8th ENISA Workshop ‘CERTs in Europe’

Report

Part I – Technical Hands-on Workshop ; Part II – ENISA/EC3 Workshop

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Jo De Muynck (ENISA)

Lauri Palkmets (ENISA)

Contact

For contacting the authors please use cert-relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu**.**

Acknowledgements

The drafting of this Report would not have been possible without the feedback and cooperation kindly provided by a large number of organisations and individuals. Without endeavouring to be exhaustive, the authors would like to thank all who presented and participated in Part I and/or Part II of the workshop for their valuable input.

For Part I of the workshop ENISA also would like to thank Team Cymru and ARNIEC/RoEduNet for their part in making this workshop successful.

ENISA also would like to thank Europol and more in particular the European Cybercrime Centre (EC3) for hosting this event and the collaboration in organising the ENISA/EC3 Workshop (Part II).

ISBN 978-92-9204-085-7 doi: 10.2824/30515

Executive summary

ENISA's traditional workshop "CERTs in Europe" has been organised every year since 2005 for the national/governmental (n/g) CERTs in Europe and is one of the most efficient and indispensable methods for ENISA to support the teams in their daily work and to assist in improving their capabilities.

In 2011, ENISA started to collaborate with Europol and the first joint workshop was held in Prague that year. The next years the annual ENISA workshop was split in two parts, one part aimed only at n/g CERTs that had a more technical focus and one part aimed at both n/g CERTs and law enforcement representatives, organised together with Europol. The topic of the latter meetings were on cooperation in the fight against cybercrime.

This year too, the first part of the workshop focused on hands-on technical training for n/g CERTs in Europe. Doing so, ENISA enhances CERTs capabilities in the EU Member States by provision of good operational practice and the facilitation of suitable training and exercises. Hands-on training for CERT team members on operational topics is essential to improve the capabilities of the team as a whole.

Part II of the workshop, the ENISA/EC3 workshop, served as a foreseen follow up event of the workshop held last year together with Europol. It kept the same focus on cooperation between n/g CERTs in Europe and their national law enforcement counterparts. The topic this year was (automated) information sharing.

In both events 106 participants were gathered. Austria, Belgium, Croatia, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom were the 24 EU Member States that were represented as well as Norway and Switzerland. The following organisations were also represented: CEPOL, ECB, ENISA, European Commission (DG Home), Council of Europe, CERT EU and Europol (EC3).

Both events were well received. According to the feedback from the participants given in the evaluation forms, they scored the meeting of their expectations of these workshops on average 4.4 out of 5.

This document serves as a means to report on the purpose of these two meetings and is not meant to serve as a set of detailed minutes, especially as a large part of these workshops was focused on trainings as well as invitation-only information sharing through the Traffic Light Protocol - TLP RED.

Table of Contents

1 Introduction

ENISA's traditional workshop "CERTs in Europe" has been organised every year since 2005 for the national/governmental (n/g) CERTs in Europe and is one of the most efficient and indispensable methods for ENISA for supporting the teams in their daily work and improving their capabilities.

Back in 2011 ENISA started to collaborate with Europol on this topic. The first joint workshop was held in Prague that year and had a focus on CERT cooperation with law enforcement. The need to continue with meetings on this topic was identified during this first meeting.

In addition, the ENISA study on CERT Operational Gaps and Overlaps[1] from 2011 pointed out that training and education is considered most important by the majority of the CERTs, indicating the insufficient amount of training opportunities for the CERTs currently within the community.

ENISA already partially fills this void by supporting TRANSITS trainings and also by facilitating the pan-European incident response exercises which are aimed at the different CERTs, amongst others, because of their role in CIIP[2]. These exercises are of strategic importance in enhancing the security and resilience of the CII sector, in particular by focusing on flexible strategies and processes for dealing with the unpredictability of potential cyber-attacks.

ENISA also currently investigates how further technical training could be organised for the operational security specialists (CERTs) and ENISA's role in this process. By providing this particular training to members of n/g CERTs, ENISA continues to support the CERT community.

This is the reasoning behind the decision to split the annual ENISA workshop in two parts since 2012, one part aimed only at n/g CERTs and had a more technical focus and the second part aimed at n/g CERTs and law enforcement representatives, organised together with Europol.

This year too, the first part of the workshop focused on hands-on technical training for n/g CERTs in Europe. Doing so, ENISA enhanced CERTs capabilities in the EU MS by provision of good operational practice and the facilitation of suitable training and exercises. Hands-on training for CERT team members on operational topics is essential to improve the capabilities of the team as a whole.

Part II of the workshop, the ENISA/EC3 workshop, served as a foreseen follow up event to the workshop held last year together with Europol. It kept the same focus on cooperation between n/g CERTs in Europe and their national Law Enforcement counterparts. The topic this year was on (automated) information sharing.

For reference purposes the previous workshops are listed below:

- 1st CERT workshop (2005, Brussels, Belgium): Lessons learned and good practices on setting up a CERT, tools used by CERTs, cooperation and legal issues;
- 2nd CERT workshop (2006, Brussels, Belgium): Setting-up and cooperation;
- 3rd CERT workshop (2007, Porto, Portugal): Mitigation of Massive Cyber attacks;
- 4th CERT workshop (2008, Athens, Greece): The role of CERT teams in national incident response plans;
- 5th CERT workshop (2010, Heraklion, Crete, Greece): The role of n/g CERTs in national and cross-border exercises and on sharing information;
- 6th CERT workshop (2011, Prague, Czech Republic): Addressing NIS aspects of cybercrime;

[1] http://www.enisa.europa.eu/activities/cert/other-work/files/operational-gaps-overlaps
[2] http://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip

- 7th CERT workshop part I (2012, Valetta, Malta): hands-on technical training;
- 7th CERT workshop part II (2012, The Hague, The Netherlands): Addressing NIS aspects of cybercrime;
- 8th CERT workshop part I (2013, Bucharest, Romania): Hands-on technical training;
- 8th CERT workshop part II (2013, The Hague, The Netherlands): ENISA/EC3 Workshop on (automated) information sharing.

2 Methodology

Co-locating ENISA Workshop Part I with 39th TF-CSIRTmeeting

Based on the participants' feedback of the previous year ENISA decided to co-locate the Part I with another major CERT event organised in Europe. This was also one of the recommendations in another ENISA study on Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime - A first collection of practices[3] from 2011. The recommendation made in this report was that "cooperation between conference and meeting organisers should be encouraged and meetings should be coordinated as much as possible, to reduce travel and time costs to the minimum".

The TF-CSIRT meetings regularly gather a large number of experts from the CERT operational community in Europe. With this in mind, ENISA addressed RoEduNet, the national research and education network in Romania, and the host of the 39th TF-CSIRT meeting in order to discuss opportunities regarding a suitable venue for this workshop. Cooperation with the RoEduNet was fruitful and they agreed to host this workshop in the hotel Radisson Blu in Bucharest.

Based on ENISA CERT exercise material and Tean Cymrus[4] training portfolio, a two day training agenda was created including for the first time ENISA trainers presenting a part of the ENISA CERT Exercises[5].

The agenda covered two full days of in depth technical training. ENISA's CERT-relations team worked together with Team Cymru, a not-for-profit Internet security firm that is well known in the CERT community, to deliver a high reputable training for the n/g CERTs representatives. The sessions provided in-depth technical diving into several current security topics including botnets and reverse engineering. Team Cymru Research NFP is an Illinois non-profit and a US Federal 501(c)3 organization. They are a group of technologists dedicated to making the Internet more secure. They work closely with and within Internet security communities, as well as with all kinds of other organisations – recognising the fact that almost every organization in the modern world is connected to the Internet in some way or another, and they all need help to ensure that their parts of the network remain safe and secure. Team Cymru supports the global CERT community on regular basis.

The two experienced trainers from Team Cymru, Cecil Goldstein[6] and Kevin Henry, ensured that all participants receive well prepared and accurate content and training.

