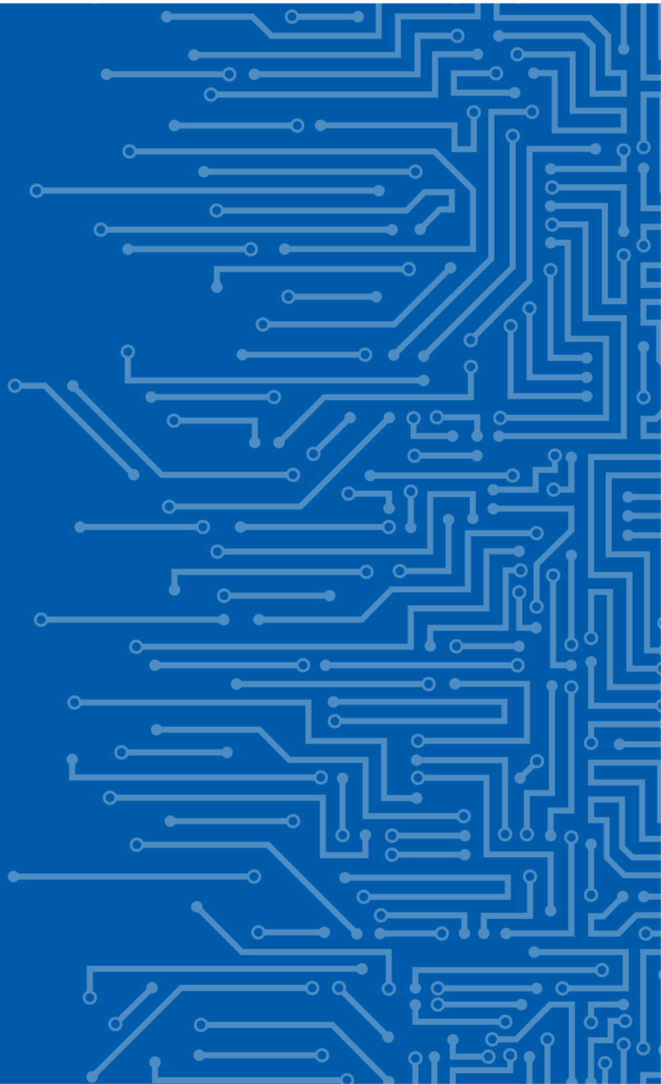
THE EU CYBERSECURITY AGENCY

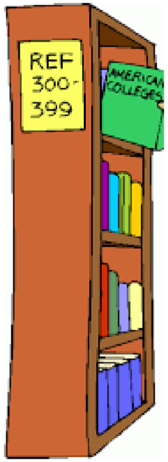
TRAINING IN INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS)

Fabio Di Franco, Ph.D.
SNE in COD3 – Operational Security Unit

29 | 01 | 2019



TRAINING



CONTENT

AUDIENCE

Creation of New Material

Update the material

ENISA activities in cyber education and training

On-line training on ENISA website

Training for cybersecurity specialist

Summer school

ENISA-FORTH
SUMMER SCHOOL
on Network &
Information Security

Ad hoc on-site training

On requests of member states and EU institutions

On line training material

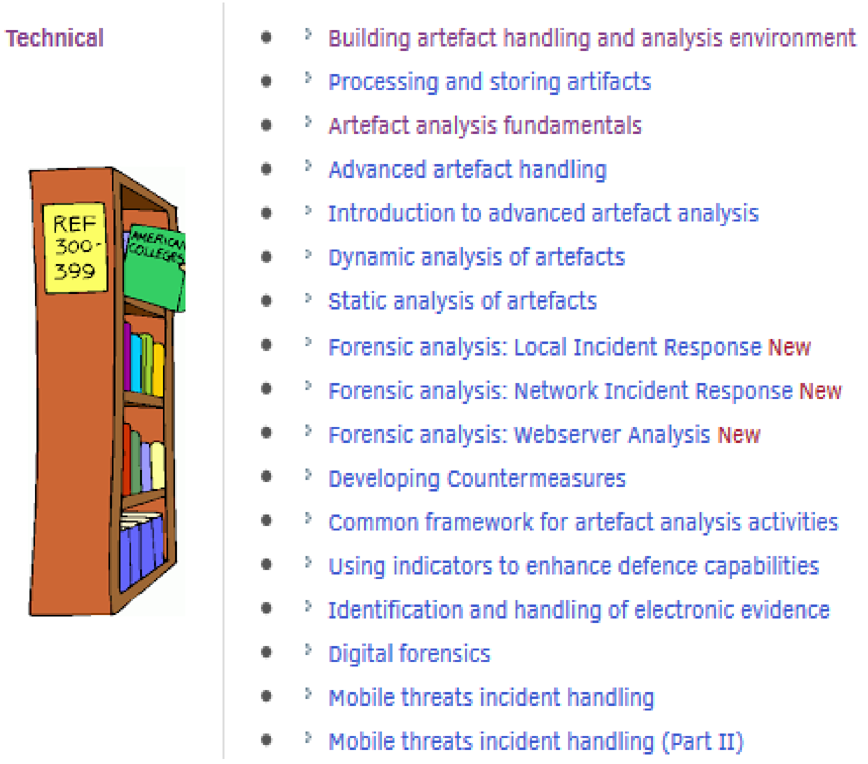
In the field of information security and for the CSIRT community

Technical

Operational

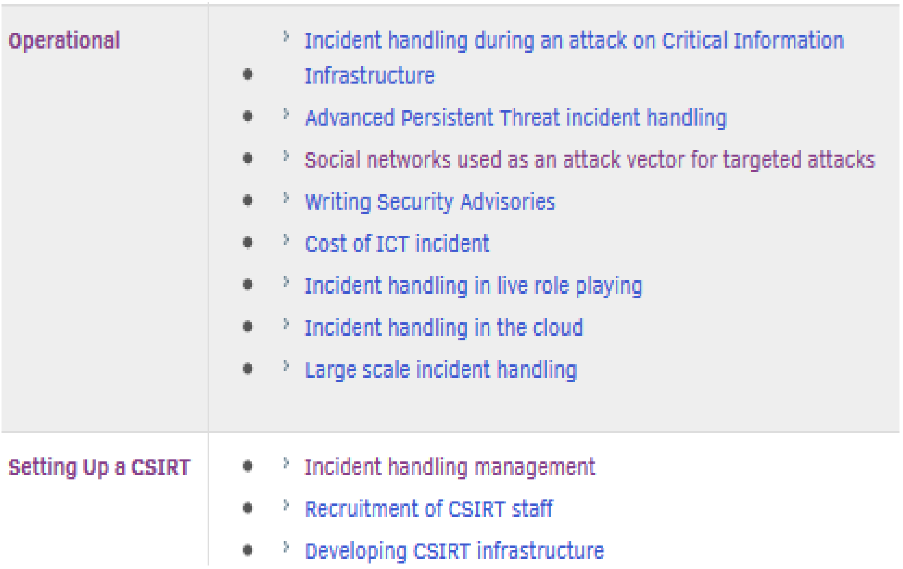
Legal and Cooperation

Setting up the CSIRT



Technical

- Building artefact handling and analysis environment
- Processing and storing artifacts
- Artefact analysis fundamentals
- Advanced artefact handling
- Introduction to advanced artefact analysis
- Dynamic analysis of artefacts
- Static analysis of artefacts
- Forensic analysis: Local Incident Response New
- Forensic analysis: Network Incident Response New
- Forensic analysis: Webserver Analysis New
- Developing Countermeasures
- Common framework for artefact analysis activities
- Using indicators to enhance defence capabilities
- Identification and handling of electronic evidence
- Digital forensics
- Mobile threats incident handling
- Mobile threats incident handling (Part II)

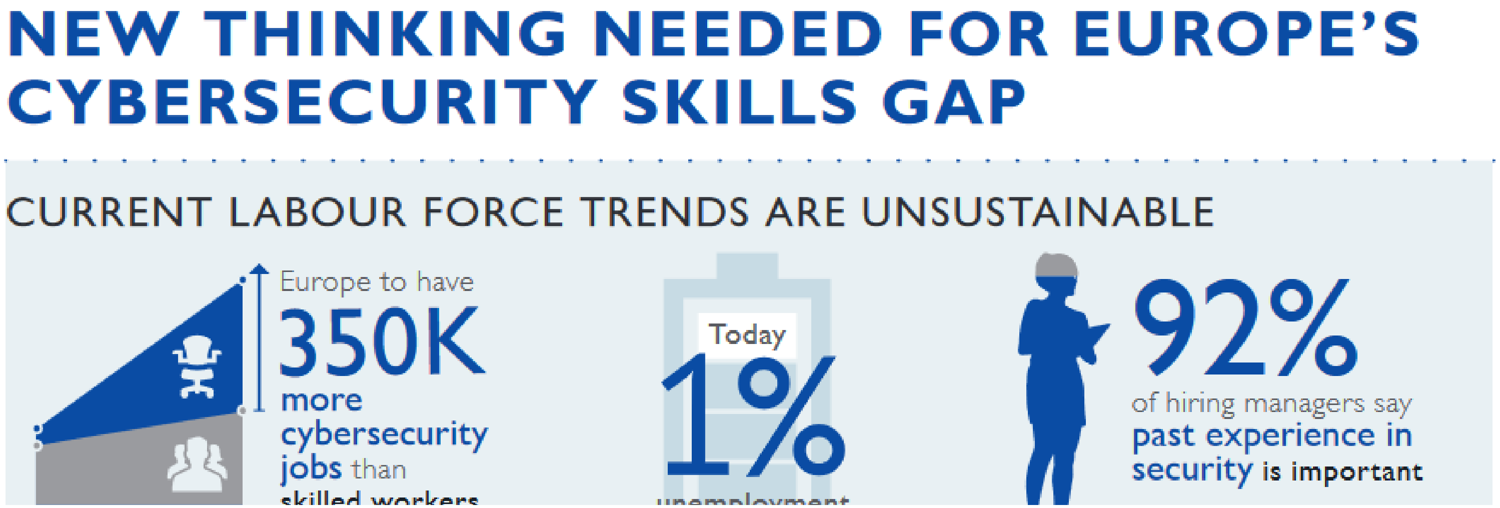


Operational

- Incident handling during an attack on Critical Information Infrastructure
- Advanced Persistent Threat incident handling
- Social networks used as an attack vector for targeted attacks
- Writing Security Advisories
- Cost of ICT incident
- Incident handling in live role playing
- Incident handling in the cloud
- Large scale incident handling

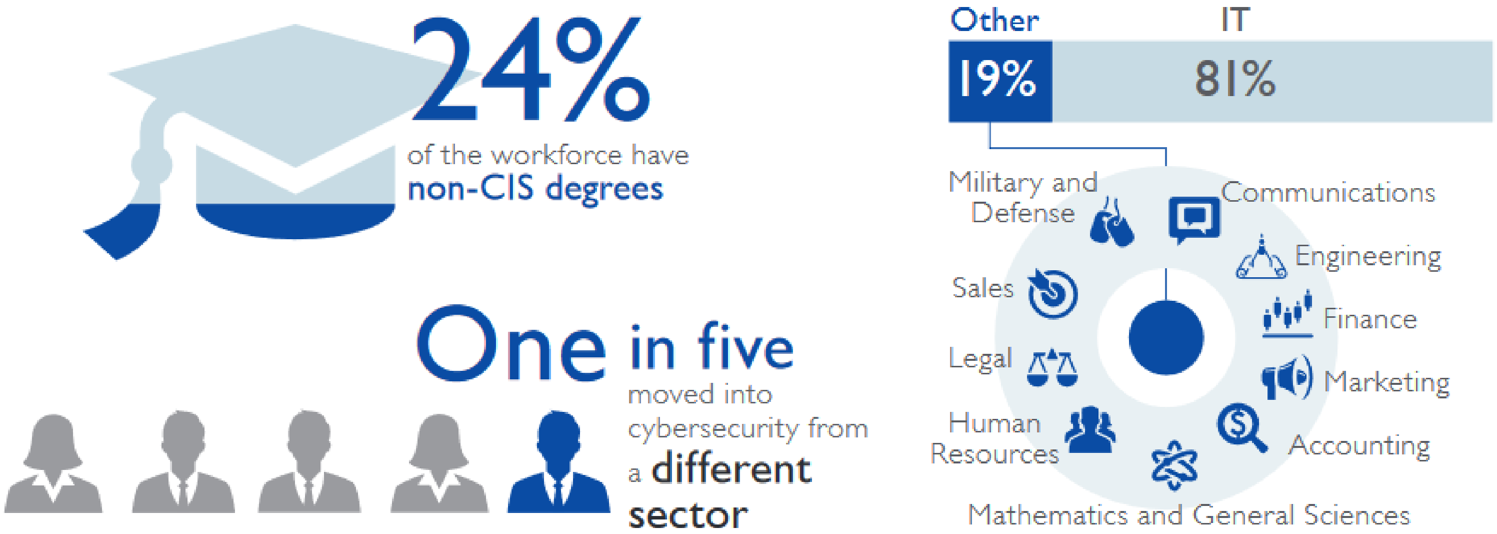
Setting Up a CSIRT

- Incident handling management
- Recruitment of CSIRT staff
- Developing CSIRT infrastructure



Do you have enough cybersecurity experts as civil servants?

Which kind of expertise in cybersecurity is mostly required in the public sector?



2017 Global Information Security Workforce Study

New Training material in
Information Security Management

- Reinforce knowledge in cybersecurity.
- Improve skills and abilities in order to protect information and IT systems
- Implement information security policy
- Analyze critical assets and identify weaknesses and vulnerability to intrusion or attack
- Develop a business continuity plan

Objective of the training:

Increase Capacity in information security in the public sector

Improve CIS skills and competencies of civil servants in order to occupy positions in information security management

Updated and new trainings will be accessible on ENISA e-learning platform

SUPPORT NEEDED FROM MEMBER STATES

Collaborations for developing joint material with national partners (eg. universities)

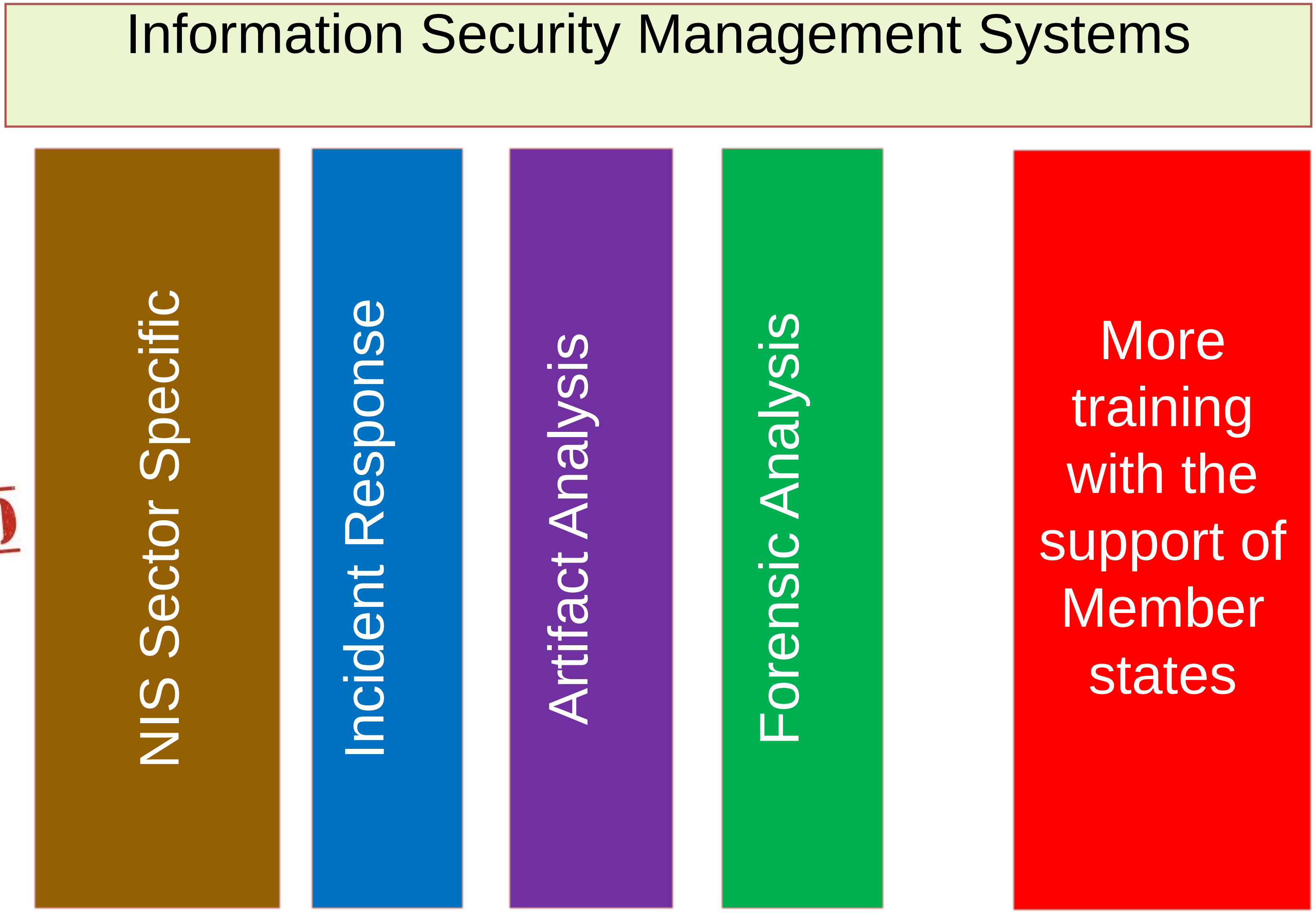
One–stop shop for cybersecurity training in Europe

Support of cyber-security training at national level

Localization of the material (translation)

Summary: E-learning trainings in 2019

NEW



Information Security Management Systems

NIS Sector Specific

Incident Response

Artifact Analysis

Forensic Analysis

More training with the support of Member states

NEW

&

UPDATED

Technical Training

THANKS

Discussion points:

Collaborations for developing joint material with national partners (eg. universities)

How to support cyber security training and Localization of the material (translation)

Enisa as One–stop shop for cybersecurity training in Europe

fabio.difranco@enisa.europa.eu