



ENISA's Action for CERTs Impact Analysis

Lionel Ferette | NIS Expert
TF-CSIRT | Poznan, Poland | 21/05/2015

European Union Agency for Network and Information Security



Agenda



- 1** 2014 Project

- 2** Main Findings

- 3** Proposed Roadmap

- 4** 2015 Update Project

2014 Impact Assessment and Roadmap



Project Objectives



Aim:

- ✓ Analyse the impact of ENISA's support to CERTs from ENISA's inception until today, and
- ✓ Provide a roadmap for the period until 2020.

Deloitte.

Key objectives:

- ✓ Take stock of ENISA achievements related to EU CERTs, and in light of relevant policy documents
- ✓ Impact analysis of ENISA's achievements to CERTs and other operational communities
- ✓ Propose roadmap to 2020 based on the impact analysis

Impact Assessment – 2 Perspectives



Legislative and regulatory

Focused on relevant **policy documents**

- EU Cybersecurity Strategy
- Proposed NIS Directive
- ENISA Regulation
- Work Programmes 2013/14

Operational

Focused on **3 activity pillars**:

- Baseline capabilities for CERTs
- Capacity building for CERTs
- Support for CERT-LEA Cooperation

Stakeholder Categories



Main Findings



Main Findings



Respondents were generally aware of, and happy with, ENISA's action for CERTs

Highest praises for trainings

Main request: "More of the same, please"

Beyond - ?

Proposed Roadmap



Legislative and Regulatory



Actions	Timeline
Act as the voice for CERTs in the European policy context	M-L
Cybersecurity Strategy: <ul style="list-style-type: none">Assist in creation of cross-border operational and crisis management processes - technical guidelines and recommendations for cyber resilience capabilitiesDevelop models of cooperation with clear balance between level of response, obligations, and incentives for cooperation	M-L
NIS Directive: <ul style="list-style-type: none">Create guidance for CERTs to comply with NIS DirectiveEnable n/g CERTs to support other CERTs in different industries (finance, CIIP) by promoting the increase ministry level support	M-L

Operational – Baseline Capabilities for CERTs



Actions	Timeline
Continued support for new CERTs - clear focus on “new team support”: <ul style="list-style-type: none">• Regular updates of CERT baseline capability materials• Greater focus on technical updates, checklists, summaries	M–L
<ul style="list-style-type: none">• Reinforced Information Exchange and Connector Role:• Improved communication and enhanced information sharing• Website – mailing lists – networking	S–M
Raise awareness and take-up of ENISA materials (baseline capability) by advertising them more widely, and measuring impact: <ul style="list-style-type: none">• CERT community• Other operational communities	M–L

Operational – Capacity Building



Actions	Timeline
<ul style="list-style-type: none"> Continue support for mature CERTs and update CERT baseline capability material with a focus on “advanced team support”. Regular updates of CERT capacity building material. 	M-L
<p>Reinforced Information Exchange and Connector Role:</p> <ul style="list-style-type: none"> Improved communication and enhanced information sharing Website – mailing lists – networking 	S-M
<p>Clearer focus on operational vs strategic reports:</p> <ul style="list-style-type: none"> More technical reports for practitioners Policy-related reports for decision makers 	S-M
<p>Raise awareness and take-up of ENISA materials (capacity building) by advertising them more widely, and measuring impact:</p> <ul style="list-style-type: none"> CERT community Other operational communities 	S-M

Operational – Support for CERT-LEA Collaboration



Actions	Timeline
Facilitate more joint CERT-LEA events and training	S-M
Enhanced support to the fight against cybercrime	S-M
Raise awareness and take-up of ENISA materials (CERT-LEA) by advertising/ disseminating them more widely, and measuring impact: <ul style="list-style-type: none">• CERT community• Other operational communities (LEAs etc)	S-M

360 Feedback



Actions	Timeline
Awareness raising: <ul style="list-style-type: none">• Key publications• Trainings• Events• Clarification of ENISA role vis-a vis CERT community	S-M
Accreditation and certification of CERTs	M-L
Identification and promotion of common standards for CERT community and other operational communities	M-L
Compilation of protection and detection methods: <ul style="list-style-type: none">• Continue past efforts - regular updates of “Clearinghouse for Incident Handling Tools” on the ENISA website• Creating of ‘playbook’ on cyber issues & recommendations	M-L

2015 Update Project



Project Objectives



Overall project aim:

To generate a structured document with references to policy documents, stakeholders opinions, positions, ideas and input, and other ENISA reports and to provide **conclusions** out of them that point to an updated and **extended impact analysis** of ENISA's achievements regarding **CERTs**.