ENISA/EC3 Workshop hosted by Europol

The ENISA/Europol event was hosted by Europol in 2012. As most of the participants seemed to find this venue very suitable for these type of meetings and as the European Cybercrime Centre (EC3) was established in January of 2013 Europol offered to host this meeting for a second time.

The structure of this meeting changed in comparison to the meeting last year. It was decided to have in the first part keynotes from both ENISA and EC3 as well as presentations by ACDC[7], DG Home[8] and the Dutch NCSC[9].

[3] http://www.enisa.europa.eu/activities/cert/support/supporting-fight-against-cybercrime
[4] http://www.team-cymru.org/
[5] https://www.enisa.europa.eu/activities/cert/support/exercise
[6] http://au.linkedin.com/pub/cecil-goldstein/6/24a/b57
[7] http://www.botfree.eu/
[8] http://ec.europa.eu/dgs/home-affairs/
[9] https://www.ncsc.nl/

In the second part of this meeting trainings were provided by ENISA trainers. The training used new material[10] produced in 2013. It was considered valuable to have this training, also to initiate the discussion and to look at the training material with both the prespective from CERTs and law enforcement.

The third part of this meeting was organised as a round table discussion under Traffic Light Protocol [11](TLP) Code Red. Among the topics discussed were issues, cases and (good) practices on cooperation between CERTs and law enforcement.

Further details are provided below.

[10] http://www.enisa.europa.eu/activities/cert/support/exercise

[11] http://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/information-disclosure

3 8th Workshop Part I – Technical Hands-on Training – 21-22.05.2013

ENISA CERT Workshop part I was in many aspects unique. It was the first time that ENISA CERT training was delivered to the European CERT community by ENISA. The topics were chosen in a way that best suited most of the participants and based on the feedback of the community[12]. The workshop was carried out in two parallel tracks, one track focused on honeypots, while the other group received trained in the area of SCADA security and mobile malware.

ENISA CERT training scenario 13: Incident handling during an attack on Critical Information Infrastructure[13]

In this exercise, more than 20 participants were able to familiarise themselves with specifics on how to conduct incident handling during an attack against Critical Information Infrastructure (CII) and Supervisory Control and Data Acquisition (SCADA) systems.

The training contained a role-playing part, with the ENISA trainer acting as "operator". Additionally the exercise had technical features that required examining network and log information.

During the course of the exercise, a broad range of indicators of compromise and material for investigation was presented. This enabled the participants to develop different approaches and paths from the start to the end to make the story more realistic.

In the beginning ENISA presented a general introduction to the basics of industrial control systems, that enabled the participants to develop a general technical understanding of SCADA/CII environments and get more familiar with how to handle the organisational obstacles met in typical industrial units.

The presentation was followed by a technical case study where ENISA presented evidence in a Virtual Image to build up a case in order for participants to have hands-on experience. The time allocated for the hands-on part was limited and proved to be the bottleneck of the exercise as participants noted on the feedback sheets that there should have been more time allocated to the exercise. This is a learning point for future exercises of this type.

[12] ENISA asked the n/g CERT community about their preferences prior to the training.
[13] https://www.enisa.europa.eu/activities/cert/support/exercise

ENISA CERT training scenario 16: Mobile threats incident handling[14]

The aim of this training session was to bring into this workshop a "flavour" of mobile devices and their specifications. This part of the workshop was mostly hands-on and focused on a known malware related to Zeus that was placed inside an emulated Android phone. The malware (Zitmo) was created to intercept SMS messages containing transaction authentication numbers (TAN) and forward them to a server controlled by the attackers. During the investigation participants could clearly see the malicious transaction that application initiated. There was additionally a reverse engineering part where participants used different tools to rebuild Android application source code as close to original code as possible.

Apart from the technical challenge, this training covered also legal challenges impacting the ability to handle incidents, acquire and analyse data. Especially in combination with "Bring Your Own Device" (BYOD) or the usage of company owned devices for private purposes that might impact the ability to handle incidents.

