CSIRT capacity building

Andrea Dufkova | CSIRT-relations, COD1

NLO meeting | Athens | June 8

European Union Agency for Network and Information Security

Capacity and community building for CSIRTs

2005 Start up program for CSIRTs (ENISA guidelines and support on how to set up and operate CSIRT)

2008 Focus on national and governmental CSIRTs – defining minimum requirements for operations (baseline capabilities for n/g CSIRTs)

2010 Cyber Europe Exercise (EUROPE's first ever EU cyber security exercise; continued in 2012, 2014, 2016)

2011 CSIRT and Law Enforcement cooperation support (information sharing and fight against cybercrime)

2013 Operational training program (for CSIRTs and other ICT security specialists)

2016 CSIRT network support (NISD)

Incident Response Teams worldwide

- ✓ **273 Europe**

(28 Germany, 22 UK, 17 France, 16 Spain, 16 Netherlands, 11 Sweden)

- ✓ **102 America**

(74 USA, 12 Canada, 7 Central America, 21 South America)

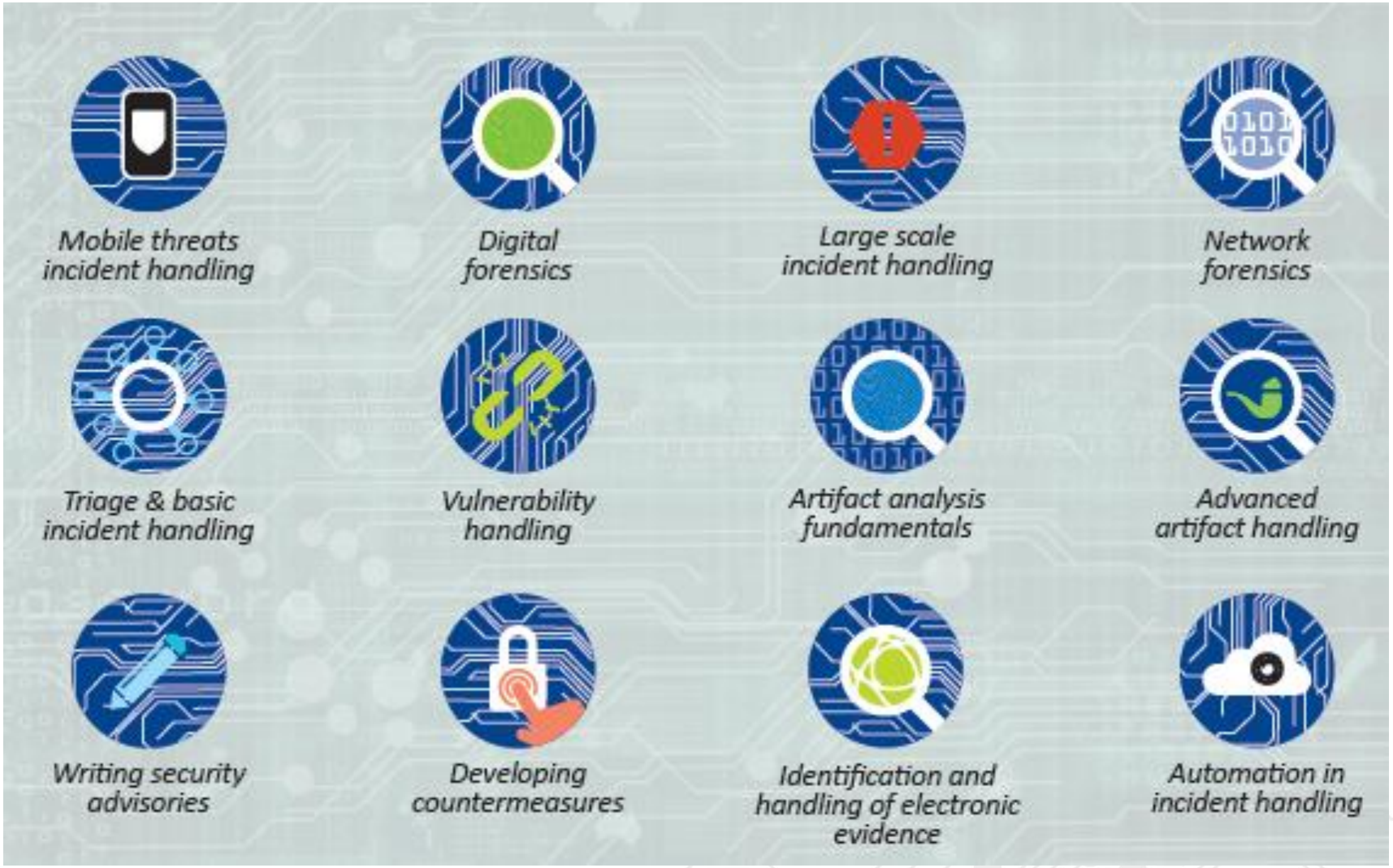
- ✓ **8 Africa**
- ✓ **6 Australia**
- ✓ **57 Asia**

(3 Russia, 4 China, 26 Japan, 8 Korea)

** source: ENISA CSIRT Inventory and FIRST db*

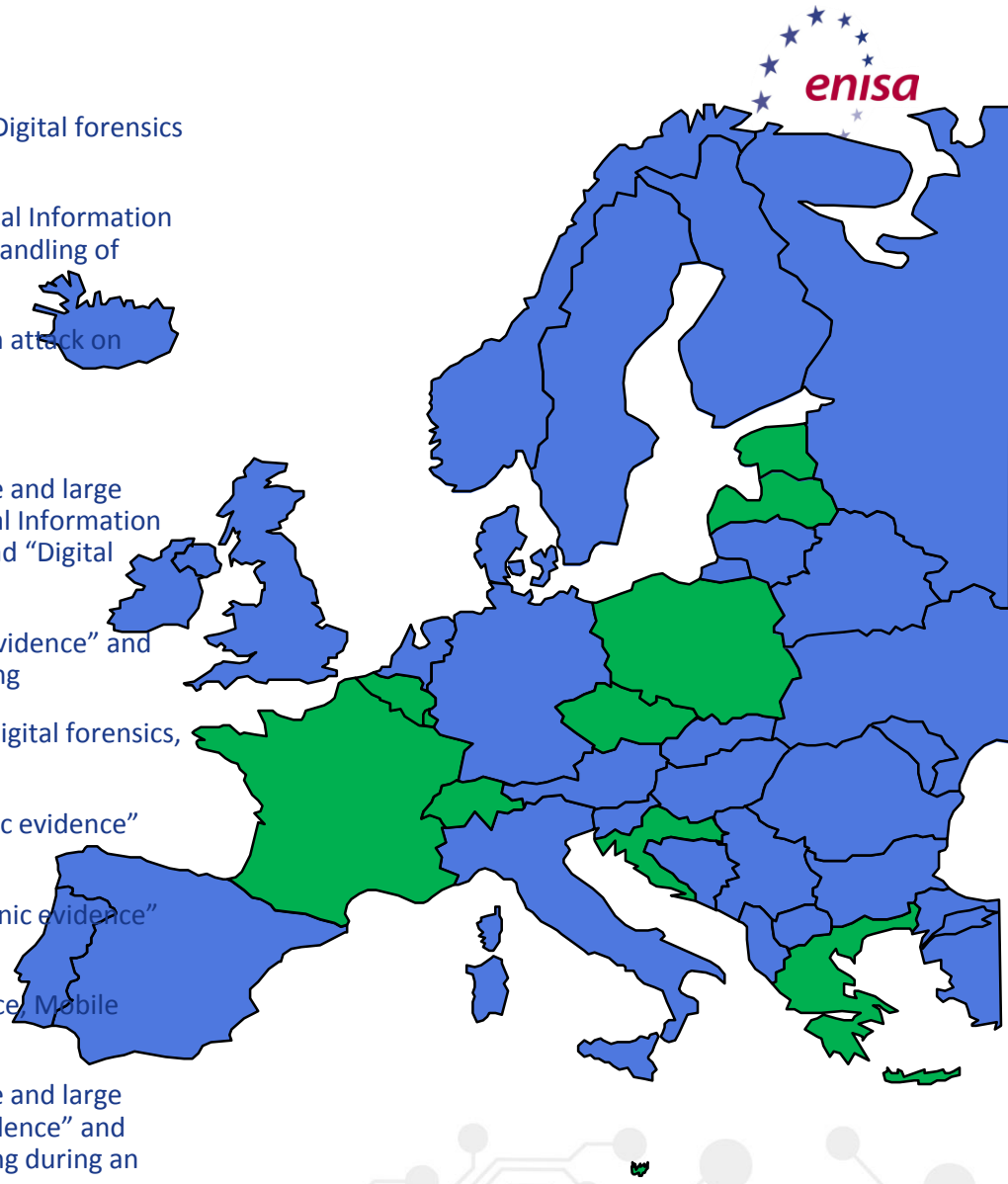
Capacity building

Training portfolio



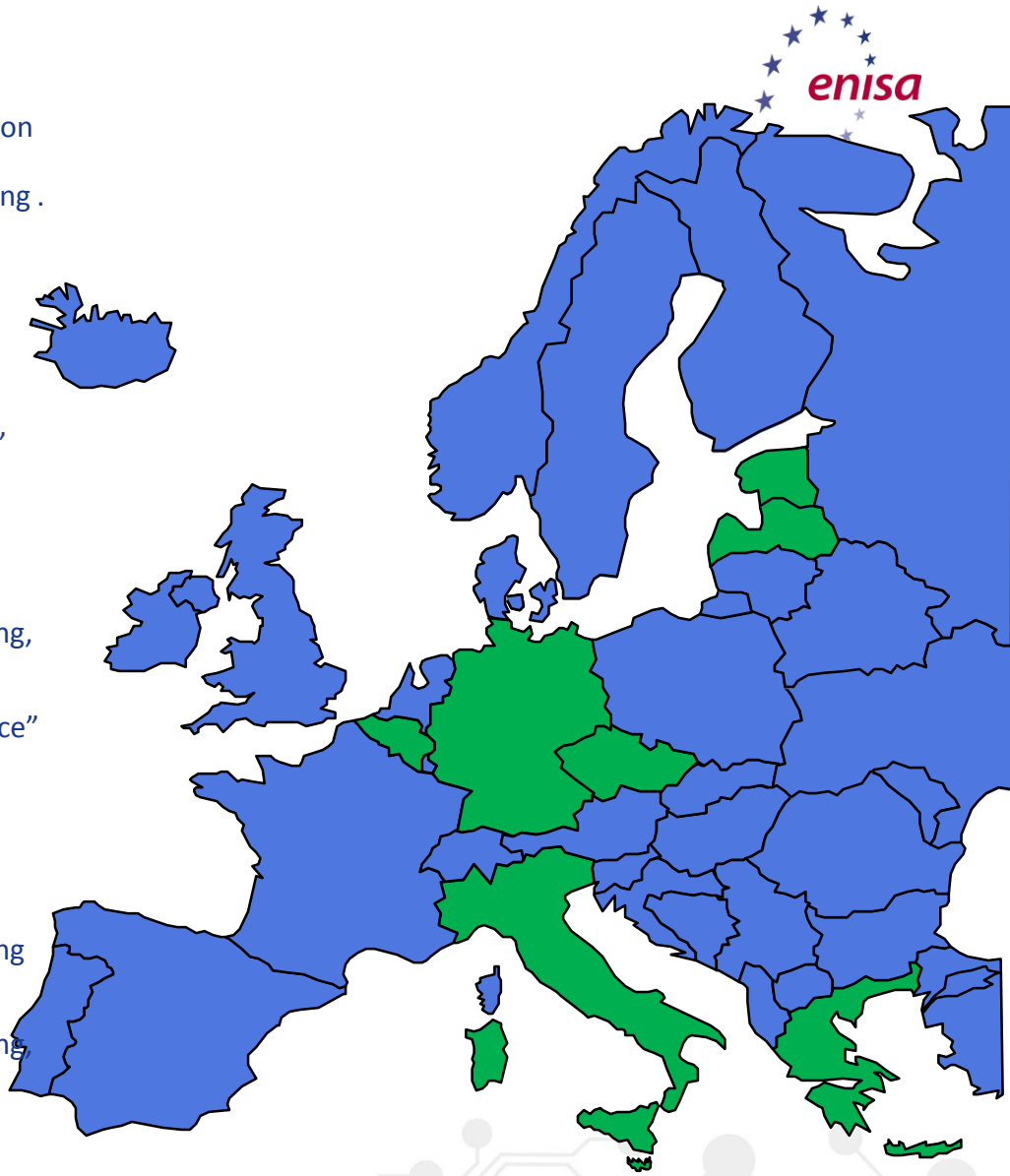
Trainings 2014

1. **TF-CSIRT**: “Identification and handling of electronic evidence” and “Digital forensics (Switzerland)
2. **Croatia (national CSIRT):** Incident handling during an attack on Critical Information Infrastructure, Mobile threats incident handling, Identification and handling of electronic evidence” and “Digital forensics, Network forensics
3. **Czech Republic (national CSIRT, CZ.NIC):** Incident handling during an attack on Critical Information Infrastructure, Mobile threats incident handling
4. **GEANT - TRANSITS**: Incident handling (France)
5. **Malta(CIP):** Introduction to Incident handling and procedures, Triage and large scale incident handling, Incident handling during an attack on Critical Information Infrastructure, Identification and handling of electronic evidence” and “Digital forensics
6. **Latvia(national CERT.LV) :**Identification and handling of electronic evidence” and “Digital forensics, Network forensics, Mobile threats incident handling
7. **EU ECSM:** Identification and handling of electronic evidence” and “Digital forensics, Mobile threats incident handling (Belgium)
8. **Luxembourg(CIRCL, Hack.lu):**Identification and handling of electronic evidence” and “Digital forensics, Mobile threats incident handling
9. **Greece (ISACA, KEMEA(GCC)):** Identification and handling of electronic evidence” and “Digital forensics, Mobile threats incident handling
10. **Poland (SCSConference):** Identifying and handling electronic evidence, Mobile threats incident handling
11. **Malta(CIP):** Introduction to Incident handling and procedures, Triage and large scale incident handling, Identification and handling of electronic evidence” and “Digital forensics, Mobile Threats Incident Handling, Incident handling during an attack on Critical Information Infrastructure
12. **CCDCOE**: Smartphone forensics, Mobile threats incident handling (Estonia)



