CSIRT maturity and TI certification scheme in details

Andrea Dufkova, ENISA and Baiba Kaskina, CERT.LV

47th TF-CSIRT meeting, Prague, January 25-27
Contents

We are going to talk about...

- CSIRT maturity
- SIM3 and TI certification
- Certification as the way forward
- Small project in 2015
- Challenging parameters from the team point of view
- Parameters that need update vs. future tasks of the team
- Conclusions
CSIRT maturity

- Several models/scheme exist for CSIRTs
- Community based (TF-CSIRT/TI, FIRST, ENISA recommendations)
- Standards (ISO27035) only on incident response processes

Three-tier maturity model, which is based on the ongoing work of the FIRST Education Committee.

SIM3 and TI certification
little background

- SIM3 (Security Incident Management Maturity Model) is a tool to assess incident management capability and maturity

- Drafted by Don Stikvoort and Klaus-Peter Kossakowski

- It is used in support of the TI Certification framework

- Adopted by the TF-CSIRT community 5-6 years ago

• SIM3 describes 45 parameters, divided over four categories: Organisation, Human, Tools, Processes

- Minimum score needs to be attained for each parameter

- The minimum scores are defined by the TF-CSIRT Steering Committee (adhoc not regular updates)

- The TI Certification can take from 3 to 12 months

https://www.trusted-introducer.org/processes/certification.html
Certification as the way forward

• CSIRT maturity
  - Listing (132)
  - Accreditation (112/5)
  - Certification (15/6)

• Why certification?
  - Public Relation reasons – locally and internationally
  - to evaluate CSIRT organization against international criteria
  - an external drive to understand, document and put in order processes within the CSIRT team
  - to establish or put in order auditing, accountability and reporting schemes
  - to implement continuous improvement in a quality management framework
  - applicable for all kinds of teams
The document serves as a guidance tool for all teams that are aiming to advance their maturity in all aspects related to CSIRT work.

• First document to discuss in detail the TI certification process and application of SIM3 model

• CSIRT Capabilities - How to assess maturity?
  - Guidelines for national and governmental CSIRTs

• Info on certification process

• Info on how to tackle all SIM3 parameters
  - General suggestions
  - CERT.LV as a case study
  - Comments from certified governmental and national CSIRT teams

• Practical feedback & recommendations for those planning certification
Thank you!

- TI - Don Stikvoort, Klaus-Peter Kossakowski
- NCSC-NL - Martijn de Hamer, Aart Jochem
- SWITCH CERT - Serge Droz
- CERT-SE - Robert Jonsson, Erika Stockinger
- NCSC-FI - Bryk Harri
Challenging parameters from the team’s point of view

- O-8 – Incident classification
- O-10 – Organizational Framework
- H-3 - Skillset description
- H-4,5,6 – Training
- T-1 - IT Resources List (for n/g CSIRTs)
- T-8,9,10 - Incident toolset
- P-4,5,6 - Incident processes
- P-8 - Audit/Feedback Processes
SIM3 model - parameters that need update vs. future tasks of the team

- To add parameter on social media?
- Introduce different requirements for sectoral CSIRTs?
- Change requirements for P-10 Best practice e-mail and web presence?
- To join T-8 with P-4, T-9 with P-5 and T-10 with P-6?
- P-7 clarification on Specific Incident Processes
- P-17 Peer-to-Peer Process
Conclusions

• First document to discuss in detail the TI certification process and application of SIM3 model
• Focused on governmental and national CSIRTs, but usable by all
• Meant to help teams who wants to go for certification and to convince those who are doubting
• Alongside with CSIRT Maturity Kit (by NCSC-NL ) meant to assure evolution of teams’ capabilities
• Community feedback important for further evolvement of SIM3 model
Thank you

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

To read the document: