

ENERGY SOAR

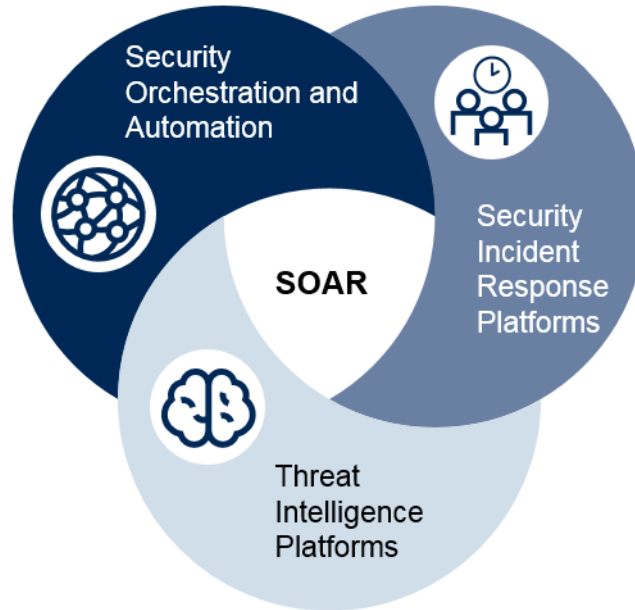


Energize your IT security

Jakub Goral
Security Architect

SOAR components

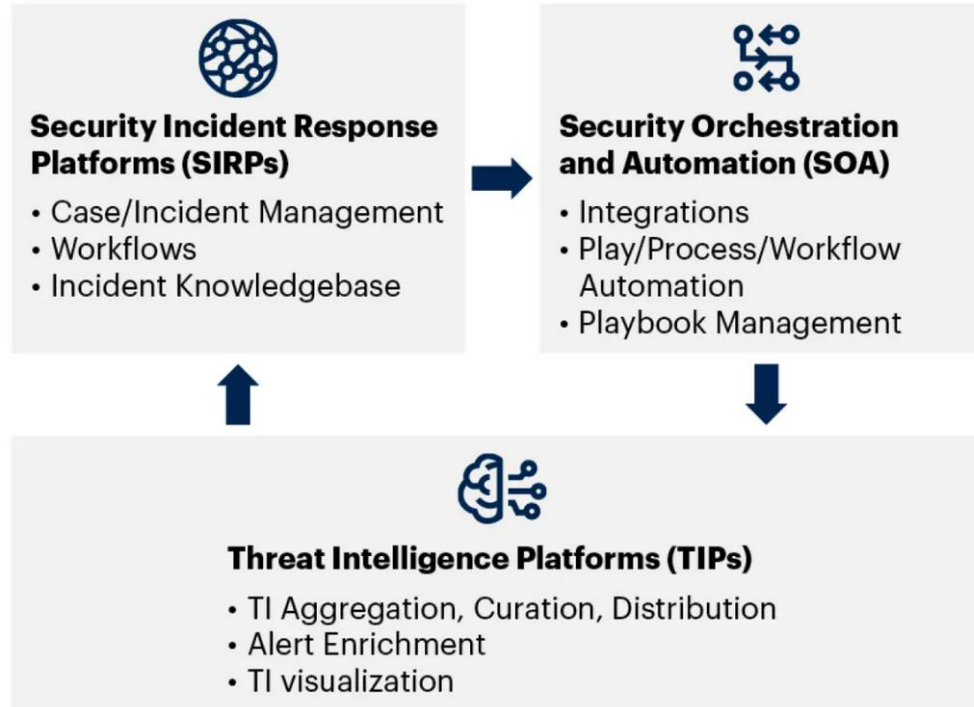
SOAR Types



$$\text{SOAR} = \text{SOA} + \text{SIR} + \text{TIP}$$

SOAR components

SOAR Convergence of Three Technologies (SIRP, SOA and TIP)



Security Operations Problems

Limited resources



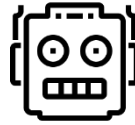
- Shortage of security professionals

Too many products



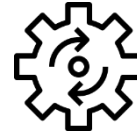
- Different product UIs
- Products without orchestration