Some participants gave very good feedback to this exercise, but a general remark was the limited time allocated to the hands on part and that the tutor progressed too quickly as a result of this.

ENISA CERT training scenario 23: Honeypots[15]

Honeypots provide for a proactive approach in detecting security incidents before they happen without any impact on the production environment.

The objective of the training was to familiarise students with two kinds of honeypots: client-side and server-side honeypots.

In the first part of the training a couple of scenarios related to the client-side honeypots posing as vulnerable browsers trying to visit compromised websites URL which had different behaviours depending on the browser. The attendees had to analyse the output of the honeypot and find which browser version was targeted by the webpage.

In the second part other scenarios related to server-side honeypots

[14] https://www.enisa.europa.eu/activities/cert/support/exercise
[15] https://www.enisa.europa.eu/activities/cert/support/exercise

were presented. In this case the honeypots behaved like vulnerable servers which were attacked and compromised. Again the attendees had to analyse the events and identify the type of attacks, attack vectors and source of the attacks.

A day in the life of malware-example

On the second day Team Cymru focused on understanding the operations and nature of malware by following the life cycle of a piece of malware from compromising a target machine and creation of a botnet, to the observation and identification of malware, its capture, extraction and subsequent analysis. In the analysis phase emphasis was given on how to understand if the analysis can provide clues and information to assist tracking the botnet.

Participants were heavily engaged in the identification of the botnet through network based analysis, followed by extraction and analysis of malware using both static and dynamic processes. The exercises were conducted on virtual machines.

4 8th Workshop Part II – ENISA/EC3 Workshop – 02-03.10.2013

This workshop followed up on last year's event and was held in the Europol premises on 2nd and 3rd of October in The Hague, The Netherlands.

As already mentioned, the structure of this meeting changed this year compared to the meeting last year. This year it was decided to have in the first part keynotes from both ENISA and EC3 as well as presentations by the ACDC project, DG Home and the Dutch NCSC. These presentations and keynotes served as a "warm-up" exercise for the participants and to identify some upcoming relevant regulations.

The second part of this meeting consisted of training sessions provided by ENISA trainers. The training used new training material produced in 2013. It was considered valuable to have this training also to initiate the discussion and to look at the training topics with both from the prespectives from CERTs and from law enforcement. There were two separate training sessions, namely:

- Presenting, correlating and filtering logs and various security feeds; and
- Identification and handling of electronic evidence.

A third part of this meeting consisted of a round table discussion under Traffic Light Protocol (TLP) Red.

Keynotes

Both organising organisations, ENISA and Europol (EC3), gave a keynote.

For ENISA, Steve Purser, Head of the Core Operations Department talked about the EU Cyber Security Strategy[16] and the Proposal for an NIS Directive and the impact this Strategy and Directive will have. He also mentioned the importance of meetings such as this ENISA/EC3 meeting.

Troels Oerting, Head of European Cybercrime Centre (EC3), talked about the importance of collaboration and of the newly set up European Cybercrime Centre and its recent activities. He also stressed the importance of cooperation and mentioned that EC3 is actively cooperating with for example the Dutch NCSC.

Presentations

a) The European Commission (DG HOME, César Alonso Iriarte and Cathrin Bauer-Bulst) gave a brief update on the legislative and practical framework for cooperation and information exchange between the public and private sectors. César Alonso Iriarte reported on the findings of his fellowship research on public-private cooperation, highlighting the need for setting up arrangements allowing to overcome potential hurdles to the activities involved in the partnership under each legal order, such as those deriving from rules on privacy, classified information, liability and competition; incentives for both sides to participate; a certain stability of the interaction; and, perhaps most importantly, a measure of trust between the participants. Cathrin Bauer-Bulst spoke about the current rules on reporting and legislative proposals in the pipeline that include reporting obligations, such as the proposal for a Network and Information Security directive recently made by DG Connect. She also gave an overview of a few coordination initiatives and of EU funding in this area.

