Co-funded by the European Union

Course: Real time Cyber Threat Detection and Mitigation

Project: Cyber Security 4 ALL(CS4ALL)

Co-funded by
the European Union

Chapter 3: Enterprise Network Security

INDEX

Co-funded by the European Union

3.1 Enterprise Network

- The foundation of any contemporary midsize to large organization.
- Complex infrastructure
- difficult and expensive to build, maintain, manage, and secure
- Vital to smooth-running business operations.

An enterprise network elements:

1. Endpoints
2. Network Devices
3. Communication Protocol
4. Local Area Network
5. Wide Area Network

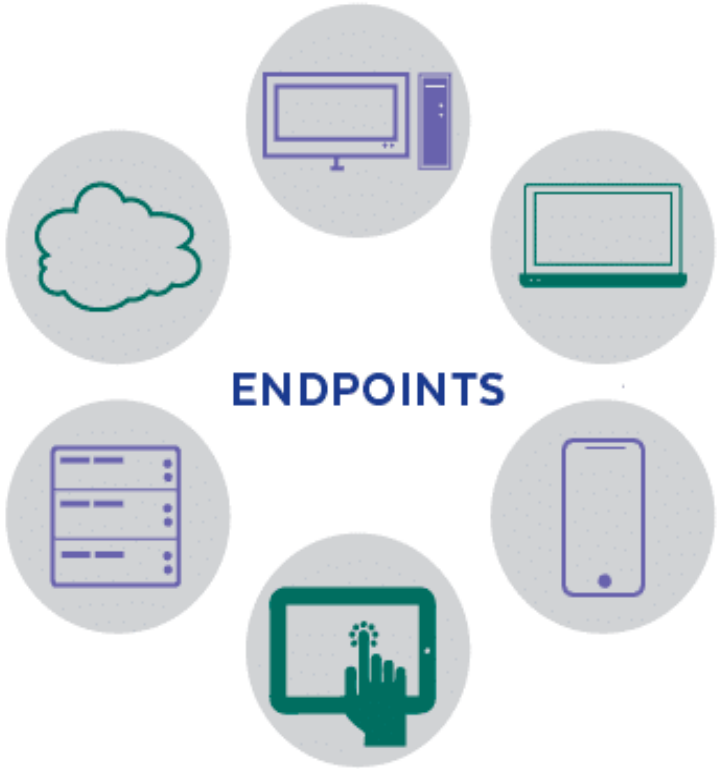
Co-funded by the European Union

Enterprise Network consist of

1. Endpoints: A remote computing device that can communicate with the network it is connected to.

Examples of endpoints:

- Desktop computers
- Laptops
- Smartphones
- Tablets
- Servers
- Workstations
- Internet of things (IoT)



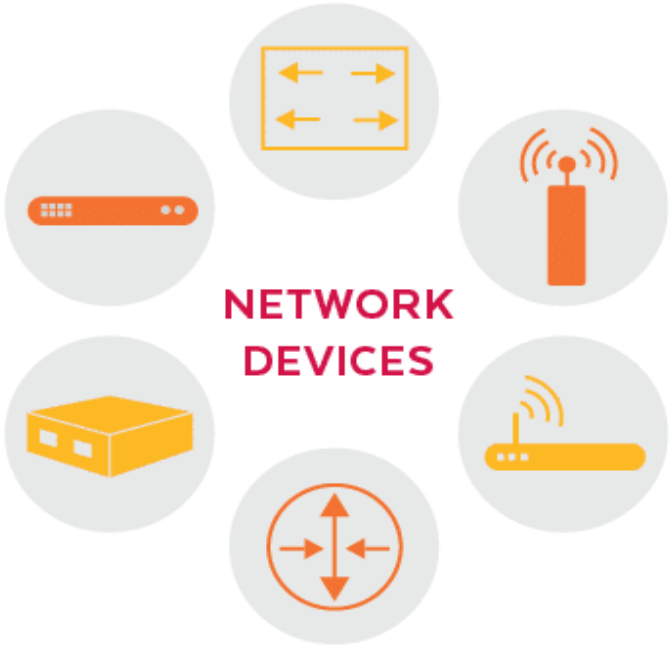
Co-funded by the European Union

Enterprise Network consist of

2. Network Devices: A physical apparatus required to obtain interaction/communication between hardware on a computer network.

List of common network Devices :

- Hub, Repeater, Switch
- Router, Bridge
- Gateway
- Modem
- Access Point



Enterprise Network consist of

3. Communication protocols: set of digital message formats and rules needed to exchange messages in or between computing systems.

List of communication protocols:

- File Transfer Protocol (FTP)
- Transmission Control Protocol/Internet Protocol (TCP/IP) and User Datagram Protocol (DP)
- Hypertext Transfer Protocol (HTTP)
- Post Office Protocol (POP3)
- Internet Message Access Protocol (IMAP)
- Simple Mail Transfer Protocol (SMTP)

Co-funded by the European Union

Enterprise Network consist of

4 Local Area Networks (LANs):

- An assemblage of connected devices in one physical location, such as a building, office, or home.
- A LAN can be large or small
- must be contained in one finite area.

