CYNET-CSIRT's founding journey has reached a successful destination

Co-financed by the European Union
Connecting Europe Facility

Talk Outline

- Main objective of the Action
- Establishment and Key Responsibilities of CYNET-CSIRT
- Services
- Incident Report Forms
- International Collaborations and Achievements of the CYNET-CSIRT Team
- Development of Tools for Cyber Attack Prevention
- Testing Scenarios & Results
- Annual CYNET-CSIRT Incidents
- Training of the CYNET-CSIRT Team
- New era for CYNET-CSIRT
- Lessons Learned

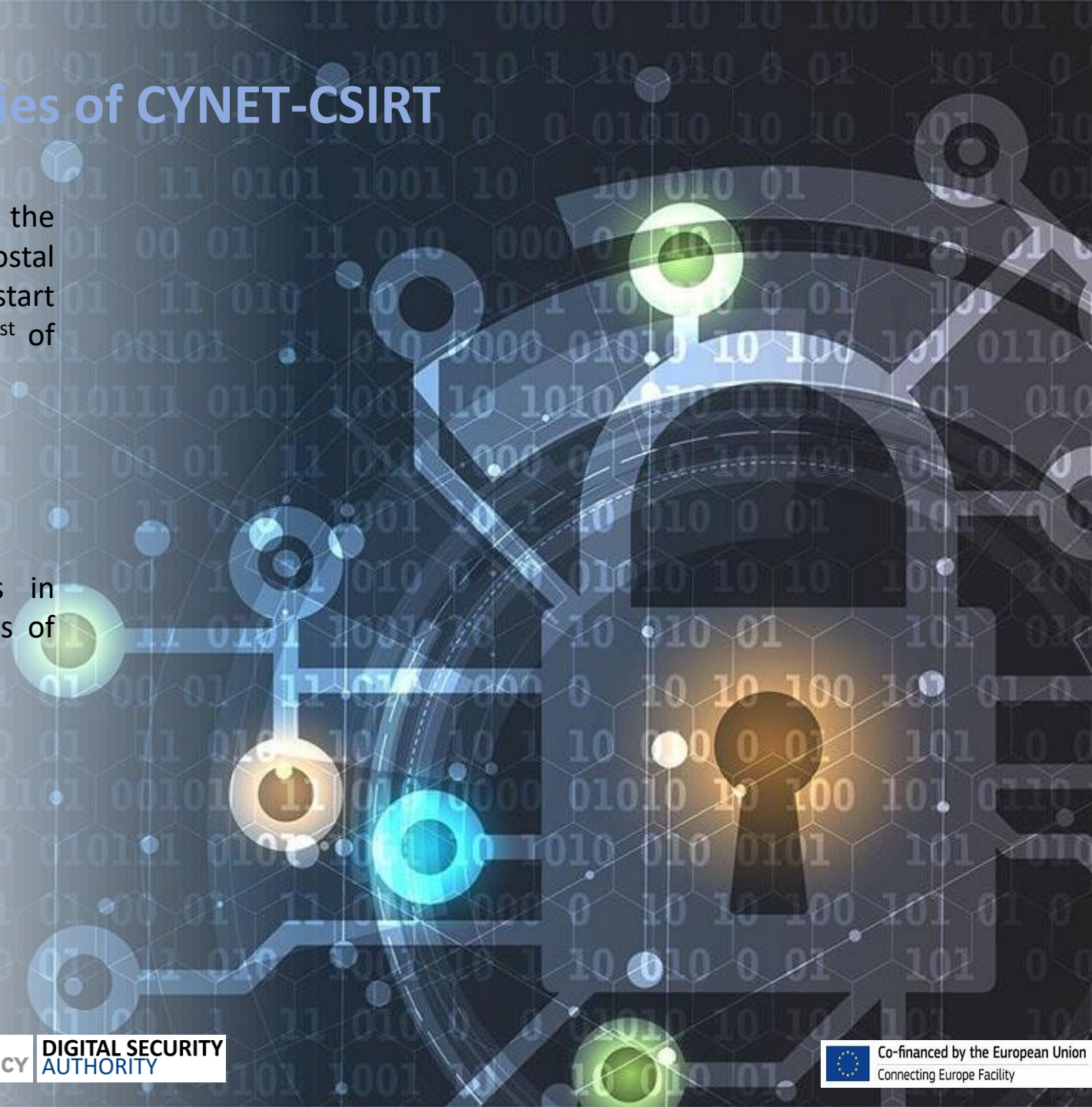
Co-financed by the European Union
Connecting Europe Facility

Establishment and Key Responsibilities of CYNET-CSIRT

- CYNET-CSIRT was established in 2017 according to the Commissioner of Electronic Communications and Postal Regulation decision Action No. 358/2010. The effective start date where the team went into operation was Thursday 1st of September 2018.

