Co-funded by the
Erasmus+ Programme
of the European Union

Introduction to Cybersecurity

February 2021

Domain: Wireless Networks and Analytics
Universiti Putra Malaysia (UPM)

Co-funded by the
Erasmus+ Programme
of the European Union

Topic

1. Cybersecurity Fundamentals
2. Cybersecurity Domain
3. Cybersecurity Threat: Malware
4. Cybersecurity Threat: Security Breaches
5. Cybersecurity Threat: Cyber Attacks
6. Critical Cyber Threats
7. Countermeasures and Defense

Co-funded by the
Erasmus+ Programme
of the European Union

Topic 1: Cybersecurity Fundamentals

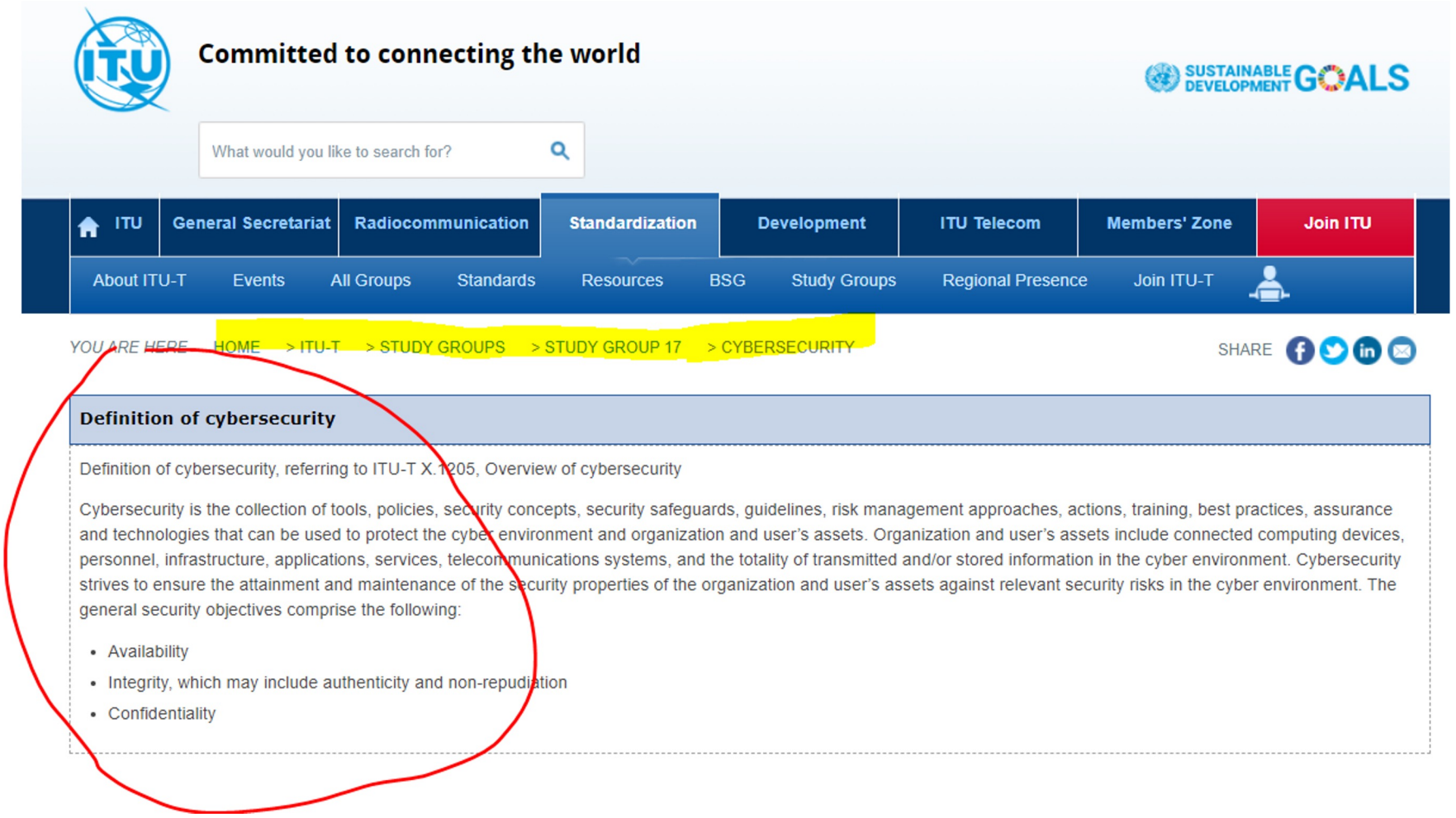
Co-funded by the
Erasmus+ Programme
of the European Union

