and Mail Server Logs





# Reviewing Incidents and Threats

Run MISP Analyzer from within SOAR



ENERGY SOAR + New Case My tasks 0 Waiting tasks 713 Alerts 2992 Dashboards

## Report of MISP\_2\_1 analysis

MISP - 5 results

- 1272 - CIRCL #159628 - Malicious email invoice (using NetwiredRC)
- 195160 - Daily Incremental ThreatFox Import - 2023-09-25
- 195367 - Daily Incremental ThreatFox Import - 2023-09-27
- 195659 - IP feed
- 206229 - RemcosRAT in email (RAR) attachment

**EventID:** 206229

**Event info:** RemcosRAT in email (RAR) attachment

**UUID:** 41a848a1-2023-43ae-80f2-fca6b45f4872

**From:** MORS\_142

**Tags:**

- Remcos Remote Access Trojan
- Remote Access Trojan
- MalSpam
- Remcos RAT
- RemcosRAT
- misp-galaxy:malpedia="Remcos"
- misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001"
- misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529"



ENERGY SOAR + New Case My tasks 0 Waiting tasks 713 Alerts 3008 Dashboards

## Report of MISPWarningLists\_2\_0 analysis

MISP warning lists information for **13.107.128.10**

**Results:** Observable was found in following MISP warning lists:

- 13.107.128.0/19 - microsoft-azure - ver. 20240104
- 13.107.128.0/22 - microsoft-office365-ip - ver. 20240104

# Reviewing Incidents and Threats



Energy SOAR displays the highest priority cases overnight

ENERGY SOAR + New Case My tasks 4 Waiting tasks 111 Alerts 36748 Dashboards Reports Workflows Configure Plugins Search Caseld Organisation SOC/SOC

### Case by Status

Status	Count
Open	~60
Resolved	~40

### Case by Resolution

Resolution	Count
TruePositive	~50
FalsePositive	~30
Indeterminate	~20

### Top 5 tags

Tag	Count
WAZUH	~30
ALERT_HIGH	~25
common-taxonomy:information-gathering='scanning'	~15
scan	~10
Auto created general case	~10

### Filters

status Any Of Open Enter a status

+ Add a filter X Clear Search

1 filter(s) applied: status Open X Clear filters

First Previous 1 2 3 4 5 ... Next Last

Status	# Number	Title	Severity	Details	Assignee	Dates	S.	C.	U.
Open	15 minutes	#88 - AUTOAUTOID [mail] BL LADING 3678920	H	Tasks: 0, Observables: 3, TTPs: 0	A	S. 10/21/21 11:18, C. 10/21/21 11:18, U. 07/27/22 09:20			
Open	15 minutes	#86 - Wazuh alert [HIGH] - rule group: web_scan	H	Tasks: 0, Observables: 2, TTPs: 5	JG	S. 10/19/21 15:45, C. 10/19/21 15:45, U. 07/27/22 09:18			



# Pro-active Threat Hunting

Use Energy SIEM's User Entity Behavior Analysis (UEBA) to uncover irregular user and entity activities – Utilizing AI built user and entity profiles



10:00 AM  
UEBA

## User Entity Behavior Analysis



Investigate advanced and chained alerts. Correlate data across endpoints, network, vulnerability databases, and Cloud to identify complex threat indicators and gain actionable insights. <https://energysoar.com/energy-soar-for-vulnerability-management/>

Identify patterns of lateral movement, data exfiltration, privilege escalation and other strategies used by attackers to deepen access.