[16] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

b) Elly van den Heuvel, General Manager at the Dutch National Cyber Security Center (NCSC) presented on the Dutch perspective. The NCSC is a government initiative and aims at bringing several existing initiatives together. In general, secure networks are the responsibility of various different parties in The Netherlands, and its NCSCs task to provide links between these parties. From the organisational point of view the centre falls under the responsibility of the National Coordinator for Counterterrorism and Security of the Ministry of Security and Justice. Its foundations however are organised in a public-private cooperation. Elly van den Heuvel stressed the importance of cooperation and collaboration.

c) Wout de Natris and Thorsten Kraft on the Advanced Cyber Defence Centre (ACDC). ACDC aims to set up national support centres in Europe with the German botfrei.de[17] initiative as an example. The project consists of two parts.
   - The first basic idea is to clean up end user systems through an alert to the affected end user system. This initiative would include the aid of a support centre and would also involve a corresponding website and free disinfection tools which would be provided through this website.
   - The second part of the project is about gathering, analysing and distributing data on botnet generated traffic and abuse in and through a central database.

   The ACDC project seeked for partners in the (mainly CERT) community.

Training sessions

One full morning was spent on a technical training given by ENISA trainers from the CERT relations team. The training used new training material produced in the year 2013, namely:

- Presenting, correlating and filtering logs and various security feeds; and
- Identification and handling of electronic evidence.

Presenting, correlating and filtering logs and various security feeds

In this training the participants learned through practical examples, how to correlate different logs and several security feeds, in order to identify on-going attacks, investigate past attacks and automate the incident handling process.

Identification and handling of electronic evidence

In this part the trainees were presented with the principles of evidence gathering. A common knowledge of the requirements regarding evidence admissibility in a court of law was established. The exercise also gave an overview of malware characteristics, methods of identification and tools that may be used at the scene.

Round table discussion

The biggest part of this workshop was a round table discussion under TLP Code Red to discuss about the current issues on cooperation between CERTs and LEA in Europe. The session was moderated by ENISA. Due to the TLP Red status,it is not possible to summarise this debate in this report. However, before the round table discussion started, Jaap van Oss, head of Focal Point Cyborg of the EC3, was invited to present a proposal about the necessity to have new and innovative ways of conducting investigations between law enforcement and non-law enforcement entities (e.g. CERTs). The question at hand was if it would be possible to set up operations together with CERTs to take down

[17] https://www.botfrei.de/

botnets. On the one hand, this encourages CERTs to help law enforcement and keep them up to date and on the other, it provides law enforcement to benefit from the expertise of CERTs. EC3 offered to facilitate and guide these 'joint operations'. The question was if there is an interest in such cooperation and if CERTs and law enforcement would be able to participate in the near future? Additionally, which information and legislation is necessary for such cooperation and what would be needed to combine/exchange information? The process would include the exchange of intelligences packages and could have three different levels of escalating mitigation measures in mind.

From the discussion it became clear that for law enforcement and (most of the) CERTs represented in the room there is a clear willingness for such cooperation. To actually organise a 'joint operation', it is necessary to have proper coordination to overcome the legal and operational challenges. Additionally it is necessary to create a framework to exchange information. This will take time and will not be perfect the first time, but is a system that needs to grow. The difficulty is that CERTs do not have the same organisation or mandate in the different countries; these particularities must be taken into account in such cooperation efforts. Nevertheless, the relationship between law enforcement and CERTs needs to deepen.

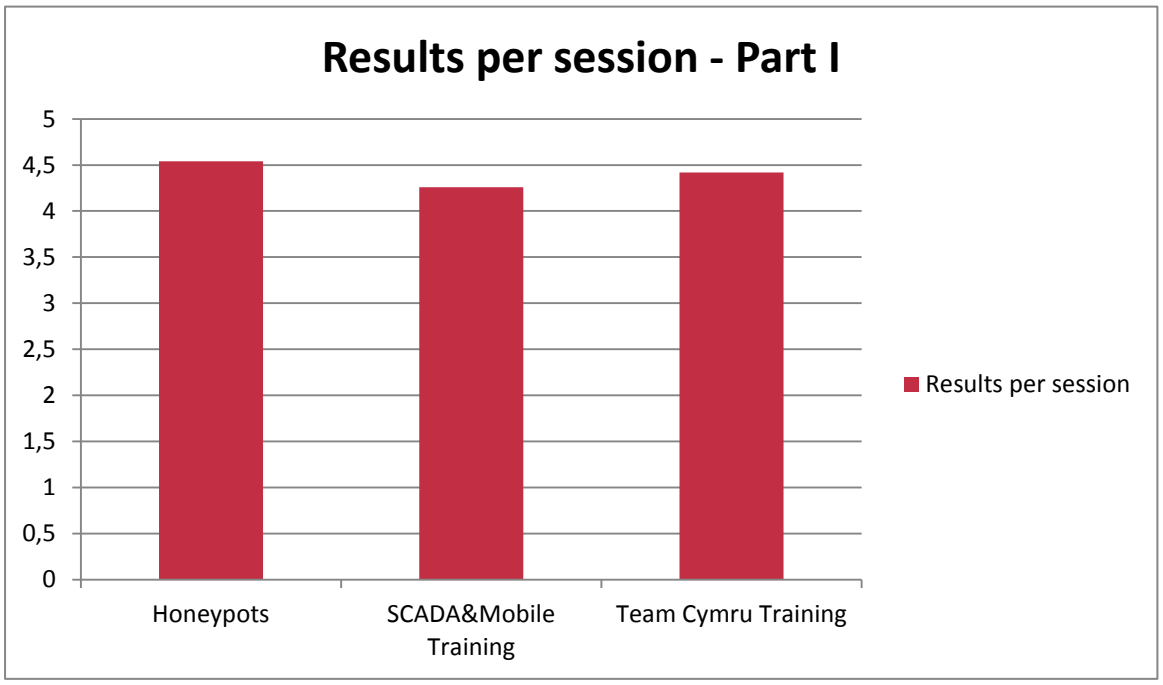
5 Evaluation and lessons learnt

Spread over both events 106 participants were representing 24 EU Member States as well as Norway and Switzerland. Also CEPOL, ECB, ENISA, European Commission, Council of Europe, CERT EU and Europol (EC3) had sent representatives.

The workshops were a great success. According to the feedback from the participants given in the evaluation forms, they scored the meeting of their expectations of these workshops on average 4.4 out of 5. With regards to the overall evaluation of the event ENISA is satisfied with the level of active participation in the trainings. Orally, ENISA received some very good feedback on the quality of the training from the participants directly during the events. Their satisfaction was also confirmed in their evaluation with high scores of their expectations of the workshops.

8th Workshop Part I – Technical Hands-on Training

For Part I of the Workshop ENISA received overall a score of 4,41 out of 5, which is an excellent result, especially taking into account that this was the first time that ENISA experts gave such trainings! All participants who filled in the feedback gave very positive impression with regards to the current and future workshops.



Some recommendations from participants for further improvement included the following thoughts:

a) open source tools should be more extensively used during training;

b) there should be more assurance that all participants can follow the content, there were occasions where the tempo was too quick;

c) training should always be lifelike and as close to reality as possible;

d) interaction with participants should be more encouraged;

Team Cymru was also very pleased with the level of experience of the group. According to the trainer, Cecil Goldstein from Team Cymru, they were a good group to work with and for the most part, more experienced than they had anticipated. It is always very hard to assess the level of experience of the participants before the training. That's why we asked Team Cymru to be flexible in

this regard and to be able to adapt to a more experienced group. However, a comment we heard a lot, both orally but also written in the evaluation forms, is that people would prefer to have two tracks with different level of difficulty. This is certainly something we have to keep in mind for a next training workshop.

