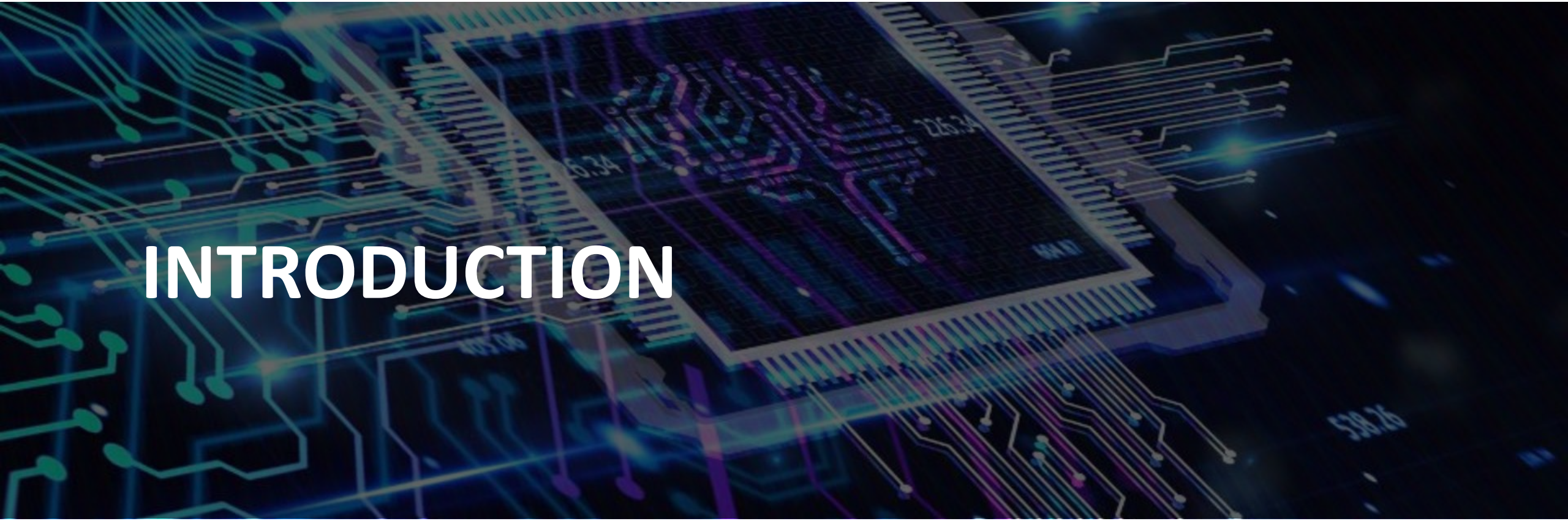
EAGLE
DIGITAL SKILLS TRAINING

Project EAGLE

CovEring the trAining Gap in digital skills for European SMEs manpowEr

This project has received funding from the European Union's Digital Europe Programme (DIGITAL) under grant agreement No 101100660. Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

EAGLE
DIGITAL SKILLS TRAINING



INTRODUCTION

Co-funded by
the European Union

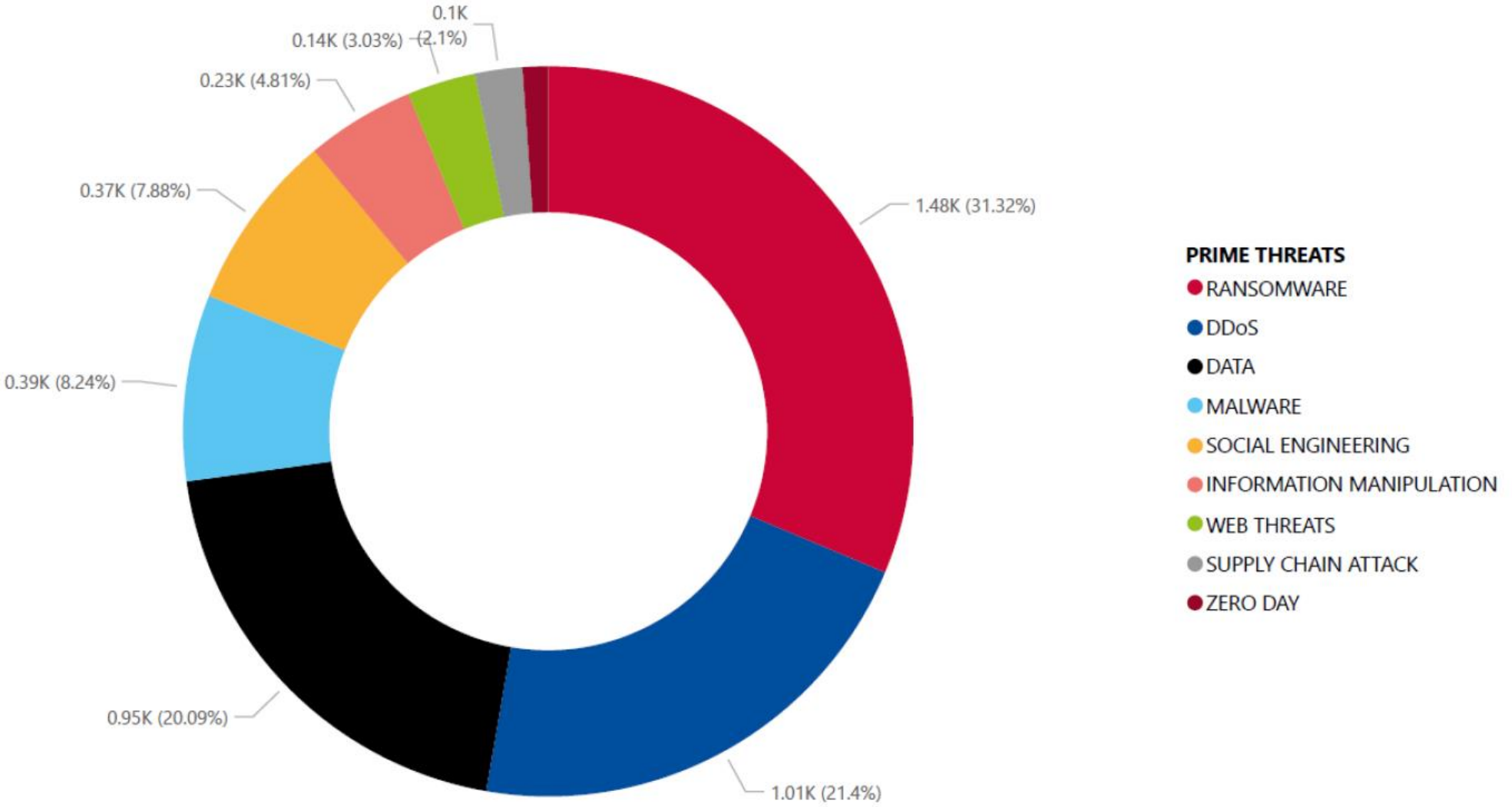
Cybersecurity

Cyber threats (attacks) are becoming an increasingly common phenomenon of the 21st century, so **cybersecurity is taking on** an increasingly important role in our lives. Cyber-attacks are usually launched directly against people **(social engineering)** rather than information systems, so the human factor **remains the most vulnerable part of cybersecurity.**

We will also must look at the additional measures and rules that must be followed to ensure adequate data security *(such as secure use of internet and e-mail functionality; software updates; device security; clean desk policy; document printing and storage; password use and management; behaviour in non-work environments, etc.) to ensure compliance.*

Co-funded by
the European Union

Co-funded by the European Union



Co-funded by
the European Union

Motivation

- **Financial gain**: any financially related action (carried out by mostly cybercrime groups);
- **Espionage**: gaining information on IP (Intellectual Property), sensitive data, classified data (mostly executed by state-sponsored groups);
- **Disruption**: any disruptive action done in the name of geopolitics (mostly carried out by state-sponsored groups);
- **Destruction**: any destructive action that could have irreversible consequences;
- **Ideological**: any action backed up with an ideology behind it (such as hacktivism).