11:00 AM  
IDENTIFY PATTERNS

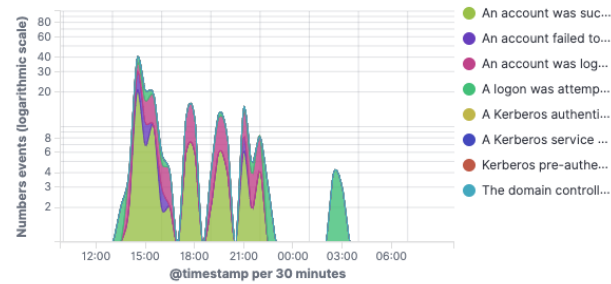
## Privilege Escalation

# Pro-active Threat Hunting

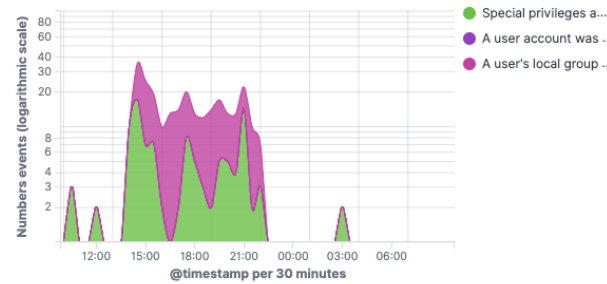


Energy SIEM UEBA Dashboard showing internal behaviour analysis

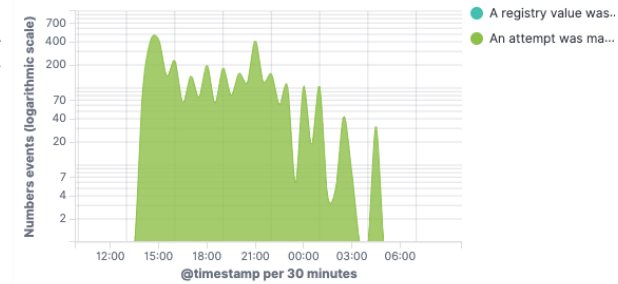
### Login and authentication actions



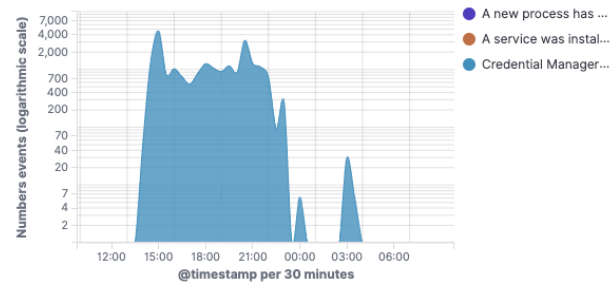
### Access and privilege management



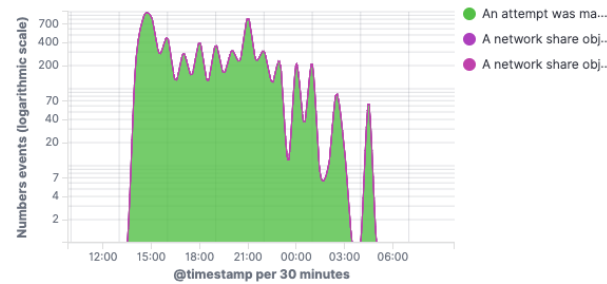
### Configuration and system registry management



### Service and process management



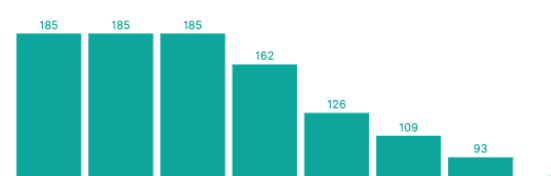
### Management of facilities and access to resources



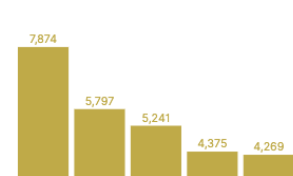
### Account and group management



### Top 10 reported events



### Top users by docs count graph



### Top 5 users by docs count

User	Sum of doc_count	Sum of doc_count...
rkakol	7,874	28.575%
mdrab	5,797	21.037%
dniewadzisz	5,241	19.019%

# Pro-active Threat hunting

Hover over Actions to inspect



Users

Events



Docs count timeseries with users



# Pro-active Threat Hunting



Data Exfiltration example: <https://energysoar.com/netflow-alert-enrichment/>

**ENERGY SOAR** + New Case My tasks 0 Waiting tasks 704 Alerts 2884 Dashboards Reports Workflows Configure Plugins Search

---

Case # 113 - Netflow - Data Exfiltration

socadmin 01/12/24 10:51 3 days 1 alert Sharing (0) Close Flag Merge Remove Export (0) Responders

Details Tasks 7 Observables 1 TTPs Chat Related Graph

### Basic Information

**Title** Netflow - Data Exfiltration

**Severity** H

**TLP** TLP:AMBER

**PAP** PAP:AMBER

**Assignee** socadmin

**Date** 01/12/24 10:51

**Tags** workflow\_started EMCA-81jz netflow network

**Additional information** + Add Layout

*No additional information have been specified*

### Description

Our network monitoring systems have detected unusual data transfer activity that exceeds our established threshold. An instance of large-scale data exfiltration involving a transfer of over 2GB of data within a 1-hour period has been identified. Immediate attention and investigation are required.

IP	81.200.197.163
Sum bytes	3076397686.0

Threshold violation, sum:netflow.bytes 3076397686.0 (min: None max : 2000000000)

# Pro-active Threat Hunting

Energy SOAR contains task lists

List of tasks (7 of 7)

<input type="checkbox"/>	Group	Task
<input type="checkbox"/>	default	Check if the file was downloaded from a public repository.
<input type="checkbox"/>	default	Investigate the logs to find out who was authorized using the given IP address.
<input type="checkbox"/>	default	Is there any public service available at the IP address?
<input type="checkbox"/>	default	Determine the quantity of data downloaded from the particular address within 1 and 7 day periods.
<input type="checkbox"/>	default	Examine the first connection recorded on the firewall from the specified IP address.
<input type="checkbox"/>	default	Verify the information concerning the IP address and check its presence on blacklists.
<input type="checkbox"/>	Action	Take action depending on the risk

## Task logs

[+ Add new task log](#) [Sort by: Newest first](#)