5. Wide Area Networks (WANs):

- A collection of LANs that communicate with each other.
- it is a network of networks.
- The internet is the largest WAN in the world.

Co-funded by the European Union

Benefits of an Enterprise Network

1. Scans incoming data
2. Provides a high level of control over corporate resources
3. Speeds up routine operation
4. Provides virtualization
5. Offers improved Quality of Service (QoS)
6. Seamless connectivity between users and the cloud

Co-funded by the European Union

Enterprise Networking Security (ENS)

- The protection of a network that connects systems, mainframes, and devices like smartphones and tablets within an enterprise.
- Companies, universities, governments, and other entities use enterprise networks to help connect their users to information and people.
- As networks grow in size and complexity, security concerns also increase.

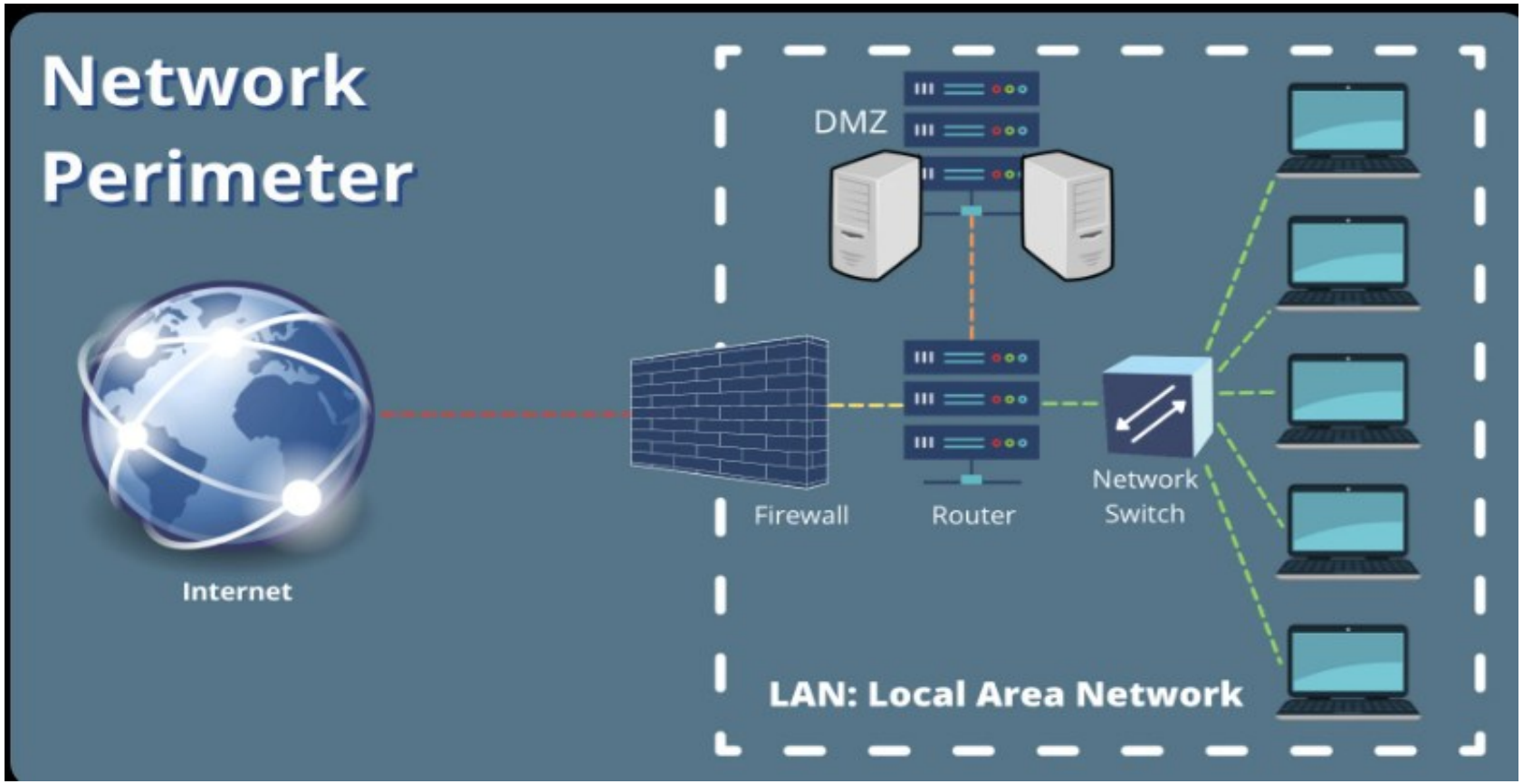
Co-funded by the European Union

ENS best practices

1. Create a comprehensive view of network infrastructure,
2. Employ network security solutions and Secure wireless networks.
3. Divide enterprise network into zones.
4. Use both hardware and software firewalls.
5. Use Virtual Private Networks (VPNs).
6. Enforce both multi-factor authentication (MFA) and strong passwords.
7. Establish a zero-trust strategy.
8. Train your employees to adhere to security policies and Conduct security audits and install updates.

Co-funded by the European Union

3.2 Network Perimeters



- Separates an organization's internal network from external networks
- Eg: Firewalls, IDPS, ACL

Network Perimeter

12

Network Perimeters Limitation

1. Insider threats
2. East-west traffic
3. Malware on mobile devices
4. Lateral movement
5. Vulnerabilities
6. False sense of security
7. Remote access

Co-funded by
the European Union

3.3 Perimeter Holes

Vulnerabilities in an organization's defenses that attackers exploit to gain unauthorized access. These can include:

1. Misconfigured Firewalls
2. Unpatched Software
3. Weak Authentication Protocols

Co-funded by the European Union

3.4 Third-Party Security

- Organization that has a business relationship and that has access to the organization's protected data assets.
- Third-party vendors and suppliers represent a severe security risk
- Cause for several global-scale attacks.
- Sets of practices, services, and technologies
- Can identify risks and protect organization from security threats associated with third-party vendors.

Co-funded by the European Union

3.5 Advanced Persistent Threats (APTs)

- Sophisticated cyber-attacks aim to steal sensitive information or compromise systems over a prolonged period
- Characterized by their stealth and persistence, often involving multiple stages.
- "Advanced" because they use clever, cutting-edge techniques
- "Persistent" because they don't give up easily and can stay hidden for a long time
- "Threat" because they can cause serious damage to an organization

Co-funded by the European Union

3.6 Large Government Agency Attack

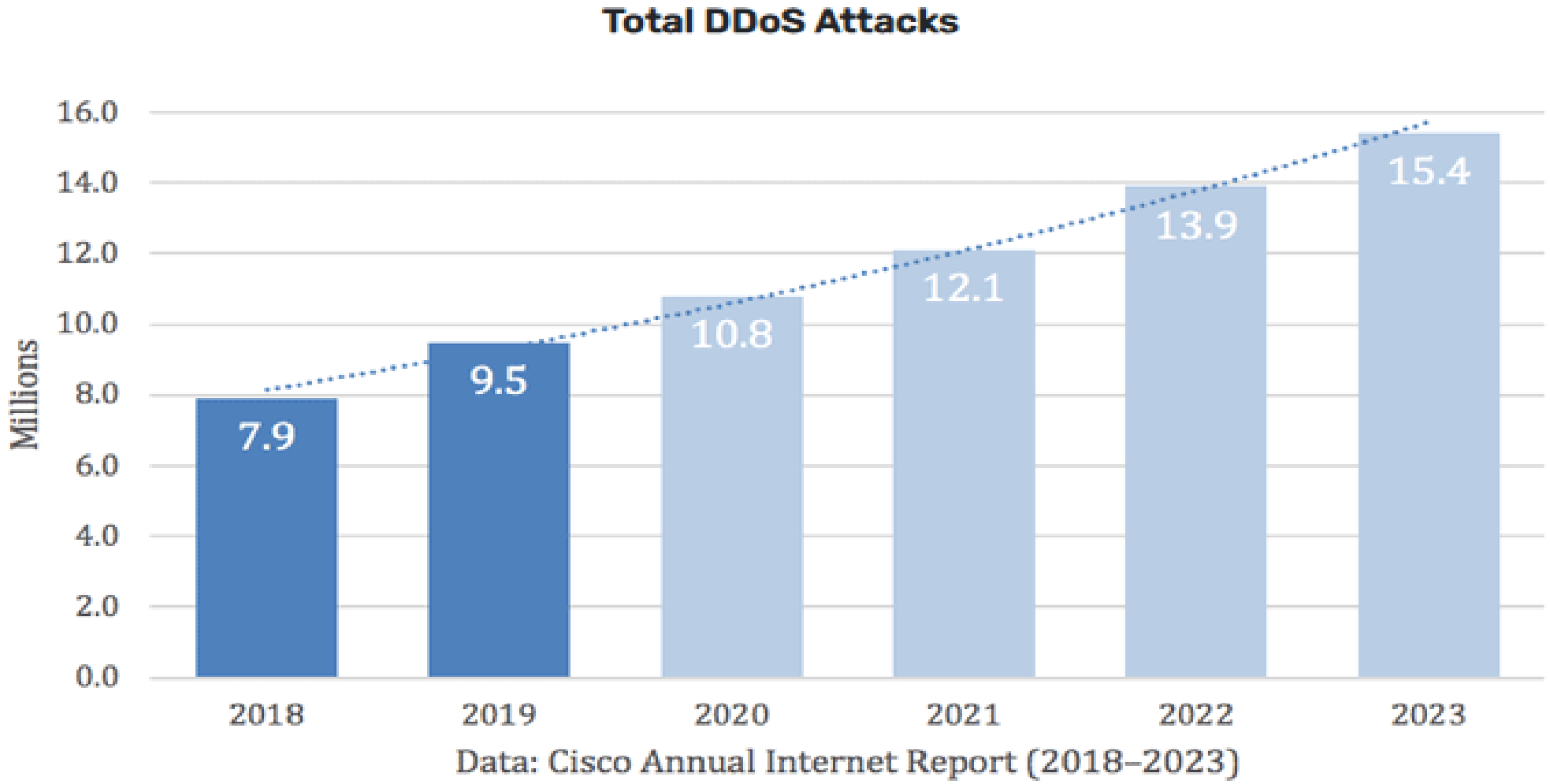
- On October 12, 2020,Commercial establishments in Mumbai, Thane and Navi Mumbai was hit by a massive power outage.
- Cyberattack on data service provider SITA resulted in the leaking of personal data of passengers of Air India between August 2011 and February 2021.

Co-funded by the European Union

History of DDoS Attacks

- The **first known** Distributed Denial of Service attack occurred in **1996**.
- **Panix**, now one of the oldest internet service providers, was knocked offline for several days by a SYN flood
- A technique that has become a classic DDoS attack.
- Cisco predicts that the DDoS attacks will double from the **7.9 million** seen in **2018** to something over **15 million** by **2023.**

Co-funded by the European Union



Co-funded by the European Union

DDOS Attack history from 2018 to 2023

19

3.7 Layer 3 DDOS Attack

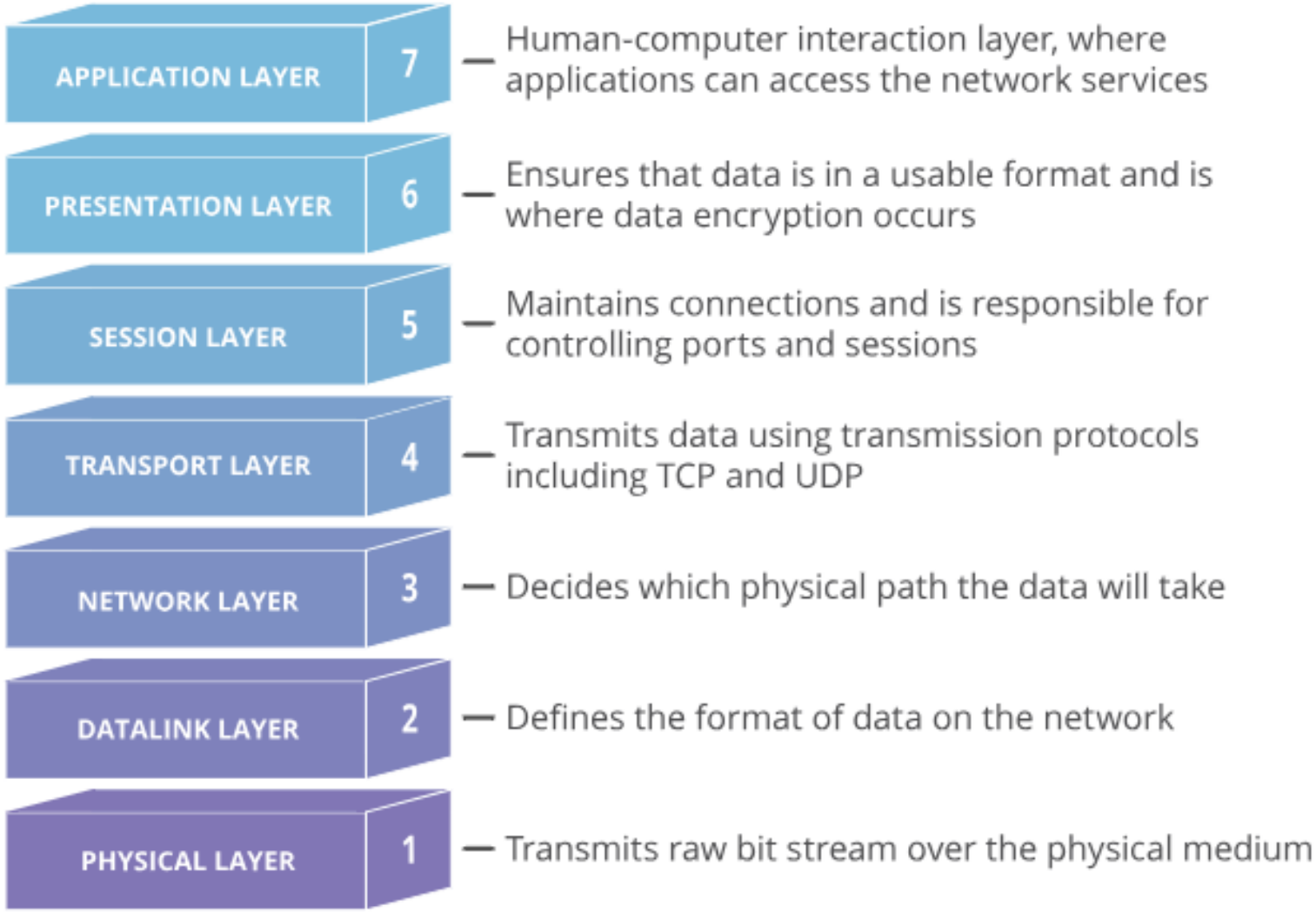
- An attack attempts to overwhelm its target with large amounts of data.
- An attacks target layer 3 (L3) in the OSI model
- Goal is to slow down or crash a program, service, computer, or network
- An attack fill up capacity so that no one else can receive service
- L3 DDoS attacks typically accomplish this by targeting network equipment and infrastructure.

Co-funded by the European Union

OSI model

- Conceptual model of how the Internet works
- Helps people talk about networking equipment and protocols
- Determine which protocols are used by which software and hardware
- It shows how the Internet can function regardless of the underlying hardware
- Divides the different technologies that make the Internet work into layers

Co-funded by the European Union



OSI Model

Co-funded by the European Union

OSI Model Layer 3

- **Layer 3 (Network Layer)** comprises the protocols and technologies that make interconnected networks.
- Routing across networks takes place.
- The most important protocol for this process is the **Internet Protocol (IP).**
- Layer 3 - **connectionless**,
- layer 3 DDoS attacks do not need to open a connection via TCP
- Layer 3 DDoS attacks target the network software a computer is running instead of a specific port.

Co-funded by the European Union

Layer 3 Protocols

The most widely used layer 3 protocols are

- **IP:** routes and addresses packets of data so that they arrive at the correct destination.
- Every device that connects to the Internet has an IP address
- **IPsec:**suite of several protocols, not a single protocol.
- encrypted version of IP used by VPNs

Co-funded by the European Union

Layer 3 Protocols (cont…)

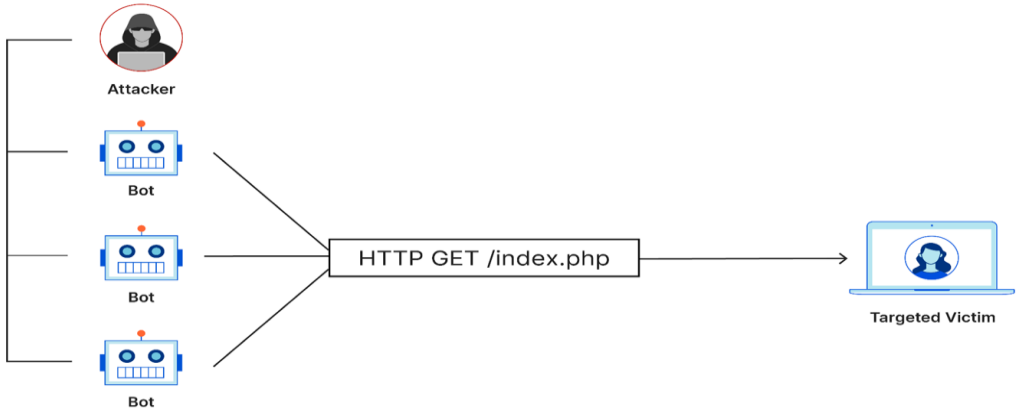
- **ICMP**: The Internet Control Message Protocol (ICMP) handles error reports and testing.
- A connectionless protocol
- IICMP packets are sent over IP alone.

- **IGMP:** The Internet Group Message Protocol manages IP multicast groups, enabling multiple devices within a network to receive the same IP traffic.

Co-funded by the European Union

Working of L3 DDoS

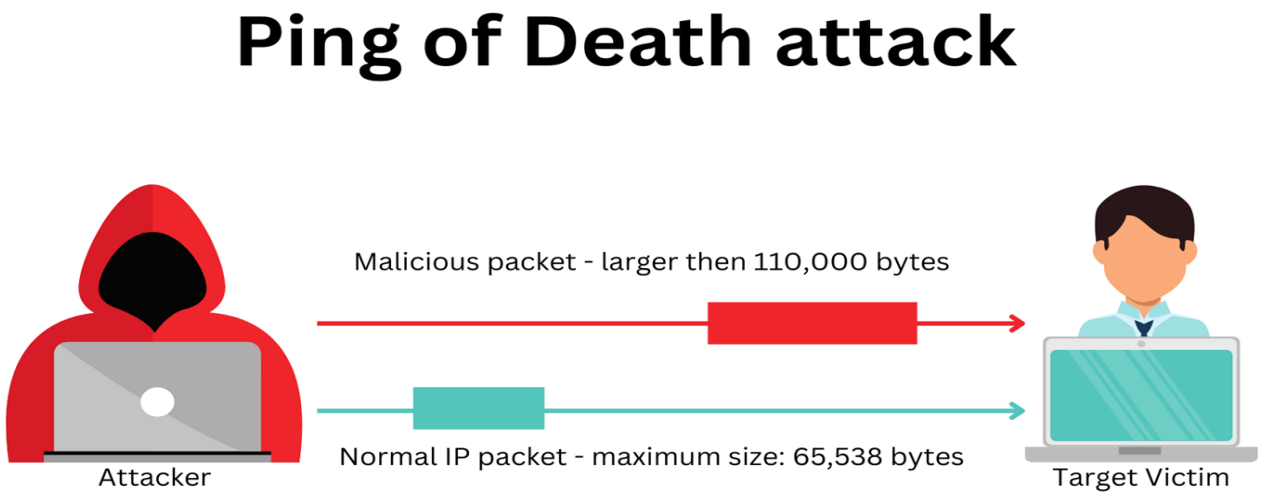
- Sends a large volume of junk network traffic via these protocols.
- Junk traffic gets in the way of legitimate user requests, slowing down responses to them or blocking them altogether.
- Sometimes there is so much junk data that it overwhelms the target's resources, and the target crashes.



Co-funded by the European Union

Types of L3 DDoS Attack

1. Ping flood
2. Smurf attack
3. Ping of death



ClouDNS

CS4ALL

Co-funded by the European Union

3.8 Layer 7 DDOS Attack

- Targets the application layer of the OSI model.
- attack focuses on disrupting specific functions or features of a website or online service.
- attacks leverage loopholes, vulnerabilities, or business logic flaws in the application layer to orchestrate the attacks.

Co-funded by the European Union

Working of L7 DDoS

- Floods of malicious requests that mimic legitimate user behavior.
- attack starts with reconnaissance, recruit a botnet, and then sends commands to initiate the attack.
- The DDoS botnet sends a high volume of HTTP GET or POST requests
- DNS query floods that target DNS servers with a high volume of queries for non-existent domains.

Co-funded by the European Union

Types of L7 DDoS Attack

- challenging to detect
- imitate legitimate user behavior, making distinguishing between normal traffic and malicious activity difficult
- There are several forms attacks

1. HTTP Floods
2. Slowloris Attack
3. DNS Query Floods
4. Resource-Intensive Queries

Co-funded by the European Union

Types of L7 DDoS Attack (cont…)

- **HTTP Floods**
  - Basic HTTP Floods
  - Randomized HTTP Floods
  - Cache-Bypass HTTP Floods
  - WordPress XML-RPC Floods

Co-funded by the European Union

3.9 DDoS Attacks on Financial Services Industry

- The report of FS-ISAC states that more than one-third (35%) of all DDoS attacks in 2023 were aimed at the financial services industry

- Driven by a dramatic surge in the power of botnets and hacktivism motivated by the Russia-Ukraine War, the financial services industry experienced a 154% increase in DDoS attacks between 2022 to 2023.

Co-funded by the European Union

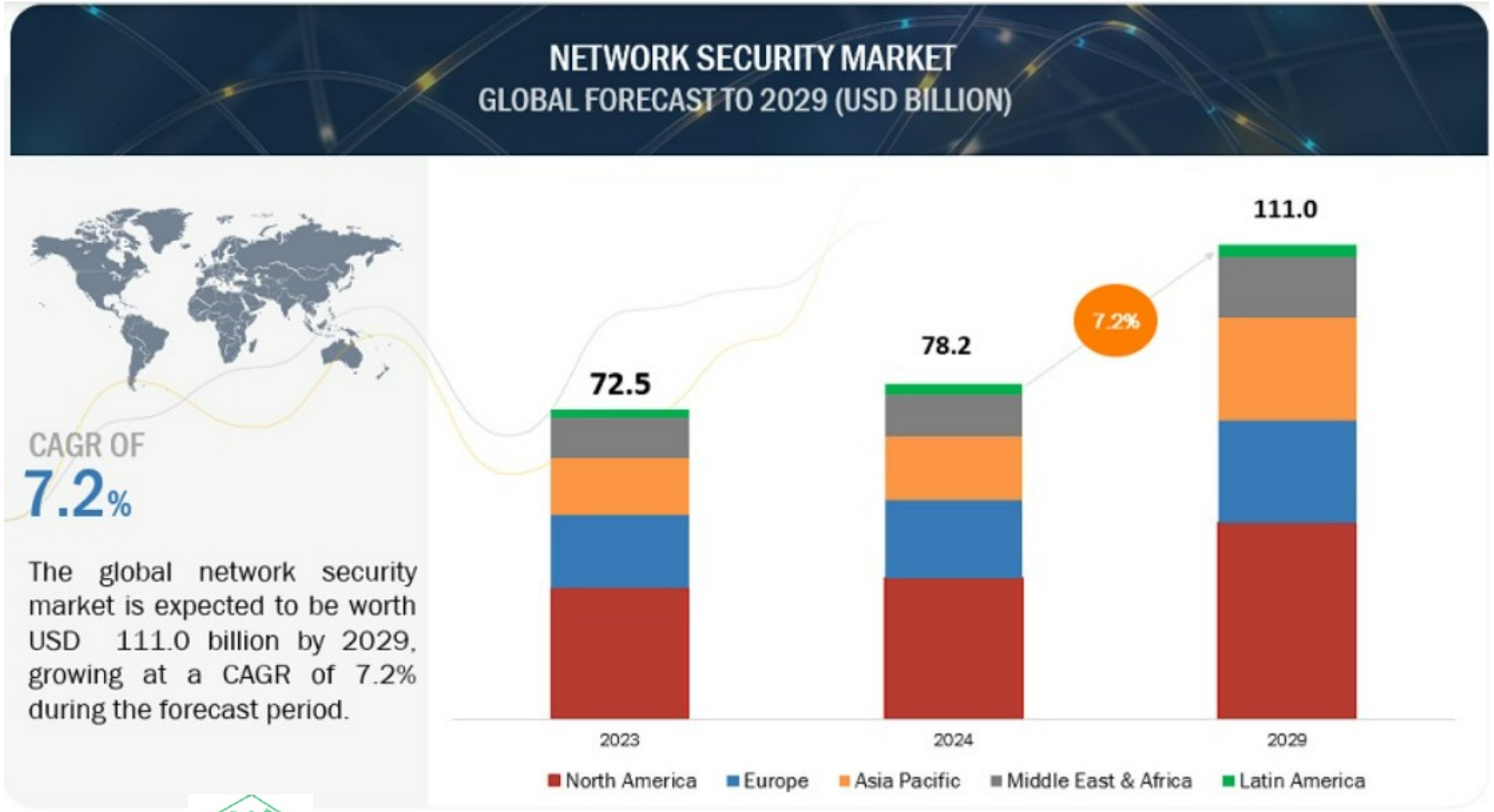
DDoS Attacks on Financial Services Industry (cont…)

- On September 5, 2023, at approximately 19:31 UTC, Akamai Prolexic, successfully detected and prevented DDoS attack directed at one of the influential U.S. financial institutions on the Prolexic platform.
- Cybercriminals used a combination of ACK, PUSH, RESET, and SYN flood attack vectors, peaking at 633.7 gigabits per second (Gbps) and 55.1 million packets per second (Mpps). The attack lasted for less than 2 minutes, and was proactively mitigated.

3.10 Network Security Industry Overview

- According to SkyQuest Report, the global network security market is projected to grow significantly
- Expanding from approximately USD 22.45 billion in 2023 to USD 58.42 billion by 2031, achieving a compound annual growth rate (CAGR) of 12.70% during this period
- Another forecast from MarketsandMarkets Report estimates the market size will reach USD 111.0 billion by 2029, growing at a CAGR of 7.2% from USD 78.2 billion in 2024

Co-funded by the European Union



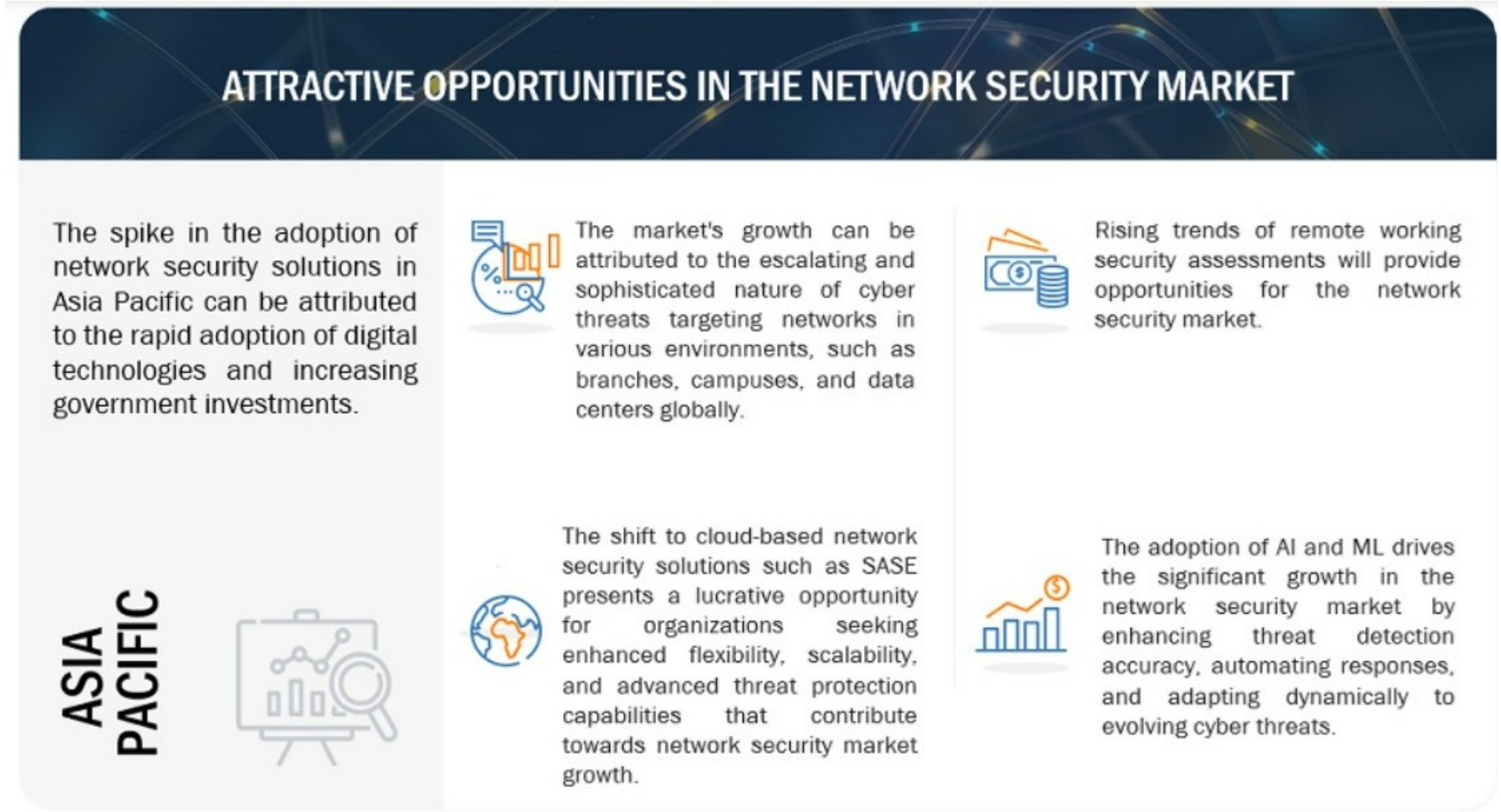
Co-funded by the European Union

Network Security Market

Key Drivers for Growth

- **Rising Cyber Threats:** Increased frequency and sophistication of attacks.
- **Cloud Adoption:** Growing need for security in cloud environments.
- **Regulatory Compliance:** Stricter data protection regulations.

Co-funded by the European Union



Co-funded by the European Union

Opportunity in Network Security Market

Key Solutions

- Major solutions include VPN, Data Loss Prevention, Firewalls, Secure Web Gateways, and DDoS Mitigation.
- Network Access Control (NAC) is anticipated to grow significantly due to its role in protecting organizational data.

Co-funded by the European Union

Challenges

- High costs of deployment and a shortage of skilled cybersecurity professionals are significant barriers to market growth.
- Resistance to adopting new security measures can hinder implementation.

Co-funded by the European Union

Learning Outcome

1. Students will able to understand the core components of enterprise networks, including endpoints, network devices, and communication protocols.
2. Students will be able to recognize practical limitations of network perimeters and the risks posed by insider threats and malware.
3. Students will learn the characteristics and implications of Advanced Persistent Threats (APTs) and Distributed Denial of Service (DDoS) attacks.