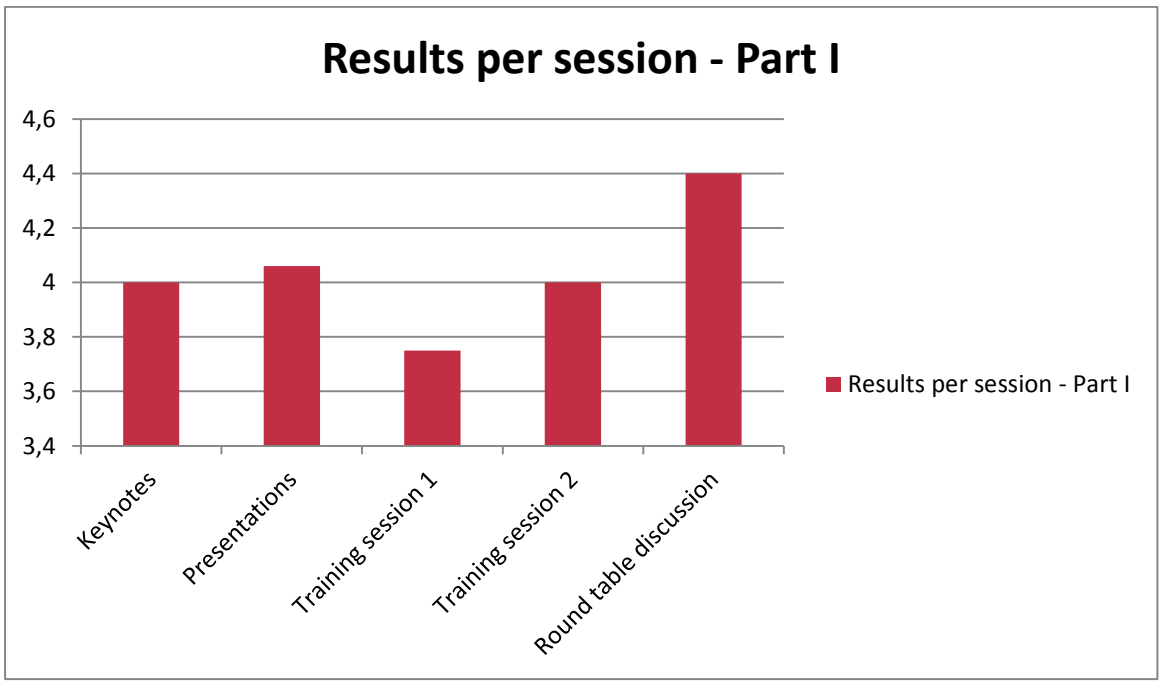
8th Workshop Part II – ENISA/EC3 Workshop

The total average score the participants gave for this workshop in the evaluation was 4.21 out of 5.

The presentations, keynotes and especially the round table discussion was found interesting by most participants.

Regarding the trainings the opinions were more divided. This was also the most prominent feedback that was provided, namely that for the next workshop we should specify more precisely in our invitations which kind of representatives we expect. At this workshop there was a mix of more technical and managerial people.

Most participants expressed their interest to participate in the follow up of this event and found the venue very suitable for these kind of meetings.



6 Action points

There are no action points for Part I of the workshop. The following sessions hence only covers action points from the ENISA/EC3 Workshop (Part II).

1. EC3, together with ENISA, will come up with a proposal of what exactly they request from the CERTs with regards to the cooperation on the takedown of botnets. This would be sent to the participants of the meeting, as well to the ENISA n/g CERTs mailing list to reach out to teams that were not represented. The CERTs should from their part analyse if this proposal is possible and provide feedback.

2. An analysis should be made of the target audience for these meetings. A clear goal and agenda should be created to make sure the right people are attending. This analysis should be done by the EC3 and ENISA when preparing for next years meeting.

3. The question was raised if training opportunities are useful in these CERT-LEA meetings? The answer to this question heavily depends on the analysis of the target audience. This question should be answered by ENISA and EC3when preparing for next years meeting.

TP-04-13-183-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN 978-92-9204-085-7
9 789292 040857
doi: 10.2824/30515

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu