EE-ISAC

Information sharing in network of trust

Mission Statement

> “The EE-ISAC was launched in December 2015 to improve the **resilience** and **security** of the European energy infrastructure. We do so through trust-based **information sharing** and by enabling a **joint effort** for the analysis of threats, vulnerabilities, incidents, solutions and opportunities. EE-ISAC offers a **community of communities** to facilitate this proactive information sharing and analysis, allowing its members to take their own effective measures”

Technical Task Forces

MISP Threat Sharing

Goals

- identify threats artefacts and malicious activities
- detect analysis and subsequent phases of incident handling
- share information in quasi-real-time

Activities & Updates

- platform connection to Eurocontrol increased +50.000 new entries
- supervision of the system to ensure efficiency and reliability
- update of user access credentials on the system and VPN infrastructure

Coordinator

- Siemens (Marcel)

Participants

- Enel (Massimo)
- Brandenburg University (Dmytro Cherkashyn)

Threat Landscape

Goals

- define and edit annual threat landscape document for the energy sector
- collect feedbacks on threats and emerging scenarios from Members

Activities & Updates

- insights into top cyber tends and attacks against energy sector

Coordinator

- ENISA (Konstantinos Moulinos)

Participants

- Applied Risk (Jalal Bouhdada)

Threat Intelligence & Incident Analysis-Response

Goals

- establish threat modeling standard
- build capabilities and new competences within the EE-ISAC and in partnership with other ISACs/ENISA

Activities & Updates

- edit annual threat intelligence publication
- edit annual incident response publication
- cooperate with other ISACs and expert communities to define common practices

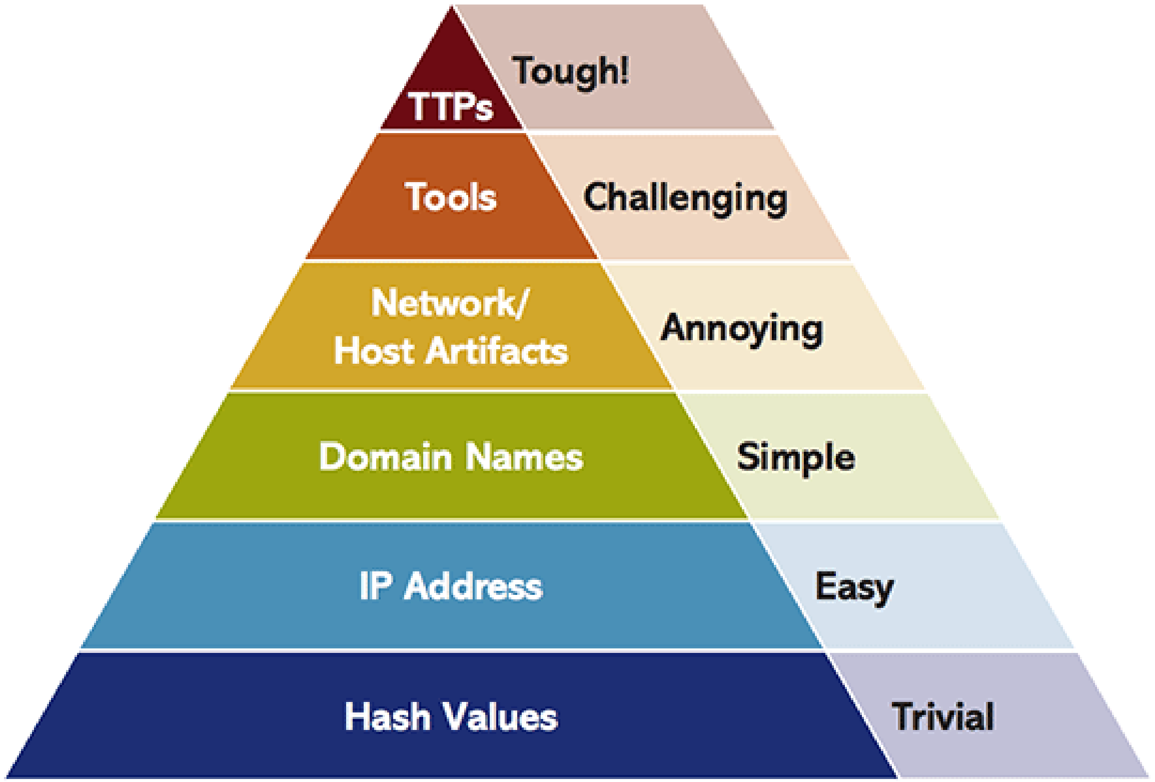
Coordinator

- E.ON (Alexander Harsh)

Participants

- Brandenburg University (Jugersa Smaja)

Digital Information Sharing



Vmoso

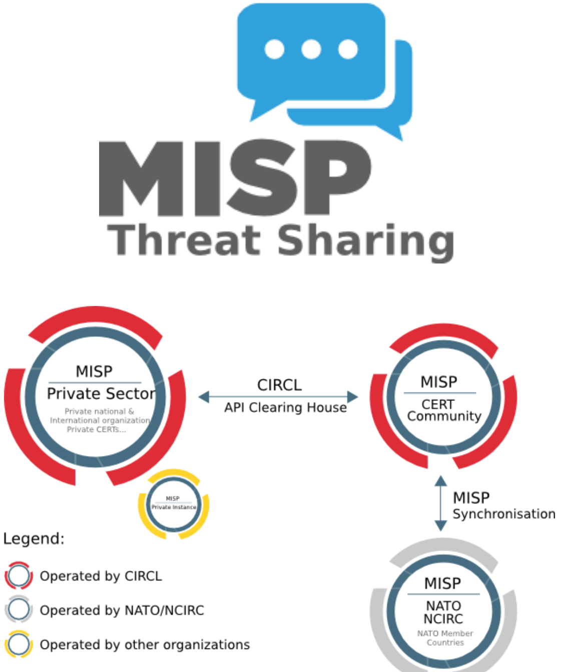
MISP
Threat Sharing

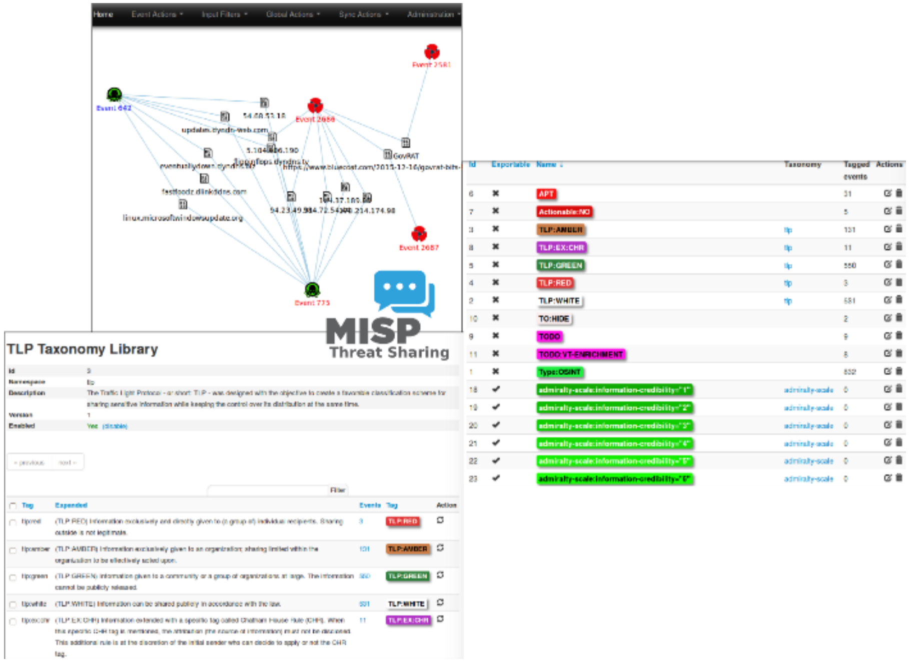
Source: Netsurion, https://www.netsurion.com/articles/the-pyramid-of-pain

MISP

MISP is a de-facto standard:

- An efficient IoC and database about malware samples, incidents & attackers
- Automatic correlation finding relationships between attributes & indicators





Id	Exportable	Name	Taxonomy	Tagged events	Actions
6	✖	APT		31	
7	✖	Actionable:NO		5	
3	✖	TLP:AMBER	tlp	131	
8	✖	TLP:EX:CHR	tlp	11	
5	✖	TLP:GREEN	tlp	550	
4	✖	TLP:RED	tlp	3	
2	✖	TLP:WHITE	tlp	581	
10	✖	TO:HIDE		2	
9	✖	TODO		9	
11	✖	TODO:VT-ENRICHMENT		5	
1	✖	Type:OSINT		632	
18	✓	admiralty-scale:information-credibility="1"	admiralty-scale	0	
19	✓	admiralty-scale:information-credibility="2"	admiralty-scale	0	
20	✓	admiralty-scale:information-credibility="3"	admiralty-scale	0	
21	✓	admiralty-scale:information-credibility="4"	admiralty-scale	0	
22	✓	admiralty-scale:information-credibility="5"	admiralty-scale	0	
23	✓	admiralty-scale:information-credibility="6"	admiralty-scale	0	

TLP Taxonomy Library

Id	3
Namespace	tlp
Description	The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.
Version	1
Enabled	Yes (disable)

« previous next »

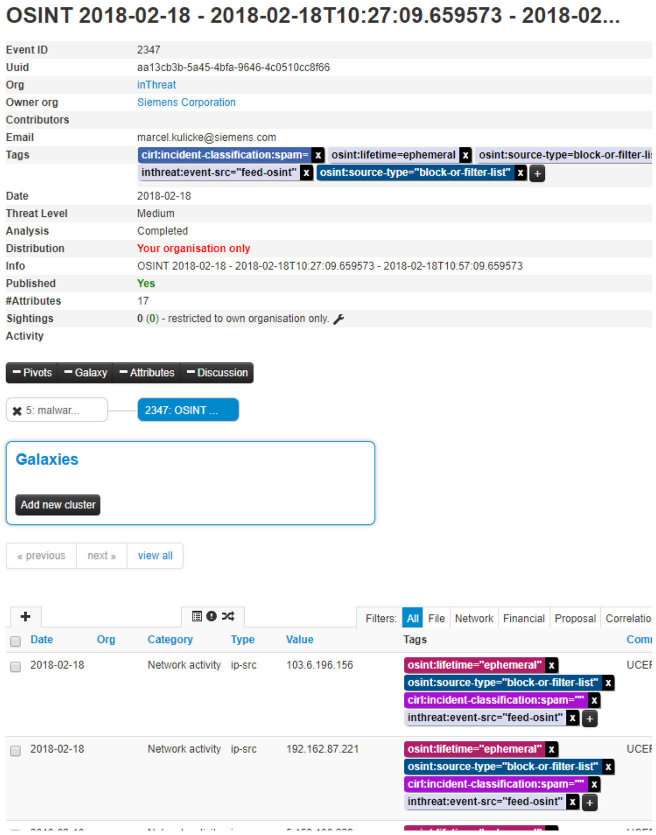
Filter

□	Tag	Expanded	Events	Tag	Action
□	tlp:red	(TLP:RED) Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not legitimate.	3	TLP:RED	
□	tlp:amber	(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.	131	TLP:AMBER	
□	tlp:green	(TLP:GREEN) Information given to a community or a group of organizations at large. The information cannot be publicly released.	550	TLP:GREEN	
□	tlp:white	(TLP:WHITE) Information can be shared publicly in accordance with the law.	581	TLP:WHITE	
□	tlp:ex:chr	(TLP:EX:CHR) Information extended with a specific tag called Chatham House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. This additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag.	11	TLP:EX:CHR	

Co-financed by the European Union
Connecting Europe Facility

MISP - How does the sharing look like?

- MISP **events** are encapsulations for contextually linked information
- MISP **attributes** initially started with a standard set of ”cyber security” indicators.
- MISP **objects** are attribute compositions describing points of data
- MISP **galaxies** granularly contextualize, classify and categorize data based on threat actors, preventive measures or tools used by adversaries.
- MISP **sightings** allow a further classification based on the amount of hits.
- MISP **tags** allow for further sorting and clustering
- MISP **taxonomies** allow for further classification along national or international standards



OSINT 2018-02-18 - 2018-02-18T10:27:09.659573 - 2018-02...

Event ID	2347
Uuid	aa13cb3b-5a45-4bfa-9646-4c0510cc8f66
Org	inThreat
Owner org	Siemens Corporation
Contributors	
Email	marcel.kulicke@siemens.com
Tags	cirl:incident-classification:spam= x osint:lifetime=ephemeral x osint:source-type=block-or-filter-li inthreat:event-src="feed-osint" x osint:source-type="block-or-filter-list" x +
Date	2018-02-18
Threat Level	Medium
Analysis	Completed
Distribution	Your organisation only
Info	OSINT 2018-02-18 - 2018-02-18T10:27:09.659573 - 2018-02-18T10:57:09.659573
Published	Yes
#Attributes	17
Sightings	0 (0) - restricted to own organisation only.
Activity	

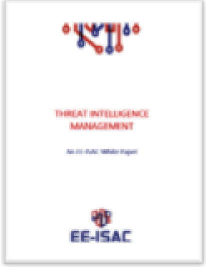
□	Date	Org	Category	Type	Value	Tags	Com
□	2018-02-18		Network activity	ip-src	103.6.196.156	osint:lifetime="ephemeral" x osint:source-type="block-or-filter-list" x cirl:incident-classification:spam="" x inthreat:event-src="feed-osint" x +	UCEF
□	2018-02-18		Network activity	ip-src	192.162.87.221	osint:lifetime="ephemeral" x osint:source-type="block-or-filter-list" x cirl:incident-classification:spam="" x inthreat:event-src="feed-osint" x +	UCEF

White Papers 2020

Threat Intelligence Management

EE-ISAC members believe that Threat Intelligence can play a very important role in both, preventive and reactive cyber security. Considering the additionally complexity arising from Industrial Control System (ICS) Attack Vectors, the energy sector, more than other sectors, seems to depend even more on good Threat Intelligence Management. This paper explicitly addresses the needs of small and medium enterprises (particularly, these are enterprises with a headcount of less than two thousand employees and cyber security departments with a headcount of one to five) in the energy sector, planning to use Threat Intelligence to improve detective and reactive cyber security controls in their organisation.

Alexander Harsch, Marcel Kulicke, Kostantinos Moulinos, Andreas Seiler, Christina Skouloudi, Antigone Zisi (2020)



THREAT INTELLIGENCE MANAGEMENT

An EE-ISAC White Paper

EE-ISAC

Cyber Security Incident Response

EE-ISAC has gathered a synthesis of experience from their membership to offer some useful guidance, especially to assist smaller businesses to prepare and respond adequately to cyber incidents. In recent years several incidents have targeted critical infrastructures, including the energy sector. As devices used in Operational Technology (OT) facilities trust each other and their users, one compromised device can allow a compromise to the whole system. With an increasing likelihood of incidents, and both small and larger organisations being targeted, it is essential to prepare incident response capability in order to safeguard society's dependency on energy. Regulations such as the Network and Information Security (NIS) Directive are now enforcing the requirement for an Incident Response capability. This document aims to offer some assistance in building that capability.

Paul Smith, Tania Wallis, Christina Skouloudi, Konstantinos Moulinos, Alexander Harsch, Marius Staggenbrog, Massimo Rocca, Daniel dos Santos, Jalal Bouhdada, Marcel Kulicke, Aleksander Wiśniewski, Alexander Novotny, Michael Knuchel, Dmytro Cherkashyn, Ivan Dragnev, Andreas Seiler (2020)

CYBER SECURITY INCIDENT RESPONSE

An EE-ISAC White Paper

EE-ISAC

Let’s discuss further

Marcel Kulicke

CONTACT US

contact@ee-isac.eu

www.ee-isac.eu

EE-ISAC