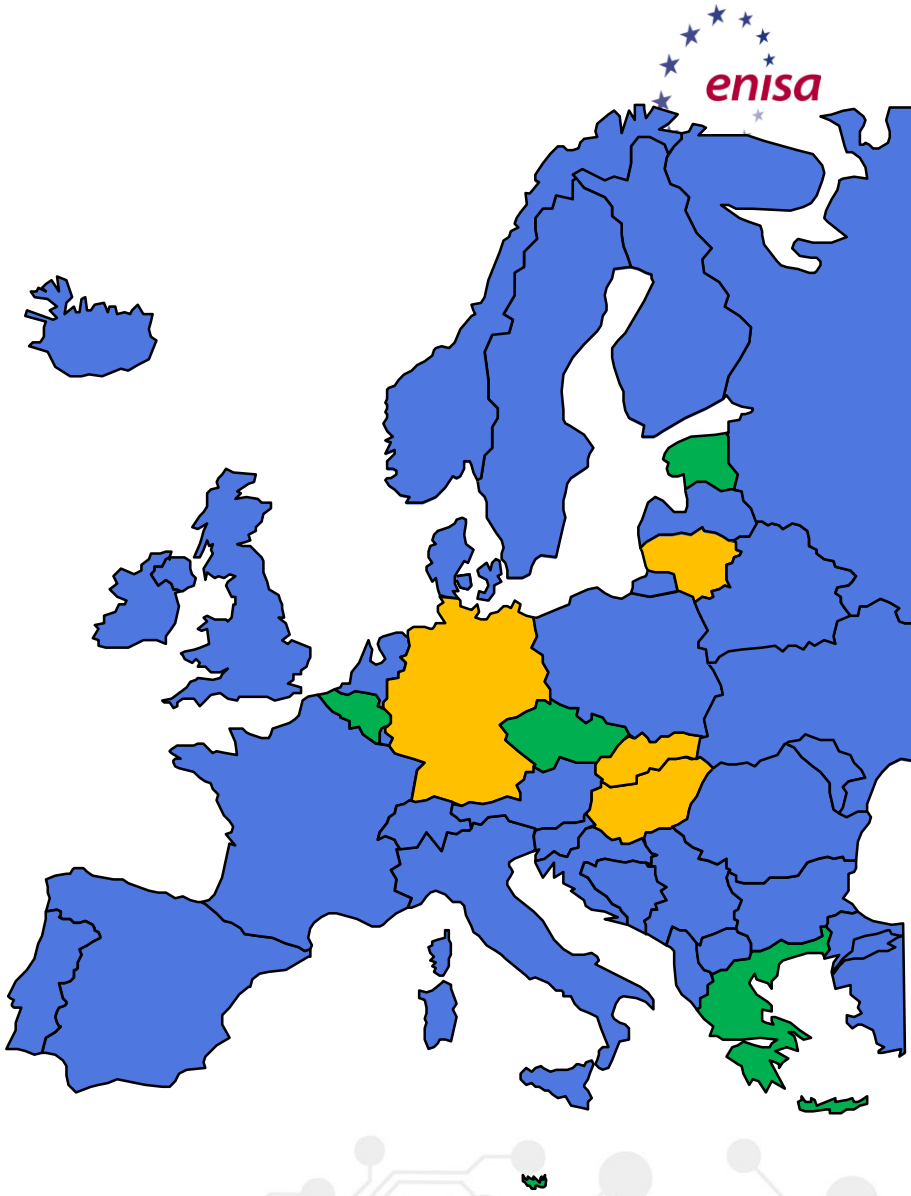
Trainings 2015

1. **Greece (Ministry of Education):** Network forensics, “Identification and handling of electronic evidence” and “Digital forensics”, Automation in incident handling, Mobile threats incident handling .
2. **CEPOL: “**Identification and handling of electronic evidence” and “Digital forensics”, Introduction to Incident handling and procedures (Estonia)
3. **Estonia (CERT.EE):** Incident handling automation
4. **Italy (ECSM)**: Identification and handling of electronic evidence” and “Digital forensics, Mobile threats incident handling
5. **FIRST**: **(Train the Trainers)** (Germany)
6. **Latvia (CERT.LV):** Identification and handling of electronic evidence” and “Digital forensics, Mobile threats incident handling, Artifact analysis
7. **Greece (ADAE):** Identification and handling of electronic evidence” and “Digital forensics, Mobile threats incident handling, Artifact analysis
8. **TF-CSIRT: (Train the Trainers)** (Estonia)
9. **Belgium (ECSM):** Identification and handling of electronic evidence” and “Digital forensics, Mobile threats incident handling
10. **Greece (KEMEA(GCC)**): Identification and handling of electronic evidence” and “Digital forensics, Mobile threats incident handling, Network forensics.
11. **GEANT - TRANSITS**: Artifact analysis (Czech Republic)
12. **CCDCOE:** Smartphone forensics, Mobile threats incident handling (Estonia)