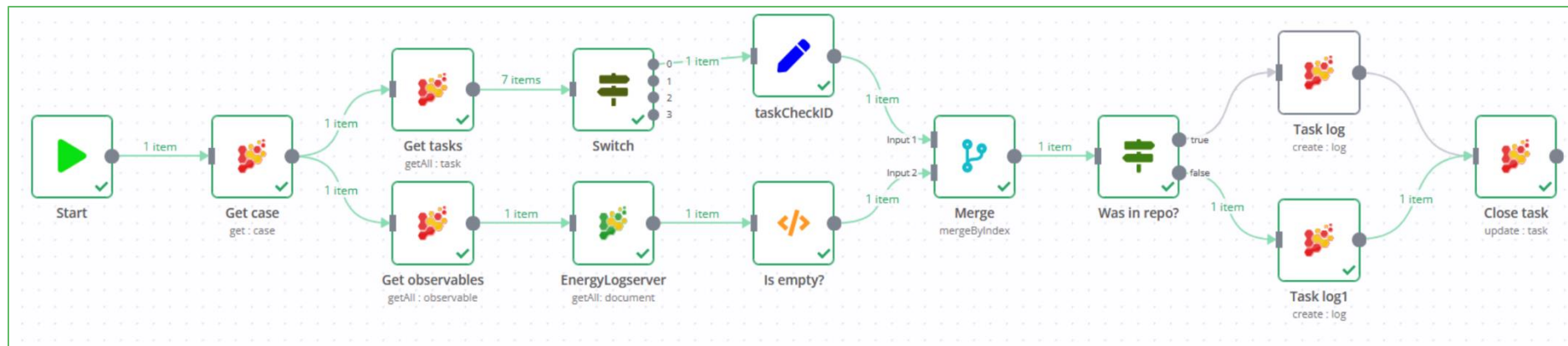


soc/socuser

Data downloaded within last 1 day: **3.44 GB**

Data downloaded within last 7 days: **12.25 GB**

Use SOAR workflows to build automation





# Pro-active Threat Hunting



Vulnerability Checking <https://energysoar.com/energy-soar-for-vulnerability-management/>

**ENERGY SOAR** + New Case My tasks 3 Waiting tasks 642 Alerts 3114 Dashboards Reports

Case # 91 - Oracle Linux 8 : ncurses (ELSA-2023-5249)

Energy Logserver 11/27/23 9:10 2 months 21 cases 1 alert

Details Tasks 4 Observables 1 TTPs Chat Related Graph

**Basic Information**

Title	Oracle Linux 8 : ncurses (ELSA-2023-5249)
Severity	H
TLP	TLP:AMBER
PAP	PAP:AMBER
Assignee	socadmin
Date	11/27/23 9:10
Tags	Tenable Security Center

**Additional information** + Add Layout

pluginFamily	53
--------------	----

## Description

### Synopsis

The remote Oracle Linux host is missing a security update.

### Description

The remote Oracle Linux 8 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2023-5249 advisory.

- ncurses before 6.4 20230408, when used by a setuid application, allows local users to trigger security- relevant memory corruption via malformed data in the TERMINFO or TERM environment variable. (CVE-2023-29491)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### Solution

Update the affected packages.

### Plugin Output

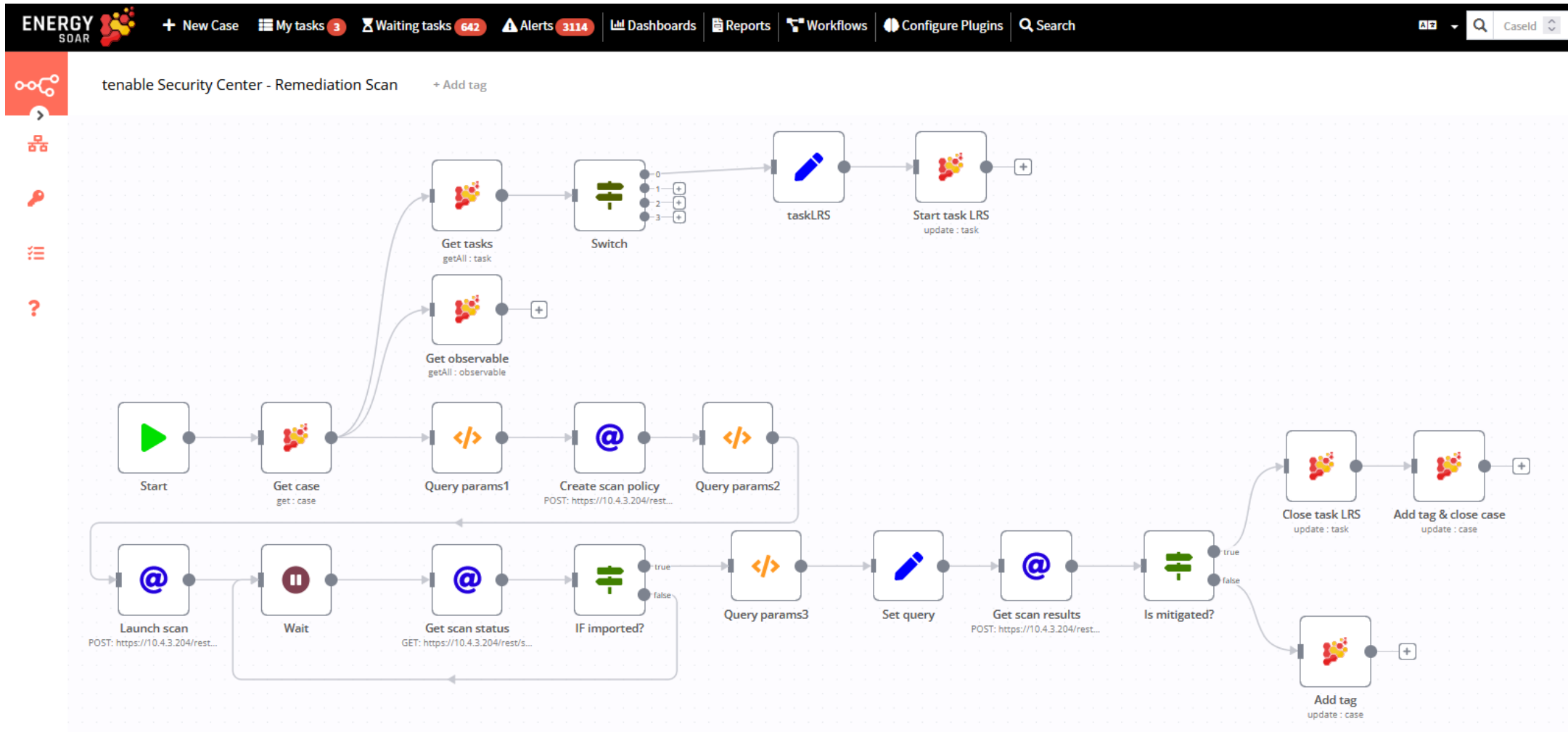
Remote package installed : ncurses-6.1-9.20180224.el8 Should be : ncurses-6.1-9.20180224.el8\_8.1