- Responsibilities of CYNET-CSIRT:

1. The response to the information security incidents in cooperation with the universities and research institutes of Cyprus, as well as similar organisations;
2. Awareness raising in the field of information security;
3. Cooperation with European CSIRT teams;



Co-financed by the European Union
Connecting Europe Facility

Services

- Reactive Services
  - Alerts & Warnings
  - Incident Response
    - Incident Triage
    - Incident Coordination
    - Incident Resolution

- Proactive Services
  - Security announcements
  - Real-time data analysis
  - Vulnerability analysis
  - Malware classification
  - Threat intelligence sharing

- Security Quality Management Services
  - Awareness Building
  - Education & Training

Co-financed by the European Union
Connecting Europe Facility

Incident Report Forms

- The incident report form is available on the website https://csirt.cynet.ac.cy. Incidents or related information can be reported via email on reporting.csirt@cynet.ac.cy or via the phone on 1490 on a 24/7 basis.

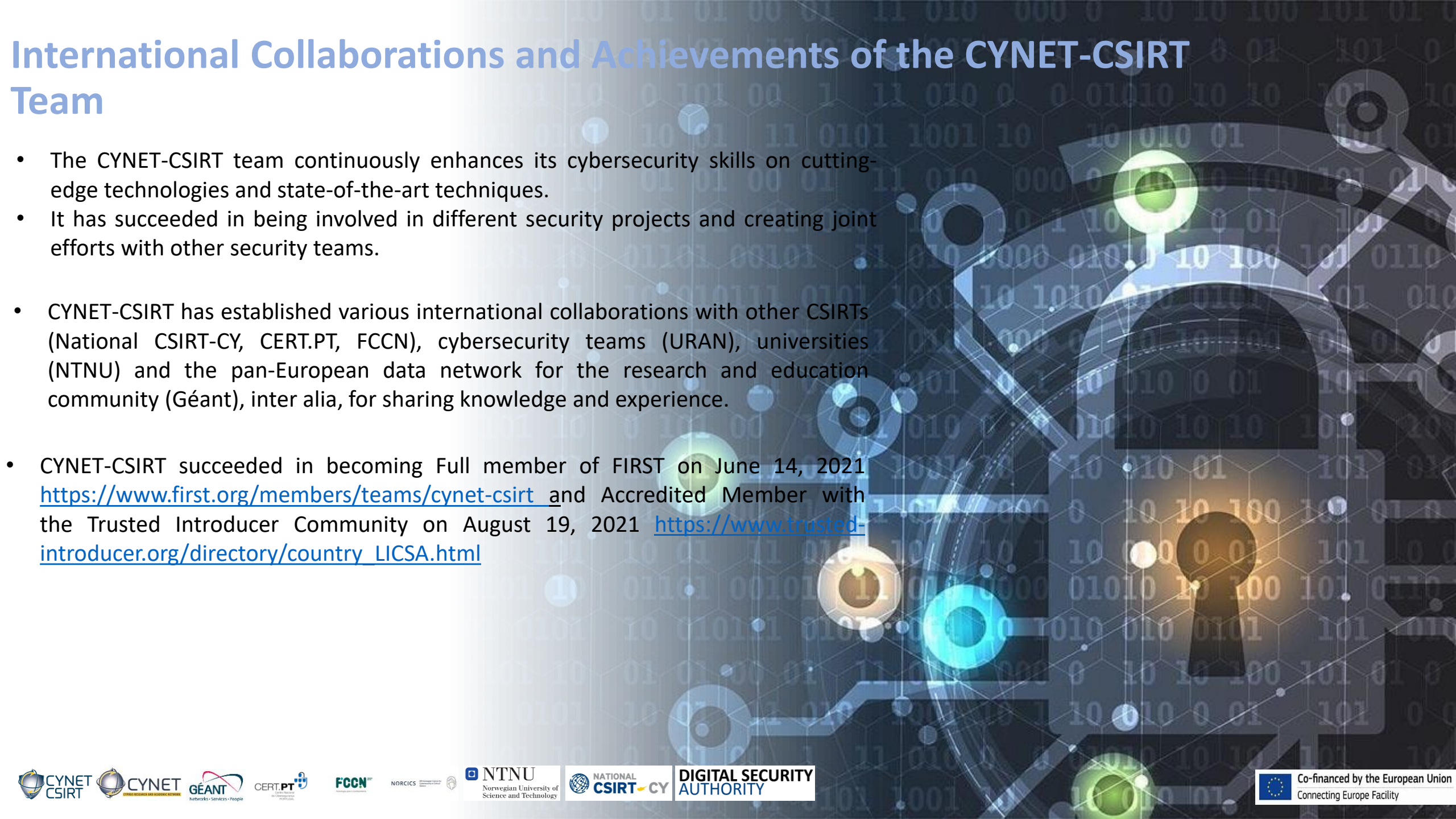
Co-financed by the European Union
Connecting Europe Facility

International Collaborations and Achievements of the CYNET-CSIRT Team

- The CYNET-CSIRT team continuously enhances its cybersecurity skills on cutting-edge technologies and state-of-the-art techniques.
- It has succeeded in being involved in different security projects and creating joint efforts with other security teams.

