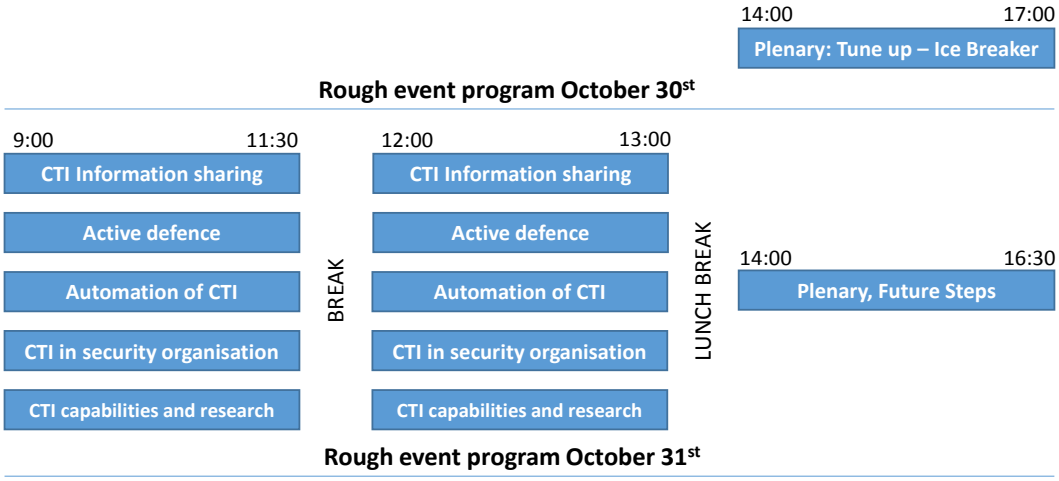
ENISA CTI – EU: Draft Structure of the Event

1 Overview of the event



2 Content and structure

30th October 2017: Tune up - Ice breaker

Facilitator: Louis Marinos

State of play: a common session with EDA, EC3, CERT-EU and ENISA on how CTI is being considered within their activities.

31st October 2017:

Session 1: CTI Information sharing:

Sharing of CTI is key for all kinds of players involved in the creation, dissemination and consumption of threat intelligence. Yet, several issues are related to CTI information sharing. In this session, participants will debate on their experience with CTI sharing and will bring in their views regarding such issues (below some examples):

- Options/standards for formatting CTI information
- Quality and usability issues of CTI information
- Incentives for CTI information sharing
- Legal issues of CTI information sharing
- Current sharing practices
- Current information sharing platforms (MISP, CIF, etc.)
- Future trends in CTI information sharing

Facilitators: Jane Ginn, Stavros Lingris

Active supporters: Bret Jordan, Trey Darley, Andras Iklody (confirmed)

Session 2: Active defence

Active defence is considered as an effective strategy to turn launching of various cyber-threats costly and inefficient. Based on available cyber-threat intelligence, active defence may inverse the "asymmetry" of many cyber-threats/cyber-attacks and create additional obstacles to adversaries. Indicative topics to be covered are:

- Purpose and objectives
- Areas of applicability of active defence
- Active defence elements/processes
- Active defence methods & frameworks
- Active defence tools
- Intelligence-led active defence

Facilitators: Antonio Forzieri, Cosmin Ciobanu

Active supporters: David Barroso (confirmed)

Session 3: Automation of CTI

Adapted to the needs of various user groups, usage scenarios and differentiated user capability and maturity levels, automation methods of CTI play an important role. Their uptake will affect the level CTI will penetrate the cyber-security field. Indicatively, various issues to be discussed in this area are:

- CTI elements (current, desired, future, etc.)
- Formulation of CTI program requirements (understanding the needs, manage expectations, leverage on available resources)
- Purpose/use cases of CTI information; target groups (e.g. security, technical, non-technical, decision maker)
- CTI modelling, taxonomies, frameworks and workflow issues
- Integrating/Mapping CTI to related internal processes and available governance and control structures (e.g. SOC, Hunting, SIEM, Red teaming, Risk Governance, Compliance, etc.)
- Tailoring CTI information to own needs
- Identify role of CTI in internal value creation processes and integrated it in decision making (i.e. tools for the board, HR, etc.)
- Legal aspects of CTI
- The role of CTI in coverage of legal/compliance requirements

Facilitators: Neil Thacker, Alexandre Dulaunoy

Active supporters: Jussi Eronen, Alexandru Ciobanu, Pawel Pawlinski (confirmed)

Session 4: Embedding CTI in security organization and good practices

Cyber Resilience requires a defense in depth approach containing several layers of defense. However implementing multiple layers of defense everywhere is too costly. This session will explain how to use Cyber Intelligence to plan your identify the most effective controls using the Kill Chain approach. Some indicative areas for the discussions are:

- CTI elements (current, desired, future, etc.)

- Formulation of CTI program requirements (understanding the needs, manage expectations, leverage on available resources)
- Purpose/use cases of CTI information; target groups (e.g. security, technical, non-technical, decision maker)
- CTI modelling, taxonomies, frameworks and workflow issues
- Integrating/Mapping CTI to related internal processes and available governance and control structures (e.g. SOC, Hunting, SIEM, Red teaming, Risk Governance, Compliance, etc.)
- Tailoring CTI information to own needs
- Identify role of CTI in internal value creation processes and integrated it in decision making (i.e. tools for the board, HR, etc.)
- Legal aspects of CTI
- The role of CTI in coverage of legal/compliance requirements

Facilitator: Paul Samwel, Andrea Rigoni (tentative)

Active supporters:

Session 5: CTI capabilities, skills, education training and research

CTI capabilities and skills is one of the most important aspects for the usage of CTI as tool in all concerned organisations, networks of stakeholders, interested businesses and education. Main parameter for the identification of capability level and skill profiles will be the proportionality of CTI usage in organisations and the required maturity level.

During this session we will focus on different aspects of Cyber Threat Intelligence. CTI analyst's skillset will be analysed regarding tactical, operational as well as strategic threat intelligence and different use cases. We will also discuss the current skills gap in the market, the high demand for capable CTI analysts and how this gap can be bridged. Then, we will explore the current training opportunities (from paid and university courses to publicly available material), how a course syllabus would look ideal and what would be its content. Finally, we will pay special attention to current EU research efforts in the area of CTI and CTI horizon research.

Facilitator: Jart Armin, Andreas Sfakianakis

Active supporters: Adam Kozakiewicz, Ms Heidi Kivekäs, Selene Giupponi, Prof Latif Ladid, Prof Marco Cremonini (confirmed)

Demonstrators

Various players from industry, national organisations, academia and research will perform demonstrations of available good practices and tools. This activity will run in parallel to the event.

Facilitator: Louis Marinos