Maturity Reference for CSIRTs – Executive Summary

How to become Certifiable?

SENSITIVE-CSIRTS NETWORK ONLY

DECEMBER 2017

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.

Contact

For queries in relation to this paper, please use csirt-relations@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

Mention not paid contributors here e.g. the analysis in this document was produced in collaboration with expert X), experts interviewed, members of expert groups, etc. (space for names of experts, organisations, et cetera)

ISBN SHOULD BE PLACED HERE, DOI SHOULD BE PLACED HERE (IF APPLICABLE)

Executive Summary

The common model used for gauging CSIRT maturity in the CSIRTs community is the Security Incident Management Maturity Model (SIM3). ENISA has added to SIM3 a three-stage approach for maturity assessment, with maturity increasing via the basic and intermediate stages to finally certifiable as highest stage. A self-assessment tool and peer review methodology were coupled to that, which are being piloted in the CSIRTs Network.

As an accompanying measure, a project was defined aimed to give to teams pragmatically implementable information on how to reach the higher maturity levels– notably so, the levels 3 and 4 of the SIM3 model. This project was to explain for all 44 SIM3 parameters, how to reach those levels 3 and 4 – with examples and templates to be made available where possible. Given the sensitive nature of the collected information the results are meant to be available only to members of the CSIRTs Network.

The target audience for this study is primarily the middle management layer in the CSIRTs, responsible for increasing the team's maturity. The study will help them to more easily and quickly implement real maturity improvement, following self-assessment and peer review process.

This Maturity Reference Document is the first part of the results of that project. It contains the general framework needed to understand how to reach higher levels of CSIRT maturity – and then it goes on to describe more in detail how to do this for the first 8 parameters of SIM3 model for which the highest maturity demands (level 4) are in place, in the context of the "certifiable" level as has been defined in ENISA's three-stage approach. Two more parameters were added (O-7 and O-10) for which the "certifiable" demand is one degree lower (level 3) – as these two parameters are seen to be logically complementary to the group of Organisational ('O') parameters at this stage of the project.

In the next version of this Maturity Reference Document, due early 2018, this approach will be extended to cover all 44 SIM3 parameters.

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 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

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