ENISA CTI – EU: Final Agenda of the Event

The event is organized in cooperation with:

DG Connect/H1 | Europol EC3 | CERT-EU | European Defence Agency

30 October 2017	
Opening Session: CTI in EU Institutions	
14:00 – 16:00	• Welcome address *Minister Vincenzo Scotti, President of Link Campus University* • Introduction, organisational issues *Louis Marinos* • Cyber Threat Intelligence Information Sharing for EU-led military Operations – Is the time ready now? *Wolfgang Röhrig*, European Defence Agency • Cyber Threat Intelligence at CERT EU *Kyriakos Satlas*, CERT EU • CTI at ENISA: now and then *Louis Marinos* • Cyber Intelligence within EC3 operations *Álvaro Azofra-Martínez*
16:00 – 16:30	Break
16:30 – 17:00	• Digging in the dark web *Pierluigi Paganini*
17:00	**END OF DAY ONE**

31 October 2017	
Parallel Session 1 – CTI Information Sharing	
09:00 – 11:30	Facilitators*: Jane Ginn, Stavros Lingris* • Introduction *Stavros Lingris, CERT-EU* • Active supporters' contributions - *Andras Iklody* - *Bret Jordan* - *Raymond van der Velde* - *Trey Darley* *CONTRIBUTIONS FROM PARTICIPANTS*
11:30 – 12:00	Break
12:00 – 13:00	• Stand up pitches from the audience (anyone can join, no slides needed) • Active discussion with all participants - What are the issues faced by audience members? - What are the challenges? - Brainstorming on objectives for CTI information sharing - What does the future look like? *Jane Ginn, Moderation* *CONSOLIDATION OF DISCUSSIONS*
13:00 – 14:00	Lunch Break

31 October 2017	
Parallel Session 2 – Active Defence	
09:00 – 11:30	*Facilitators: Antonio Forzieri, Cosmin Ciobanu* • Introduction *Antonio Forzieri, Cosmin Ciobanu* • Active supporters' contributions - What is active defence & areas of applicability *Cosmin Ciobanu, David Barrosso* - Real cases of active defence *Cosmin Ciobanu* - Active defence tools (honeypots & traps & canaries) *David Barrosso, Dimitris Margaritis* - Active defence strategies, methods & frameworks *David Barrosso, Dimitris Margaritis* - Potential implications (legal, defence etc.) *David Barrosso, Dimitris Margaritis* *CONTRIBUTIONS FROM PARTICIPATS*
11:30 – 12:00	Break
12:00 – 13:00	• Stand up pitches from the audience (anyone can join, no slides needed) • Active discussion with all participants - What are the issues faced by audience members? - What are the challenges? - Brainstorming on objectives for CTI information sharing - What does the future look like? *CONSOLIDATION OF DISCUSSIONS*
13:00 – 14:00	Lunch Break

31 October 2017	
Parallel Session 3 – Automation of CTI	
09:00 – 11:30	*Facilitators:* Alexandre Dulaunoy, Stuart Taylor • Introduction *Stuart Taylor* • Active supporters' contributions - CTI elements - Formulation of CTI program requirements Purpose/use cases of CTI information; target groups - CTI modelling, taxonomies, frameworks and workflow issues Integrating/Mapping CTI to related internal processes and available governance and control - Tailoring CTI information to own needs Identify role of CTI in internal value creation processes and integrated it in decision making - Legal aspects of CTI - The role of CTI in coverage of legal/compliance requirements *Jussi Eronen, Alexandru Ciobanu, Pawel Pawlinski* • CTI Automation Exercise - MISP Galaxy Cluster – ATT&CK Pattern DT exercise - IntelMQ – Incident Handling *Pawel Pawlinski, Tomás Lima* *CONTRIBUTIONS FROM PARTICIPATS*
11:30 – 12:00	Break
12:00 – 13:00	• CTI Automation Exercise Feedback - MISP Model – OSINT feed (Malware Information Sharing Platform) - IntelQM *Pawel Pawlinski, Tomás Lima* • Stand up pitches from the audience (anyone can join, no slides needed) • Active discussion with all participants - What are the issues faced by audience members? - What are the challenges? - Brainstorming on objectives for CTI information sharing - What does the future look like? *CONSOLIDATION OF DISCUSSIONS*
13:00 – 14:00	Lunch Break