Outline - Cybersecurity Fundamentals

- Definition and importance of cybersecurity
- Security goals: the CIA triad
- Vulnerabilities and threats
- Cyber space: issues and challenges
- Cybersecurity law and regulation

Co-funded by the
Erasmus+ Programme
of the European Union

Definition and Importance of Cybersecurity



Co-funded by the
Erasmus+ Programme
of the European Union

Security Goals

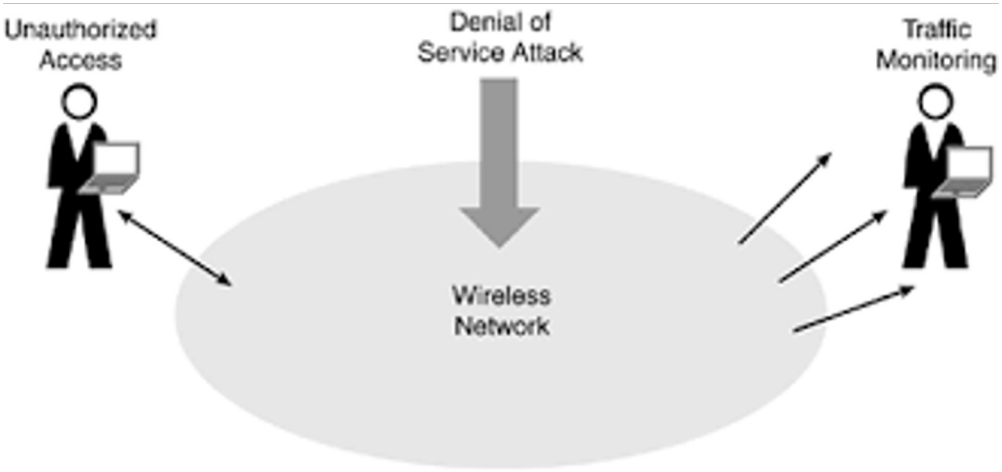
The CIA Triad refers to the 3 goals of cyber security Confidentiality, Integrity, and Availability of the organizations systems, network and data.

- Confidentiality – Keeping sensitive information private. Encryption services can protect your data at rest or in transit and prevent unauthorized access to protected data.
- Integrity – is the consistency of data, networks, and systems. This includes mitigation and proactive measures to restrict unapproved changes, while also having the ability to recover data that has been lost or compromised.
- Availability – refers to authorized users that can freely access the systems, networks, and data needed to perform their daily tasks. Resolving hardware and software conflicts, along with regular maintenance is crucial to keep systems up and available.

Co-funded by the
Erasmus+ Programme
of the European Union

Vulnerability and Threats

- Wireless Network Attacks
  - Accidental association
  - Malicious association
  - Ad-hoc networks
  - Non-traditional networks
  - Identity theft (MAC spoofing)
  - Denial of Service
  - Network injection



A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends

This paper examines the security vulnerabilities and threats in wireless communications and investigates efficient defense mechanisms for improving the security of wireless networks, with special attention to physical-layer security, an emerging paradigm.

By Yulong Zou, *Senior Member IEEE*, Jia Zhu, Xianbin Wang, *Senior Member IEEE*, and Lajos Hanzo, *Fellow IEEE*

- Reference: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7467419

Issues and Challenges

Co-funded by the Erasmus+ Programme of the European Union

Table 2 Main Protocols and Specifications of the Wireless OSI Layers

OSI Layers	Main Protocols and Specifications
Application	HTTP, FTP, SMTP [62]
Transport	TCP, UDP [63], [64]
Network	IP, ICMP [65]
MAC	CSMA/CA, ALOHA, CDMA [66], OFDMA [67]
PHY	Transmission Medium, Coding and Modulation

Table 4 Main Types of Wireless Attacks at the MAC Layer

MAC Attacks	Characteristics and Features
MAC spoofing	Falsification of MAC address [73]
Identity theft	Stealing of a legitimate user's MAC identity
MITM attack	Impersonation of a pair of communicating nodes [74]
Network injection	Injection of forged network commands and packets [75]

Table 3 Main Types of Wireless Attacks at the PHY Layer

PHY Attacks	Characteristics and Features
Eavesdropping	Interception of confidential information [71]
Jamming	Interruption of legitimate transmission [72]

Table 7 Main Types of Wireless Attacks at the Application Layer

Application Attacks	Characteristics and Features
Malware attack	Malicious software in the form of code, scripts and active content programmed by attackers [85]
SQL injection	Inserting rogue SQL statements attempting to gain unauthorized access to legitimate websites
Cross-site scripting	Injecting client-side scripts into web pages for by-passing some of the access control measures
FTP bounce	Impersonating a legtimate user to gain unauthorized access [83]
SMTP attack	Malicious attacks in e-mail transfering between the SMTP servers and clients

Table 6 Main Types of Wireless Attacks at the Transport Layer

Transport Attacks	Characteristics and Features
TCP flooding	Sending a huge number of ping requests [80], [81]
UDP flooding	Launching an overwhelming number of UDP packets [82]
TCP sequence prediction attack	Fabrication of a legitimate user's data packets using the predicted TCP sequence index

Table 5 Main Types of Wireless Attacks at the Network Layer

Network Attacks	Characteristics and Features
IP spoofing	Falsification of IP address [76]
IP hijacking	Impersonation of a legitimate user's IP address [77], [78]
Smurf attack	Paralyzation of a network by launching a huge number of ICMP requests [79]

Laws and Regulations

Co-funded by the
Erasmus+ Programme
of the European Union

Computer Crimes Act 1997

The Computer Crimes Act 1997 (CCA) created several offences relating to the misuse of computers, including unauthorised access to programmes or data stored in any computer, unauthorised modification of the contents of any computer, unauthorised modification of the contents of any computer, and wrongful communication of any means of access to a computer to an unauthorised person. The maximum financial penalties imposed under the CCA range from MYR25,000 to MYR150,000, and an individual may face imprisonment of up to ten years for crimes committed under the CCA.

Communications and Multimedia Act 1998

The Communications and Multimedia Act 1998 (CMA) provides a regulatory framework for the converging areas of communications and multimedia in Malaysia. In particular, it regulates various activities carried out by licensees registered under the CMA and ensures that information is secure, the network is reliable and service is affordable across Malaysia. The CMA includes certain provisions that deal with cybersecurity, such as prohibitions on the unlawful interception of communications and prohibitions on the creation of a system designed to fraudulently use or obtain any network facilities, network service, applications service or content application service.

Personal Data Protection Act 2010

The Personal Data Protection Act 2010 (PDPA) governs the processing of personal data in commercial transactions. Data users are generally required to adhere to the seven principles under the PDPA. The most relevant principle pertaining to cybersecurity is the security principle, where data users are required to take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. Further requirements and guidelines on the security principle are provided in the Personal Data Protection Regulations 2013 and the Personal Data Protection Standard 2015.

Digital Signature Act 1997

The Digital Signature Act 1997 (DSA) is an enabling law that promotes the development of e-commerce by securing electronic transactions using digital signatures. Put simply, digital signature is an electronic signature used to verify the identity of the sender of a message and to ensure the correctness and validity of information in electronic transactions. The DSA gives legal recognition to digital signatures and verifies the use of digital signatures through certificates issued by licensed certification authorities.

National Cyber Security Policy

Other than the legislation mentioned above, the National Cyber Security Policy (NCSP) is designed to address risks to the Critical National Information Infrastructure (CNII) concerning the networked information systems of ten sectors – ie, defence and security, transportation, banking and finance, health services, emergency services, energy, information and communications, government, food and agricultural, and water..

Co-funded by the Erasmus+ Programme of the European Union

The Eight Policy Thrusts

THRUST 1: Effective Governance

THRUST 2: Legislative & Regulatory Framework

THRUST 3: Cyber Security Technology Framework

THRUST 4: Culture of security and Capacity Building

THRUST 5: Research & Development Towards Self-Reliance

THRUST 6: Compliance and Enforcement

THRUST 7: Cyber Security Emergency Readiness

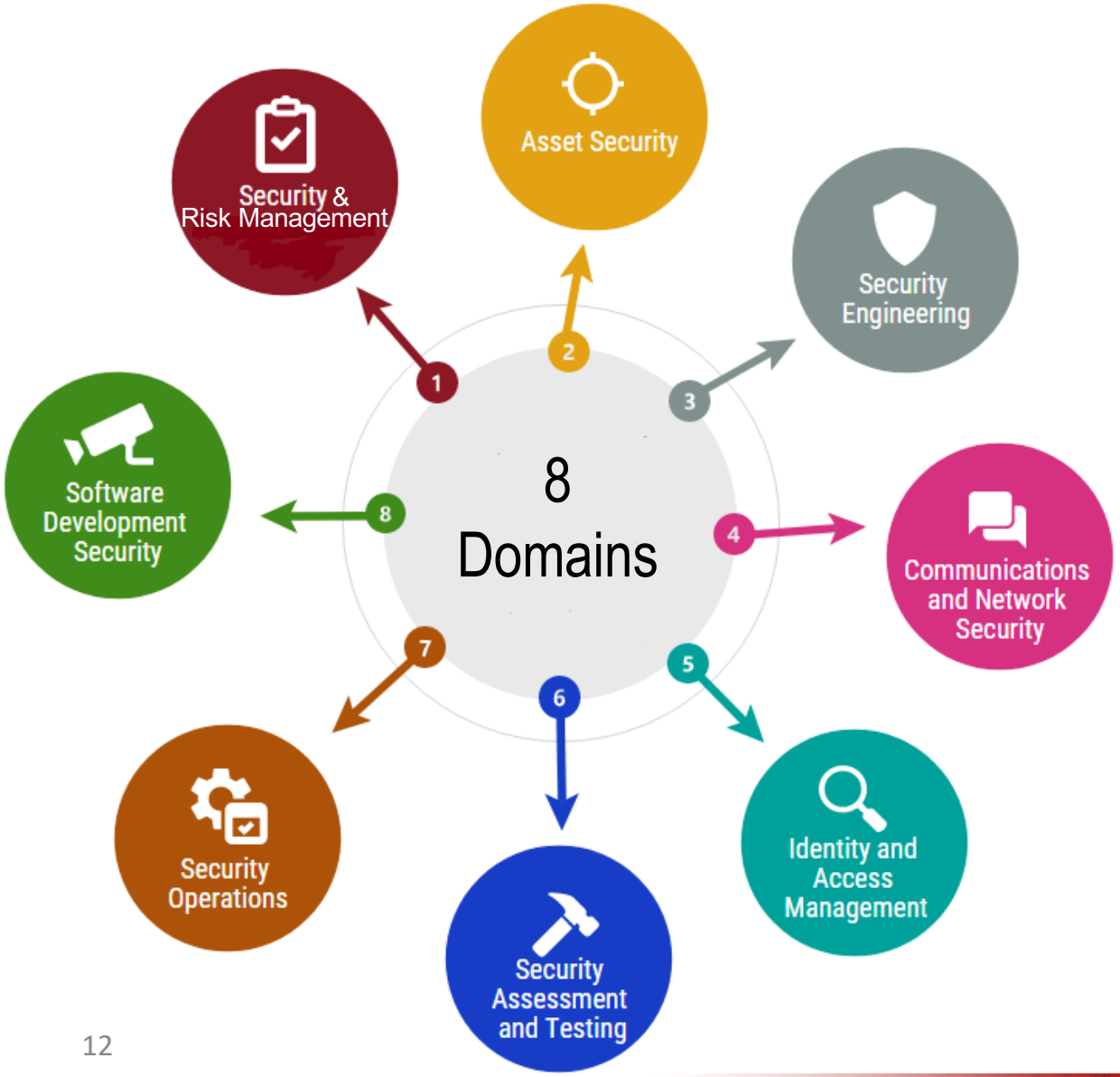
THRUST 8: International Cooperation

Reference: https://www.nacsa.gov.my/ncsp.php

Topic 2: Cybersecurity Domain

Co-funded by the
Erasmus+ Programme
of the European Union

Cybersecurity Domains



Cover various topics such as communications and network, stand alone device, security management, assessment and testing, etc.

Co-funded by the
Erasmus+ Programme
of the European Union

Security and Risk Management

Focuses on the following items:

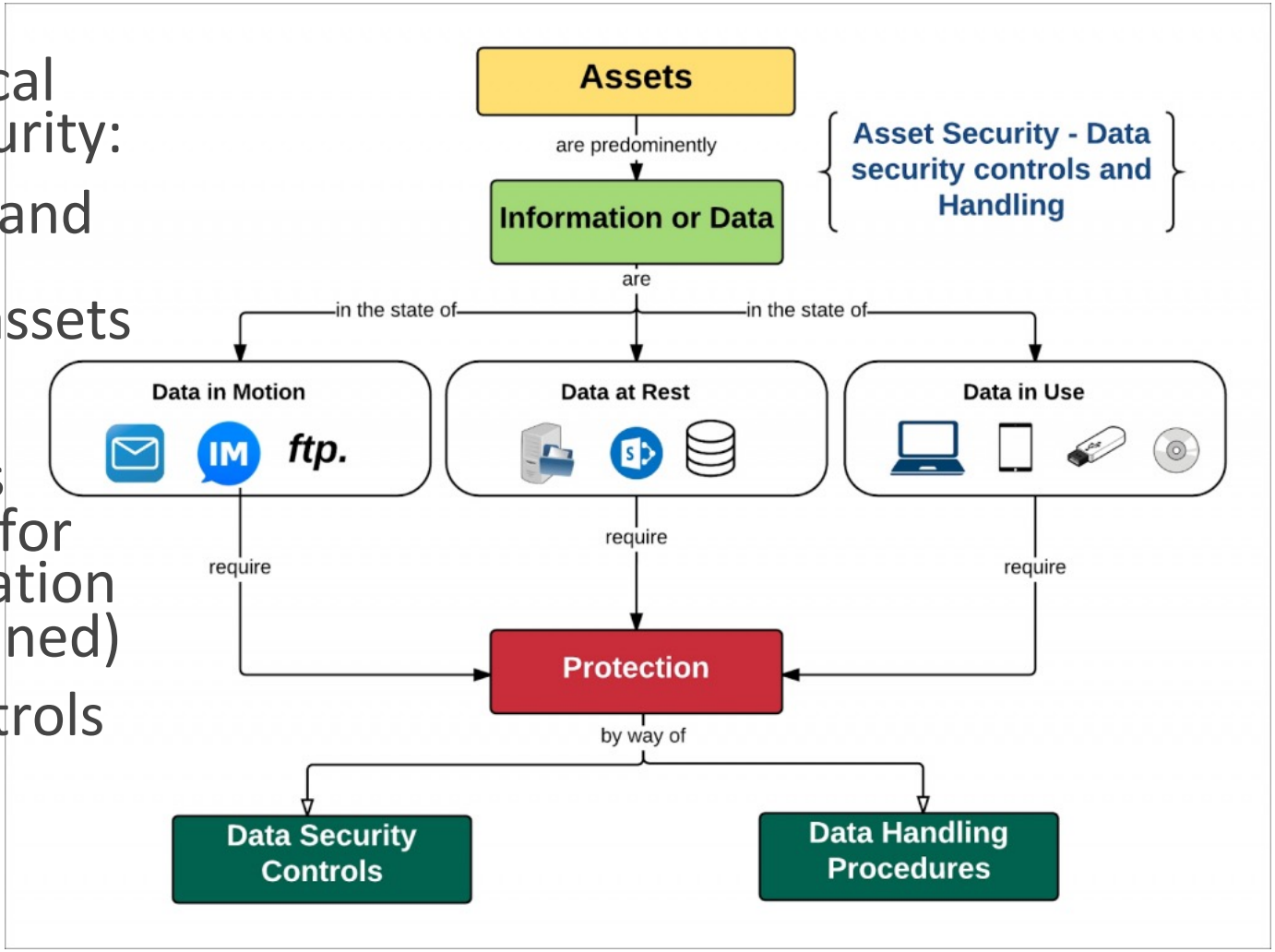
- CIA of information
- Security governance principles
- Compliance requirements
- Legal and regulatory issues relating to information security
- IT policies and procedures