Trainings 2016

1. **Belgium(national CERT.BE):** Triage and Basic Incident Handling, Artifact Analysis,
2. **Greece (Ministry of Interior, Hellenic National CERT):** Artifact Analysis, Mobile threats incident handling, “Identification and handling of electronic evidence” and “Digital forensics”
3. **Czech (national CSIRT/NIC.CZ):** Mobile threats incident handling
4. **Estonia (RIA):** Artifact Analysis, “Identification and handling of electronic evidence” and “Digital forensics”
5. **Malta(Cabinet Office of Prime Minister/CIP):** Artifact Analysis, Mobile threats incident handling, “Identification and handling of electronic evidence” and “Digital forensics”.
6. **Slovak (Ministry of Defense and national CSIRT.SK):** Artifact Analysis, Mobile threats incident handling, “Identification and handling of electronic evidence” and “Digital forensics”
7. **Lithuania (national Cyber Security Centre):** Artifact Analysis, Mobile threats incident handling, “Identification and handling of electronic evidence” and “Digital forensics”.
8. **Germany (BSI):**Smartphone forensics, Mobile threats incident handling
9. **Hungary (governmental CSIRT):** Triage and Basic Incident Handling, national cyber crisis cooperation exercise
10. **Sweden (MSB)** – regional training for Nordic countries
11. **Latvia (national CSIRT)** – regional training for Baltic countries
12. **Romania (national CSIRT)** – national training



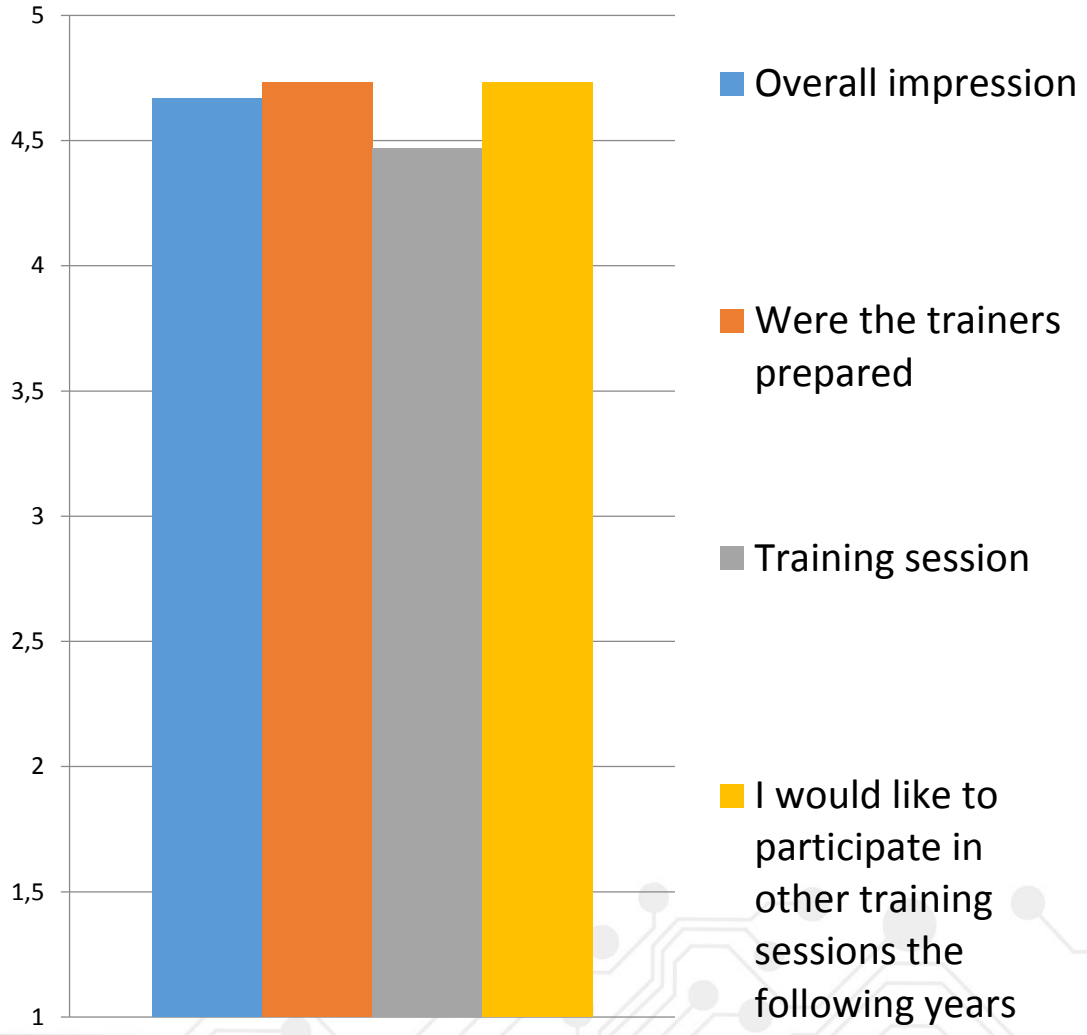
Success rate

Guiding potential trainers

Supporting with material

Creating joint efforts

Feedback 4,5 out of 5



Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu