EUROPEAN COMMISSION
NEIGHBOURHOOD AND ENLARGEMENT NEGOTIATIONS

C - Neighbourhood East and Institution Building
DG NEAR C1

EU4Digital

Cybersecurity EAST

EU4DIGITAL 4TH STEERING COMMITTEE **25TH OCTOBER 2022**

Project implemented by

GFA CONSULTING GROUP

eGA e-governance academy

DETECON CONSULTING

ACTION DIPLOMACY

Federal Office for Information Security

Besnik LIMAJ
Team Leader

Beneficiary
EaP Countries

PROJECT SYNOPSIS

1

Project Synopsis

Cybersecurity EAST

FUNDS 1

EU
DG NEAR

BUDGET 2

3.1 MILLION
EUR

DURATION 3

JAN - 2020
NOV - 2022

COUNTRIES 4

EASTERN
PARTNERSHIP
COUNTRIES

THREE COMPONENTS

COMPONENT 1

Approximation of legislations and legal frameworks in line with the EU NIS Directive

COMPONENT 2

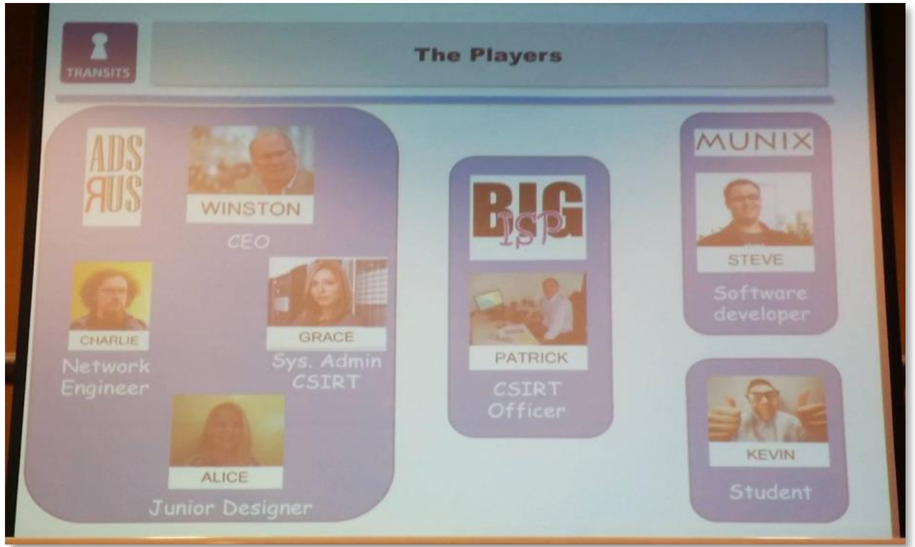
Identification of Operators of Essential Services (OES's) in line with NIS Directive

COMPONENT 3

Increased operational capabilities for cyber incidents and crisis management

METHODOLOGY

Cyber Security Table-Top Exercise
Simulation of Cyber Attack - Role playing exercise



TRANSITS

The Players

ADS R US

WINSTON
CEO

CHARLIE
Network Engineer

GRACE
Sys. Admin CSIRT

ALICE
Junior Designer

BIG ISP

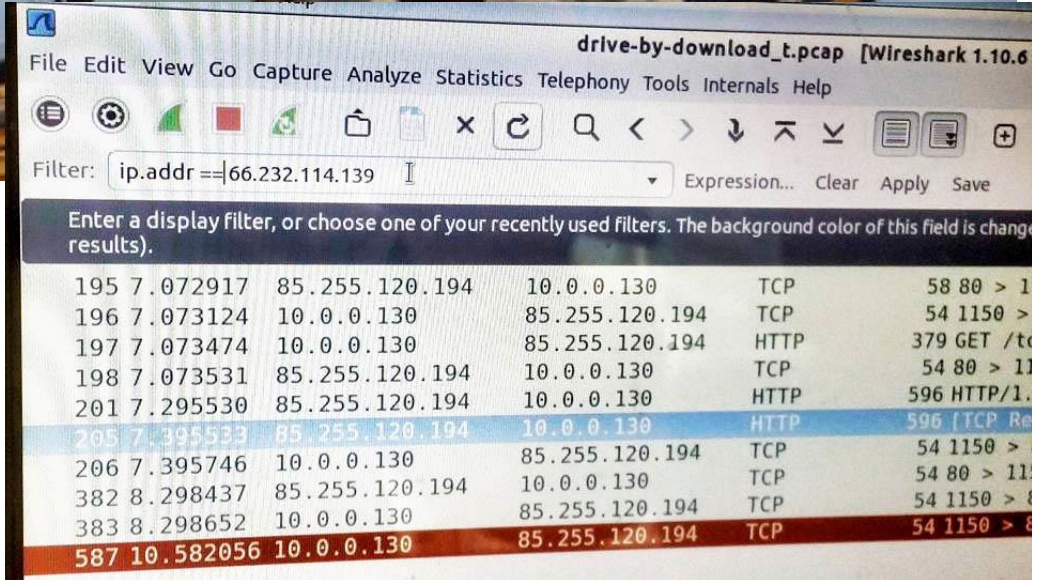
PATRICK
CSIRT Officer

MUNIX

STEVE
Software developer

KEVIN
Student

CYBER SECURITY TECHNICAL EXERCISE (CYBERDRILL)


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

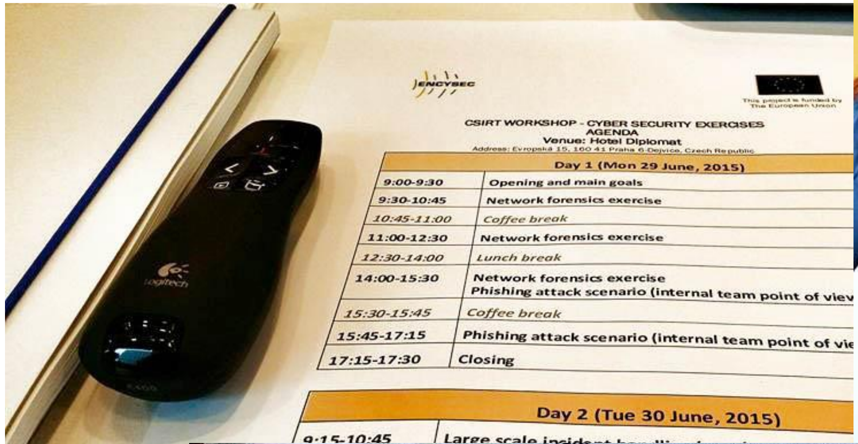
drive-by-download_t.pcap [Wireshark 1.10.6

Filter: ip.addr ==66.232.114.139

Enter a display filter, or choose one of your recently used filters. The background color of this field is chang
results).

```
195 7.072917  85.255.120.194   10.0.0.130       TCP    58 80 > 1
196 7.073124  10.0.0.130       85.255.120.194   TCP    54 1150 >
197 7.073474  10.0.0.130       85.255.120.194   HTTP   379 GET /t
198 7.073531  85.255.120.194   10.0.0.130       TCP    54 80 > 11
201 7.295530  85.255.120.194   10.0.0.130       HTTP   596 HTTP/1.
205 7.395533  85.255.120.194   10.0.0.130       HTTP   596 [TCP Re
206 7.395746  10.0.0.130       85.255.120.194   TCP    54 1150 >
382 8.298437  85.255.120.194   10.0.0.130       TCP    54 80 > 11
383 8.298652  10.0.0.130       85.255.120.194   TCP    54 1150 >
587 10.582056 10.0.0.130       85.255.120.194   TCP    54 1150 >
```

Cyber Security Technical Exercise



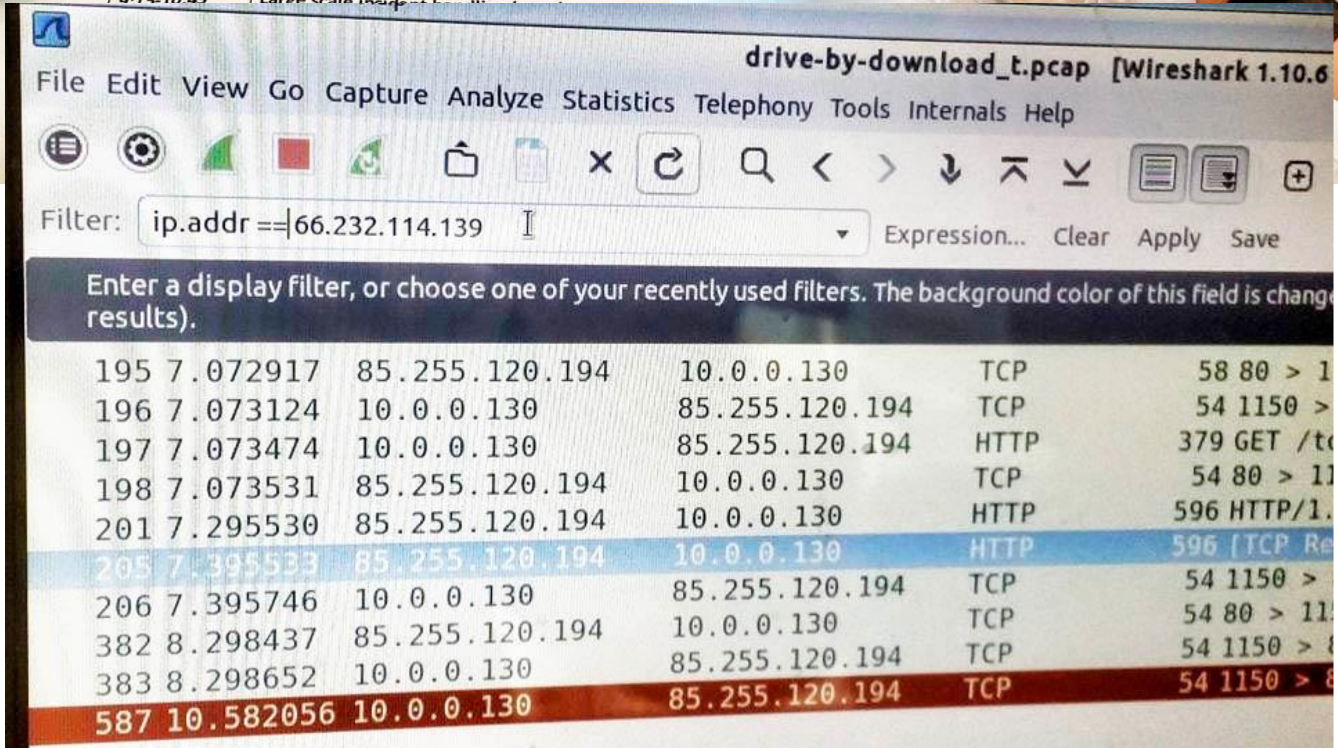
ENCYSEC

This project is funded by The European Union

CSIRT WORKSHOP - CYBER SECURITY EXERCISES
AGENDA
Venue: Hotel Diplomat
Address: Evropská 15, 160 41 Praha 6-Dejvice, Czech Republic

Day 1 (Mon 29 June, 2015)	
9:00-9:30	Opening and main goals
9:30-10:45	Network forensics exercise
10:45-11:00	*Coffee break*
11:00-12:30	Network forensics exercise
12:30-14:00	*Lunch break*
14:00-15:30	Network forensics exercise Phishing attack scenario (internal team point of viev
15:30-15:45	*Coffee break*
15:45-17:15	Phishing attack scenario (internal team point of vie
17:15-17:30	Closing

Day 2 (Tue 30 June, 2015)	
9:15-10:45	Large scale incid



Filter: ip.addr ==66.232.114.139

Enter a display filter, or choose one of your recently used filters. The background color of this field is change results).

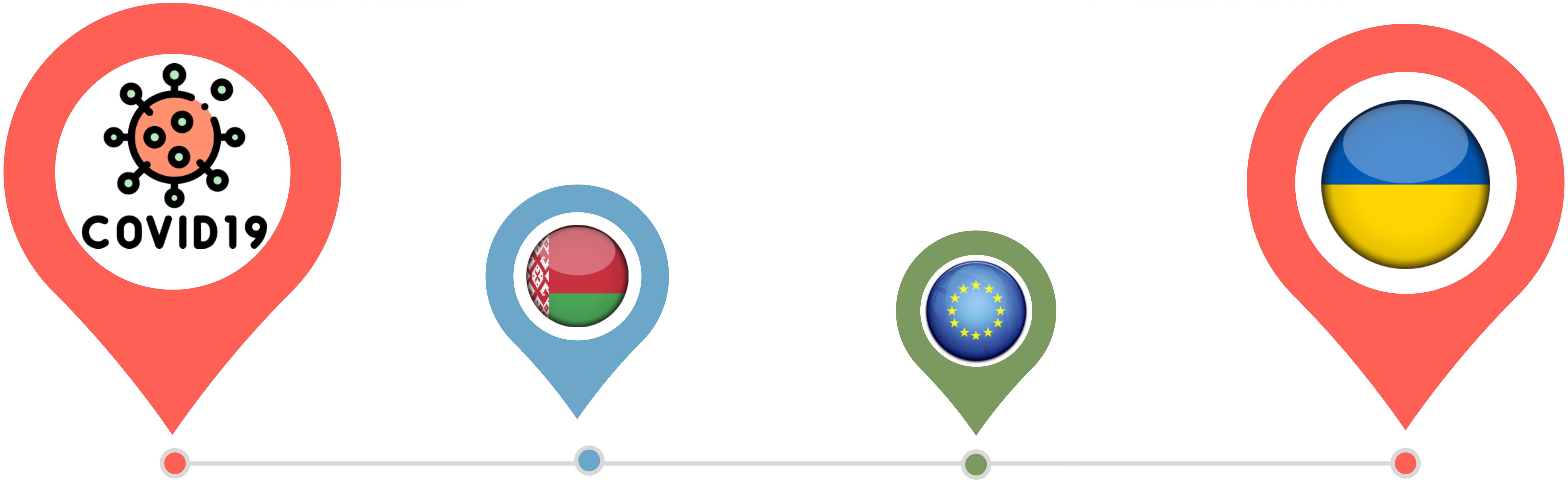
```
195 7.072917  85.255.120.194   10.0.0.130       TCP    58 80 > 1
196 7.073124  10.0.0.130       85.255.120.194   TCP    54 1150 >
197 7.073474  10.0.0.130       85.255.120.194   HTTP   379 GET /t
198 7.073531  85.255.120.194   10.0.0.130       TCP    54 80 > 11
201 7.295530  85.255.120.194   10.0.0.130       HTTP   596 HTTP/1.
205 7.395533  85.255.120.194   10.0.0.130       HTTP   596 [TCP Re
206 7.395746  10.0.0.130       85.255.120.194   TCP    54 1150 >
382 8.298437  85.255.120.194   10.0.0.130       TCP    54 80 > 11
383 8.298652  10.0.0.130       85.255.120.194   TCP    54 1150 >
587 10.582056 10.0.0.130       85.255.120.194   TCP    54 1150 > 8
```

EXPECTATIONS

EXPECTATIONS

REALITY

Encountered challenges



2020

CORONA VIRUS OUTBREAK

Immediate cessation of all physical presence activities

2020

BELARUS SANCTIONS

Immediate cessation of activities in Belarus

2021

CHANGE IN EU DG NEAR PROJECT MANAGEMENT

2022

WAR IN UKRAINE

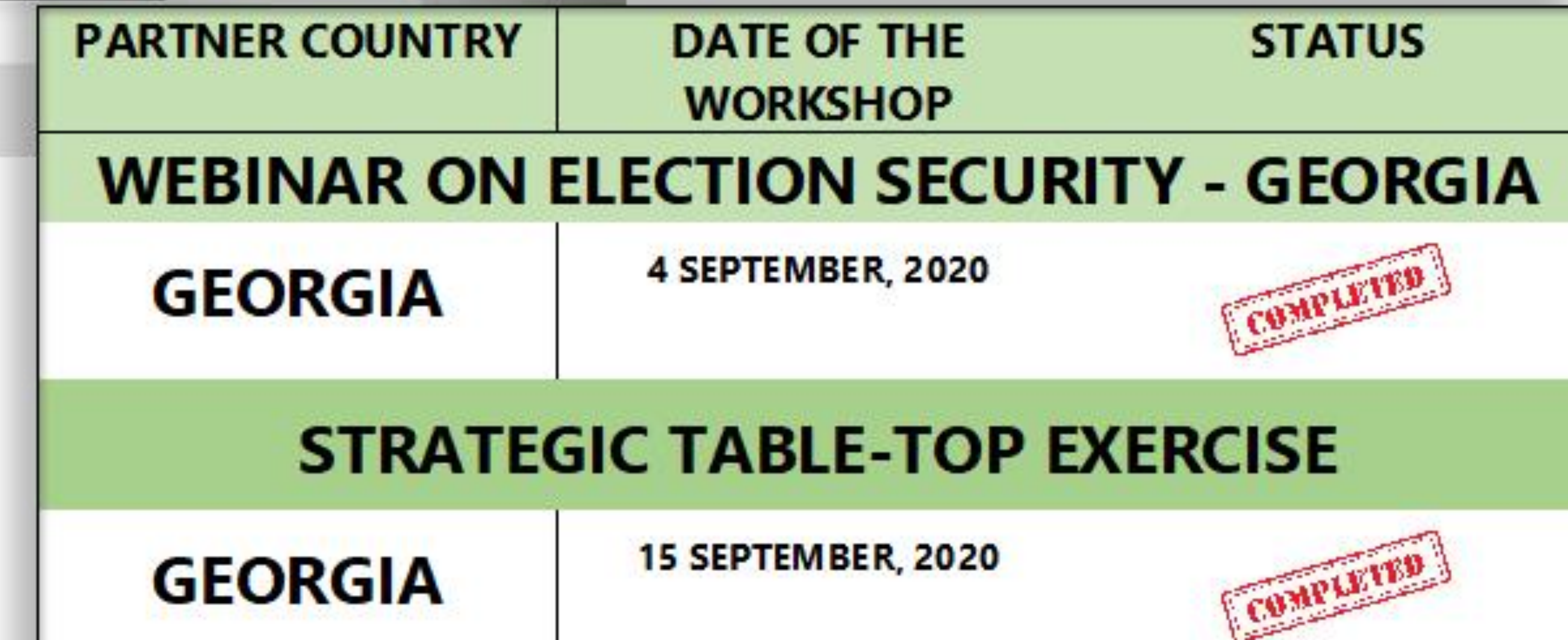
Immediate cessation of activities in Ukraine

IMPLEMENTED ACTIVITIES

2

Tailor Made Activities

ELECTION SYSTEM
CYBERSECURITY
BALLOT



PARTNER COUNTRY	DATE OF THE WORKSHOP	STATUS
WEBINAR ON ELECTION SECURITY - GEORGIA		
GEORGIA	4 SEPTEMBER, 2020	COMPLETED
STRATEGIC TABLE-TOP EXERCISE		
GEORGIA	15 SEPTEMBER, 2020	COMPLETED

MOLDOVA CYBER WEEK

MOLDOVA CYBER WEEK 2020

ONLINE STREAMING

Under the patronage

GOVERNMENT OF REPUBLIC OF MOLOVA

Organized by

INFORMATION TECHNOLOGY AND CYBER SECURITY SERVICE

TECHNICAL UNIVERSITY OF MOLDOVA

BUILDING A STRONG CYBERSECURITY INFRASTRUCTURE IN THE NEW NORMAL

25-27 NOVEMBER 2020

WWW.MOLDOVACYBERWEEK.MD

LIVE

Co-Organizers:

ITU

Strategic Partners:

moldova IT PARK

Tekwill

Sweden Sverige

USAID FROM THE AMERICAN PEOPLE

Main Partners:

CISCO

MUK Classics of distribution

Partners:

XONTECH SYSTEMS

THALES

MICRO FOCUS

HUAWEI

Elcore Elcore Distribution

GTB Technologies Data Security that Works

it lab

kaspersky

MOLDATSA

simpals

cooperare germană

Implemented by giz

20 ANI

rapidLINK

SUPPORT THE CONFERENCE AND THE WORKSHOP WITH SPEAKERS AND TRAINERS

Gap Analysis - Enisa Guidelines - Nis Directive -

NATIONAL
CYBERSECURITY
STRATEGY
UKRAINE

NATIONAL
CYBERSECURITY
STRATEGY
GEORGIA

INFORMATION
SECURITY
STRATEGY
MOLDOVA

Overview of Key elements of National Cybersecurity Strategies

- Develop national cyber contingency plans
- Protect critical information infrastructure
- Organise cyber security exercises
- Establish baseline security measures
- Establish incident reporting mechanisms

- Raise user awareness
- Strengthen training and educational programs
- Establish an incident response capability
- Address cyber crime
- Engage in international cooperation

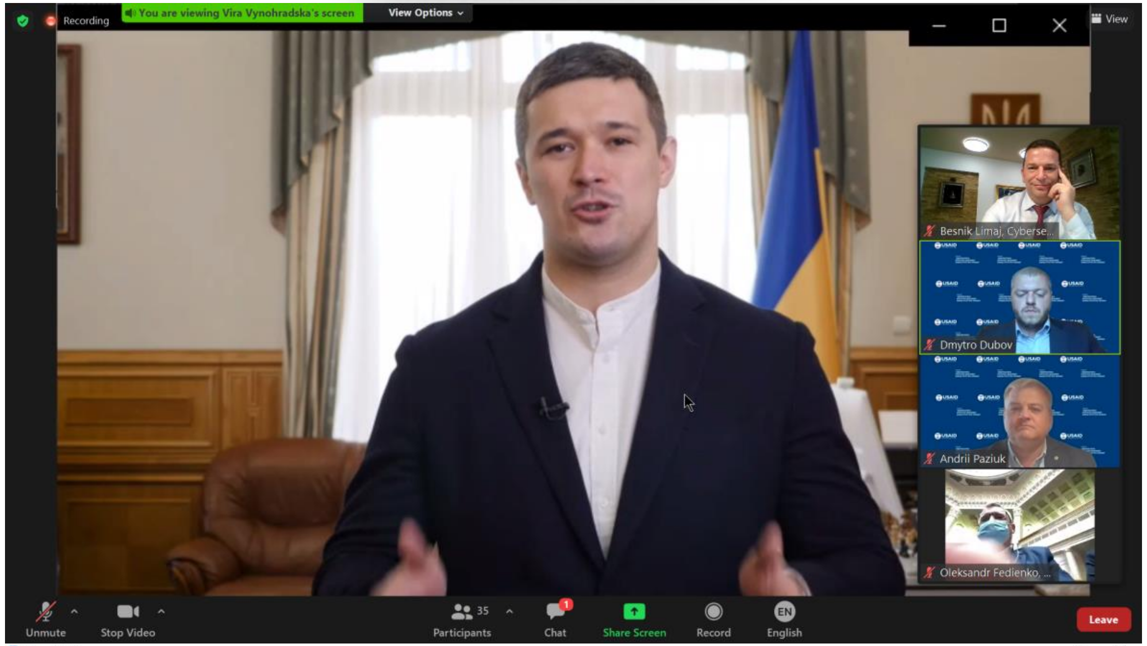
- Establish a public-private partnership
- Balance security with privacy and data protection
- Institutionalise cooperation between public agencies
- Foster R&D in cyber security
- Provide incentives for the private sector to invest in sec. measures

Source: ENISA NCSS Good Practice Guide

Cybersecurity EAST

EU4Digital

Presentation of Gap Analysis of Cybersecurity Strategy in front of the Vice Prime Minister Mykhailo Fedorov, MP's, NSDC who is in charge of the Strategy and other Stakeholders ...

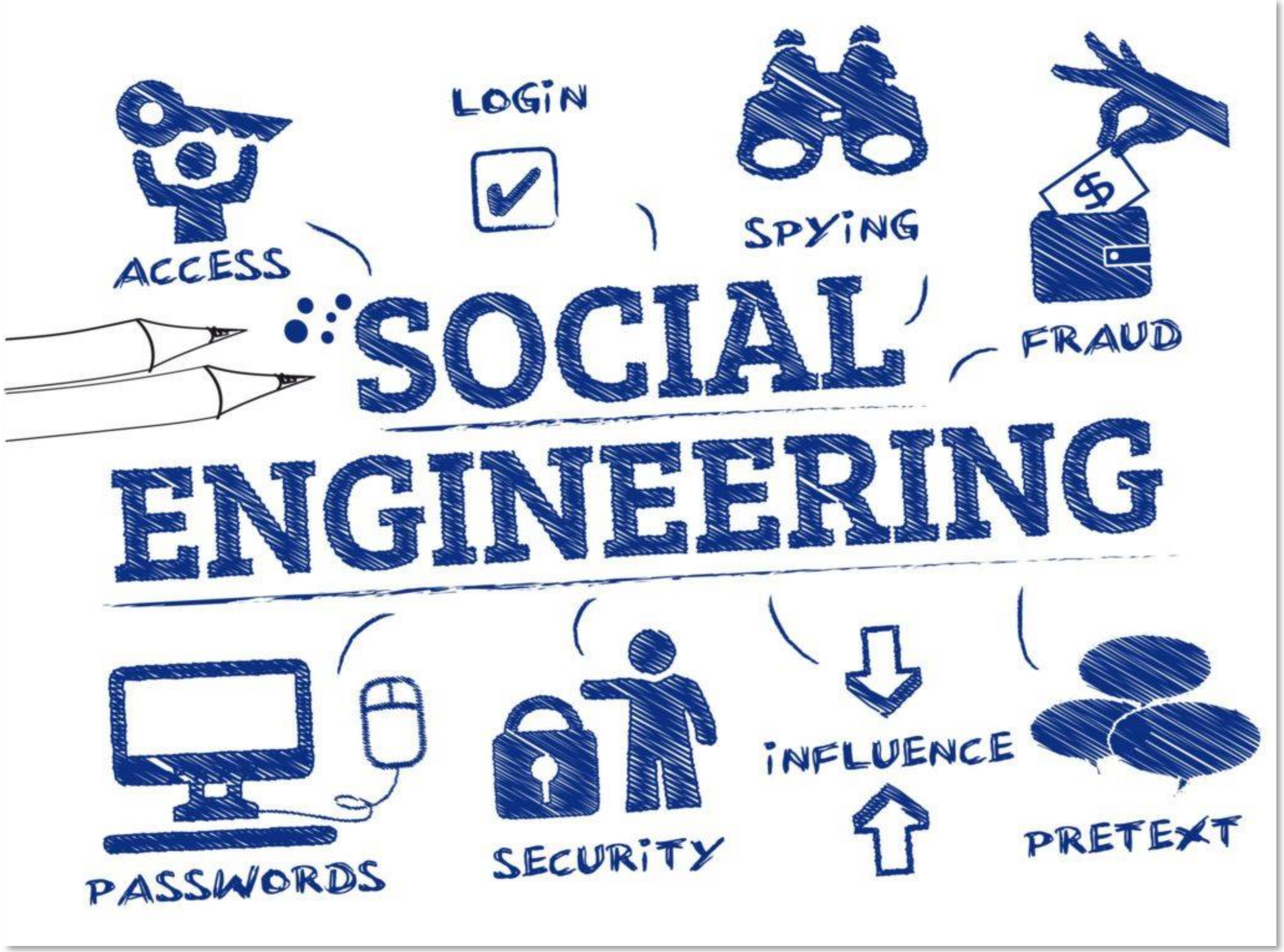


Gap Analysis - Enisa Guidelines - Nis Directive -

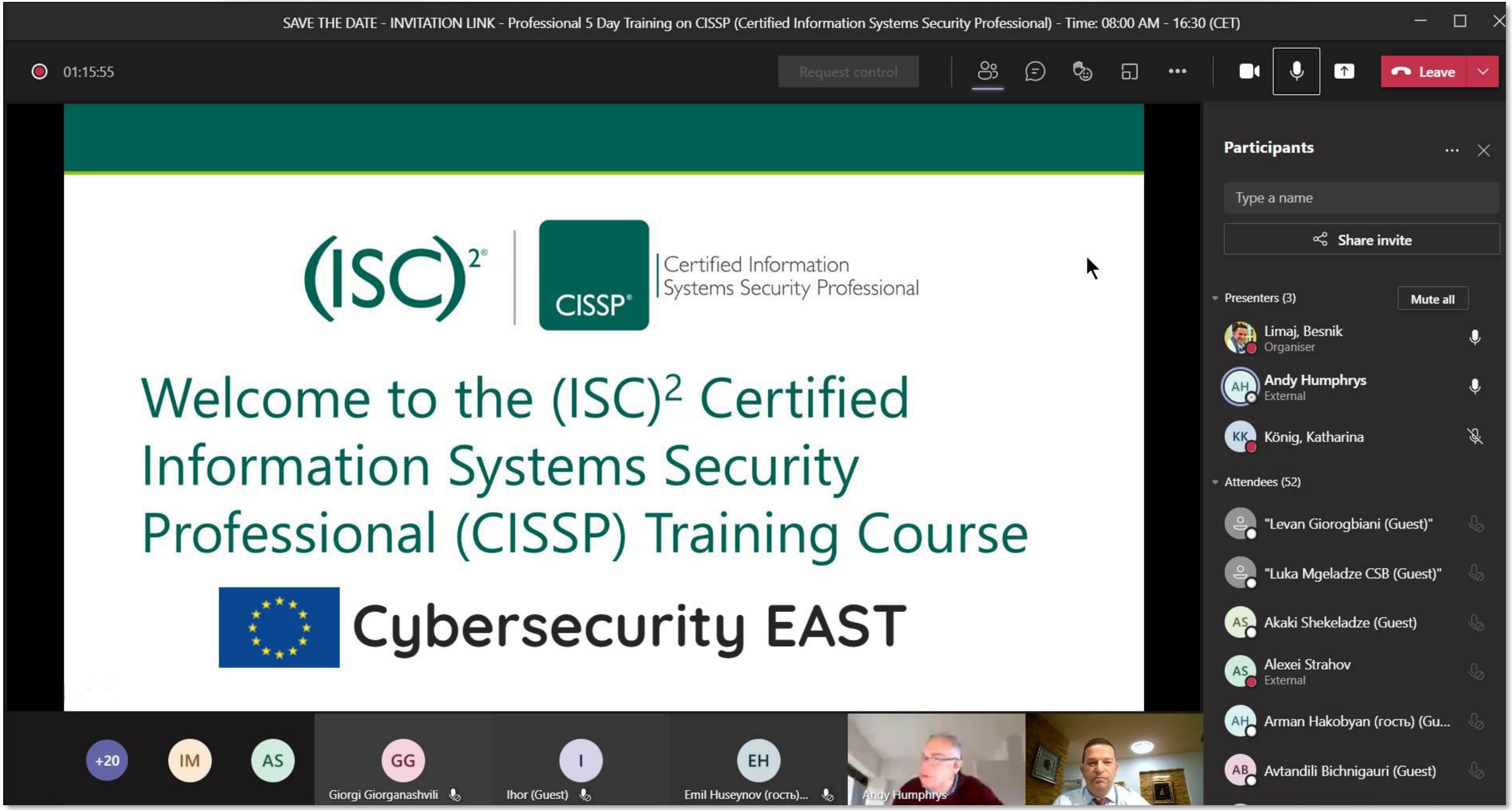
Training Workshops

Cybersecurity EAST

Training Workshop – Defensive Social Engineering



5 DAY - INTENSIVE CISSP TRAINING



SAVE THE DATE - INVITATION LINK - Professional 5 Day Training on CISSP (Certified Information Systems Security Professional) - Time: 08:00 AM - 16:30 (CET)

01:15:55

(ISC)² | CISSP® Certified Information Systems Security Professional

Welcome to the (ISC)² Certified Information Systems Security Professional (CISSP) Training Course

Cybersecurity EAST

Participants

Presenters (3)

- Limaj, Besnik Organiser
- Andy Humphrys External
- König, Katharina

Attendees (52)

- "Levan Giorogbiani (Guest)"
- "Luka Mgeladze CSB (Guest)"
- Akaki Shekeladze (Guest)
- Alexei Strahov External
- Arman Hakobyan (гость) (Gu...
- Avtandili Bichnigauri (Guest)

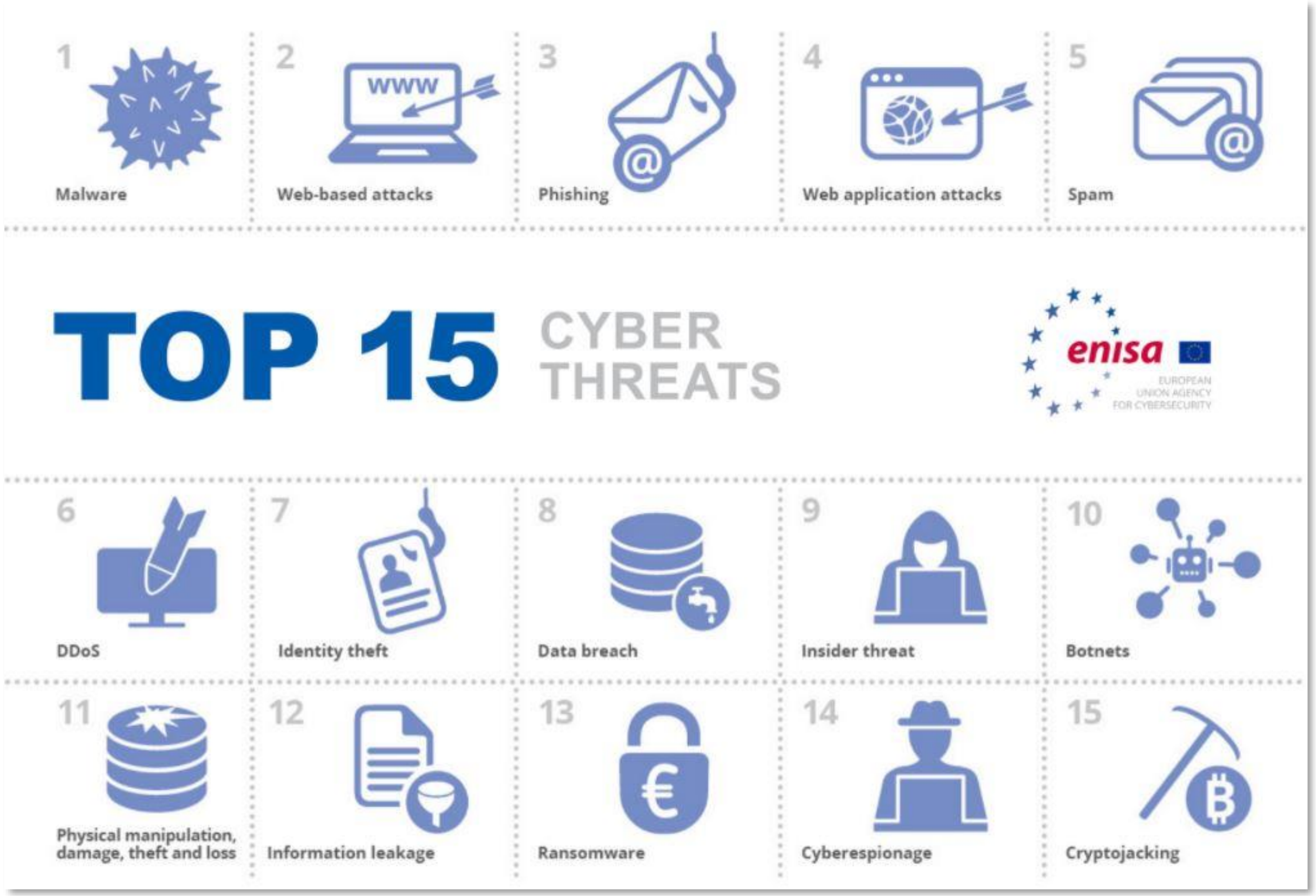
Giorgi Giorganashvili

Ihor (Guest)

Emil Huseynov (гость)...

Andy Humphrys

ENISA Threat Landscape - Workshop



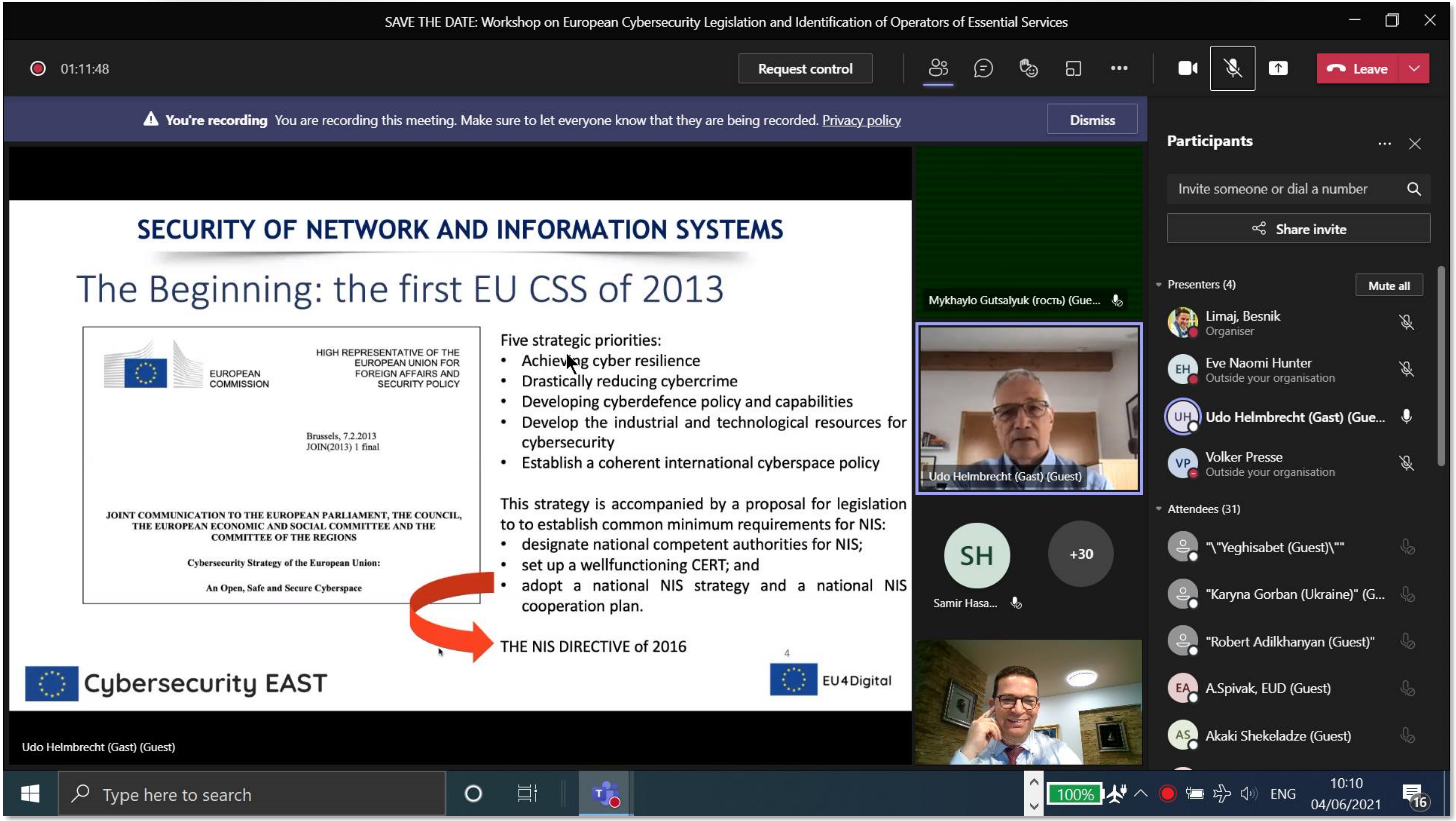
Cybersecurity Threat Landscape Methodology & Examples

1. The Methodology
2. ENISA's Threat Landscape Mapping during COVID-19
3. The State of IT Security in Germany
4. The Franco-German Common Situational Picture

Best Practices

- ISO 27001 ISMS Guidelines
- ISMS in Practice
- NIST-CSF
- MITRE att&ck
- Threat Modelling (MISP, STIX/TAXII)

European Cybersecurity Legislation and Identification of Operators of Essential Services
June 2021



SAVE THE DATE: Workshop on European Cybersecurity Legislation and Identification of Operators of Essential Services

01:11:48

⚠ **You're recording** You are recording this meeting. Make sure to let everyone know that they are being recorded. Privacy policy

SECURITY OF NETWORK AND INFORMATION SYSTEMS

The Beginning: the first EU CSS of 2013

EUROPEAN COMMISSION

HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

Brussels, 7.2.2013
JOIN(2013) 1 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace

Five strategic priorities:

- Achieving cyber resilience
- Drastically reducing cybercrime
- Developing cyberdefence policy and capabilities
- Develop the industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy

This strategy is accompanied by a proposal for legislation to to establish common minimum requirements for NIS:

- designate national competent authorities for NIS;
- set up a wellfunctioning CERT; and
- adopt a national NIS strategy and a national NIS cooperation plan.

THE NIS DIRECTIVE of 2016

Cybersecurity EAST

4

EU4Digital

Udo Helmbrecht (Gast) (Guest)

Participants

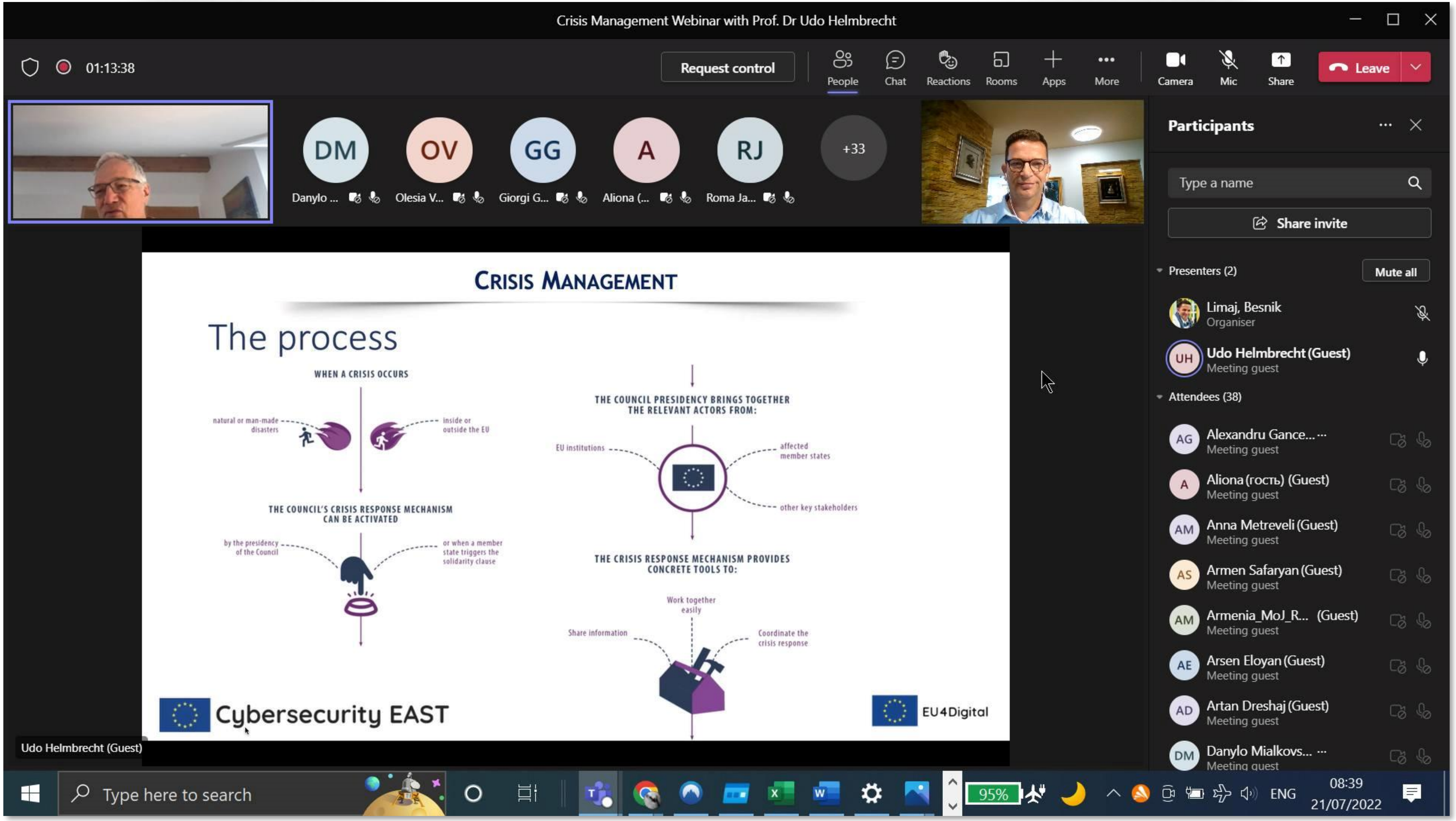
Presenters (4)

- Limaj, Besnik — Organiser
- Eve Naomi Hunter — Outside your organisation
- Udo Helmbrecht (Gast) (Gue...
- Volker Presse — Outside your organisation

Attendees (31)

- "\"Yeghisabet (Guest)\""
- "Karyna Gorban (Ukraine)" (G...
- "Robert Adilkhanyan (Guest)"
- A.Spivak, EUD (Guest)
- Akaki Shekeladze (Guest)

Cybersecurity Crisis Management
July 2022



Crisis Management Webinar with Prof. Dr Udo Helmbrecht

Crisis Management

The process

WHEN A CRISIS OCCURS

natural or man-made disasters — inside or outside the EU

THE COUNCIL'S CRISIS RESPONSE MECHANISM CAN BE ACTIVATED

by the presidency of the Council — or when a member state triggers the solidarity clause

THE COUNCIL PRESIDENCY BRINGS TOGETHER THE RELEVANT ACTORS FROM:

EU institutions — affected member states — other key stakeholders

THE CRISIS RESPONSE MECHANISM PROVIDES CONCRETE TOOLS TO:

Work together easily — Share information — Coordinate the crisis response

Cybersecurity EAST

EU4Digital

Participants

Type a name

Share invite

Presenters (2) — Mute all

Limaj, Besnik
Organiser

Udo Helmbrecht (Guest)
Meeting guest

Attendees (38)

Alexandru Gance... ···
Meeting guest

Aliona (гость) (Guest)
Meeting guest

Anna Metreveli (Guest)
Meeting guest

Armen Safaryan (Guest)
Meeting guest

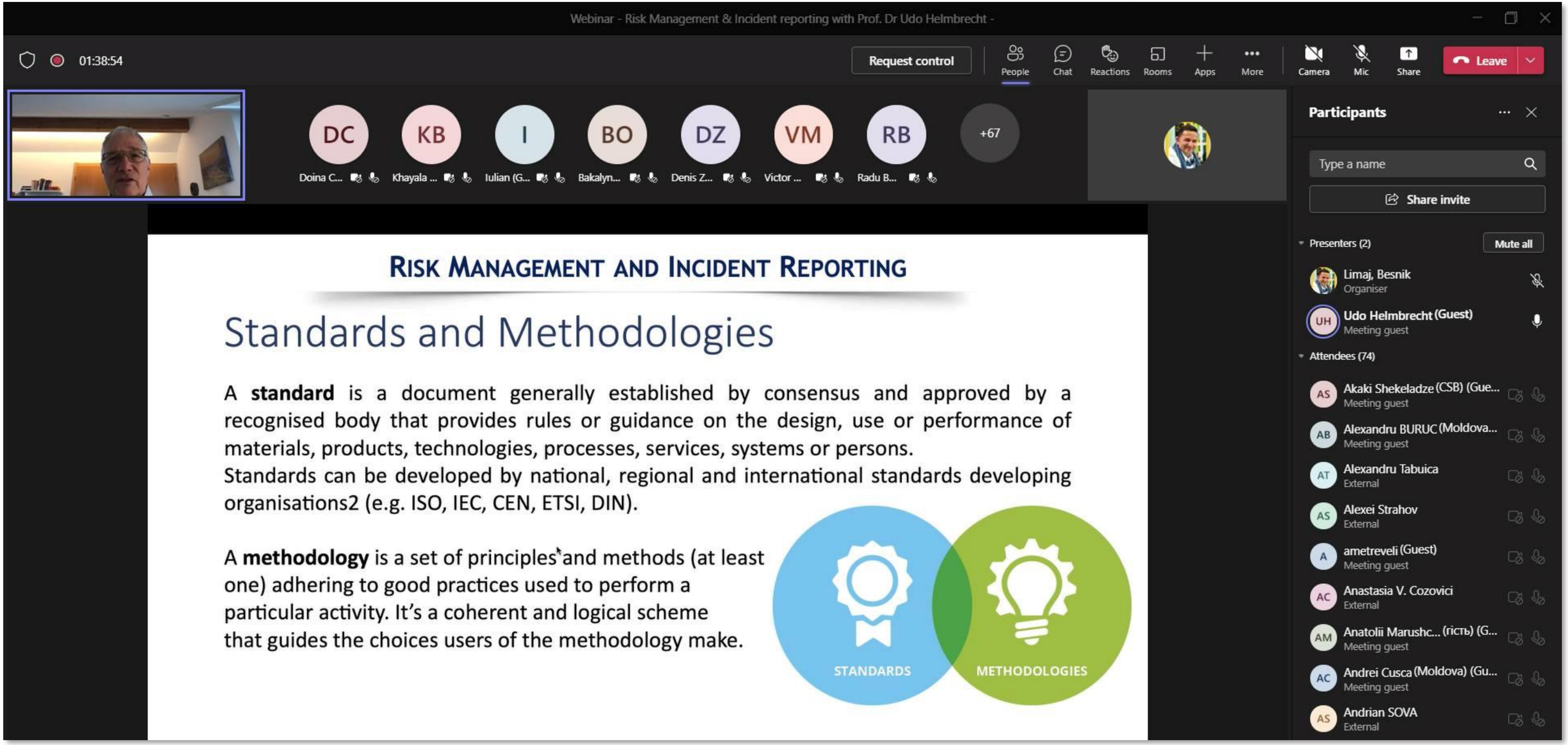
Armenia_MoJ_R... (Guest)
Meeting guest

Arsen Eloyan (Guest)
Meeting guest

Artan Dreshaj (Guest)
Meeting guest

Danylo Mialkovs... ···
Meeting guest

Cybersecurity Risk Management and Incident Reporting
June 2022



Risk Management and Incident Reporting

Standards and Methodologies

A **standard** is a document generally established by consensus and approved by a recognised body that provides rules or guidance on the design, use or performance of materials, products, technologies, processes, services, systems or persons.
Standards can be developed by national, regional and international standards developing organisations2 (e.g. ISO, IEC, CEN, ETSI, DIN).

A **methodology** is a set of principles and methods (at least one) adhering to good practices used to perform a particular activity. It's a coherent and logical scheme that guides the choices users of the methodology make.

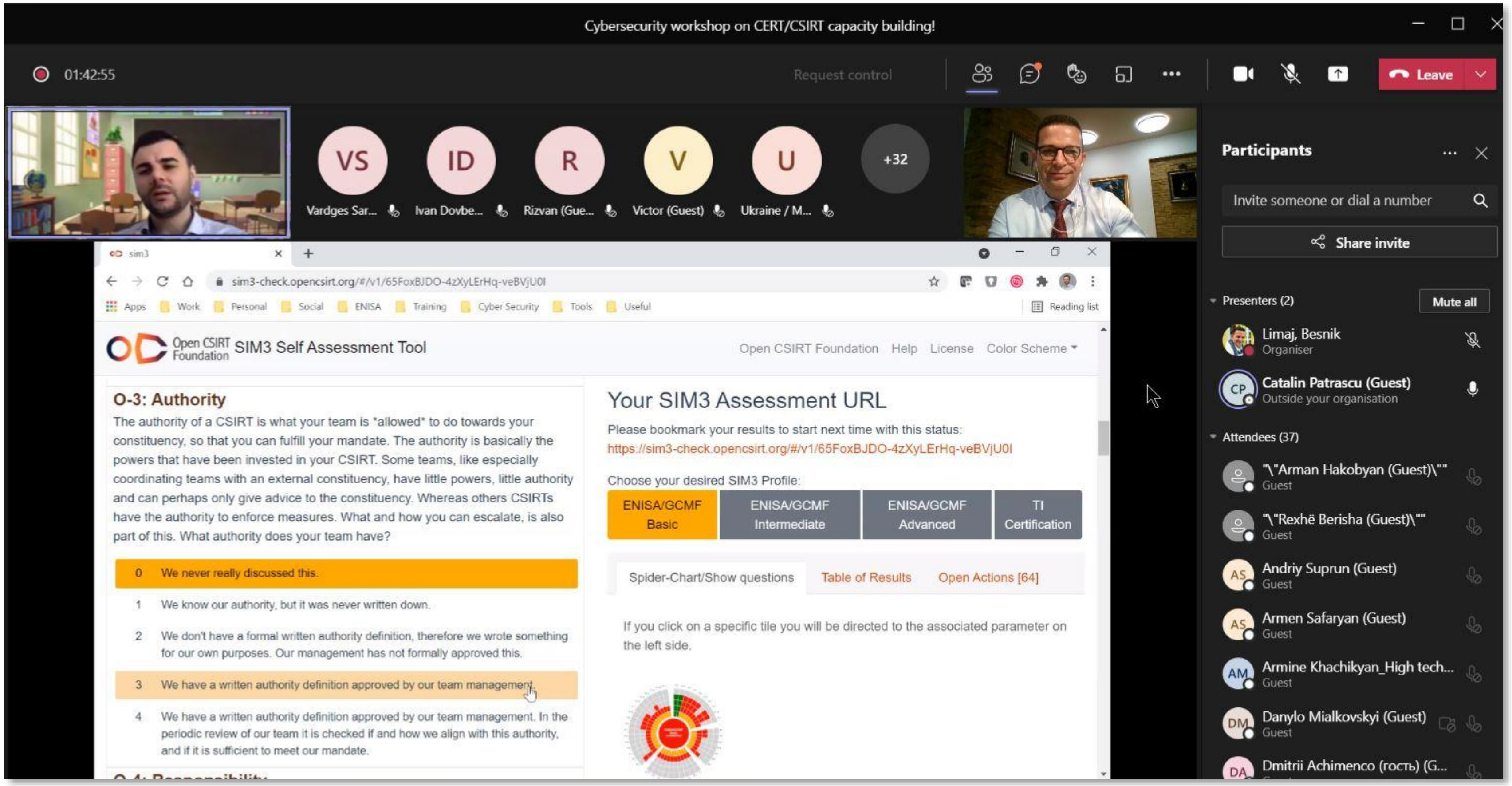
CERT/CSIRT TRAINING

CSIRTs MATURITY ASSESSMENT enisa

Cortex & TheHive

MISP Threat Sharing

INTELMQ



Cybersecurity workshop on CERT/CSIRT capacity building!

01:42:55 Request control Leave

VS Vardges Sar... | ID Ivan Dovbe... | R Rizvan (Gue... | V Victor (Guest) | U Ukraine / M... | +32

sim3

sim3-check.opencsirt.org/#/v1/65FoxBJDO-4zXyLErHq-veBVjU0I

Apps | Work | Personal | Social | ENISA | Training | Cyber Security | Tools | Useful | Reading list

Open CSIRT Foundation SIM3 Self Assessment Tool — Open CSIRT Foundation | Help | License | Color Scheme

O-3: Authority

The authority of a CSIRT is what your team is "allowed" to do towards your constituency, so that you can fulfill your mandate. The authority is basically the powers that have been invested in your CSIRT. Some teams, like especially coordinating teams with an external constituency, have little powers, little authority and can perhaps only give advice to the constituency. Whereas others CSIRTs have the authority to enforce measures. What and how you can escalate, is also part of this. What authority does your team have?

0 We never really discussed this.

1 We know our authority, but it was never written down.

2 We don't have a formal written authority definition, therefore we wrote something for our own purposes. Our management has not formally approved this.

3 We have a written authority definition approved by our team management.

4 We have a written authority definition approved by our team management. In the periodic review of our team it is checked if and how we align with this authority, and if it is sufficient to meet our mandate.

O-4: Responsibility

Your SIM3 Assessment URL

Please bookmark your results to start next time with this status:
https://sim3-check.opencsirt.org/#/v1/65FoxBJDO-4zXyLErHq-veBVjU0I

Choose your desired SIM3 Profile:

ENISA/GCMF Basic | ENISA/GCMF Intermediate | ENISA/GCMF Advanced | TI Certification

Spider-Chart/Show questions | Table of Results | Open Actions [64]

If you click on a specific tile you will be directed to the associated parameter on the left side.

Participants

Invite someone or dial a number

Share invite

Presenters (2) — Mute all

Limaj, Besnik — Organiser

Catalin Patrascu (Guest) — Outside your organisation

Attendees (37)

"\"Arman Hakobyan (Guest)\"" — Guest

"\"Rexhë Berisha (Guest)\"" — Guest

Andriy Suprun (Guest) — Guest

Armen Safaryan (Guest) — Guest

Armine Khachikyan_High tech... — Guest

Danylo Mialkovskyi (Guest) — Guest

Dmitrii Achimenco (гость) (G...

elasticsearch + logstash + kibana

3 x 5 day intensive professional CompTIA training’s

Tailor Made Trainings!

TRAINING

1 DAY Training

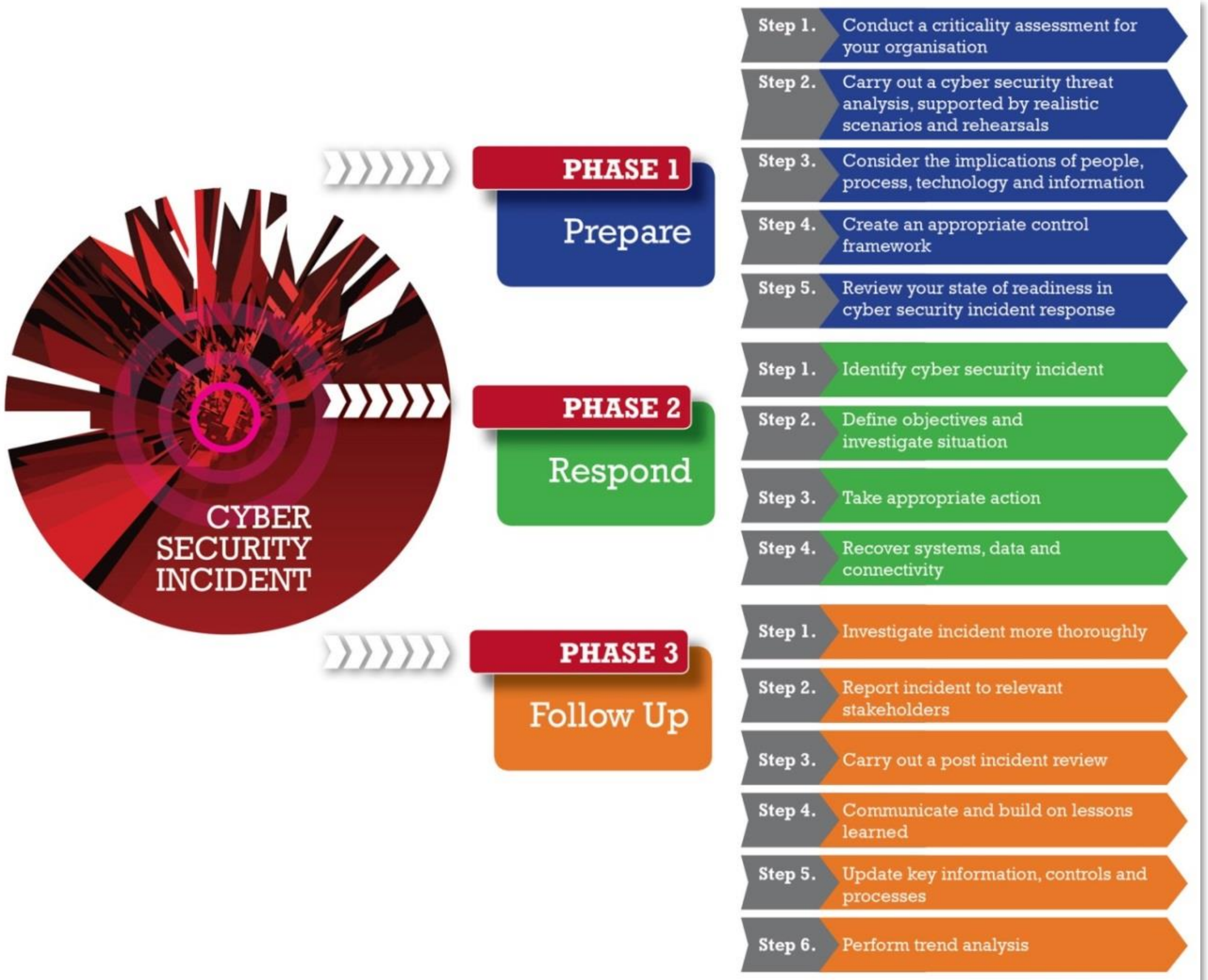
4 DAYS Training

Cybersecurity EAST

CYBERSECURITY TRAINING MARATHON
JULY 2022

CYBERSECURITY MARATHON	
SESSION I	Lesson 1: Planning a CSIRT Implementation
SESSION II	Lesson 2: Incident Response Frameworks Steps and Playbooks
SESSION III	Lesson 3: CIS Controls
SESSION IV	Lesson 4: SIM3
SESSION V	Lesson 5: Governance
SESSION VI	Lesson 6: Risk Management
SESSION VII	Lesson 7: NIST Cybersecurity Framework
SESSION VIII	Lesson 8: ISO/IEC 27001
SESSION IX	Lesson 9: CTI Overview
SESSION X	Lesson 10: CVEs and CVSS
SESSION XI	Lesson 11: Compliance/Auditing
SESSION XII	Lesson 12: Education/Training

SIM3 - Security Incident Management Maturity Model



PHASE 1 Prepare

- Step 1. Conduct a criticality assessment for your organisation
- Step 2. Carry out a cyber security threat analysis, supported by realistic scenarios and rehearsals
- Step 3. Consider the implications of people, process, technology and information
- Step 4. Create an appropriate control framework
- Step 5. Review your state of readiness in cyber security incident response

PHASE 2 Respond

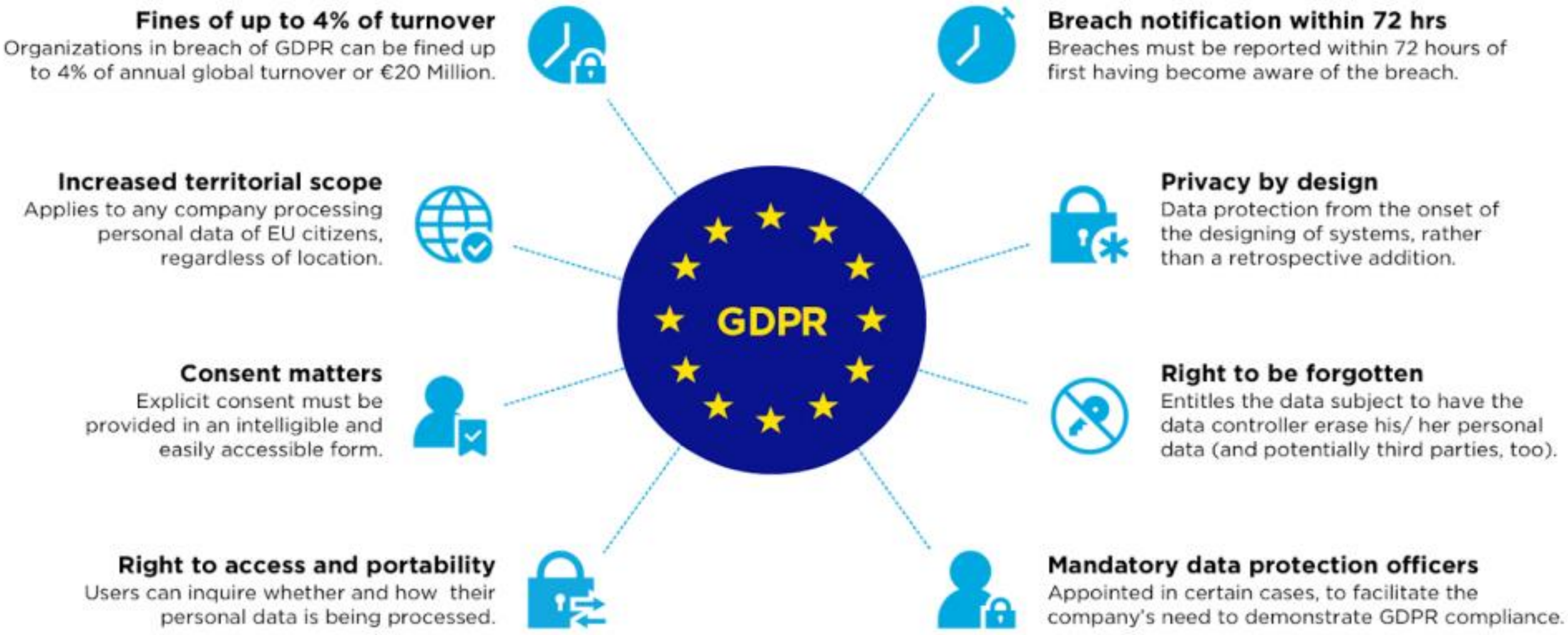
- Step 1. Identify cyber security incident
- Step 2. Define objectives and investigate situation
- Step 3. Take appropriate action
- Step 4. Recover systems, data and connectivity

PHASE 3 Follow Up

- Step 1. Investigate incident more thoroughly
- Step 2. Report incident to relevant stakeholders
- Step 3. Carry out a post incident review
- Step 4. Communicate and build on lessons learned
- Step 5. Update key information, controls and processes
- Step 6. Perform trend analysis

GDPR Experience workshop

Bigger Responsibility, Bigger Repercussions



Fines of up to 4% of turnover
Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million.

Increased territorial scope
Applies to any company processing personal data of EU citizens, regardless of location.

Consent matters
Explicit consent must be provided in an intelligible and easily accessible form.

Right to access and portability
Users can inquire whether and how their personal data is being processed.

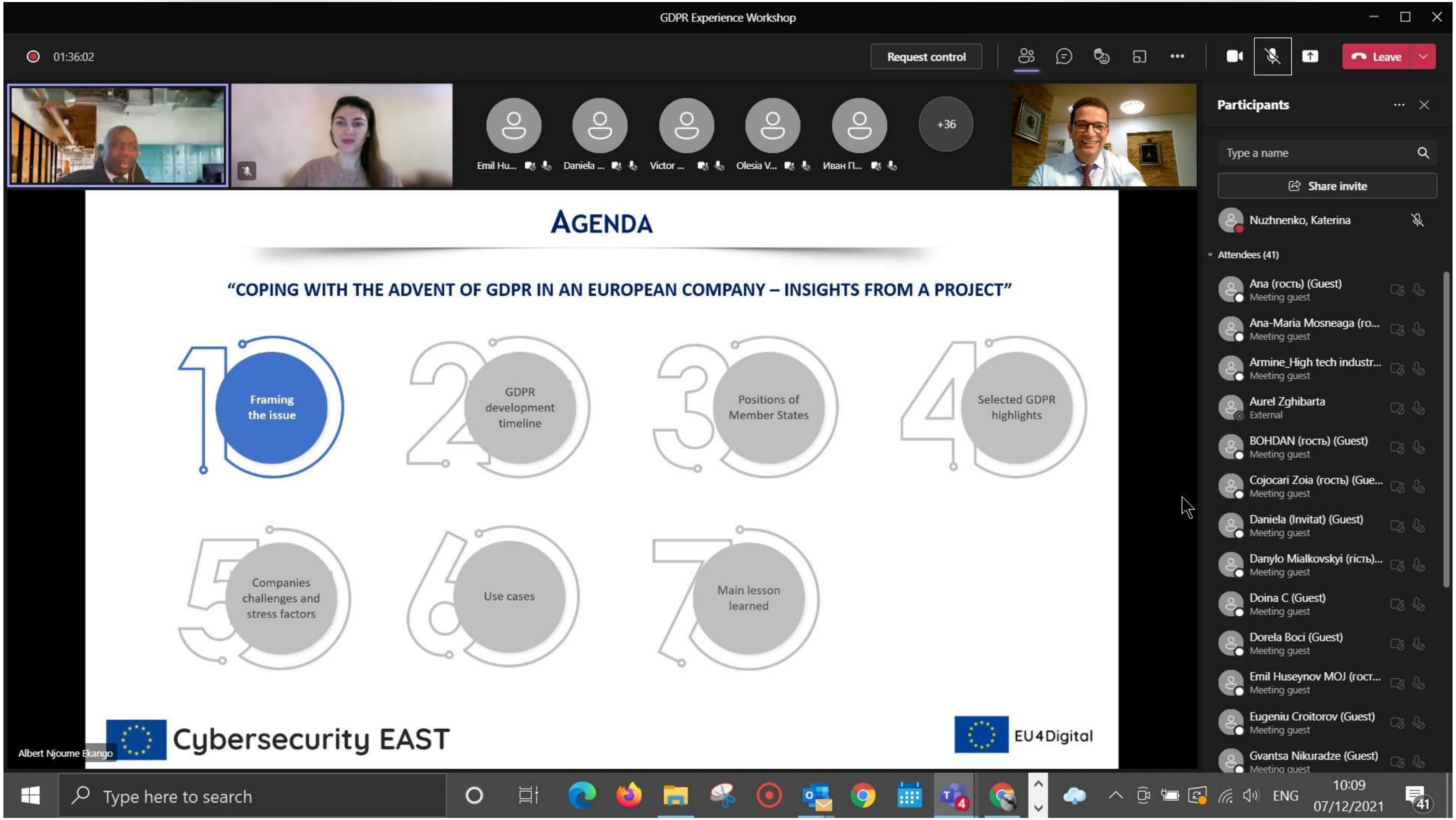
Breach notification within 72 hrs
Breaches must be reported within 72 hours of first having become aware of the breach.

Privacy by design
Data protection from the onset of the designing of systems, rather than a retrospective addition.

Right to be forgotten
Entitles the data subject to have the data controller erase his/ her personal data (and potentially third parties, too).

Mandatory data protection officers
Appointed in certain cases, to facilitate the company's need to demonstrate GDPR compliance.

GDPR Experience workshop



GDPR Experience Workshop

01:36:02

Agenda

"COPING WITH THE ADVENT OF GDPR IN AN EUROPEAN COMPANY – INSIGHTS FROM A PROJECT"

1. Framing the issue
2. GDPR development timeline
3. Positions of Member States
4. Selected GDPR highlights
5. Companies challenges and stress factors
6. Use cases
7. Main lesson learned

Cybersecurity EAST

EU4Digital

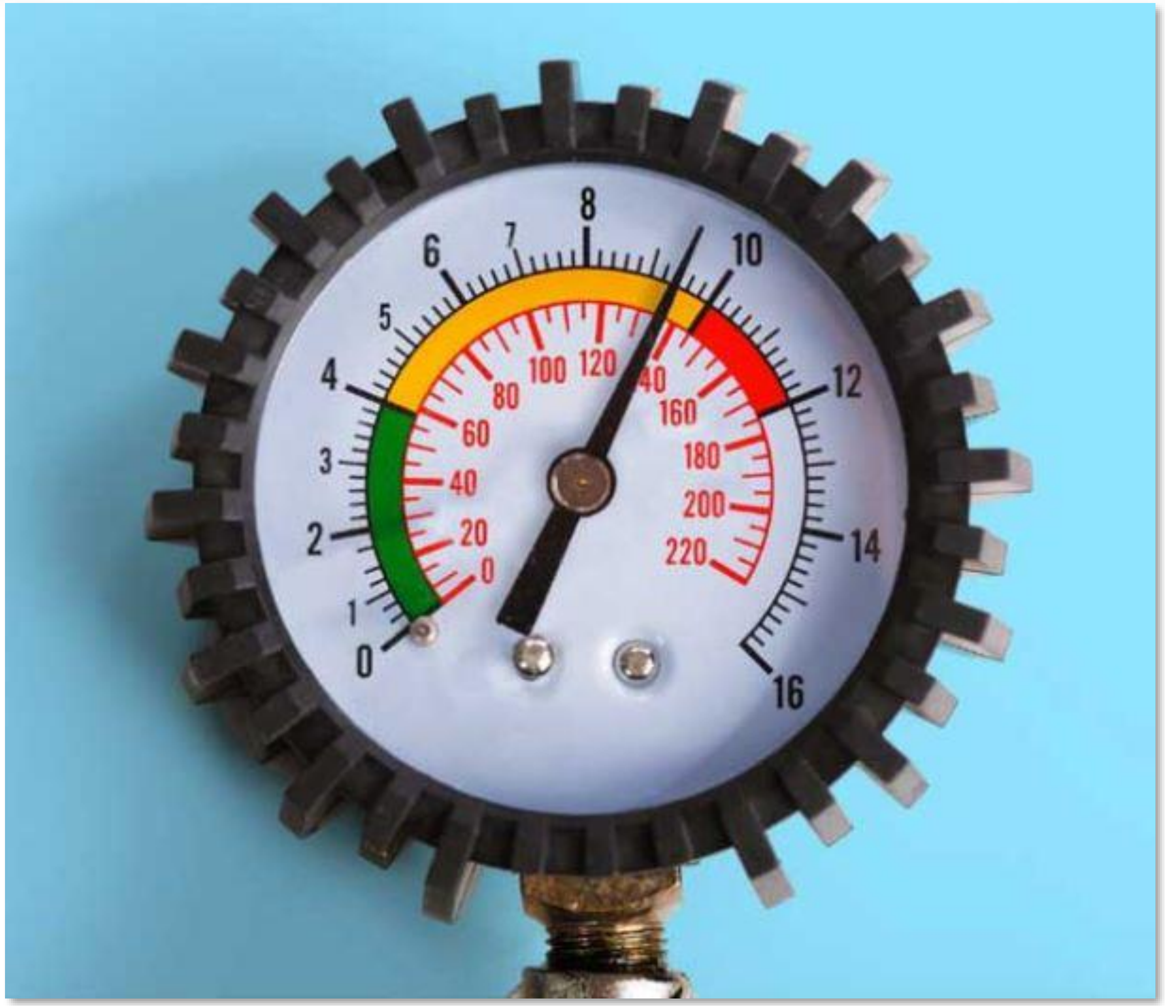
Participants

Nuzhnenko, Katerina

Attendees (41)

