ENISA publishes training course material on network forensics for cybersecurity specialists

ENISA has introduced an updated and improved set of training materials on network forensics.

Published on January 30, 2019



Tagged with

* [Training](https://www.enisa.europa.eu/search?Subject%3Alist=Training)
* [CSIRTs](https://www.enisa.europa.eu/search?Subject%3Alist=CSIRTs)

Based on current best practices, the training includes performance indicators and means that will help those who take it increase their operational skills of tackling cyber-incidents.

Network forensics is more important than ever, since more and more data is sent via networks and the internet. When there is a security incident, network forensics can help reduce the time needed to go from Detection to Containment – an essential step in any major security incident.

When used proactively, network forensics provides a better picture of what your network’s ‘normal’ traffic looks like, leading to more intelligent alerting and less false positives.

ENISA makes available a ready-to-use version, including manuals for trainers and students, and provides tools and data related to exercise scenarios through Virtual Machines.

The training consists mainly of exercises focused on logging and monitoring, detection, and analysis or data interpretation. For example, one exercise deals with an attack on an ICS/SCADA environment in the energy sector. It starts with the preparation phase and it is followed by the incident analysis and post-incident activity.

Other scenarios within the training refer to how to detect “exfiltration” in a large finance corporation environment, or the analysis of an airport third-party VPN connection compromise.

One of ENISA’s main priorities is to deliver high-quality capacity-building material and activities for the EU Member States’ CSIRTs, to manage cybersecurity threats and incidents efficiently. Within this area, ENISA provides guidance on key elements of network and information security, in line with the current technologies and methodologies.

In February 2018, ENISA launched a project aimed at updating the content of the already existing CSIRT training material produced since 2008, in the area of network forensics.

For the full training material visit: [Introduction to Network Forensics](http://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#network_forensics)

**Note for editors**

ICS/SCADA are industrial control systems that make all sorts of equipment and even complete energy and chemical plants reachable and controllable via the network.

Exfiltration is data theft, followed by sending the data out to an outside collector – a significant risk for companies, which can lead to lawsuits, high financial sanctions, reputation damage or the disclosure of company secrets or strategic documents.

According to the NIS Directive, CSIRTs – Computer Security Incident Response Teams – are specialised national authorities in the EU Member States responsible for monitoring incidents at national level, providing early warning, alerts and information to relevant stakeholders about risks and incidents, responding to incidents, providing dynamic risk, incident analysis, and increasing situational awareness.