Co-funded by the
Erasmus+ Programme
of the European Union

Asset Security

Addresses the physical requirements of security:

- The classification and ownership of information and assets
- Privacy
- Retention periods (duration of time for which the information should be maintained)
- Data security controls
- Handling requirements

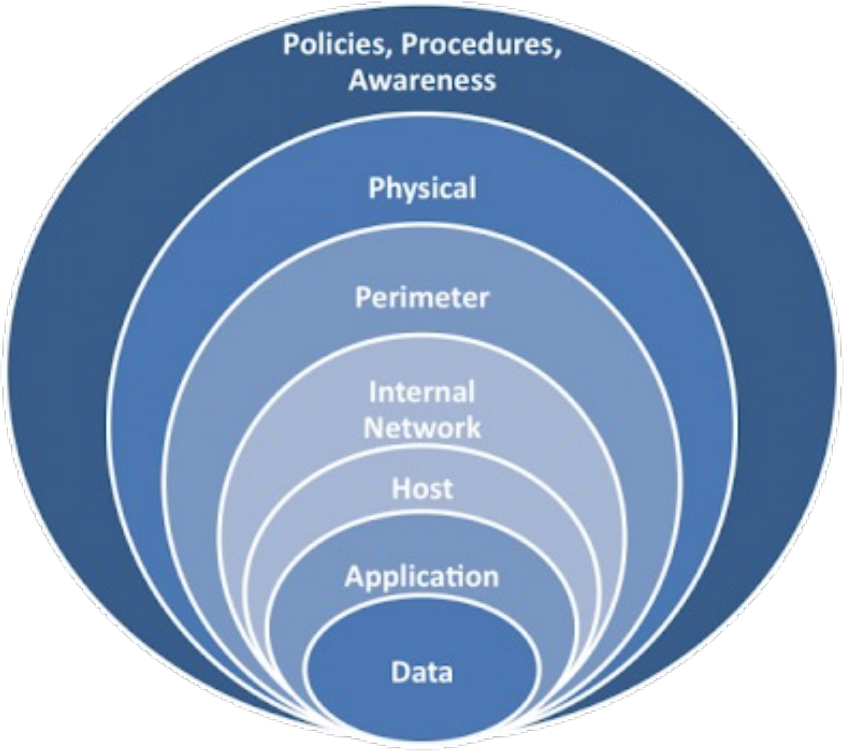


Co-funded by the
Erasmus+ Programme
of the European Union

Security Architecture and Engineering

The focus:

- Engineering processes using secure design principles
- Fundamental concepts of security models
- Security capabilities of information systems
- Assessing and mitigating vulnerabilities in systems
- Cryptography
- Designing and implementing security

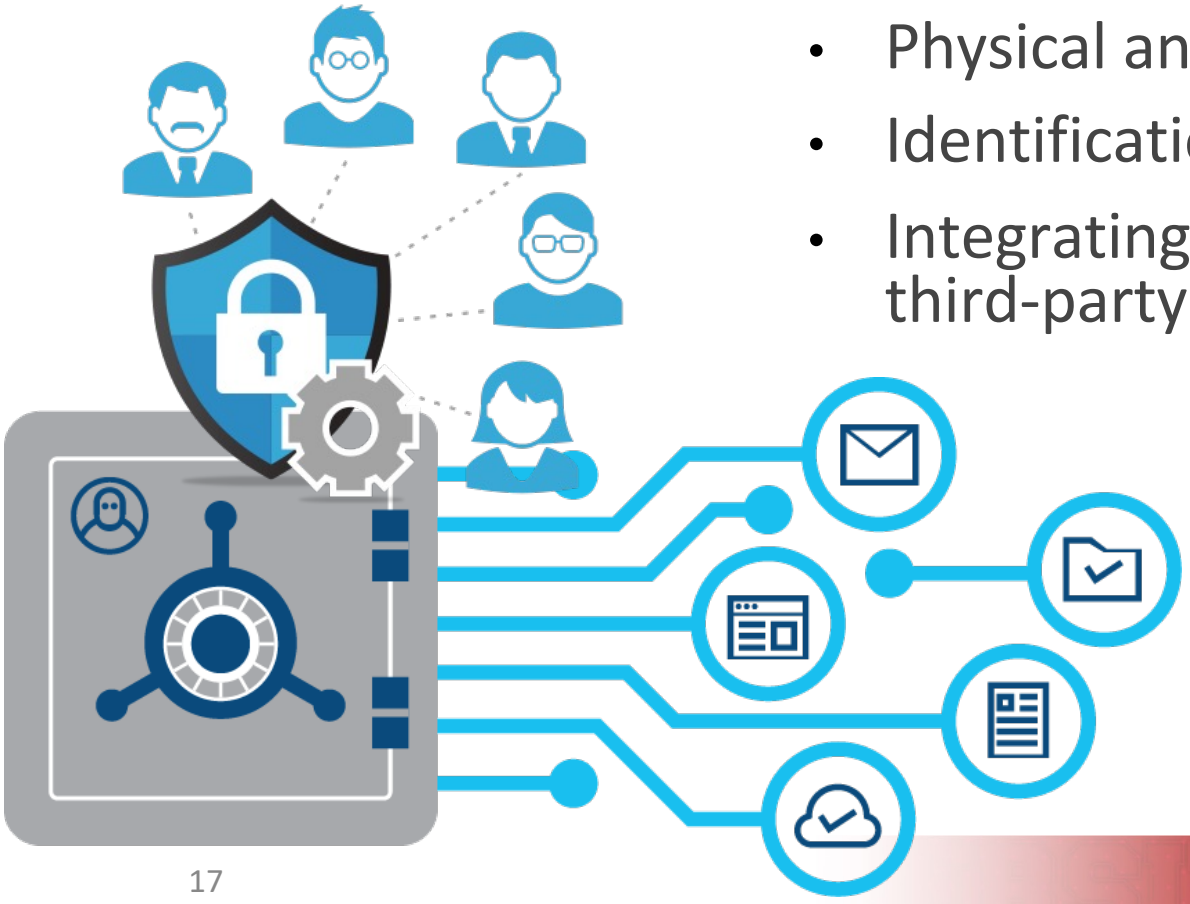


Communications and Network Security

Cover the design and protection of an organization's networks:

- Secure design principles for network architecture
  - Single point of failure?
  - Redundancy?
  - Segmentation?
- Secure network components
- Secure communication channels

Identity and Access Management



This domain focuses on data access control:

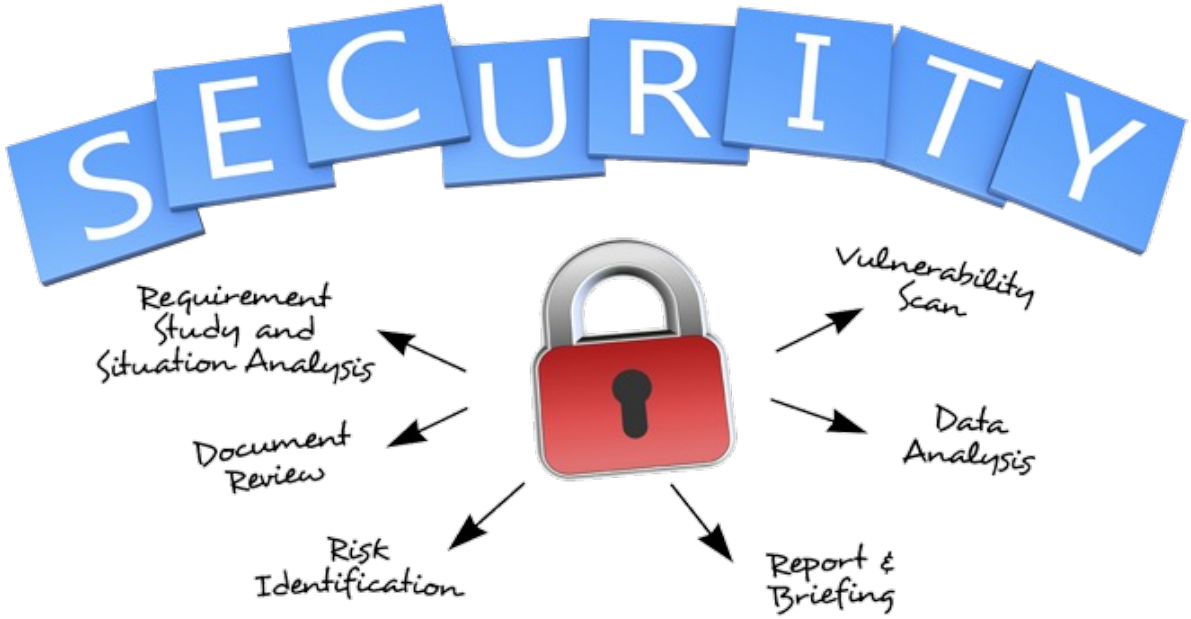
- Physical and logical access to assets
- Identification and authentication
- Integrating identity as a service and third-party identity services
- Authorization mechanisms
- The identity and access provisioning lifecycle

Co-funded by the
Erasmus+ Programme
of the European Union

Security Assessment and Testing

Focus on the design, performance and analysis of security testing:

- Designing and validating assessment and test strategies
- Security control testing
- Collecting security process data
- Test outputs
- Internal and third-party security audits



Co-funded by the
Erasmus+ Programme
of the European Union

Security Operations

This domain addresses the way plans are put into action, incident response and recovery:

- Understanding and supporting investigations
- Requirements for investigation types
- Logging and monitoring activities
- Applying resource protection techniques
- Incident management
- Disaster recovery

Co-funded by the
Erasmus+ Programme
of the European Union

Software Development Security

This domain helps professionals to understand, apply and enforce software security:

- Security in the software development life cycle
- Security controls in development environments
- The effectiveness of software security
- Secure coding guidelines and standards

Co-funded by the
Erasmus+ Programme
of the European Union

Topic 3: Cybersecurity Threat: Malware