Co-funded by
the European Union

Cybersecurity&data privacy and cybercrime: main concepts and definitions

PRIVACY AND DATA PROTECTION:

- Personal data
- Special categories of personal data
- Personal data processing
- Data controller
- Data processor
- Data subject
- Personal data breach.

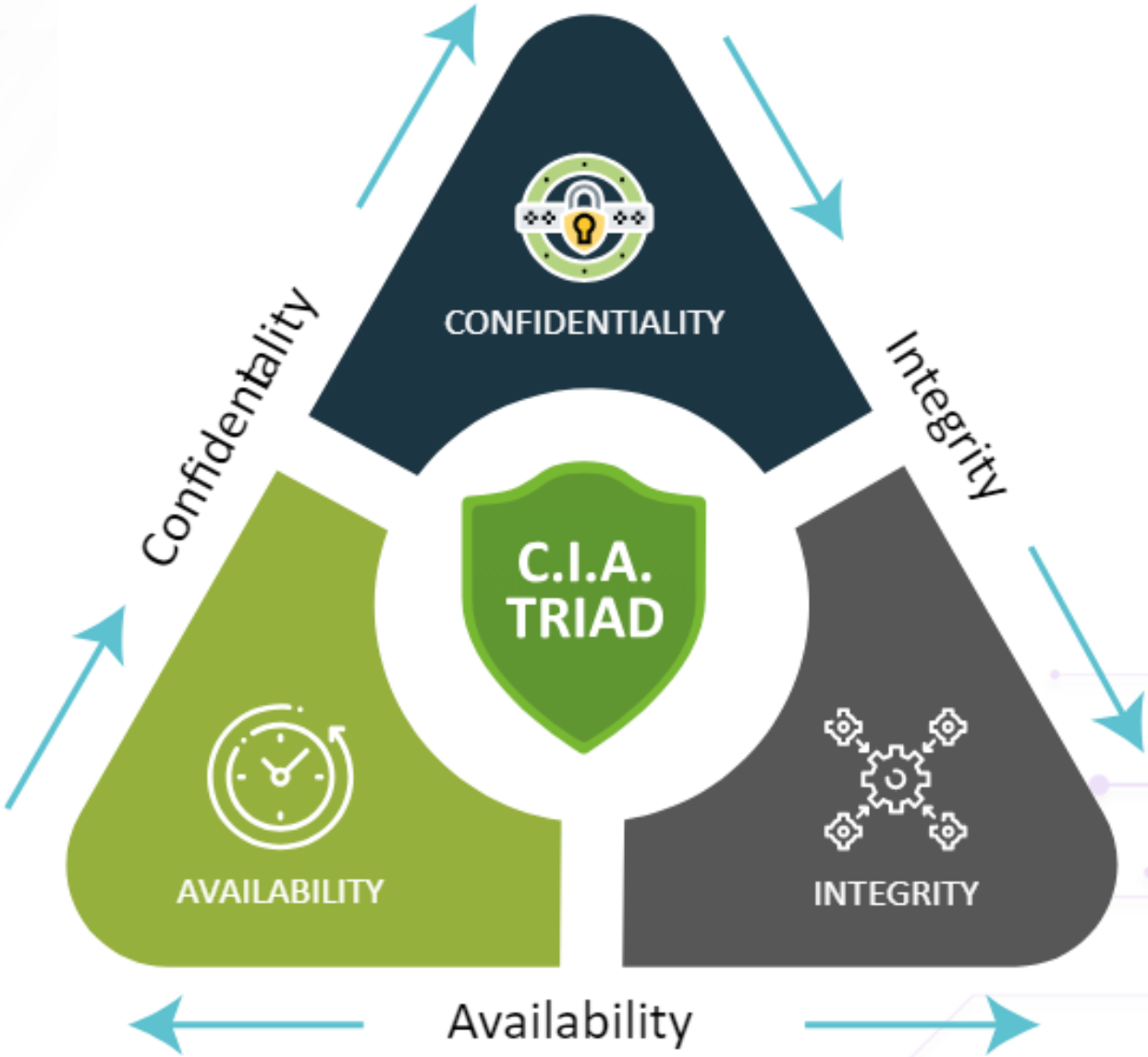
CYBERSECURITY:

- Cybersecurity subject
- Security of networks and information systems
- Incident
- Incident management
- Risk

CYBERCRIME:

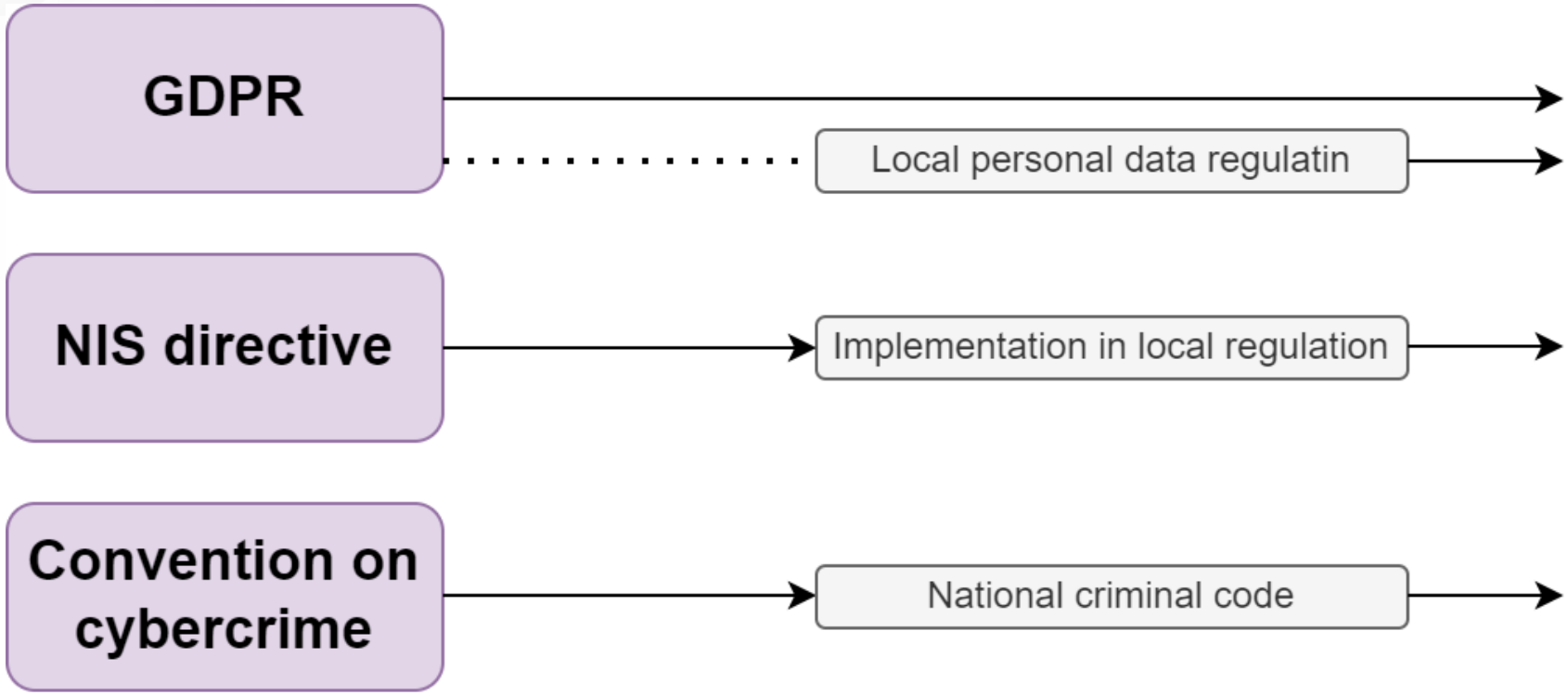
- Cybercrime
- Computer system
- Computer data
- Traffic data

Co-funded by the European Union



Co-funded by
the European Union

Cybersecurity&data privacy and cybercrime: legal environment



Co-funded by the European Union

Criminal code (Lithuanian example)

✓ ***Convention on cyber crime***.

✓ ***Criminal code of the Republic of Lithuania:***

- Unlawful access to electronic data
- Unlawful interference with an information system
- Unauthorised interception and use of electronic data
- Unauthorised access to the information system
- Unauthorised access to devices, software, passwords, codes and other data
- Traditional crimes that can be committed using cyberspace (e.g. fraud)

Co-funded by
the European Union

What is new on cyber threats

- *Supply Chain Attacks through the weakest chain part*
- *Internet of Things (IoT) Security*
- *Cloud Security - API attacks on distributed and cloud infrastructures*
- *BOYD and Shadow IT*
- *Remote work and nomads' lifestyle threats*
- *External infrastructure and social media threats*
- *Artificial Intelligence (AI)-Powered Attacks*

  - *Zero-Day Exploits + Gen AI*
  - *Business Email Compromise (BEC) + Gen AI*
  - *Deepfakes*
  - *Brand, reputation and communication attack – cheap fakes*

- *Cryptocurrency/Blockchain Threats*
- *Regulatory non-compliance scam*

Co-funded by
the European Union

How to prepare

- *Regularly updating software and systems*
- *Implementing strong password policies and multi-factor authentication*
- *Conducting regular security audits and penetration testing*
- *Encrypting sensitive data*
- *Establishing incident response plans*
- *Investing in cybersecurity insurance*
- *Working with reputable cybersecurity vendors and partners*
- *Constantly maintain CS awareness*

Co-funded by
the European Union

EAGLE
DIGITAL SKILLS TRAINING

Cybercrime, cyber threats and cybersecurity

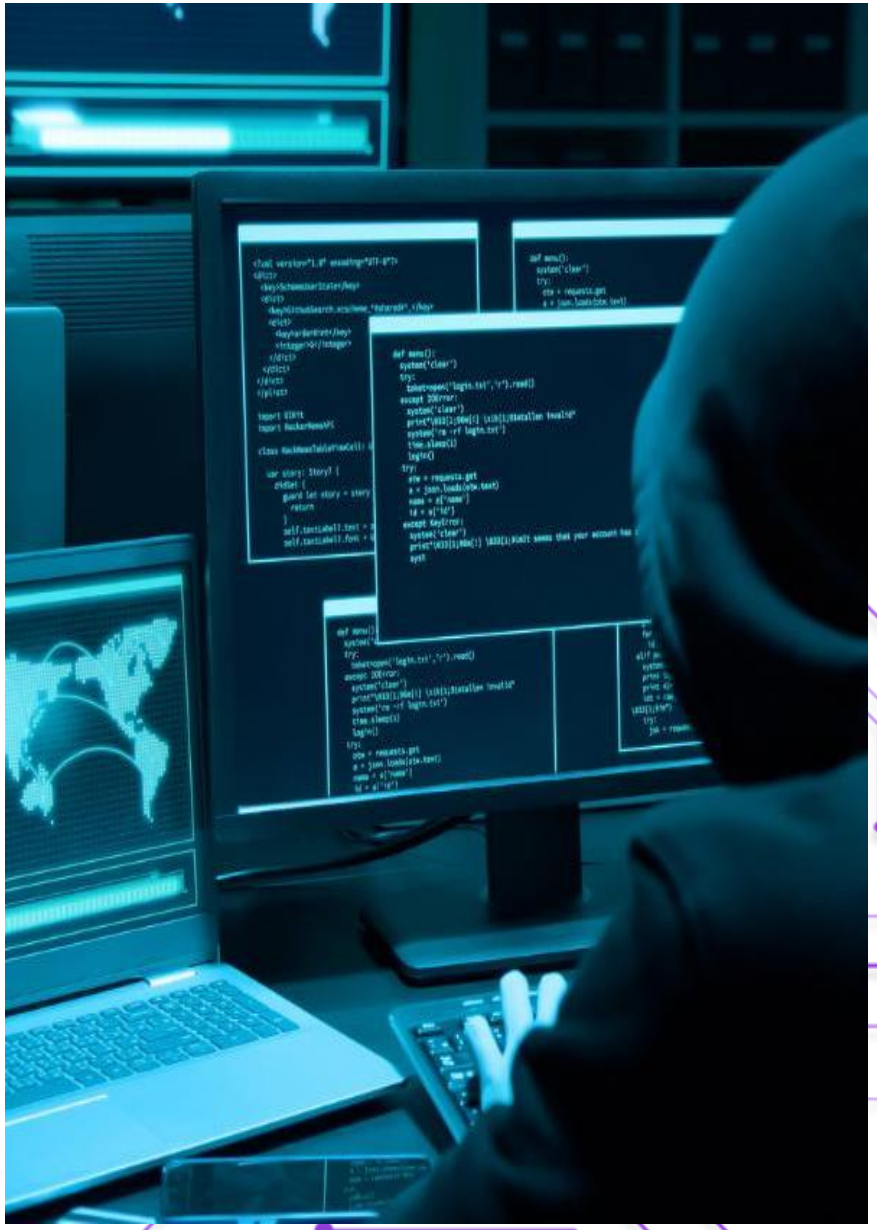
Training: June 18-19

Co-funded by
the European Union

Cybercrime, cyber threats and cybersecurity

1. Cybercrime, cybersecurity management competence and awareness, employess responsibilities and legal liability

- Cybersecurity&data privacy and cybercrime: main concepts and definitions.
- Cybersecurity&data privacy and cybercrime: legal environment.
- Cyber threats: how to recognize cyber threats. Cyber threat trends. The most common vulnerabilities.
- Hybrid threats. Practical examples.
- What must the company and/or institution ensure in order to protect itself from cyber threats?
- Knowledge of managers in the field of cyber security and their communication to employees.
- Internal cybersecurity documents. Formal compliance - how to avoid it?
- Organizational and technical security measures. Business continuity plan, etc. The importance of cyber hygiene.
- Employee duties according to the relevant segmented groups. Employee`s liability.
- How to assess the readiness of employees to recognize cyber threats? Effective methods of protection against social engineering.

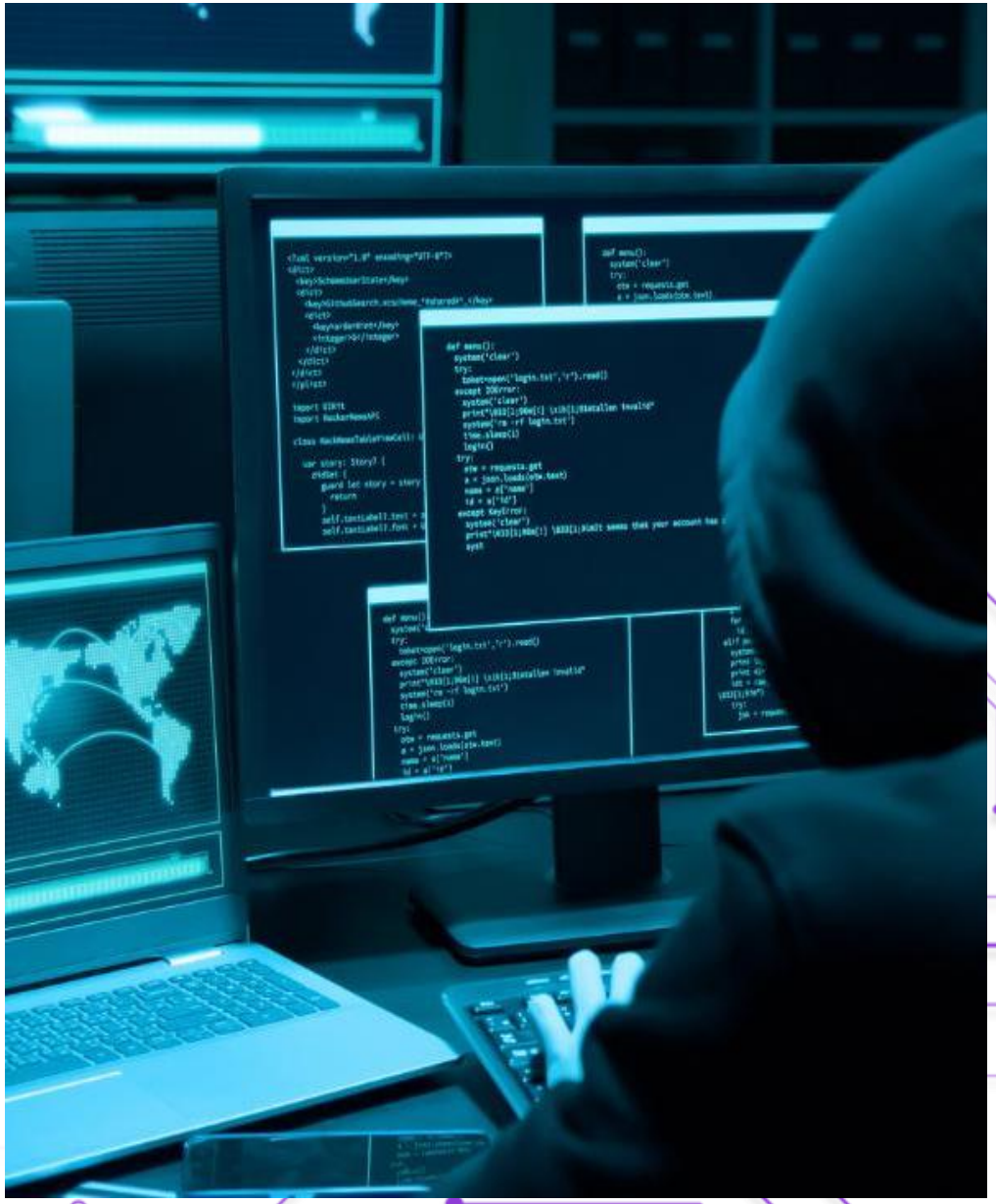


Co-funded by
the European Union

Cybercrime, cyber threats and cybersecurity

2. Cybersecurity risk assesment (data privacy impact assesment), cybersecurity incident management.

- Cybersecurity risk assesment. Risk assesment automatic tools.
- Assessment and control of suppliers' cyber security measures.
- Cyber incidents: types and duties during such incidents. How to internally and externally report a security incident. Relationship with cybercrime and personal data security breach.
- Responsible disclosure.
- How to deal with a crisis caused by a cyberattack? Practical examples.
- Awareness of cyber incidents / cybercrime and awareness through consequences.
- Institutions responsible for cybersecurity, cybercrime and data privacy. Their functions, examples of sanctions, etc.
- Practical part:
    1) Cybersecurity risk assesment using automatic risk assesment tool;
    2) Phishing exercise.



Co-funded by the European Union

EAGLE
DIGITAL SKILLS TRAINING

Register for the training:

June 18-19, 2024
Didlaukio str 55, (1st floor 102)
On-situ
Training is free of charge
NB! Limited places

EAGLE

DIGITAL SKILLS TRAINING

@projecteagle-eu

projecteagle.eu

@ProjectEAGLE_EU

EAGLE

DIGITAL SKILLS TRAINING

@projecteagle-eu

projecteagle.eu

@ProjectEAGLE_EU

UNIVERSIDAD DE BURGOS

MATEJ BEL UNIVERSITY

FAE Empresas Burgalesas

UNIVERSITY OF LIMERICK OLLSCOIL LUIMNIGH

VERNIAN rti

L3CE

DIHBU Digital Innovation Hub Industry 4.0

Slovak Chamber of Commerce and Industry

VSB TECHNICAL UNIVERSITY OF OSTRAVA

Skillnet IRELAND

TURKU AMK TURKU UNIVERSITY OF APPLIED SCIENCES

This project has received funding from the European Union's Digital Europe Programme (DIGITAL) under grant agreement No 101100660. Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.