Thematic Workshop 7
Cyber Threat Intelligence in the context of ISACs

MARCEL KULICKE, EE-ISAC | EMPOWERING EU ISACS CONSORTIUM | SEPT 30 2021
EU ISAC CONFERENCE

2nd Annual Conference | October 26
Start stream 12.45 / 13.00 – 15.00
Online | Open to all

Co-organised by:
The European Commission (DG Connect) & ENISA, the EU Agency for Cybersecurity & EU-ISACs

https://www.isacs.eu/events/2nd-annual-conference
Empowering ISACs: Support maturity of existing ISACs and support set-up emerging ISACs

**Goals**

- Support set-up of **emerging** ISACs in the EU
- Support **existing** ISACs to improve maturity
- Support **coordination** between ISACs

**Timelines**

January 2020 – December 2022

**Activities**

1. Provision of soft support to existing and emerging ISACs
2. Implementation of IT Platforms to support ISACs
3. Organize thematic workshops and conferences for the wider ISAC community
The consortium is currently already supporting a number of European ISAC initiatives. Some examples of our support:

- **Stakeholder analysis**: The project performed an analysis of the organisational landscape of an ISAC to determine which categories of stakeholders exist (including [potential] members) to determine how to involve them.

- **ISAC promotion and outreach**: The project has helped an ISAC with developing promotional material to initiate (public) outreach, for example to attract new members or create public awareness about the initiative.

- **Information-sharing platform**: The project is developing a platform to facilitate information sharing and analysis for multiple EU ISACs to make use of.

- **Working Group Efficiency**: The project helps ISACs with organising working groups (teams within an ISAC that work on a specific topic or assignment) efficiently. This involves a ‘best practice’ blueprint and concrete ad hoc advice and support.

- **Getting an ISAC started**: In multiple sectors where no European ISAC exists as of yet, the project actively supports ‘foundling members’ with their first steps with the establishment of the ISAC.

- **Formalisation**: Some ISACs look to formalise the cooperation within an ISAC, for example through documents such as an NDA, Terms of Reference or MoU. The project has supported ISACs with such steps through legal expertise, templates and practical advice.

As you can see, our support activities have different forms: it is not a one-size-fits-all approach.

* Current EU ISACs initiatives we are in contact with and/or supporting

** Sectors in which the project is initiating new EU ISACs

- Energy sector EE-ISAC
- Railway (sub)section ER-ISAC
- Maritime sector EM-ISAC
- IXP sector PISAX
- Finance sector FI ISAC
- TLD sector
- Healthcare sector
- (drinking) water sector
Who are you?

PLEASE VOTE
My organization applies public and/or commercial CTI in the daily operations
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

**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

---

**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 trends and attacks against energy sector

---

**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**
- Siemens (Marcel)

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

---

**Coordinator**
- ENISA (Konstantinos Moulinos)

**Participants**
- Applied Risk (Jalal Bouhdada)

---

**Coordinator**
- E.ON (Alexander Harsh)

**Participants**
- Brandenburg University (Jugersa Smaja)
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)

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.

Digital Information Sharing

- Hash Values: Trivial
- IP Addresses: Easy
- Domain Names: Annoying
- Network/Host Artifacts: Challenging
- Tools: Tough!
- TTPs

MISP

MISP is a de-facto standard:

- An efficient IoC and database about malware samples, incidents & attackers
- Automatic correlation finding relationships between attributes & indicators
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.
MISP - How does the sharing affect the ISAC work?

- **MISP offers** several levels for cooperation. Most of them are on the technical level and facilitate an **ongoing** exchange.

- With this **basis**, exchanges on topics higher up in the chain are **fed**.

- **Further discussions** could then take place in the plenaries and/or special webcasts and meetings if need be.

- This establishes a rather low-level **continuous** than a higher-level discrete **exchange**.

- **Benefits** for the **ISAC:**
  - In general; **Closer collaboration**
  - Base data for **further evaluations**
  - **Identification** of specific working group **topics**
Let’s discuss further

Marcel Kulicke

CONTACT US

contact@ee-isac.eu

www.ee-isac.eu
Can we help your organization? Let us know!

Contact us:

- info@isacs.eu
- Empowering EU ISACs Group
  - Tom van Schie: tom.vanschie@tno.nl
  - Roeland de Koning: roeland.de.koning@capgemini.com

Upcoming Events:

- Online Thematic Workshop 7: Cyber Threat Intelligence in the context of ISACs
  - 30/09/2021 - 11:30 - 30/09/2021 - 12:30

- 2nd Annual Conference
  - 26/10/2021 - 12:45 - 26/10/2021 - 15:30

https://www.isacs.eu/