Too many alerts



- Security teams struggling to know which alert to analyze
- Many alerts left unread

Lack of processes



- Or many complex manual playbooks

Speed



- MTTD and MTTR must improve

Costs



- Costs continue to increase

How Energy SOAR solves security operations problems

Limited resources



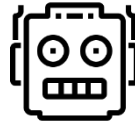
- Automate repetitive tasks
- More time for deeper analysis and threat hunting

Too many products



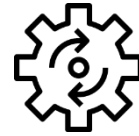
- EnergySOAR orchestrates workflows and response across security products

Too many alerts



- Clear majority of alerts

Lack of processes



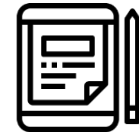
- Case templates
- Tasks
- Automatic workflow

Speed



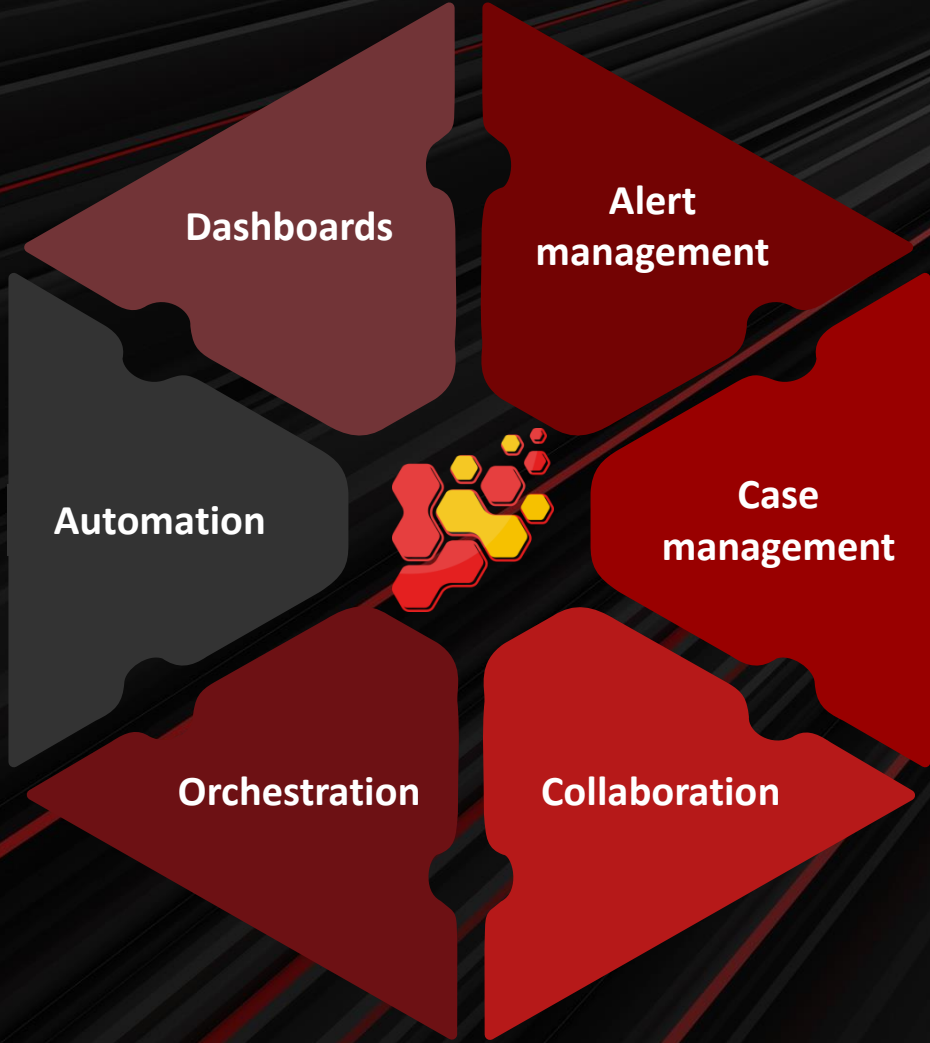
- Orchestration and automation reduce time

