TRAININGS FOR CSIRTS

ENISA started developing training material for CSIRTs in 2008 and has since produced more than 40 training topics divided in four main areas: Technical, Operational, Setting up a CSIRT and Legal - Cooperation. This content comprises of essential material to develop skills of incident responders and technical knowledge in the field of Operational Security. The training material includes tutorials for teachers, handouts for students and virtual images to support hands-on activities in the training session.

After the introduction of the NIS Directive, ENISA moved to a sectoral approach for trainings, developing and delivering these technical trainings according to the needs of the sectors covered by the Directive i.e. operators of essential services (e.g. aviation, energy or finance).

Through ENISA organised courses around 200 cybersecurity specialists are trained per year.

Trainings for CSIRTs by ENISA are to:

- support EU Member States to protect EU Digital Single Market
- raise the next generation of cybersecurity professional
- improve national incident response capability
- help operators of essential services to prevent incidents and protect assets in their networks.

https://www.enisa.europa.eu/trainings

ENISA trains
200 cybersecurity specialists per year

COMMUNITY PROJECTS

Reference Security Incident Classification Taxonomy

CSIRTs daily work relies more and more on tools and platforms, which are the result of community driven projects. The Reference Taxonomy is one example of an open-source CSIRT community initiative, which ENISA is contributing to and promoting. In 2017, ENISA together with the TF-CSIRT community agreed to create the 'Reference Security Incident Taxonomy Working Group' (RSIT WG) to promote, develop and maintain the Reference Taxonomy initiative.

Today the working group consists of more than 50 participants from over 20 European countries and meet three times a year to discuss future steps to improve incident data exchange. The machine and human readable versions of the Reference Taxonomy are available on the RSIT WG GitHub repository.

Reference Taxonomy benefits:

- to ensure that CSIRTs are 'speaking the same language'
- to facilitate sharing across different CSIRTs
- to facilitate the harmonisation of statistics between the CSIRT community
- to facilitate translation between different taxonomies, without disruption or need for major overhaul
- to get ready for automated information exchange.

https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

CONTACT

CSIRT-Relations@enisa.europa.eu
PGP key AAE2 1577 19C4 B3BE EDF7
0669 31E7 77EC 66B6 052A
www.enisa.europa.eu

European Union Agency for Cybersecurity
1 Vasilissis Sofias Str Maroussi 151 24, Attiki, Greece

EUROPEAN UNION AGENCY FOR CYBERSECURITY

BOLSTERING INCIDENT RESPONSE IN EUROPE

CSIRTS IN EUROPE

Since 2004, ENISA has been supporting the Incident Response community to build and advance Computer Security Incident Response Team (CSIRT) capabilities by providing capacity-building opportunities and by publishing over 70 dedicated studies and practices.

There are currently more than 480 teams publicly listed in the ENISA Inventory. ENISA sets up, tests and supports the development of capabilities for different type of CSIRTs around Europe. The Agency's goal is to define minimum common baseline practices across the EU, which will help to improve incident response preparedness, information exchange and operational cooperation for the next generation of cyber-attacks.

ENISA also works closely with existing CSIRT communities and organisations to foster better cooperation and information sharing through community projects and initiatives for stronger incident response in Europe.

https://www.enisa.europa.eu/csirts-map

More than
480 CSIRTs
in the ENISA inventory

CSIRTS NETWORK AND ENISA

The CSIRTs Network, composed of EU Member States and EU institutions' appointed CSIRTs was established by the NIS Directive and started its operations in 2017. It provides a forum of EU Member States where CSIRTs can actively cooperate and exchange information about cybersecurity events. The aim of the Network is to improve cross-border operational cooperation and support large-scale incident handling in a coordinated manner.

- ENISA provides the secretariat of the CSIRTs Network and actively supports the operational cooperation among CSIRTs by hosting a variety of communication tools, provoking discussions and by organising meetings to enable trust building. ENISA also provides its expertise and advice to the European Commission, which is an observer in the Network.
- ENISA continues to train and prepare CSIRTs for preventing future incidents and lays down the basis for future operational cooperation and capacity building – not only in times of emergency.
- ENISA's ultimate goal in the CSIRTs Network is to promote the highest level of incident response in the EU by providing professional and continuous support and expertise to all participating national and sectoral CSIRTs.

http://www.csirtnetwork.eu

The CSIRTs Network
started its operations in 2017

CSIRT CAPABILITIES AND MATURITY

Since 2009, ENISA has been contributing to support CSIRTs towards a higher maturity standard and advanced capabilities. ENISA assists newly and well-established incident response teams to set up their operations or develop their capabilities to face future cyber-attacks in a constantly evolving environment. ENISA maturity framework for CSIRTs enables teams to improve, mature and be better prepared to protect their constituencies. To improve capabilities evenly across a CSIRT's organisation, ENISA offers a method to evaluate maturity.

Maturity evaluation consists of two main components:

1. **ENISA CSIRT maturity assessment model**

   This model is based on the Security Incident Management Maturity Model (SIM3) that is a community driven effort to measure the maturity of CSIRTs. The ENISA CSIRT maturity assessment model also takes into account the requirements of the NIS Directive and results in a three tier assessment (Basic, Intermediate and Advanced).

2. **ENISA maturity evaluation methodology for CSIRTs consists of two main parts:**
   - Self-assessment survey - ENISA's online assessment tool.
   - Peer review workshop

Both components have been identified as indispensable elements for a successful and full-fledged evaluation process. Peer review is a process during which CSIRTs can evaluate each other based on the described methodology within parameters of the maturity assessment model.

https://www.enisa.europa.eu/csirts-maturity-sas