31 October 2017	
Parallel Session 4 – Embedding CTI in security organisation and good practices	
09:00 – 11:30	*Facilitators: Paul Samwel* • Introduction *Paul Samwel* • Using CTI for prioritizing security improvements *Paul Samwel* • Active supporters' contributions - Scaling Intelligence for communities *Chris O'Brian* - Translating intelligence for the business *Tierman Connolly* - CTI capability framework *Richard Kerkdijk* *CONTRIBUTIONS FROM PARTICIPATS*
11:30 – 12:00	Break
12:00 – 13:00	• Stand up pitches from the audience (anyone can join, no slides needed) • Active discussion with all participants - What are the issues faced by audience members? - What are the challenges? - Brainstorming on objectives for CTI information sharing - What does the future look like? *CONSOLIDATION OF DISCUSSIONS*
13:00 – 14:00	Lunch Break

31 October 2017	
Parallel Session 5 – CTI capabilities, skills, education training and research	
09:00 – 11:30	*Facilitators: Andreas Sfakianakis, Jart Armin* • Introduction to CTI capabilities, skills, education training and research *Adnreas Sfakianakis, Jart Armin* • Active supporters' contributions - CTI analyst's skillset – practical application, what is done in Finland - "Why is Finland so cyber threat free?" – What skills & methods can we learn from Finland? *Ms Heidi Kivekäs* - CTI analyst's skillset – a syllabus - SANS - FOR578: Cyber Threat Intelligence *Jess Garcia* - Current training & educational opportunities: An academic approach & what the employers need *Prof. Marco Cremonini* - Current EU research efforts in the area of CTI and Horizon 2020 research: The metrics and mapping the threats – SAINT Getting the threat data – SISSDEN *Adam Kozakiewicz, Prof. Latif Ladid* - Current skills gap for capable CTI analysts: Training for forensics & analysis *Selene Giupponi* *CONTRIBUTIONS FROM PARTICIPATS*
11:30 – 12:00	Break
12:00 – 13:00	• Stand up pitches from the audience (anyone can join, no slides needed) • Active discussion with all participants - What is the CTI analyst's skillset? - Current skills gap and how this gap can be bridged? - What and where are CTI training & educational opportunities? - EU research efforts in the area of CTI and Horizon 2020? *CONSOLIDATION OF DISCUSSIONS*
13:00 – 14:00	Lunch Break

31 October 2017	
Afternoon Plenary Session	
14:00 – 16:30	• Presentation of session results - CTI Information Sharing *Jane Ginn, Stavros Lingris* - Active Defence *Cosmin Ciobanu, Antonio Forzieri* - Automation of CTI *Alexandre Dulaunoy, Stuart Taylor* - Embedding CTI in security organisation and good practices *Paul Samuel* - CTI capabilities, skills, education, training and research *Jart Armin, Andreas Sfakianakis* • Concluding remarks *Louis Marinos*
END OF EVENT	

Demonstrators	
30th and 31st October	
SISSDEN Project	H2020 Project, https://sissden.eu/
SHIELD	H2020 Project, https://www.shield-h2020.eu/
AEGIS	H2020 Project, http://aegis-project.org/
C3ISP	H2010 Project, http://c3isp.eu
MISP	Malware Information Sharing Platform, http://www.misp-project.org/
IntelMQ	Incident Handling Automation, https://github.com/certtools/intelmq
AbuseHelper	https://github.com/abusesa/abusehelper
MineMeld	Palo Alto Networks, https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/minemeld
Lutech Cyber Threat Intelligence	Cyber threat intelligence platform, https://security.lutech-group.com/
ENISA ETL App	ETL visualisation tool, https://etl.enisa.europa.eu