Costs



- EnergySOAR saves your team time and costs

ENERGY SOAR



Orchestration - analysis

- VirusTotal: analyze file, URL, hash, domain, IP
- MaxMind: geolocate an IP
- YARA: check file against YARA rules
- Cuckoo: sandbox (file, URL)
- ANY.RUN: sandbox (file, URL)
- Threat Intelligence: e.g. MISP
- GoogleSafebrowsing: check URL



maltiverse



TALOS



IBM X-Force Exchange



OPENCTI

MALWARE bazaar
by ABUSE|CH

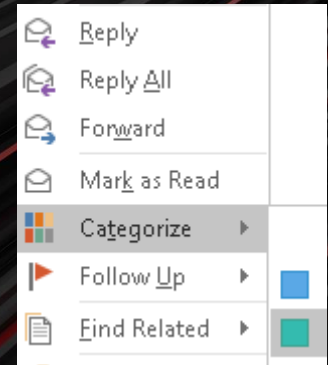
Orchestration - response

- Create ticket in external system
- Quarantine host via EDR
- Block IP using firewall or agent
- Proxy: block domain
- Gateway: add e-mail to blacklist



Microsoft Exchange – create cases automatically

- SOC receives suspicious e-mail from concerned employee as a file attachment (.msg)
- Analyst:
 - Tags the e-mail with his category (username in AD and EnergySOAR)
 - Drags and drops e-mail to the folder SOAR (only e-mail in the folder SOAR will create a case)
- Scheduled task monitors the folder and creates case



List of cases (21 of 37)

No case selected | Quick Filters | Sort by | Custom Fields | Stats | Search

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

First | Previous | 1 | 2 | Next | Last





Status	#	Number	Title	Severity	Details	Assignee
Open	1	#43	Strange email from ACME	M	Tasks: 1 Observables: 2 TTPs: 0	JG

e-mail subject -> case title
category -> case assignee

Microsoft Exchange – attachments handling

- .msg file is converted to do .eml
- Attachment and e-mail details are extracted:
 - attachment.pdf
 - sender
 - receiver
 - subject
 - headers

Observable List (2 of 2)

<input type="checkbox"/>	Type ▲▼	Value/Filename ▲▼
<input type="checkbox"/>	file	order[.]pdf  Synapse  No reports available
<input type="checkbox"/>	file	urgent-payment-order[.]eml  Synapse  No reports available

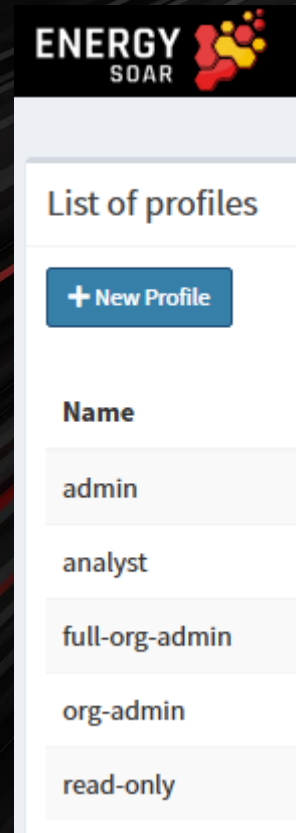
Demo

ENERGY SOAR

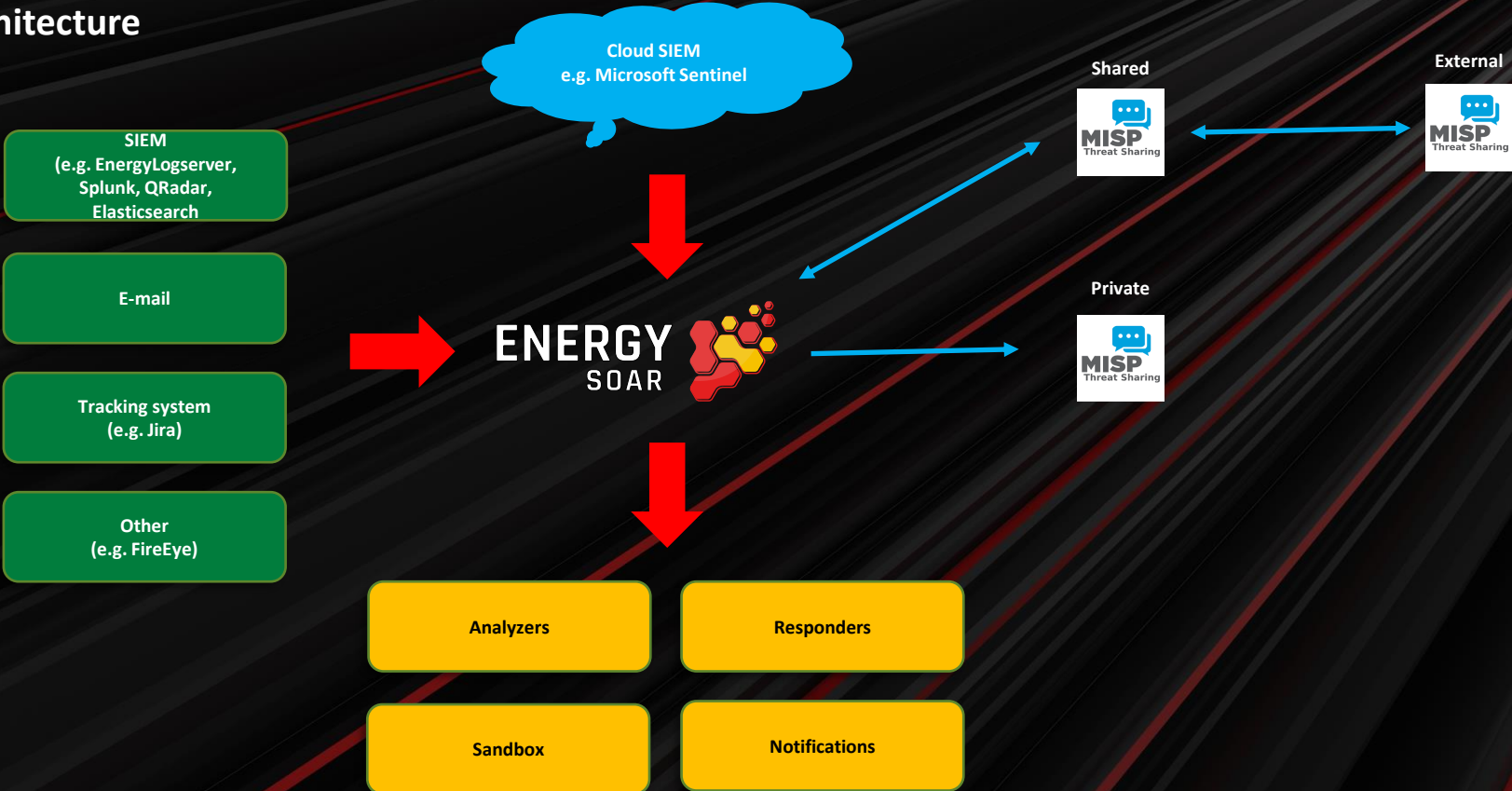


Organisations


- Organisations
 - You can create many organisations
 - You can link organisations to share cases
- Users
- Roles
- Permissions
- AD/LDAP



