GFCE
Global Forum on Cyber Expertise

CALL FOR PARTICIPATION

CSIRT Maturity Framework
stimulating the evolution of the maturity of national CSIRTs

Cybersecurity is a key global challenge to ensure a prosperous digital future. To live up to the cybersecurity challenge, nations are developing cybersecurity ecosystems: dynamic systems in which public and private actors interact intensively to enable the digitalization of society. As digitalization takes place at high speed, cybersecurity ecosystems must evolve quickly as well. The GFCE aims to develop cybersecurity frameworks applicable and usable for the development of digital ecosystems worldwide.
Key cybersecurity ecosystems elements are reflected in the five topics of the Global Agenda on Cyber Capacity Building. The CSIRT Maturity Initiative will make a CSIRT Maturity Framework available.

Developing cybersecurity ecosystem maturity models are a significant and urgent challenge. In the CSIRT area, a maturity model by the name of SIM3 has existed since 2008 and has been presented all over the world. It is extensively used in Europe and Japan, and has also been adopted by the GFCE, and by FIRST, the worldwide forum for CSIRTs. ENISA has embedded SIM3 into a framework to support the increase of national CSIRTs' maturity and to improve the cooperation between teams. This framework can be readily adapted for global use and will benefit all national CSIRTs – regardless their maturity levels. The purpose of this GFCE Initiative is to undertake this adaptation and present the results to the GFCE and the next Global Conference on Cyber Space.

CSIRT Maturity Framework

National CSIRT configurations vary in several ways. Variation can be seen in the fact that some national teams focus on the protection of the country's critical information infrastructure, whereas others have a significantly wider national scope. But also, variations in set-up and organizational embedding exist. Regardless such differences, all teams can benefit from a maturity framework that allows them to assess where they are, and what needs to be done to increase maturity.

Additionally, a maturity framework could leverage a "baseline" for CSIRT configurations, which paves the way for closer national CSIRT cooperation. By setting a maturity baseline, a standard is set for teams that (want to) establish cooperation. For instance, in a certain region, or as part of a political or economic cooperation.

For such a maturity framework to be successful worldwide, it needs to build on shared concepts that are understandable and valuable worldwide. Fortunately, the CSIRT community has been cooperating worldwide ever since its inception in 1989 – and therefore the development of frameworks for CSIRTs has always taken place in the global community.
With regards to CSIRT maturity, the leading model is named SIM3 and though it was developed in Europe in 2008, it was meant for worldwide use right from the start and therefore lacks any kind of regional focus. SIM3 has been presented to the global CSIRT community regularly, which led to its widespread adoption not only in Europe, but also in Japan, by the Nippon CSIRT Association (over 300 members). The GFCE acknowledged SIM3 as the backbone for the GFCE supported "GFCE CSIRT Maturity Kit" (CMK) in 2015. The CMK Is a structured approach to create and further develop mature CSIRTs. Continued global cooperation between 2015 and today by the GFCE, FIRST, ITU and other stakeholders, have led to a shared understanding in which SIM3 is the yardstick for CSIRT maturity overall, whereas the FIRST CSIRT Services Framework serves to define CSIRT services in more depth. These approaches have been designed in such a way that both complement each other. Recently, FIRST has also adopted SIM3 for the further development of their membership model.

The GFCE CSIRT Maturity Initiative published a “Global Good Practices - National Computer Security Incident Response Teams” in 2017. This global good practice proposed “good practices” on measuring maturity and proposed to adopt the use of SIM3. Quoted in full:

> *Another option is to define a maturity growth path. The latter approach has been adopted by the CSIRTs network, the co-operation of the national CSIRTs of the EU member states, who have defined a growth path based on SIM3 that goes from “basic” maturity level, via “intermediate” to “certifiable”. Measurements here are planned to be based on a combination of self-assessments and peer reviews. Different communities of CSIRTs can of course make their own choices in regard the SIM3 levels that they want to achieve – although some level of commonality in regard maturity at least between national CSIRTs worldwide would be helpful.*

This CSIRT maturity framework for national CSIRTs, championed by ENISA, has already been tested in 2017-18 and has been formally accepted by the EU community of national CSIRTs. As part of this framework, a SIM3 maturity self-assessment tool was made available. Framework and tools are publicly available online and maintained by ENISA.

There is the opportunity to generalize this framework in order to make it suitable for use worldwide. In communication with the not-for-profit Open CSIRT Foundation (OCF), who maintains and develops SIM3, with ENISA and the authors of the afore mentioned framework, it has been established that this should be relatively easy to do. SIM3 has a global outlook and endorsement already. The CSIRT Maturity Framework may have been written to suit the needs of national teams in the EU, however the approach taken is applicable worldwide. National CSIRTs have similar challenges all over the world, as well as the need to increase maturity.

It is expected that the diverse and global footprint of GFCE working group B will help to arrive at a CSIRT Maturity Framework that can be used successfully all over the world. To further optimize the end result, known experts from the global CSIRT community, who are not members of the working group already, will be consulted. Most of these experts have been involved in the previous GFCE work on CSIRT maturity. Among them are also the originators of the maturity approaches discussed above, which means that a wealth of knowledge and experience in this area is readily available within this project.

The resulting Framework can be used by all nation state CSIRTs, whether they be more governmentally oriented, or responsible for critical infrastructure or with an even broader national scope, as a way of helping their members to further develop the maturity of their CSIRTs.

The same Framework can be used as basis for an international stocktaking exercise. This stocktaking exercise will enable nations to identify what levels of maturity have been reached already, and what may still be lagging behind. Such knowledge is crucial for the development of national and critical infrastructure CSIRTs, and also sets the basis for such teams to improve the way(s) in which they work together. It can also serve as the basis for more in depth cooperation e.g. inside regional communities.

Call for participation

Initiated by the Netherlands, the GFCE CSIRT Maturity Initiative contributes to international cyber capacity building by publishing good practices, connecting and working together with experts and government officials. To ensure global applicability, we invite all partners and nations to contribute!

POINTS OF CONTACT

CSIRT maturity
Don Stikvoort MSc,
don.stikvoort@elsinore.nl

General coordination
Ms. Nynke Stegink, Dutch National
Cyber Security Center, NCSC-NL,
nynke.stegink@ncsc.nl

Website:
https://www.thegfce.com/Initiatives

GFCE
Global Forum on Cyber Expertise