- CYNET-CSIRT has established various international collaborations with other CSIRTs (National CSIRT-CY, CERT.PT, FCCN), cybersecurity teams (URAN), universities (NTNU) and the pan-European data network for the research and education community (Géant), inter alia, for sharing knowledge and experience.

- CYNET-CSIRT succeeded in becoming Full member of FIRST on June 14, 2021 https://www.first.org/members/teams/cynet-csirt and Accredited Member with the Trusted Introducer Community on August 19, 2021 https://www.trusted-introducer.org/directory/country_LICSA.html



Co-financed by the European Union
Connecting Europe Facility

Development of Tools for Cyber Attack Prevention

- **Real-Time Data Analysis (RTDA):** A system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. The system passively records network traffic on the entire subnet for identifying particular patterns that are related with documented attacks. Once an attack is identified or abnormal behavior is observed, the alert is sent to the administrator.

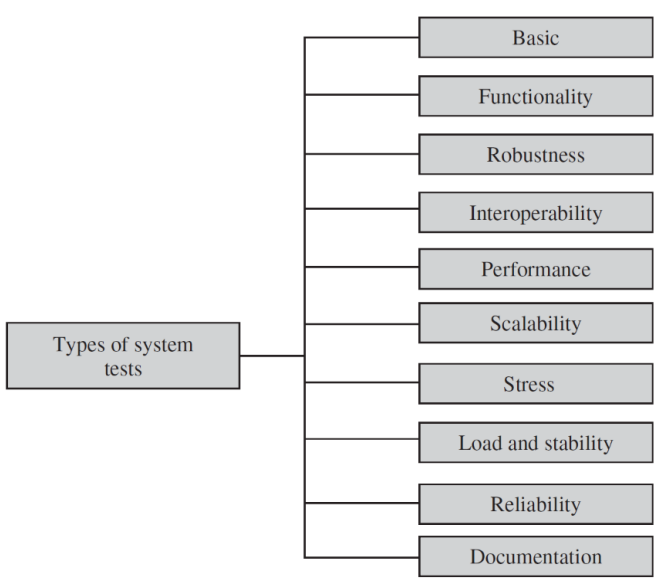
- **Malware Classification (MC):** A tool for labeling and categorizing an unidentified binary file under a particular class or family of other, previously identified malicious binary files. Such tools are usually operated by domain experts through and involve static and dynamic analysis of a given software.

- **Vulnerability Analysis (VA):** A tool for identifying and classifying potential vulnerabilities in several components in a network such as servers, applications, routers, and firewalls. The tool focuses on particular known vulnerabilities with an assigned CVE (Common Vulnerabilities and Exposures).

Co-financed by the European Union
Connecting Europe Facility

Testing Scenarios & Results

- **Taxonomy of system tests**



- **Results**

RTDA Tool: 99% of the benign activity was correctly classified, while 1% of the benign activity was incorrectly classified leading, again, to a low rate of false negatives.

MC tool: the percentage of successful identification and classification of malware is more than 90%

AV Tool: managed to scan a set of vulnerable hosts with an overall success of more than 99%.