Architecture



Energy Logserver alert



Alerts Wiki Cluster Logout

Alert Method
Energy SOAR

Alert type: Case **Follow (Active on update)**

Title **Description**

Type **Source** **Status**

Severity **TLP** **Tags**

Observable data mapping

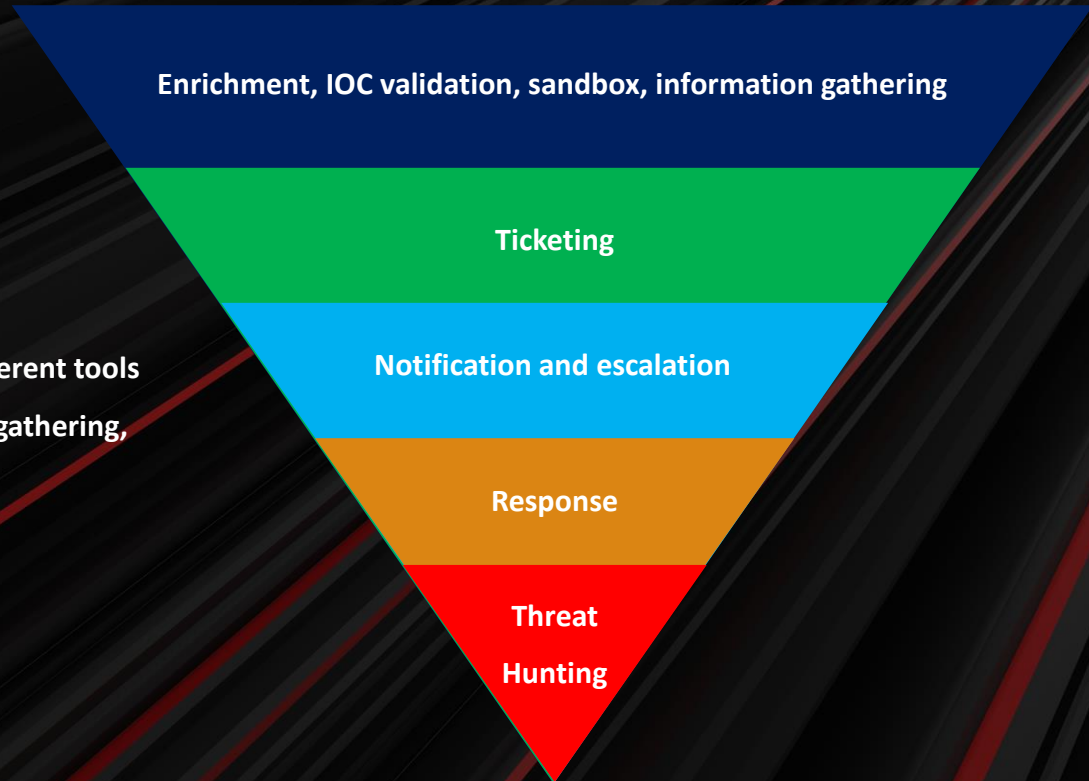
Alert text

H B I S — 66 | ☰ ☷ ☑ ▶ ◀ | 🏠 🖼️ 🔗 | </> CB

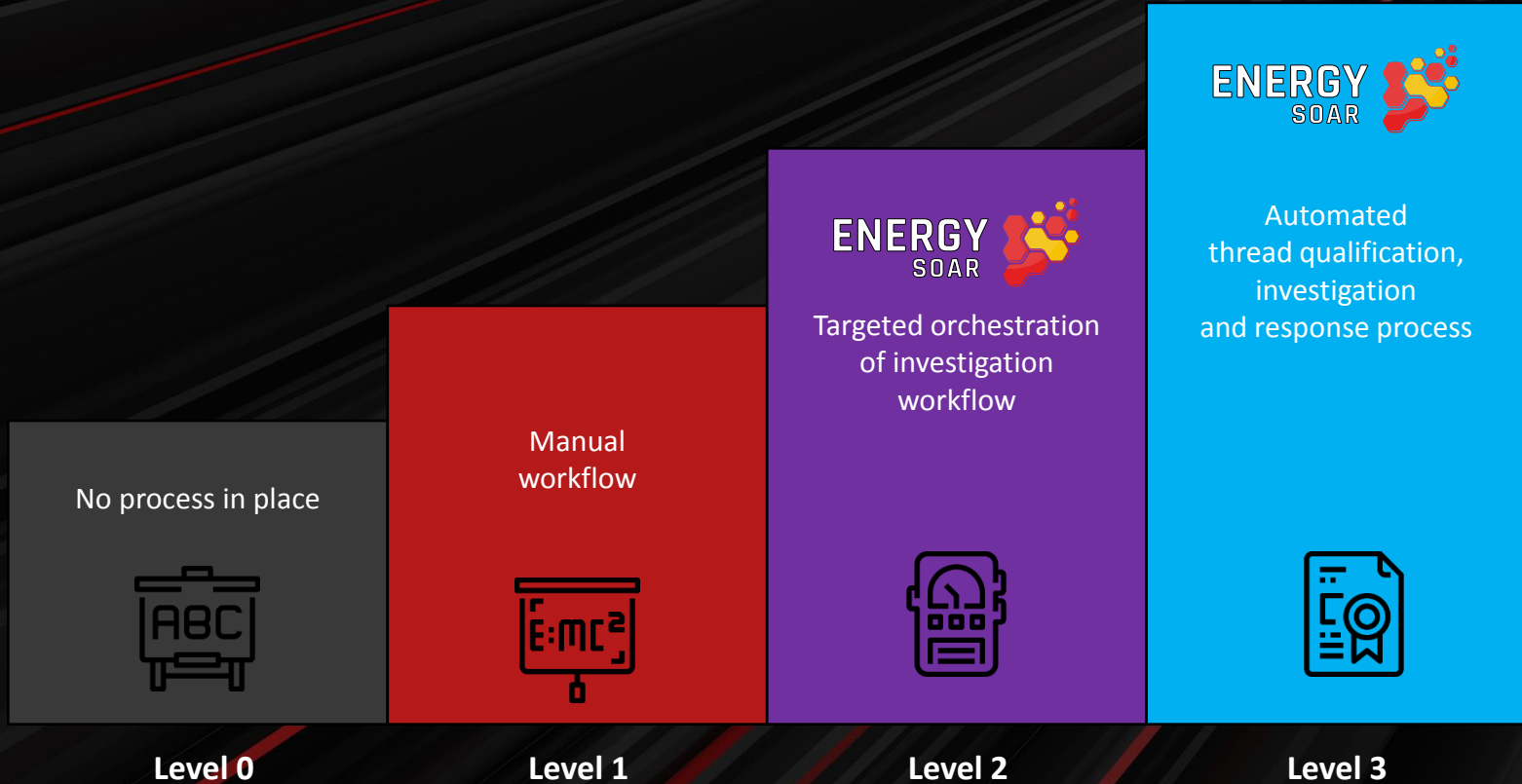


Automation

- What automation tasks should we look at first?
 - Repetitive tasks
 - Events that are happening frequently
 - Incidents that require many actions using different tools
 - Start with contextualization and information gathering, than deeper dive into responses



Security Operations



The benefits



Visibility - single pane of glass



Non-stop operation (7x24)



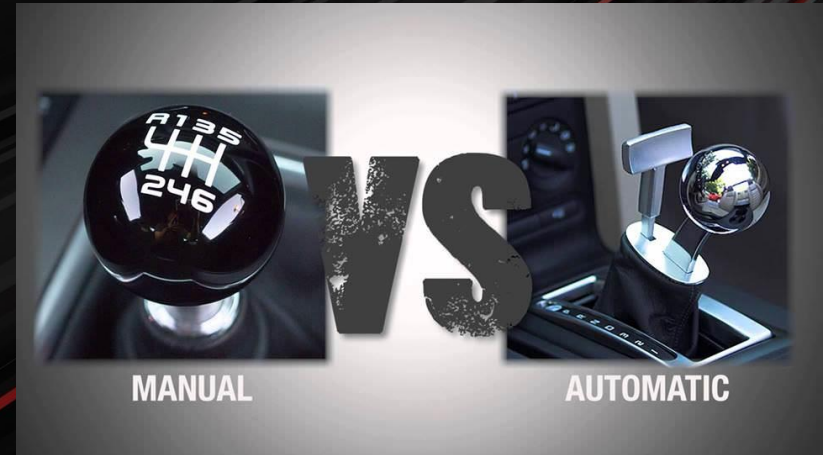
Improved time to respond



Freed up human resources for higher value-added tasks



Eliminating variations in processing



THANK YOU

ENERGY SOAR



sales@energysoar.com

energysoar.com