Two Perspectives



Legislative and regulatory

Focused on relevant **policy documents**

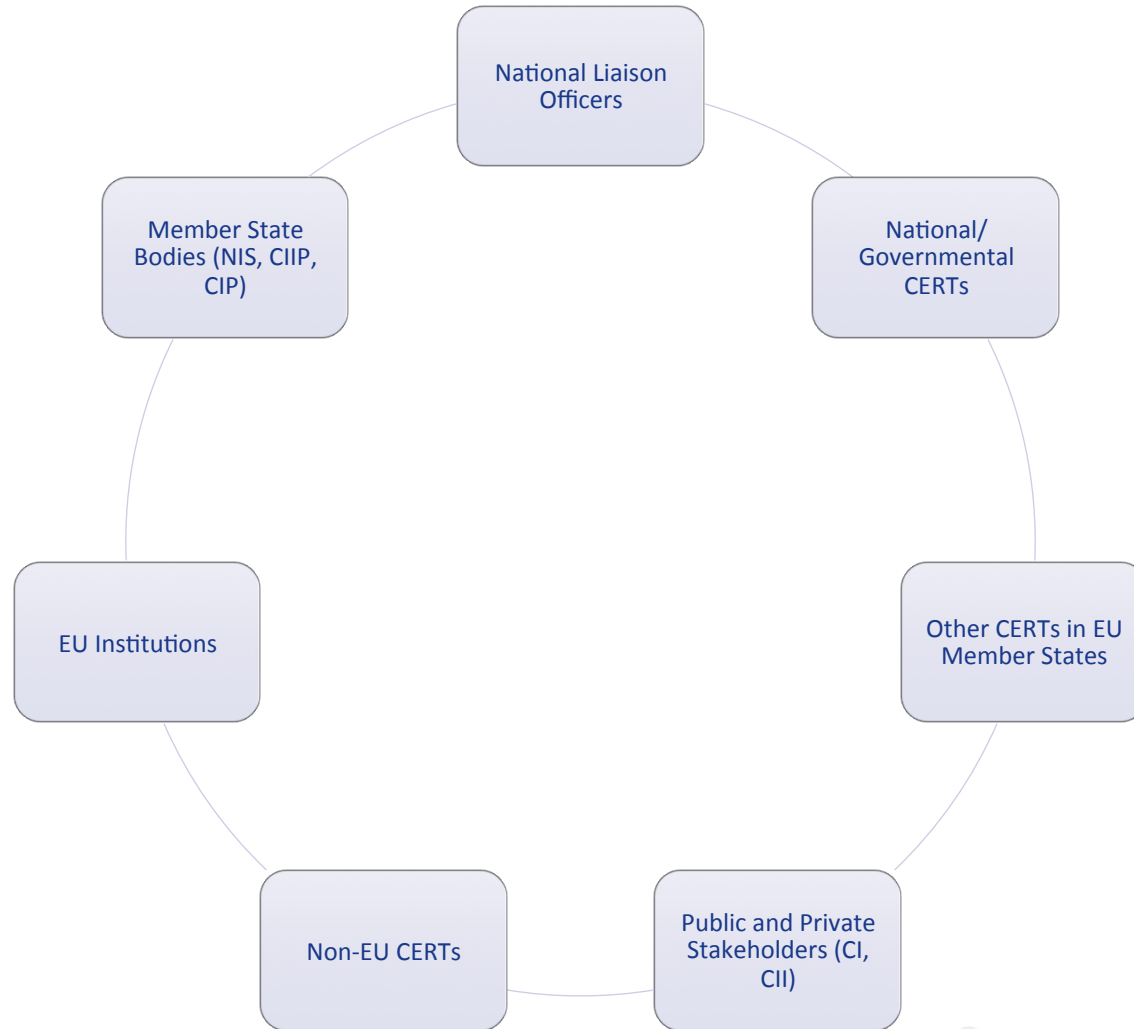
- EU Cybersecurity Strategy (and roadmap)
- *Finalised* NIS Directive
- ENISA Regulation
- Work Programmes 2015

Operational

Focused on **4 activity pillars**:

- Baseline capabilities for CERTs
- Capacity building for CERTs
- Support for CERT-LEA Cooperation
- CyberEurope Exercises

Stakeholders Categories



Next steps



Survey – Thanks for taking the time to reply

Expert Group – online meeting in September

Looking for volunteers – Thanks too!

Report in 11/2015

Summary



01 2014 Impact Analysis and Roadmap: High level conclusions

02 Update in a 2015 Project

03 You have the opportunity to have an influence

One more thing...





Thank you



PO Box 1309, 710 01 Heraklion, Greece



Tel: +30 28 14 40 9710



info@enisa.europa.eu



www.enisa.europa.eu