Remote package installed : ncurses-base-6.1-9.20180224.el8 Should be : ncurses-base-6.1-9.20180224.el8\_8.1

Remote package installed : ncurses-libs-6.1-9.20180224.el8 Should be : ncurses-libs-6.1-9.20180224.el8\_8.1

# Pro-active Threat Hunting

Instigate Patching, Run Remediation Scan, then Update External Helpdesk Ticket



# Leverage Automation

Monitor SOAR-triggered actions (e.g. quarantine, block) to ensure they are effective and accurate.

Analyze suspicious network traffic and email attachments for security evaluations.

<https://energysoar.com/observables/>



12:00 PM  
SOAR

Monitor SOAR Triggers

Refine SOAR playbooks to improve accuracy and optimize workflows for handling new threats

## LUNCH

Add new IOCs and rules for emerging threats. Keep detection parameters up-to-date.



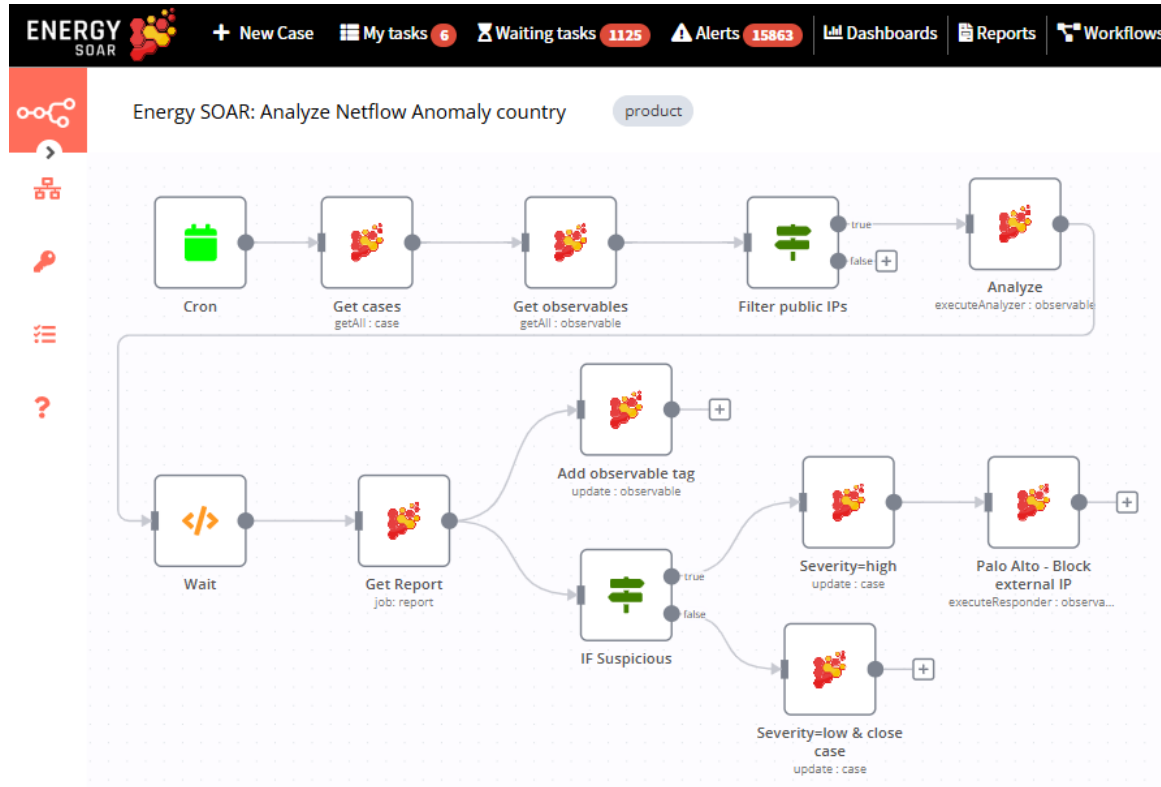
2:00 PM  
NEW IOCs AND RULES

Continuous Improvement

# Leveraging Automation as much as possible



## Energy SOAR workflows and trigger actions



Energy SOAR contains 400+ workflow examples  
SOC team to enable and refine as necessary

## Revise SOAR Playbooks

The screenshot shows the Energy SOAR interface with a list of 15 playbooks. The table below represents the data shown in the screenshot:

Display Name	Name	Severity	Tasks	Custom Fields	By	Dates	C	U	Actions
Data Theft	Data Theft	M	5	0	S	C. 02/04/22 15:50			
Short-lived account	Short-lived account	M	4	0	S	C. 02/04/22 15:50			
Unauthorized Access	Unauthorized Access	M	3	0	S	C. 02/04/22 15:50			
Denial of Service (DoS)	Denial of Service (DoS)	M	7	0	S	C. 02/04/22 15:50			
User authentication from multiple devices	User authentication from multiple devices	M	4	0	S	C. 02/04/22 15:50			
Malware	Malware	M	5	0	S	C. 02/04/22 15:50			
Suspicious User Activity	Suspicious User Activity	M	4	0	S	C. 02/04/22 15:50			
Mass deleting files or folders	Mass deleting files or folders	M	4	0	S	C. 02/04/22 15:50			
Suspicious e-mail	Suspicious e-mail	M	6	0	S	C. 02/04/22 15:50 U. 08/10/22 10:51			
Suspicious VPN connection	Suspicious VPN connection	M	4	0	S	C. 02/04/22 15:50			
Admin creation	Admin creation	M	1	0	S	C. 06/20/22 11:58			
Suspicious Network Activity	Suspicious Network Activity	M	5	0	JG	C. 07/19/22 11:39			

# All Day Incident Response

Take immediate action on critical incidents. Perform root cause analysis and forensics to investigate the origins and details of attacks



3:00 PM (and all day)  
**INCIDENT RESPONSE**

Do this all day !



Collaborate with IT teams for remediation – work together to fix vulnerabilities and restore systems

Keep all relevant parties informed of the situation. Using Energy SIEM and SOAR effectively will ensure the 5min SLA of MTTD and MTTR is attained.



4:00 PM  
**NOTIFY STAKEHOLDERS**

Incident Reporting

# Incident Response



Energy SOAR Enriches the Alert

## SOAR automatically enriches the alert with additional data:

- **Historical Log Analysis:** Examining past logs and events associated with the IP address to gain historical context.
- **Reputation Database Checks:** Checking the perpetrator's IP address in public and private IP reputation databases
- **Geolocation Correlation:** Associating the IP address with geolocation of the attack source.

## Threat Classification and Assessment:

- **Connection Attempt Frequency:** How frequently they tried to establish a connection, indicating an automated attack.
- **Targeted Services:** Which services or ports were targeted by the attack, suggesting motives and objectives of the attacker.

# Incident Response



ENERGY SOAR [+ New Case](#) [My tasks 6](#) [Waiting tasks 1131](#) [Alerts 15874](#) [Dashboards](#) [Reports](#) [Workflows](#) [Configure Plugins](#) [Search](#)

## Case # 439 - AI Netflow Anomaly Text country

Jakub G [12/13/24 12:06](#) [4 hours](#) [1 case](#) [1 alert](#)

[Sharing \(0\)](#) | [Close](#) [Flag](#) [Merge](#) [Remove](#) | [Export \(0\)](#) |

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

No observable selected [+ Add observable\(s\)](#) [Export](#) [Stats](#) [Filters](#) 15

### List of observables (2 of 2)

<input type="checkbox"/>	Flags	Type	Value/Filename	Dates	S.	C.	U.
<input type="checkbox"/>		ip	213[.]175[.]186[.]85 None <a href="#">IPVoid:Blacklists="8/78"</a> <a href="#">IPVoid:Location="Zahle/Lebanon"</a> <a href="#">MaxMind:Location="Lebanon/Asia"</a> <a href="#">MISP:Warninglists="No hits"</a> <a href="#">AbuseIPDB:Records="118"</a> <a href="#">VT:GetReport="1 resolution(s)"</a> <a href="#">VT:GetReport="11/94"</a> <a href="#">Maltiverse:Report="malicious"</a> <a href="#">Cyberprotect:ThreatScore="0.6916666666666665"</a> <a href="#">DSshield:Score="17 count(s) / 8 attack(s) / 1 threatfeed(s)"</a> <a href="#">SFS:ip="Not found"</a> <a href="#">EE:security_flagged="0/8"</a> <a href="#">EE:known_provider="0/1"</a>	<a href="#">S. 12/13/24 12:06</a> <a href="#">C. 12/13/24 12:06</a>			

# Incident Response

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)

<b>Classification</b>	malicious
<b>Type</b>	ip
<b>Tag</b>	-
<b>Creation Time</b>	2024-01-03 08:57:43
<b>Modification Time</b>	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

### EsetMachinelsoation\_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

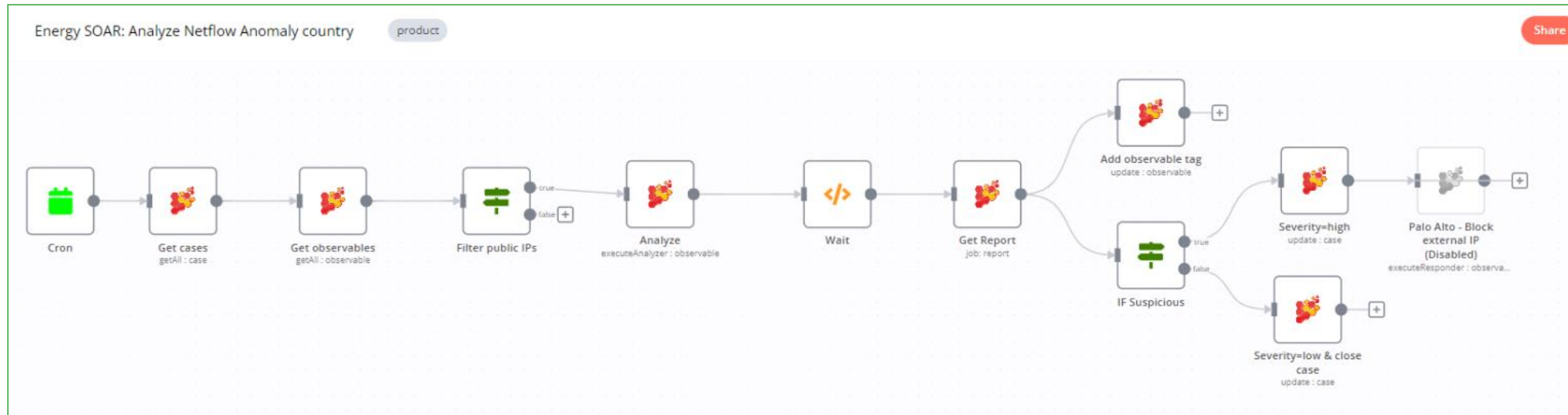
### SentinelOne-Isolate\_1\_0

Isolate a host in SentinelOne



# Incident Response

Energy SOAR analyses alerts objects and if suspicious blocks the IP



## Energy SOAR Automated actions to minimize potential damage:

- **Firewall Rule Application:** Implementing firewall rules that restrict access for the identified IP address.
- **Security Team Notifications:** Informing the security team through automated email or SMS notifications.
- **Ongoing Monitoring:** For lower-level threats, SOAR can continue to monitor the IP activity and collect more data before deciding on an intervention.

# Evening Routine

Share lessons learned with the SOC team, document for the next shift.

Generate incident summary reports and review SOAR playbook performance – update risk matrices and refine detection rules

Generate compliance and incident summary reports for stakeholders and audit purposes



6:00 PM  
REPORTING & OPTIMIZING  
Review Performance

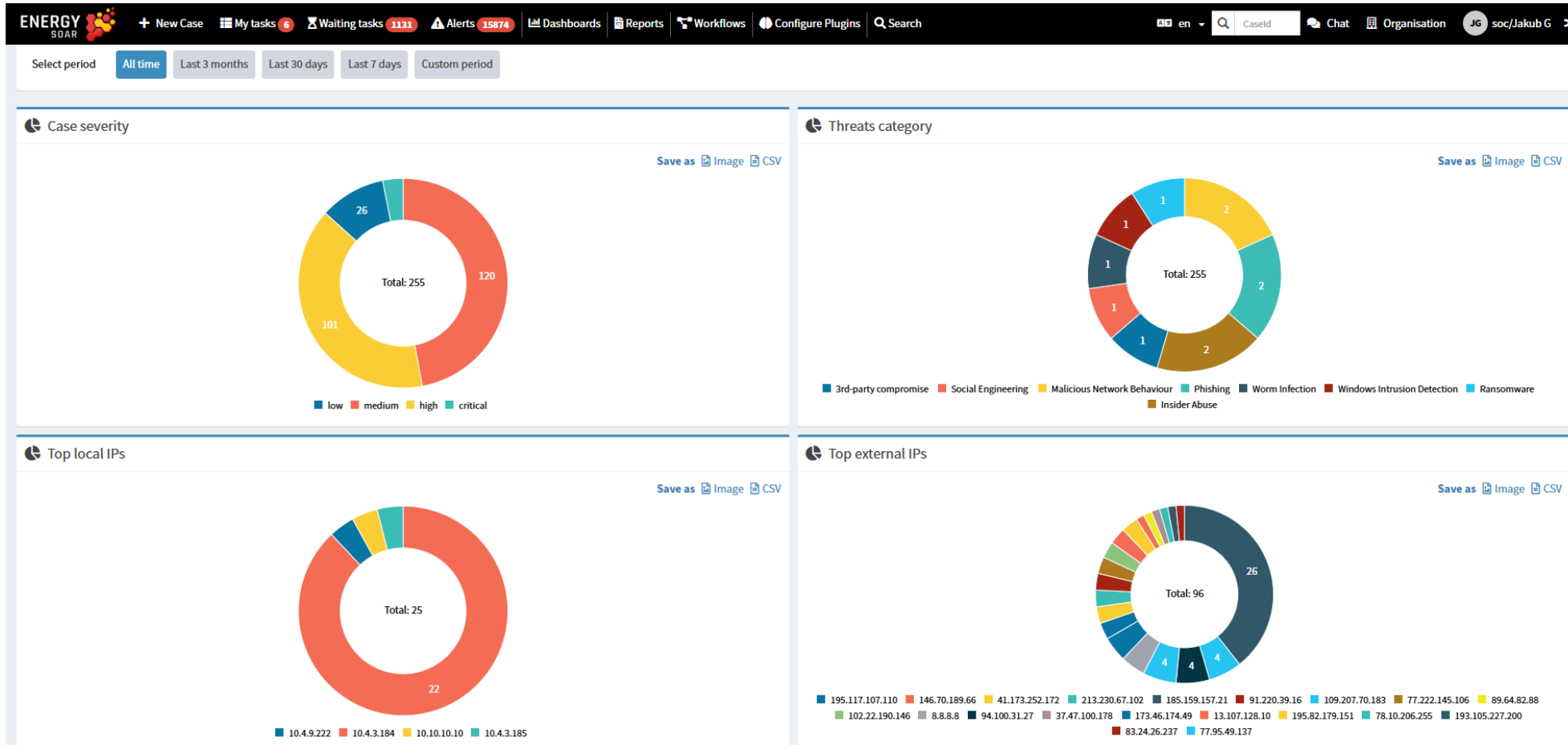


7:00 PM  
COMPLIANCE  
Generate Daily Reports

**END**

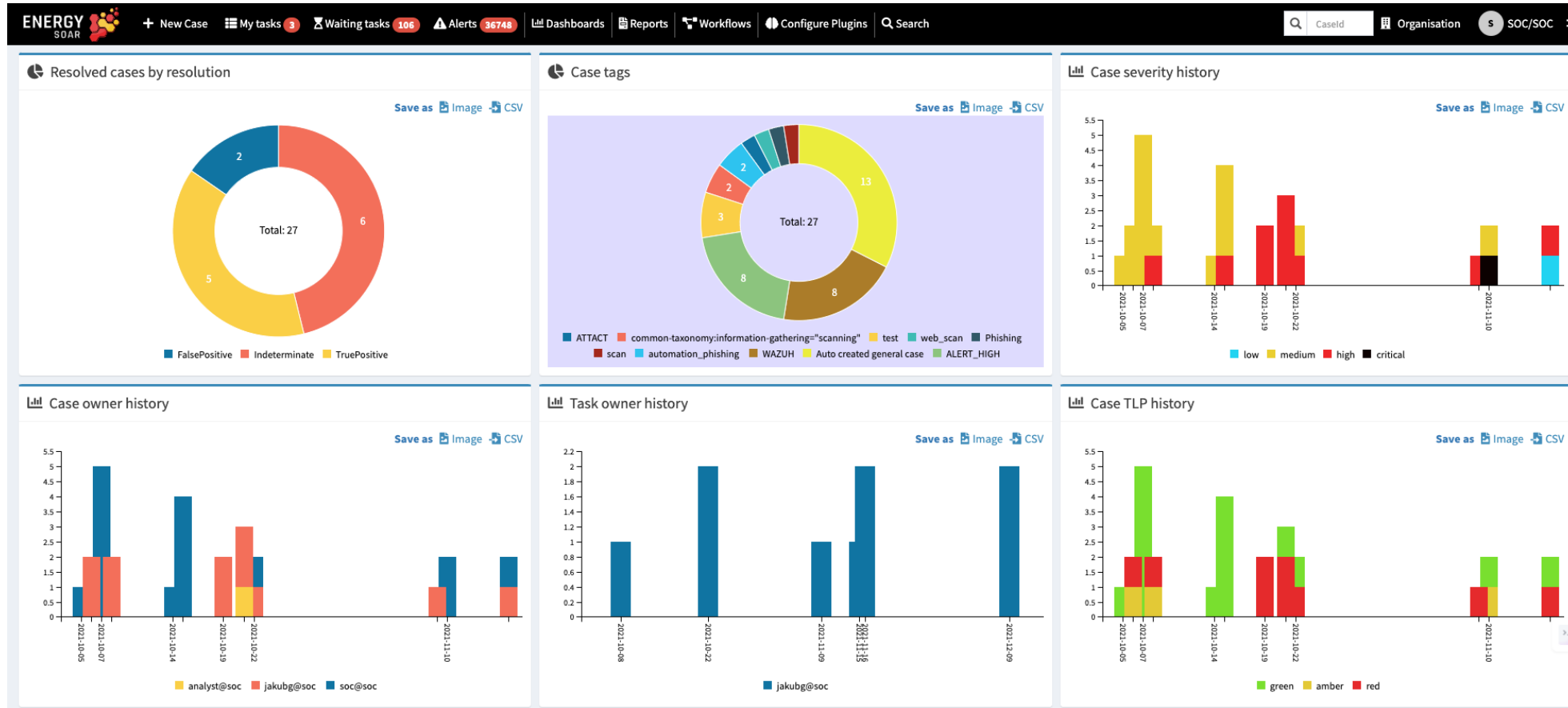
# Incident Reporting

## Energy SOAR Case summaries



# Incident Reporting

## Energy SOAR Case summaries



# Case Summary and ROI


## Energy SOAR SLAs and ROI



# Incident Reporting

Energy SOAR built-in case report card





COMPANY NAME

## Incident report

---

### Incident details

Incident name	Malware
Status	Open
Start time	2023-12-06T11:45:00.000Z
Close time	
Closed after	
Owner	jakubg@energysoar.local
Description	opis

### Tasks completed

#### Isolate host

ID:	~643436720
Title	Isolate host
Group	default
Description	Isolate workstation.
Status	Completed
Start time	2023-12-15T10:28:28.623Z
Close time	2023-12-15T10:28:47.595Z
Closed after	18 s
Owner	jakubg@energysoar.local

### Add tasks

ID:	~633110752
Title	Add tasks
Group	default
Description	workflow.id=80
Status	Completed
Start time	2023-12-15T13:55:16.192Z
Close time	2023-12-15T14:19:01.630Z
Closed after	23 min, 45 s
Owner	workflow@energysoar.local

### Scan host

ID:	~644702312
Title	Scan host
Group	default
Description	
Status	Completed
Start time	2023-12-15T13:57:41.994Z
Close time	2023-12-15T14:20:17.347Z
Closed after	22 min, 35 s
Owner	workflow@energysoar.local

### Blacklist hash

ID:	~685031496
Title	Blacklist hash
Group	default
Description	Add hash to blacklist on EDR.
Status	Completed
Start time	2023-12-15T10:28:14.772Z
Close time	2023-12-15T10:28:22.751Z
Closed after	7 s
Owner	jakubg@energysoar.local

### Summary Tasks table

ID	Title	Open time	Owner
~643436720	Isolate host	18 s	jakubg@energysoar.local
~633110752	Add tasks	23 min, 45 s	workflow@energysoar.local
~644702312	Scan host	22 min, 35 s	workflow@energysoar.local
~685031496	Blacklist hash	7 s	jakubg@energysoar.local
<b>Time spent:</b>			46 min, 45 s

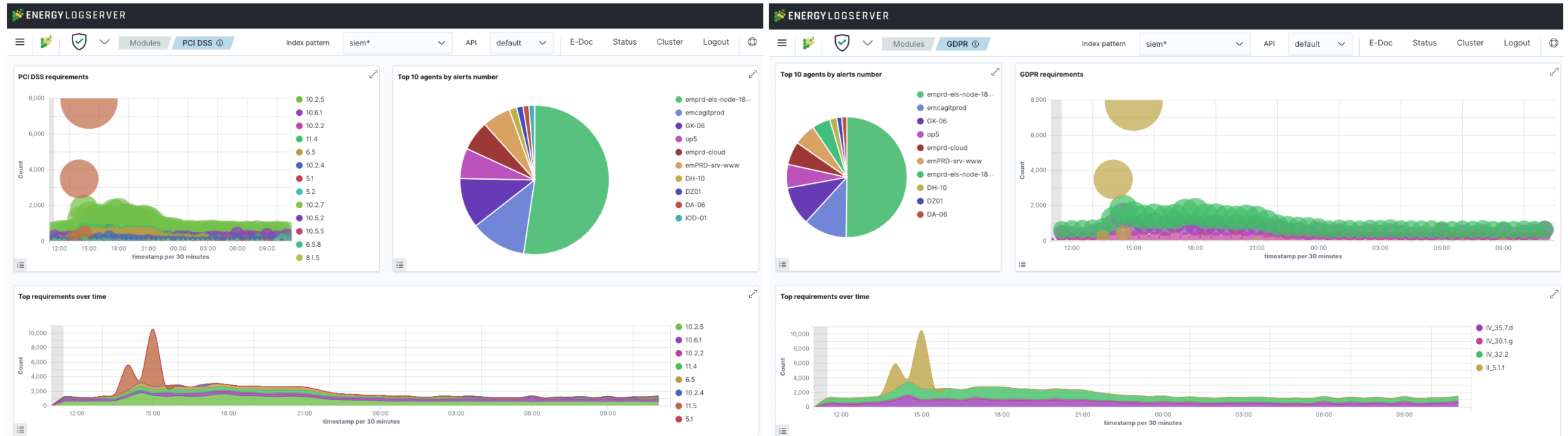
### Waiting tasks

ID	Title	Owner
~521048072	Unisolate host	workflow@energysoar.local
<b>Tasks count:</b>		1

# SIEM Compliance Report examples



Energy SIEM Compliance at a glance



Built-in Reports:

- PCI-DSS, NIST 800-53, ISO27001, GDPR, HIPAA, SOX, CMMC, FISMA, SOC2
- Local/Industry specific customized: Australian Privacy Act, Singapore PDPA etc

# BENEFITS

Key advantages using Energy SIEM and SOAR in your SOC



## *Comprehensive Threat Detection and Response*

**Real-time Monitoring:** identifying suspicious behavior and potential threats instantly.

**Automated Response:** significantly reducing the time between detection and mitigation.



## *Enhanced Security Posture*

**Centralized Management:** Unified view of your security landscape, making it easier to manage and respond to incidents.

**Advanced Analytics:** Analyze large volumes of data, improving threat detection accuracy and reducing false positives.



## *Reduced Complexity*

**Simplified Management:** Consolidate multiple security tools into a single, security platform.

**User-Friendly Interfaces:** Intuitive interfaces and dashboards for your security team to navigate and operate the system effectively.



## *Proactive Threat Hunting*

**Threat Intelligence Integration:** Integrate global threat intelligence feeds to stay ahead of emerging threats.

**Continuous Improvement:** Regular updates and improvements to the service ensure your defenses evolve with the threat landscape.



## *Scalable Solutions:*

**Pay for what you need.** As your business grows, the services can scale accordingly without requiring significant upfront investments.



## *Expertise and Support*

**Access to Experts:** Benefit from the expertise of seasoned cybersecurity professionals who continuously monitor and fine-tune the systems.



# Success

Reduce false positives with Automation – less manpower

Pro-active threat detection to improve service levels

Enhanced collaboration and streamlined workflows to improve MTTR

Cost effective & flezible pricing options