- Ana (гость) (Guest) – Meeting guest
- Ana-Maria Mosneaga (ro... – Meeting guest
- Armine_High tech industr... – Meeting guest
- Aurel Zghibarta – External
- BOHDAN (гость) (Guest) – Meeting guest
- Cojocari Zoia (гость) (Gue... – Meeting guest
- Daniela (Invitat) (Guest) – Meeting guest
- Danylo Mialkovskyi (гість)... – Meeting guest
- Doina C (Guest) – Meeting guest
- Dorela Boci (Guest) – Meeting guest
- Emil Huseynov MOJ (гост... – Meeting guest
- Eugeniu Croitorov (Guest) – Meeting guest
- Gvantsa Nikuradze (Guest) – Meeting guest

CYBERSECURITY AND CYBERCRIME BAROMETER SURVEY
(ENTERPRISES, INDIVIDUALS AND ISP’S)



Cybersecurity EAST

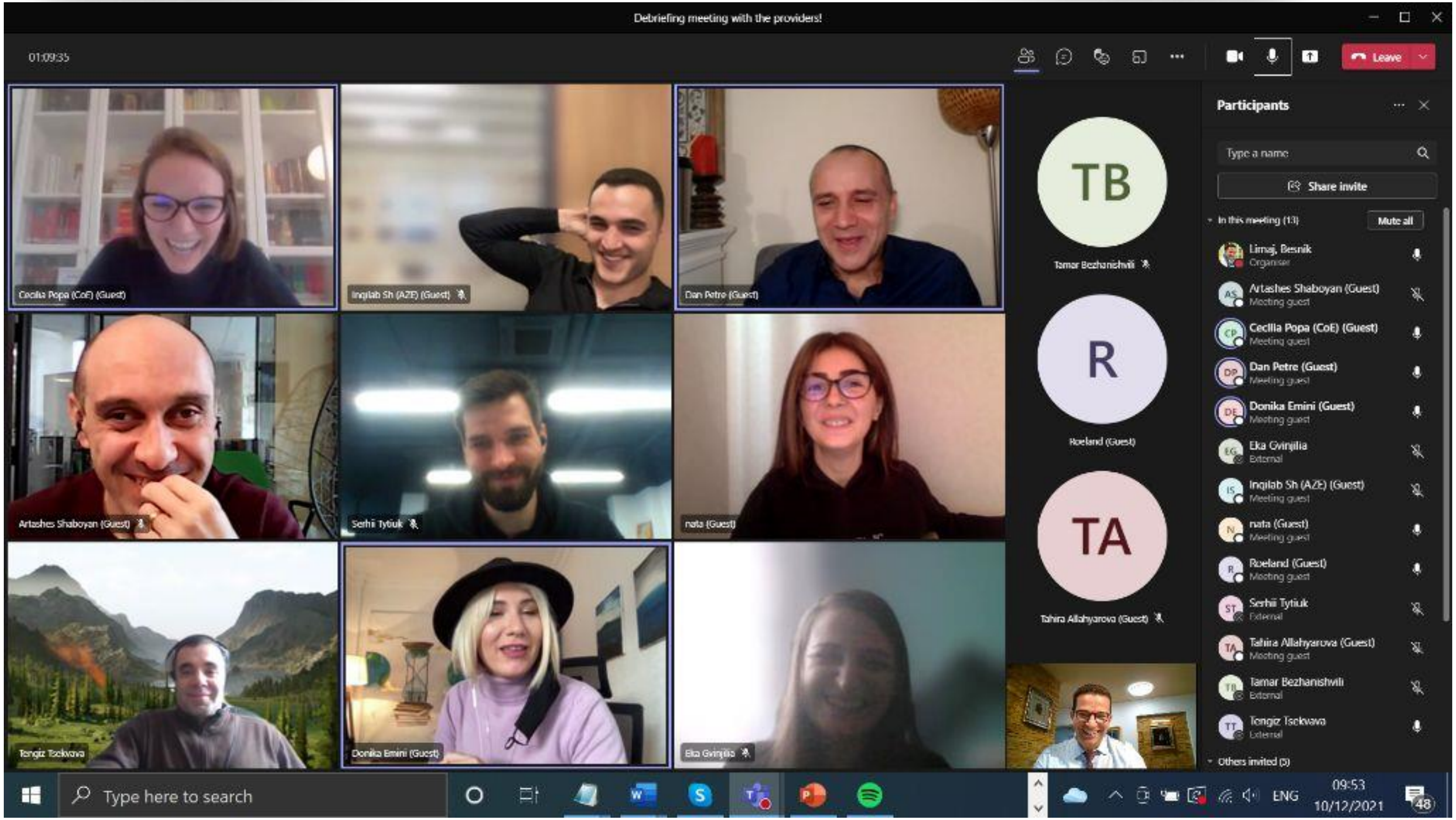
Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented by the Council of Europe

CYBERSECURITY AND CYBERCRIME BAROMETER SURVEY
(ENTERPRISES, INDIVIDUALS AND ISP'S)



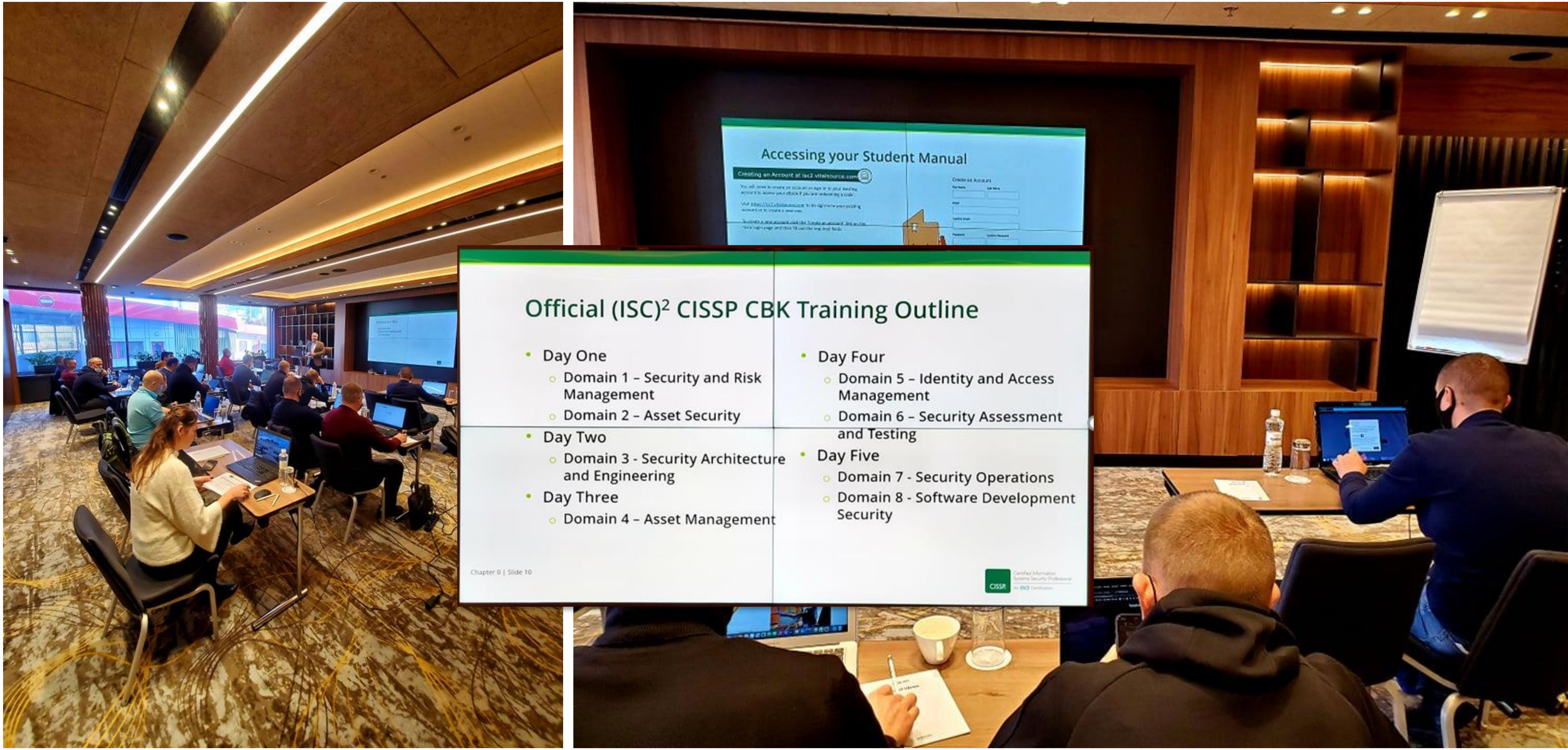
3 Day Intensive Training in Moldova

OFFENSIVE SOCIAL ENGINEERING

Cybersecurity EAST

3 Day Intensive Training

5 DAY - INTENSIVE CISSP TRAINING



Accessing your Student Manual
Creating an Account at isc2 vitalsource.com

Official (ISC)² CISSP CBK Training Outline

- Day One
  - Domain 1 – Security and Risk Management
  - Domain 2 – Asset Security
- Day Two
  - Domain 3 - Security Architecture and Engineering
- Day Three
  - Domain 4 – Asset Management
- Day Four
  - Domain 5 – Identity and Access Management
  - Domain 6 – Security Assessment and Testing
- Day Five
  - Domain 7 - Security Operations
  - Domain 8 - Software Development Security

Chapter 0 | Slide 10

CISSP

CISSP 5 DAY PROFESSIONAL TRAINING

Welcome to the (ISC)²
Certified Information Systems Security
Professional (CISSP) Training Course

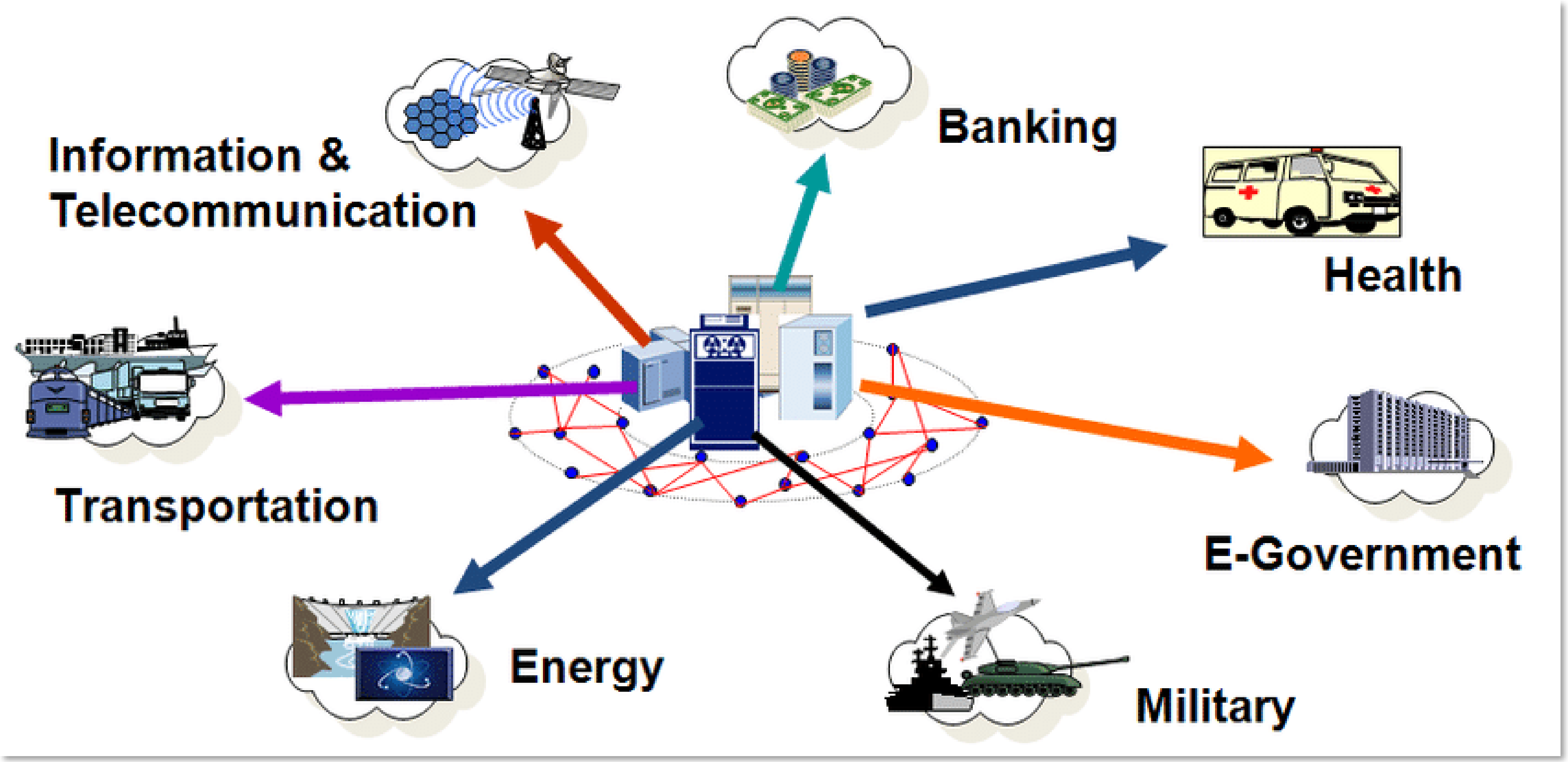
Study Visit – Estonia

Cyber Security as Enabler of Digital Society
Cybersecurity EAST
The legal and regulatory framework for e-Governance

4 day professional Training
Insider Threat and Offensive Social Engineering

CISSP
Welcome to the (ISC)²
Certified Information Systems Security
Professional (CISSP) Training Course

PROTECTION FRAMEWORKS OF CRITICAL INFORMATION INFRASTRUCTURE



Critical Information Infrastructure Protection (CIIP) Workshop

CyCON 2022

CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

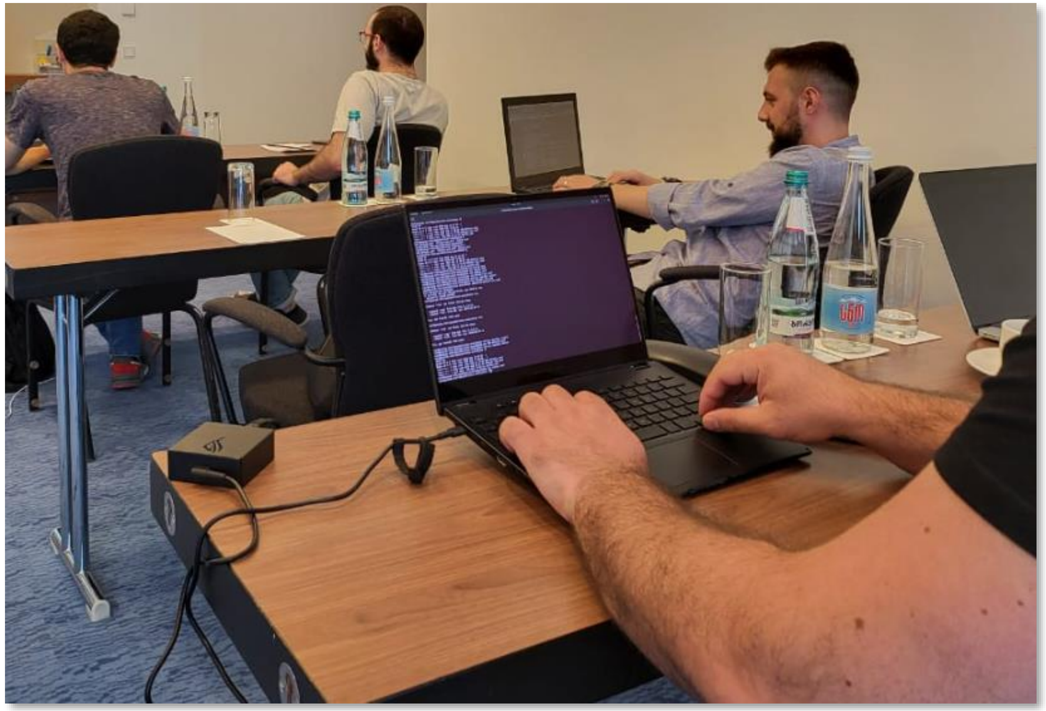
CYCON

CompTIA Security+ Training Azerbaijan 2022

CompTIA Security+

CompTIA PenTest+ Training Georgia 2022

CompTIA
PenTest+



CompTIA Security+ Training Moldova 2022

CompTIA Security+

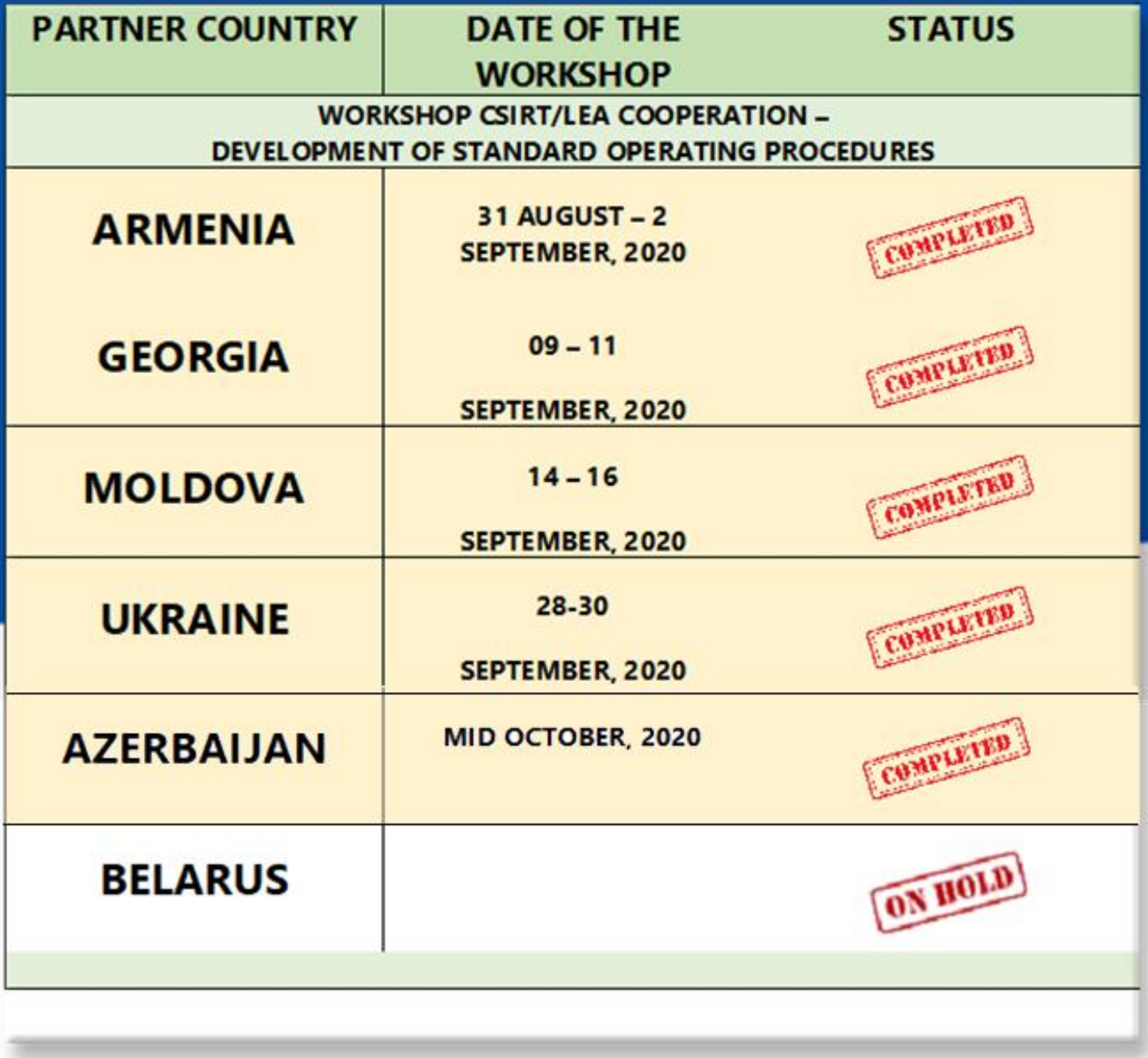
CSIRT Establishment Mission – Armenia 2022

PHASE I

JOINT WORKSHOPS

TOPICS:

- **Common taxonomy,**
- **Incident Handling,**
- **Flow of information across CSIRTs, LE and Judiciary, Segregation of duties,**
- **Criminal Intelligence**
- **Evidence collection vs damage mitigation**



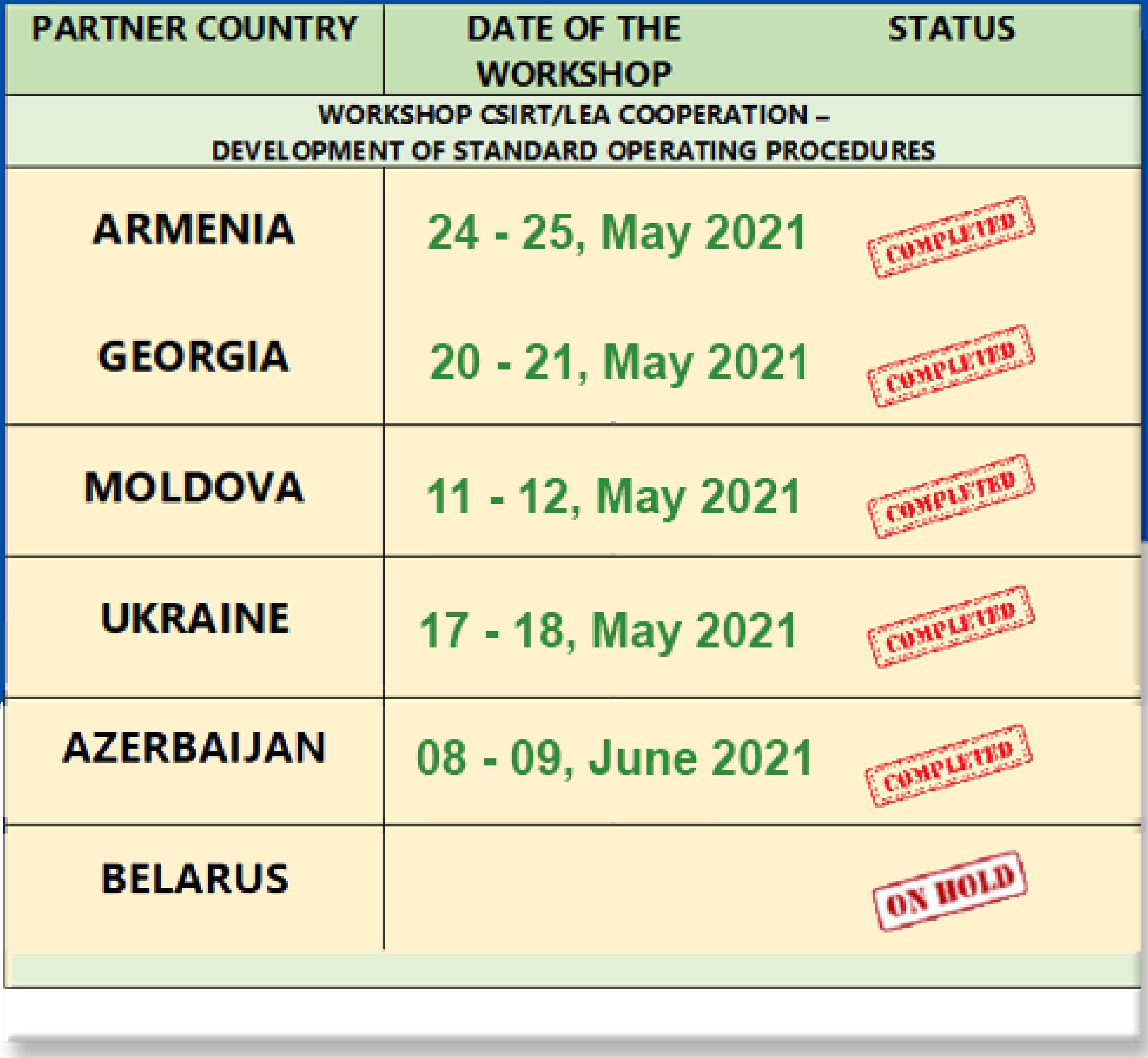
PARTNER COUNTRY	DATE OF THE WORKSHOP	STATUS
WORKSHOP CSIRT/LEA COOPERATION – DEVELOPMENT OF STANDARD OPERATING PROCEDURES		
ARMENIA	31 AUGUST – 2 SEPTEMBER, 2020	COMPLETED
GEORGIA	09 – 11 SEPTEMBER, 2020	COMPLETED
MOLDOVA	14 – 16 SEPTEMBER, 2020	COMPLETED
UKRAINE	28-30 SEPTEMBER, 2020	COMPLETED
AZERBAIJAN	MID OCTOBER, 2020	COMPLETED
BELARUS		ON HOLD

CSIRTs and LE Cooperation

PHASE II

JOINT WORKSHOPS

CSIRTs and LE Cooperation



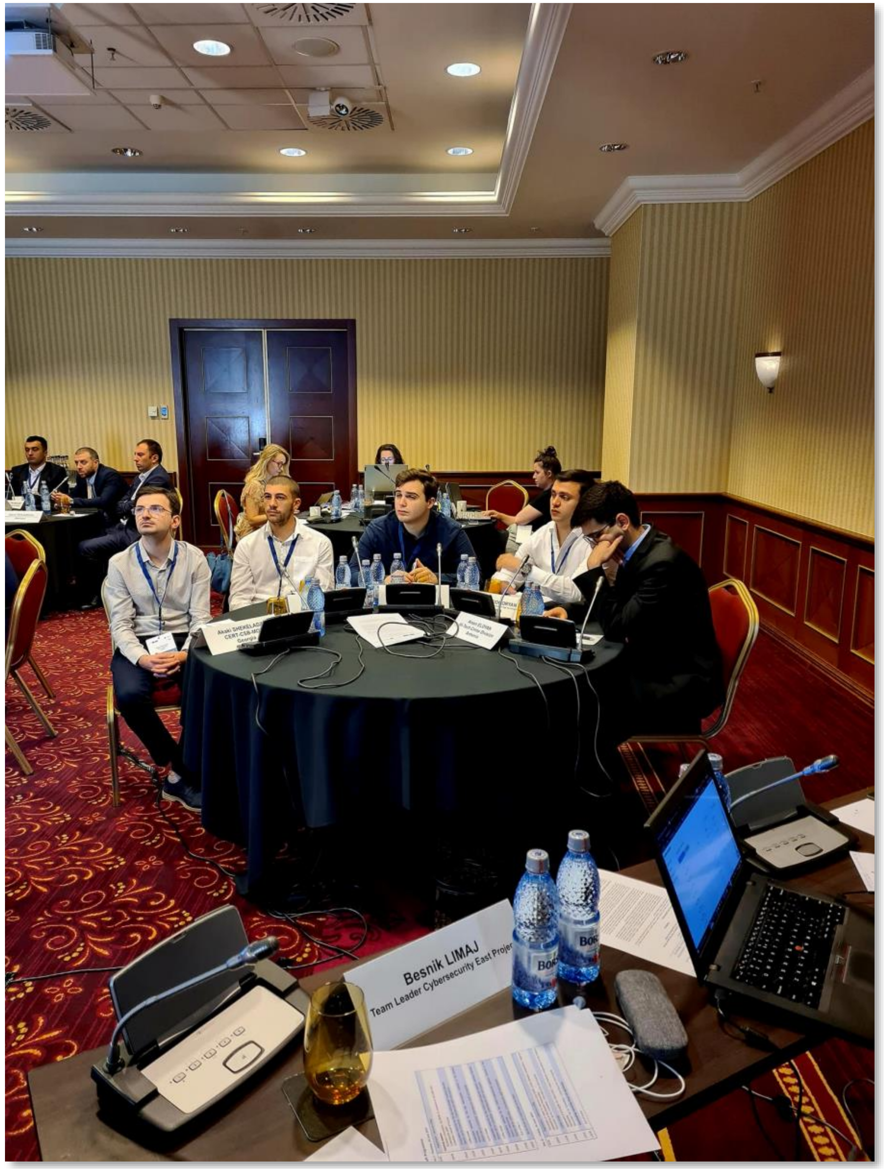
PARTNER COUNTRY	DATE OF THE WORKSHOP	STATUS
WORKSHOP CSIRT/LEA COOPERATION – DEVELOPMENT OF STANDARD OPERATING PROCEDURES		
ARMENIA	24 - 25, May 2021	COMPLETED
GEORGIA	20 - 21, May 2021	COMPLETED
MOLDOVA	11 - 12, May 2021	COMPLETED
UKRAINE	17 - 18, May 2021	COMPLETED
AZERBAIJAN	08 - 09, June 2021	COMPLETED
BELARUS		ON HOLD

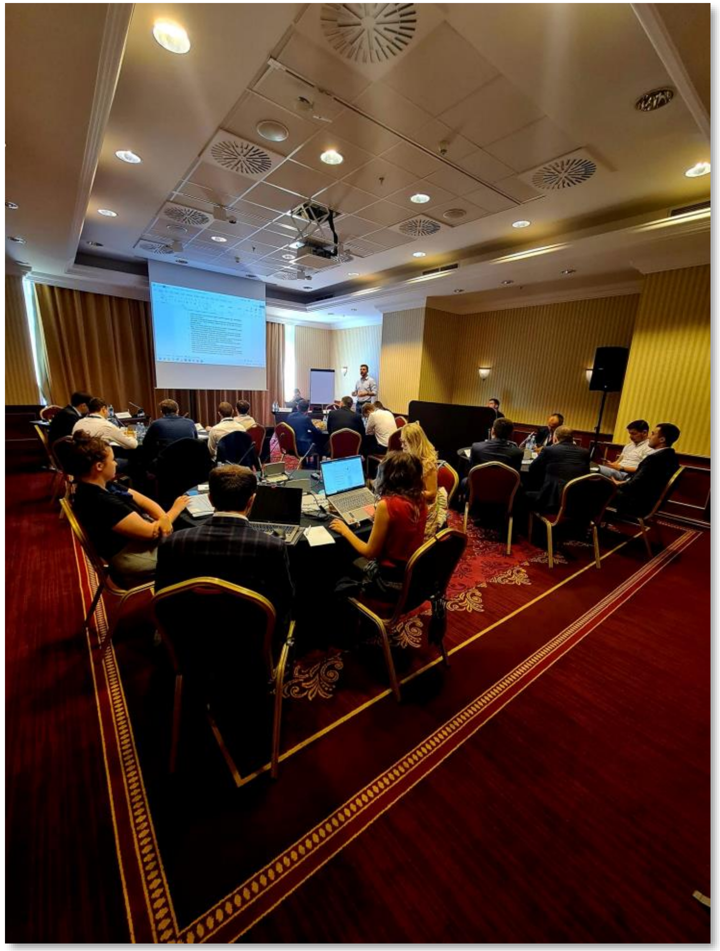
Phase III - Istanbul Forum February 2022

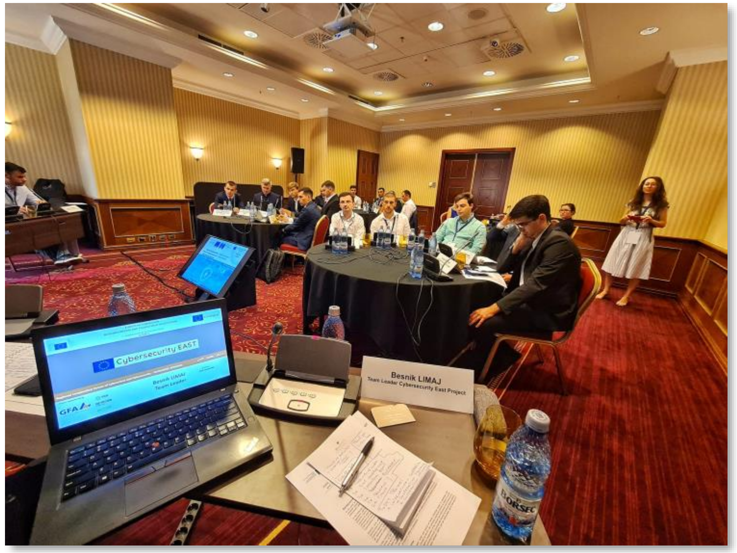
EUROPEAN COMMISSION
NEIGHBOURHOOD AND ENLARGEMENT NEGOTIATIONS
EU4Digital
Cybersecurity EAST
24TH FEBRUARY, 2022
ISTANBUL CYBER FORUM– CYBERSECURITY EAST PROJECT ACTIVITIES
Besnik LIMAJ
Team Leader
6 EaP Countries
Project implemented by
GFA CONSULTING GROUP
eGA
DETECON
ACTION
Regional Cooperation Forum of cybercrime and cybersecurity experts

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe
CYBERSECURITY EAST
&
CyberEast projects
Regional Cooperation Forum of Cybercrime and Cybersecurity Experts
Practical use cases for SOPs
Istanbul, Turkey
24 – 25 February 20
www.coe.i

Phase IV - Bucharest Forum on CSIRT and Law Enforcement Agencies (LEA) cross-network cooperation: June 2022



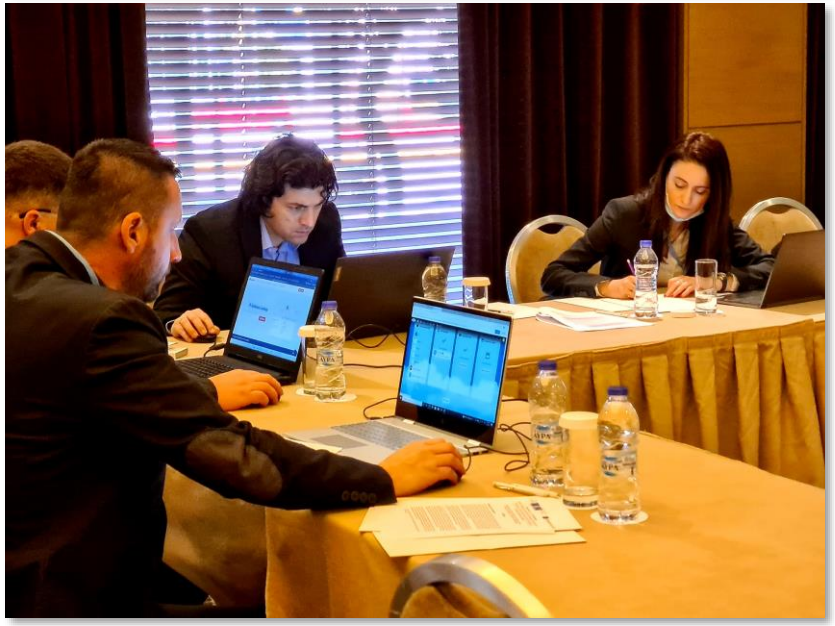




5 day Joined Technical Cyber Exercise - Athens -

5 day Joined Technical Cyber Exercise in Athens

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe
Cybersecurity EAST
CyberEast and iPROCEEDS-2 projects
Regional Cyber Exercise of Law Enforcement and CSIRT Cooperation
Athens, Greece
7 – 11 March 2022
www.coe.int/cybereast
www.coe.int/iproceeds-2
www.gfa-group.de/cyber



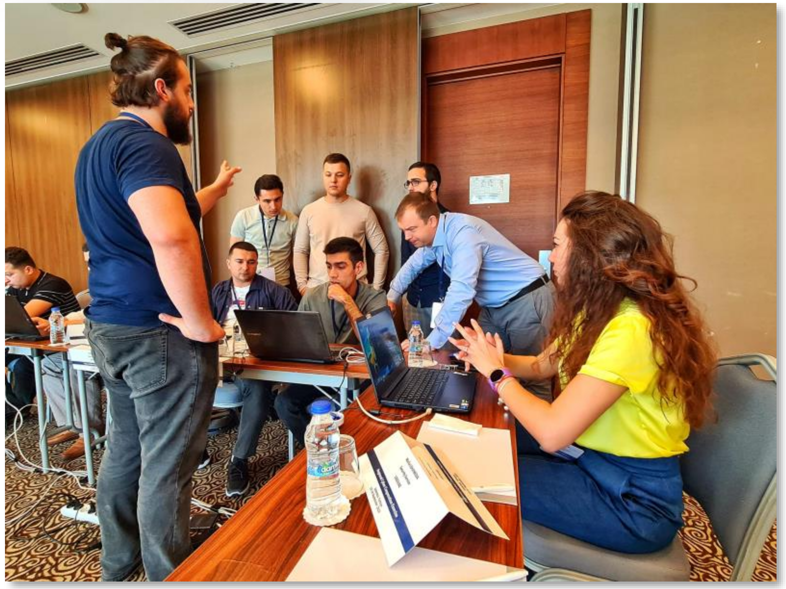
2 day Joined Table - Top Cyber Exercise

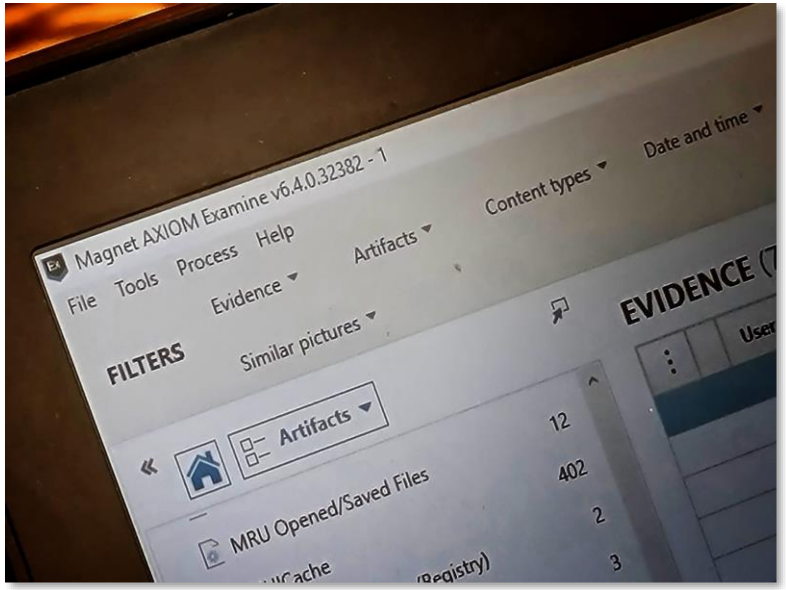
Tabletop Cyber Exercise
for policy makers on critical
information infrastructure
protection and cybercrime

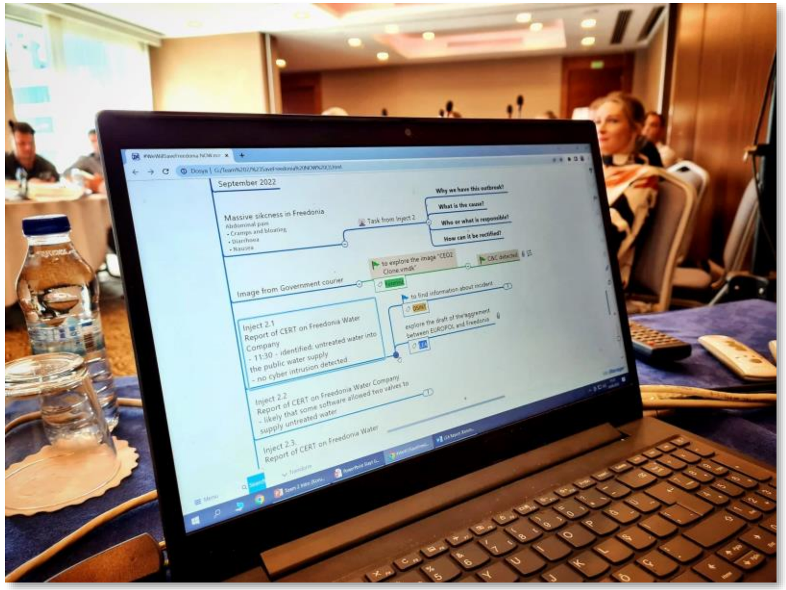
5 day Joined Technical Cyber Exercise Istanbul - September 2022

5 day Joined Technical Cyber Exercise Istanbul - September 2022

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe
CYBERSECURITY EAST
&
CyberEast projects
Regional Cyber Cooperation Exercise
Istanbul, Türkiye
13-16 September 2022
www.coe.int/cybereast
www.gfa-group.de/cybersecurity






September 2022
Massive sikcness in Freedonia
Image from Government courier
Inject 2.1
Report of CERT on Freedonia Water Company
Inject 2.2
Report of CERT on Freedonia Water Company
Inject 2.3
Report of CERT on Freedonia Water

Yandex Taxi hack creates huge traffic jam in Moscow

"Maroochy Scada Attack"

More than 1m litres of untreated sewage released into waterways and local parks

Vitek Boden

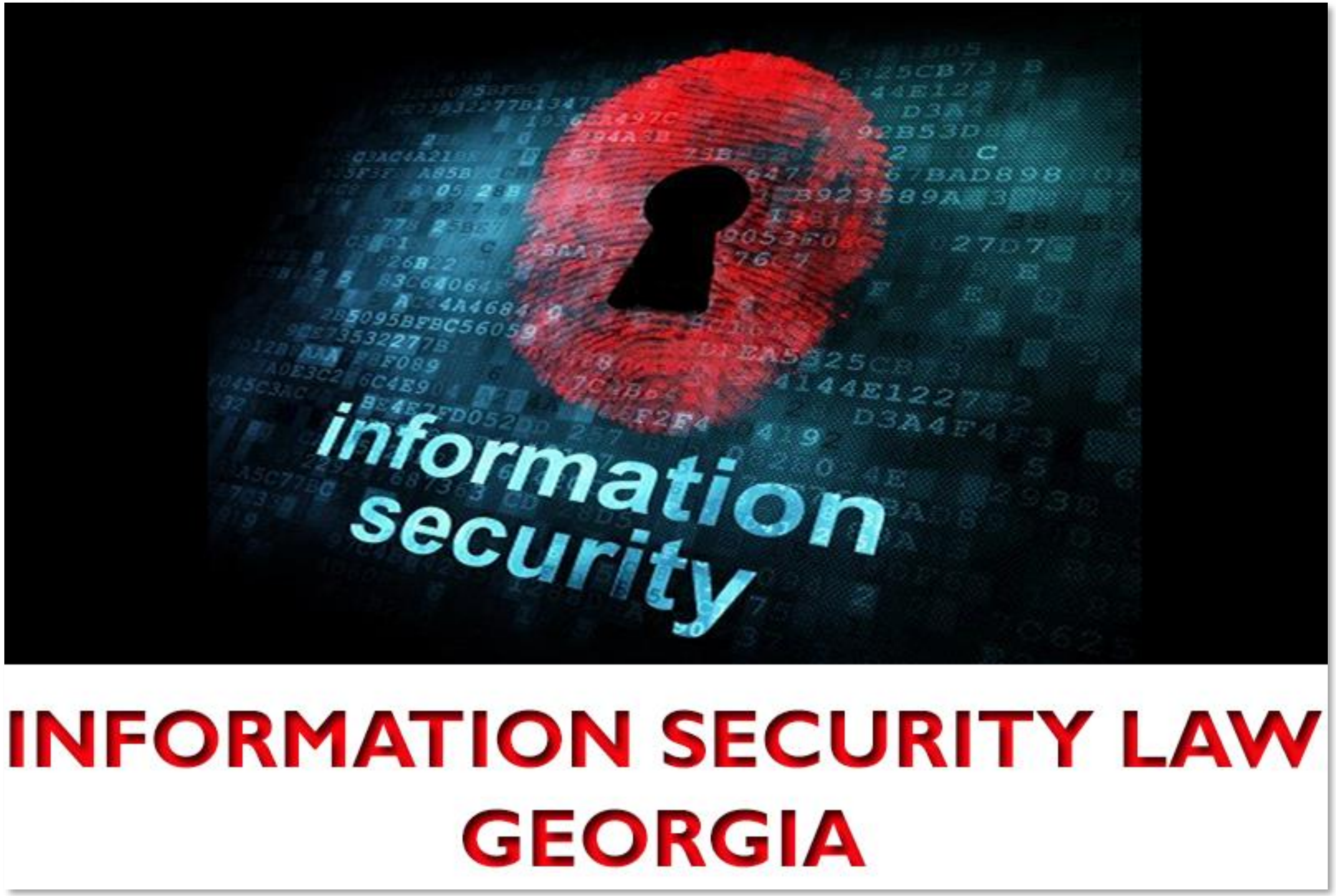
- **Vitek Boden** worked for **Hunter Watertech** (system suppliers) with responsibility for the **Maroochy system installation**.
- He left the job after **disagreements with the company**.
- He **tried to get a job** with local Council but was **refused**.

REVENGE!!

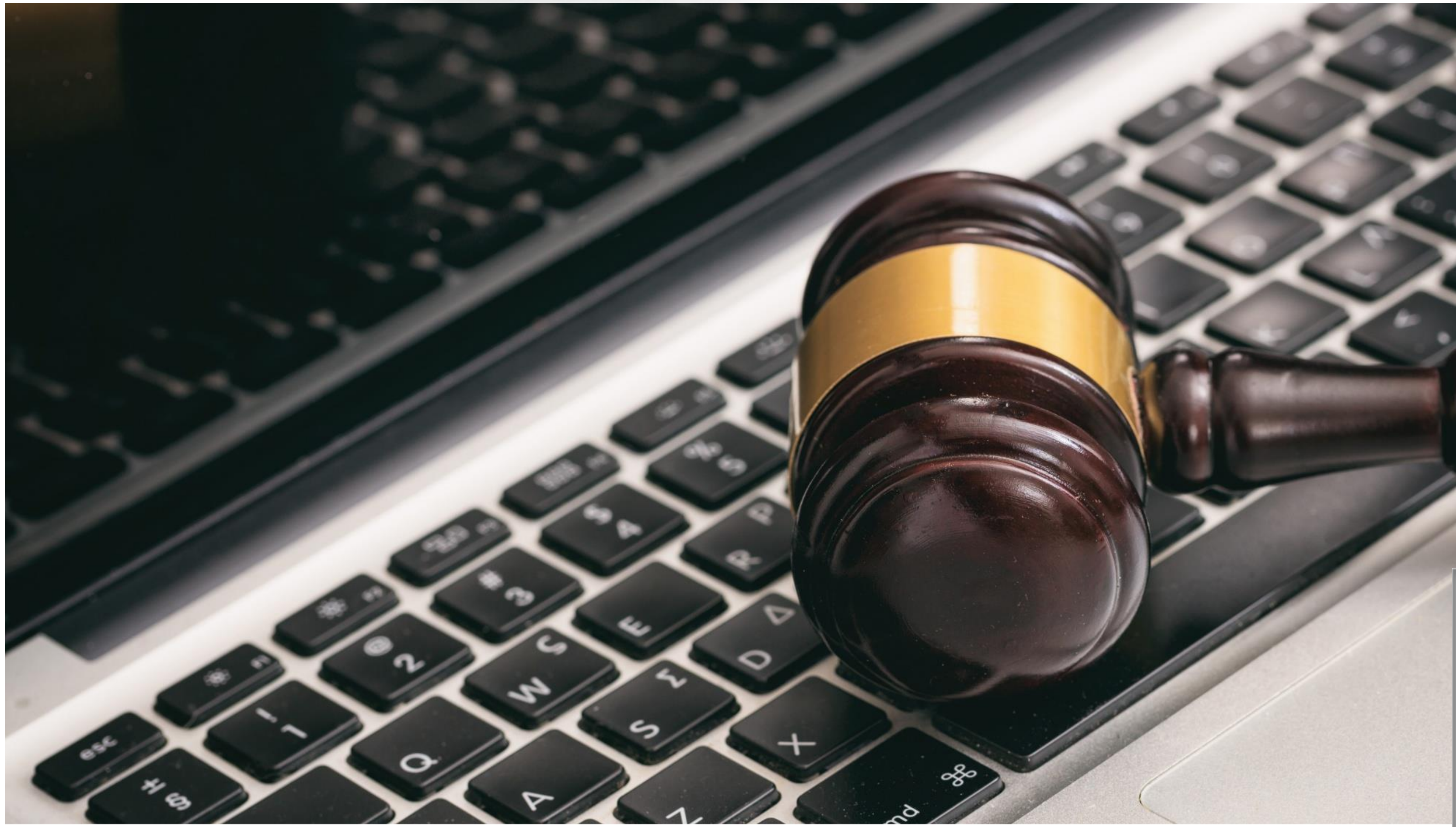
- Boden was **angry** and decided to **take revenge** on both his previous employer and the Council by **launching attacks on the SCADA control systems**
- He hoped that Hunter Watertech would be blamed for the failure

Cybersecurity Legislation: The EU NIS Directive With Prof. Dr Udo Helmbrecht

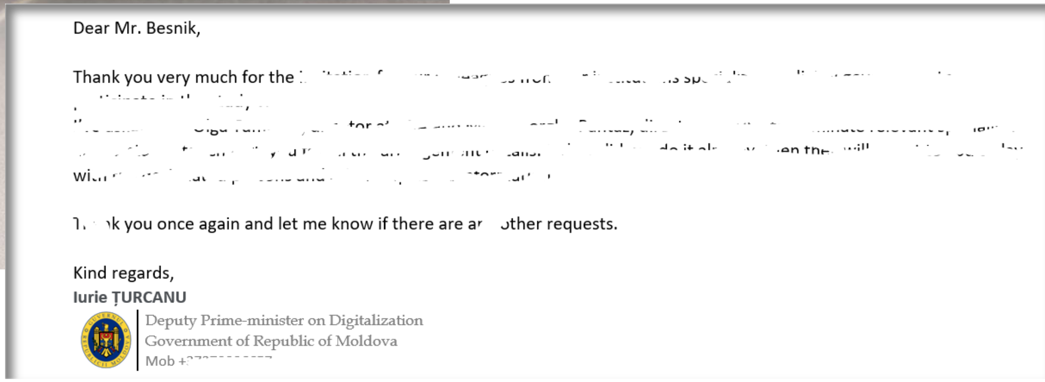
Approximation of ISL Georgia with EU NIS Directive



Cybersecurity Legislation: Support in Drafting the Cybersecurity Law in Moldova



CYBERSECURITY LAW
REPUBLIC OF MOLDOVA



Dear Mr. Besnik,

Thank you very much for the [redacted]

[redacted]

T[redacted]k you once again and let me know if there are a[redacted] other requests.

Kind regards,
Iurie ȚURCANU
Deputy Prime-minister on Digitalization
Government of Republic of Moldova
Mob +[redacted]

Cybersecurity EAST

Cybersecurity Legislation: Support in Drafting the Cybersecurity Law in Moldova

ROLE OF CIVIL SOCIETY

CYBERSECURITY LAW
REPUBLIC OF MOLDOVA

Cybersecurity EAST

LEAVE NO ONE BEHIND:
How to include civil society in cybersecurity

EU4DIGITAL IMPROVING CYBER RESILIENCE IN THE EAP COUNTRIES
This project is funded by the European Union
EIPS
European Institute for Political Studies
Cybersecurity EAST
CYBERSECURITY WORKSHOP
LEAVE NO ONE BEHIND
HOW TO INCLUDE CIVIL SOCIETY IN CYBERSECURITY

Cybersecurity and Human Rights Webinar

Cybersecurity EAST

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Joint Webinar - Hate Speech and Restrictive Measures -

Cybersecurity EAST

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Cyber Hygiene Training

DEFINIȚII

Ce este securitatea cibernetică?

Securitate cibernetică - starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spațiul cibernetic.

Măsurile proactive și reactive pot include politici, concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protejare a infrastructurilor cibernetice, managementul identității, managementul consecințelor.

EU4DIGITAL IMPROVING CYBER RESILIENCE IN THE EAP COUNTRIES

This project is funded
by the European Union

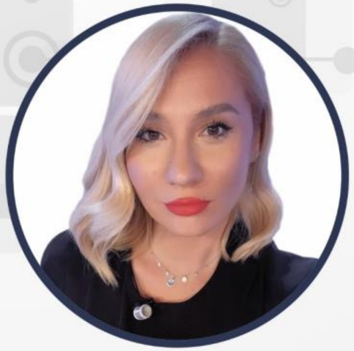
Cybersecurity EAST

WORKSHOP

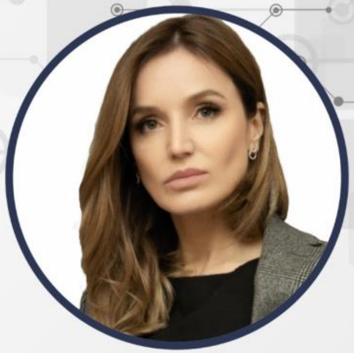
September 19th, 11:00 AM

BREAKING DOWN ONLINE DISINFORMATION: CAN WE BUILD RESILIENCE?

Besnik Limaj



Donika Emini



Natalia Spinu

Giorgi Iashvili

Roman Boiarchuk

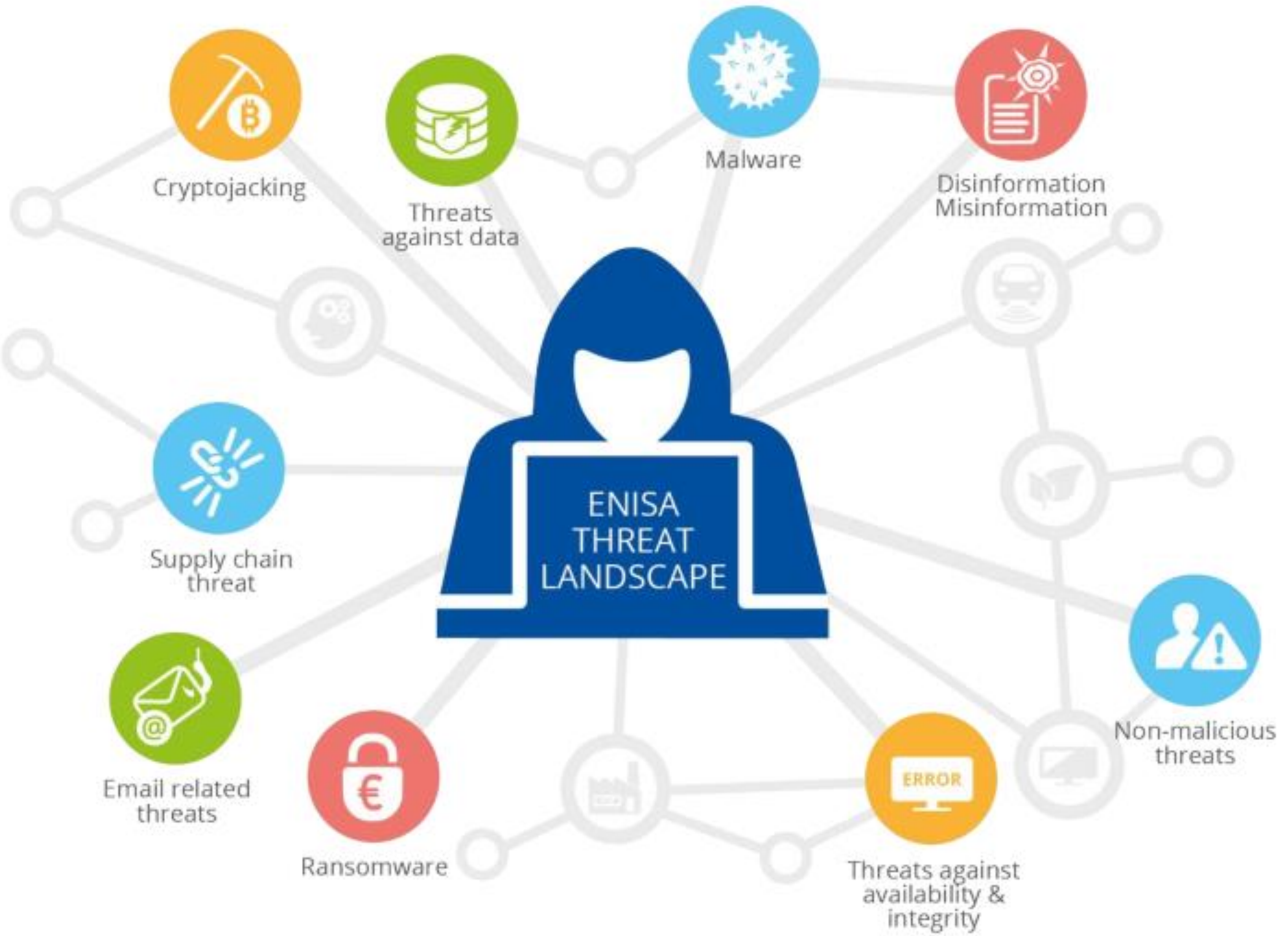
ENISA Prime Threat Landscape - Disinformation - Misinformation

enisa

ENISA THREAT LANDSCAPE 2021
October 2021

- Ransomware
- Malware
- Cryptojacking
- E-mail related threats
- Threats against data
- Threats against availability and integrity
- Disinformation – misinformation
- Non-malicious threats
- Supply-chain attacks

Figure 1: ENISA Threat Landscape 2021 - Prime threats



High Level Design – Technical Platform for CSIRT's

Cybersecurity EAST

NATIONAL / GOVERNMENT OR SECTORIAL CSIRT'S

High Level Design (HLD) of a Technical platform

Threat Assessment Handbook

CYBER
HYGIENE

EU – UKRAINE CYBER DIALOGUE -

Ministerstwo
Spraw Zagranicznych

Cybersecurity EAST

ENISA STUDY VISIT – DECEMBER 2015

enisa

THE EU
CYBERSECURITY
AGENCY

ENISA STUDY VISIT - OCTOBER 2022

Cybersecurity EAST
NEIGHBOURHOOD AND ENLARGEMENT NEGOTIATIONS
EU4Digital
3RD OCTOBER 2022
VISIT TO ENISA HQ, ATHENS, GREECE
Besnik LIMAJ
Team Leader
ENISA

Intermarium Conference – October 2022, Tbilisi, Georgia

ევროკავშირი
საქართველოსთვის
The European Union for Georgia

NATO
OTAN

ICSF

Intermarium Cyber Security Forum

“Cyber Security as a vital component of Critical Information Infrastructure Protection”

Intermarium Conference – October 2022, Tbilisi, Georgia

THE EUROPEAN UNION FOR GEORGIA
Cybersecurity EAST
Intermarium Cyber Security Forum

THE EUROPEAN UNION FOR GEORGIA
Cybersecurity EAST
Intermarium Cyber Security Forum

THE EUROPEAN UNION FOR GEORGIA
Cybersecurity EAST
Intermarium Cyber Security Forum

EU4DIGITAL IMPROVING CYBER RESILIENCE IN THE EAP COUNTRIES – CYBERSECURITY COMPONENT

This project is funded by the European Union

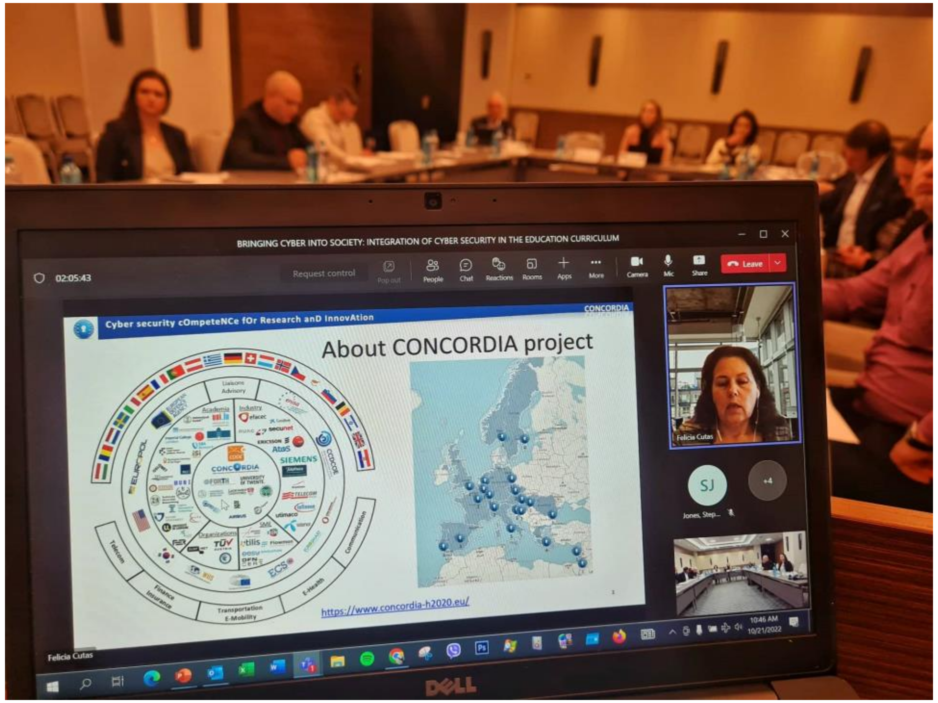
Cybersecurity EAST

CYBERSECURITY WORKSHOP

BRINGING CYBER INTO SOCIETY:

INTEGRATION OF CYBER SECURITY IN THE EDUCATION CURRICULUM

INTEGRATION OF CYBERSECURITY IN CYBER CURRICULA


BRINGING CYBER INTO SOCIETY: INTEGRATION OF CYBER SECURITY IN THE EDUCATION CURRICULUM
02:05:43
Leave
Cyber security cOmpeteNCe fOr Research anD InnovAtion
About CONCORDIA project
https://www.concordia-h2020.eu/
Felicia Cutas
SJ
DELL

BRINGING CYBER INTO SOCIETY: INTEGRATION OF CYBER SECURITY IN THE EDUCATION CURRICULUM
02:21:21
Leave
cyber discovery
A UK national cyber schools programme delivered by SANS, in partnership with HM Government
HM Government
SANS
SJ
MB
DK
LM
FC
SJ
Matt Birks (CyberStart) (Guest)
DELL

EXTENSION OF THE PROJECT

3

Project Extension

Cybersecurity EAST

FUNDS 1

EU
DG NEAR

BUDGET 2

NO COST
EXTENSTION

DURATION 3

JAN - 2023
DEC - 2023

COUNTRIES 4

EASTERN
PARTNERSHIP
COUNTRIES

THREE COMPONENTS

COMPONENT 1

Approximation of legislations and legal frameworks in line with the EU NIS Directive

COMPONENT 2

Identification of Operators of Essential Services (OES's) in line with NIS Directive

COMPONENT 3

Increased operational capabilities for cyber incidents and crisis management

METHODOLOGY

EU NIS 2.0 Directive

NIS 1

- HEALTHCARE
- TRANSPORT
- BANKING
- DIGITAL INFRASTRUCTURE
- WATER SUPPLY
- ENERGY
- DIGITAL SERVICE PROVIDERS

NIS 2

- FOOD
- MANUFACTURERS
- POSTAL & COURIER
- PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR SERVICES
- SPACE
- PUBLIC ADMINISTRATION
- DIGITAL SERVICES
- WASTE WATER AND WASTE MANAGEMENT

Empowering Women in Cyber

Women in Cyber at this week's Regional Cyber Exercise

Strengthening capacities against cybercrime and cybersecurity

CYBER
HYGIENE

TERENA
« networking the networkers »
NEWS · EVENTS · ACTIVITIES · PUBLICATIONS
ABOUT · CONTACT · SOCIAL · LOGIN ·
enter search
HOME › ACTIVITIES › TRANSITS › TRANSITS-I › PRAGUE › APR15

25th TRANSITS I Training Workshop

EU CERT's NETWORK MEETINGS

NEED FOR EXPERIENCE SHARING!!!

Tailor Made Trainings!

CompTIA Security+

CompTIA Network+

CompTIA CySA+

(ISC)² | CISSP® Certified Information Systems Security Professional

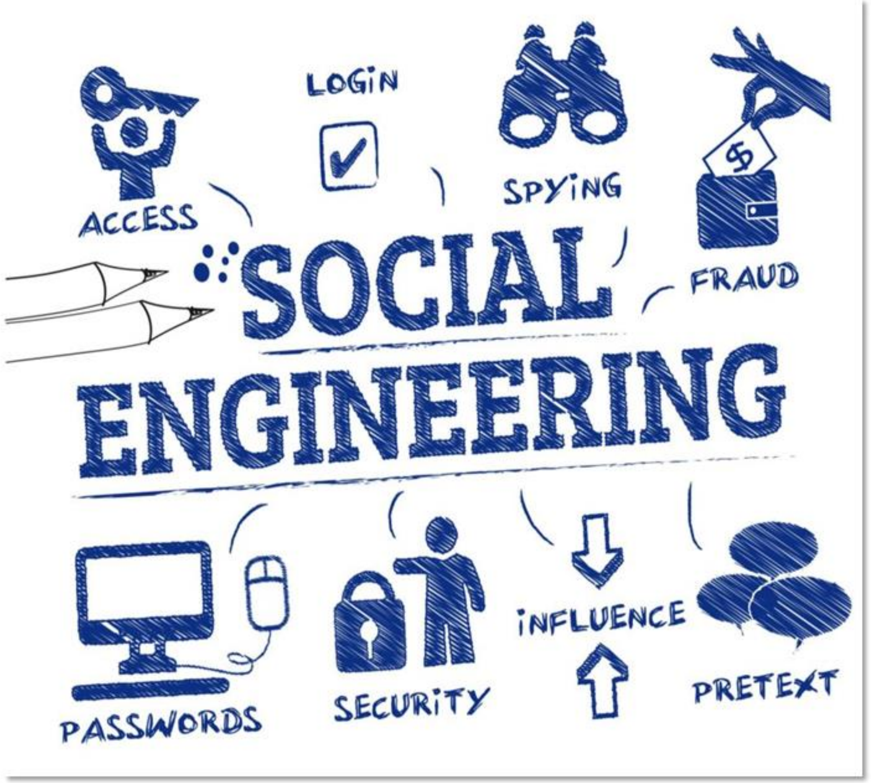
Welcome to the (ISC)² Certified Information Systems Security Professional (CISSP) Training Course

Cybersecurity EAST

Tailor Made Trainings!

OFFENSIVE SOCIAL ENGINEERING

Cybersecurity EAST



DEFENSIVE SOCIAL ENGINEERING!

Cybersecurity EAST

Tailor Made Trainings!

1 DAY Training

4 DAYS Training

Cybersecurity EAST

Tailor Made Trainings!

MATERA

MINI-MASTER in Operational Data Protection and Information Security

5 training modules in 4 days:

ROME, ITALY

AGENDA

5 training modules in 4 days:

☑ **DAY 1**

1) The protection of personal data in the GDPR, Hacking, Cybercrime and Cyber Espionage

☑ **DAY 2**

2) Security Awareness

3) Digital Self-Defense and Dark Web

☑ **DAY 3**

4) OSINT - Open Source Intelligence

☑ **DAY 4**

5) Laboratories: Cyber Crisis simulations and reporting to the Guarantor for data breach, OSINT missions. Final exam

CERT/CSIRT Tools TRAINING (ONLINE)

ARM AZE GEO MDA UKR

Cortex

&

TheHive

CSIRTs

enisa

MATURITY ASSESSMENT

MISP

Threat Sharing

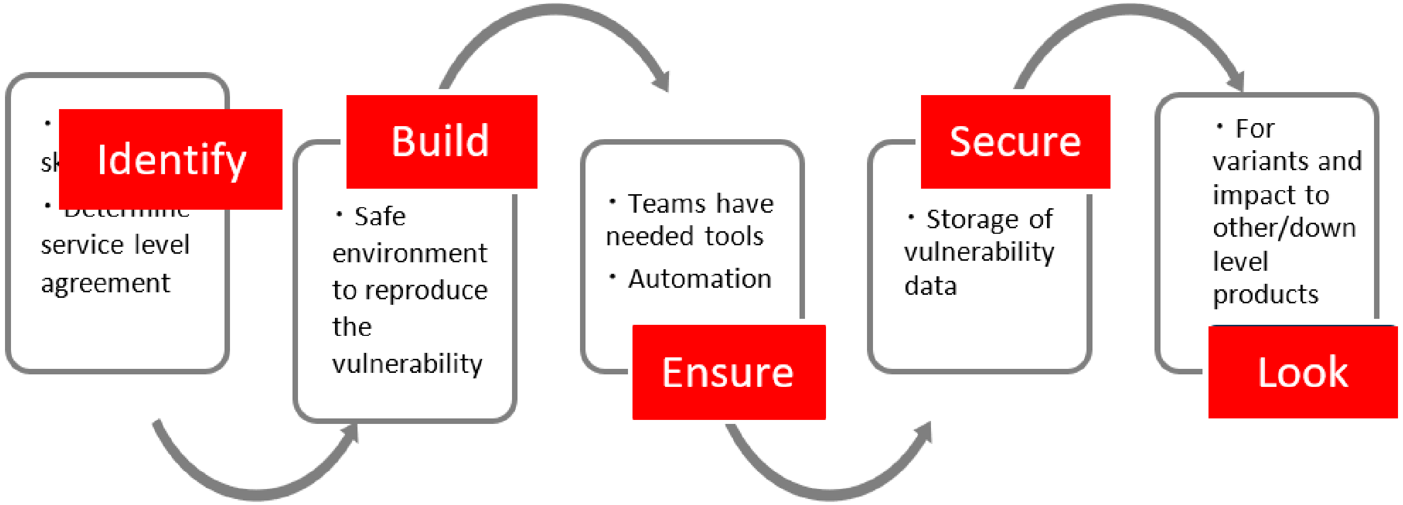
INTELMQ

elasticsearch + logstash + kibana

CERT/CSIRT TRAINING (ONLINE)

ARM AZE GEO MDA **UKR**

LINUX Forensics - Training


Identify
•
sk
• Determine service level agreement
Build
• Safe environment to reproduce the vulnerability
• Teams have needed tools
• Automation
Ensure
Secure
• Storage of vulnerability data
• For variants and impact to other/down level products
Look

FIRST CSIRT Services Framework - Training

Various Red Team - Blue Team - Technical Cybersecurity Exercises!

Study Visit for Lawmakers – Estonia

Cyber Security as Enabler of Digital Society
Cybersecurity EAST
The legal and regulatory framework for e-Governance

Study Visit for Lawmakers – Bonn & Berlin!

CSIRT – LEA Cooperation
Phase 5 and 6

Tailor Made Activities

International Cooperation

Cybersecurity EAST

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

TF-CSIRT
Trusted Introducer

GÉANT
ASSOCIATION
Networking • Services • People

FIRST
Improving Security Together

enisa

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

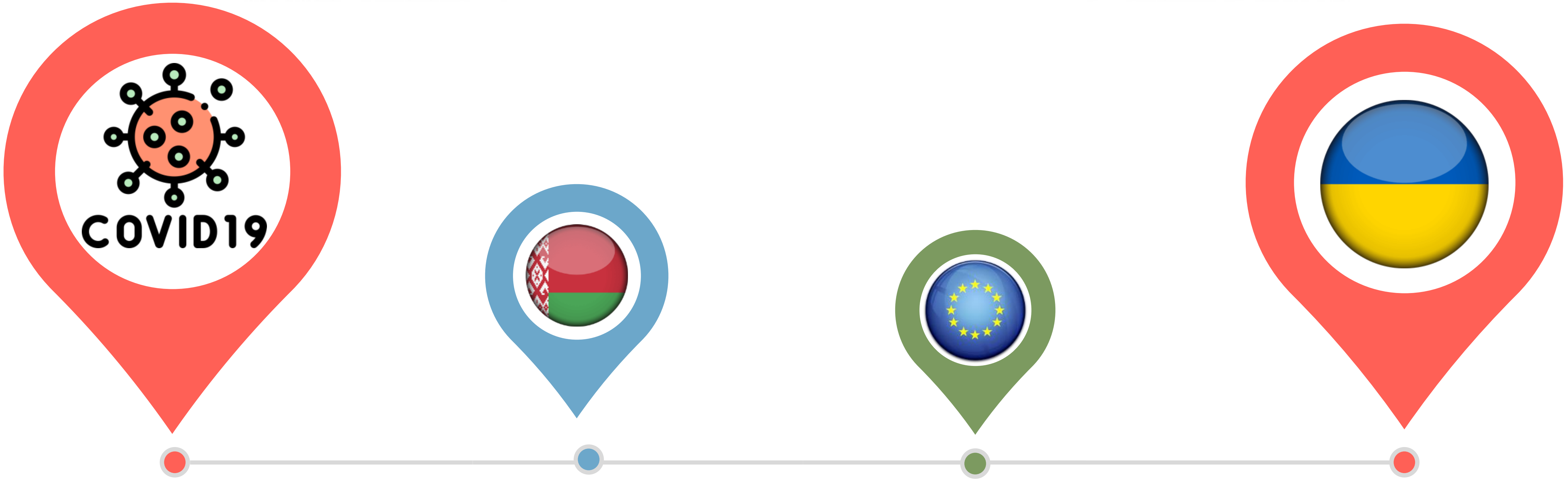
CRDFGLOBAL

INTERNATIONAL CRIMINAL INVESTIGATIVE TRAINING ASSISTANCE PROGRAM
US DEPARTMENT OF JUSTICE
ICITAP

UNDP

JICA
ジャイカ

In closing: Despite Encountered challenges



2020

CORONA VIRUS OUTBREAK

Immediate cessation of all physical presence activities

2020

BELARUS SANCTIONS

Immediate cessation of activities in Belarus

2021

CHANGE IN EU DG NEAR PROJECT MANAGEMENT

2022

WAR IN UKRAINE

Immediate cessation of activities in Ukraine

In Closing

Thank you!

Besnik LIMAJ, Team Leader
Email: besnik.limaj@gfa-group.de