Co-financed by the European Union
Connecting Europe Facility

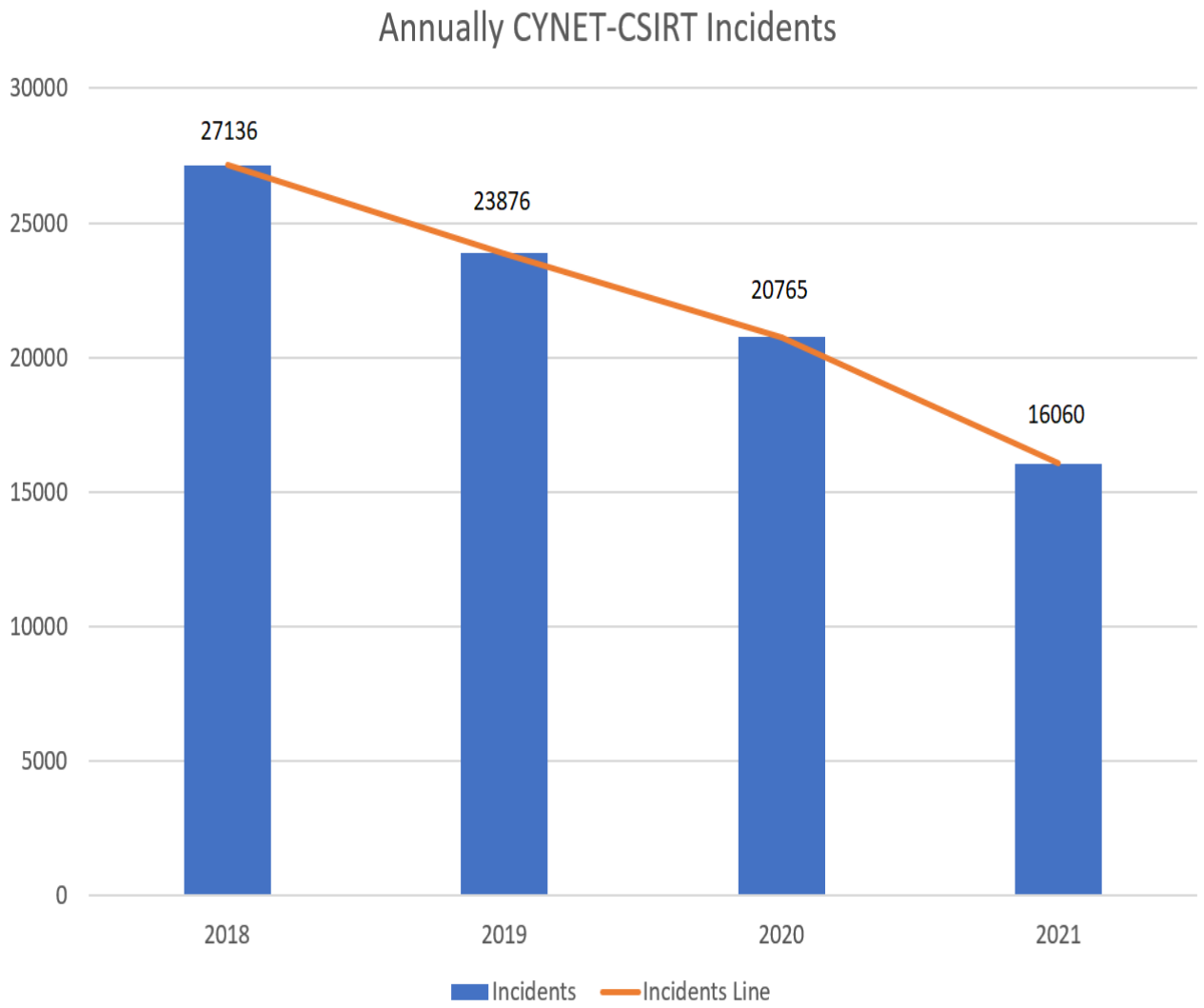
Training of the CYNET-CSIRT Team

- **A short overview of the Training Courses attended and certified by CYNET-CSIRT's Analysts:**

  - Defensive
    - Advanced incident handling and continuous security monitoring
    - Large-Scale Incident Handling
    - Threat Intelligence/Threat Hunting
    - Advanced Reverse Engineering
  - Offensive
    - Introduction to Penetration Testing
  - Forensics
    - Mobile Threats, Incident Handling & Malware Analysis and Memory Forensics
    - Digital Forensics acquisition, identification, validation and tools
    - Advanced Concepts in Digital Forensics
  - Malware Analysis
    - Advanced Malware Analysis & Threat Detection
    - Malware Analysis & Digital Forensics
  - SIM3 Certified Auditor

Co-financed by the European Union
Connecting Europe Facility

Annual CYNET-CSIRT Incidents



Co-financed by the European Union
Connecting Europe Facility

New era for CYNET-CSIRT

- **New services:**
  - Vulnerability Assessment (including website vulnerability assessment)
  - Social Engineering
  - Red Teaming
    - Penetration Testing
  - Cyber Security Continuous Monitoring

Co-financed by the European Union
Connecting Europe Facility

Lessons Learned

- Collaborations are, in fact, widely encouraged and promoted by ENISA within the CSIRTs community. A big part of a CSIRT collaboration is the exchange of knowledge and the enrichment of experience.
- We were all faced with the impacts of an unexpected circumstance, that of the COVID-19 pandemic, which drastically affected our plans for the most part of 2020.
- Another useful aspect proved to be the pre-existing knowledge of the National CSIRT-CY on fundamental issues.
- Finding effective solutions to complex problems isn't easy, but with the use of the right methods and state-of-the-art techniques, you can help your team be **more efficient** in the process.

Co-financed by the European Union
Connecting Europe Facility

Thank you for your attention!

Co-financed by the European Union
Connecting Europe Facility