4. Students will learn best practices for implementing effective network security measures, including the use of firewalls, VPNs, and multi-factor authentication (MFA).
5. Students will able to analyze trends in the network security industry, including market growth forecasts and key drivers such as rising cyber threats and cloud adoption.
6. Students will able to propose effective security measures to enhance the protection of enterprise networks based on identified vulnerabilities.

Question no 01

Which of the following is not an endpoint in Enterprise Networking?

A. Desktop computers
B. Smartphones
C. Servers
D. Gateway

Co-funded by the European Union

Question no 02

Which of the following is not a Network Device in Enterprise Networking?

A. Workstations
B. Access Point
C. Modem
D. Gateway

Co-funded by the European Union

Question no 03

The first known Distributed Denial of Service attack occurred in

A. 1994
B. 1996
C. 1998
D. 2000

Co-funded by the European Union

Question no 04

What is a key characteristic of a Local Area Network (LAN)?

A. Spread across multiple countries
B. Can only connect mobile devices
C. Limited to a single physical location like a building
D. Always includes internet connectivity

Co-funded by the European Union

Question no 05

What is one of the limitations of network perimeters in enterprise security?

A. Cannot prevent lateral movement
B. Always prevents malware
C. Blocks all remote access
D. Eliminates insider threats

Co-funded by the European Union

Question no 06

What can cause perimeter holes in enterprise network security?

A. Strong firewalls
B. Unpatched software
C. Using encryption
D. VPN implementation

Co-funded by the European Union

Question no 07

Advanced Persistent Threats (APTs) are characterized by which of the following?

A. Short-term attacks that cause immediate damage
B. Use of simple techniques
C. Long-term, stealthy infiltration with advanced techniques
D. Reliance on insider threats

Co-funded by the European Union

Question no 08

What type of DDoS attack targets the Layer 3 (Network Layer) of the OSI model?

A. HTTP flood
B. SYN flood
C. ICMP ping flood
D. DNS query flood

Co-funded by the European Union

Answers

1. D) Gateway
2. A) Workstations
3. B) 1996
4. C) Limited to a single physical location like a building
5. A) Cannot prevent lateral movement
6. B) Unpatched software
7. C) Long-term, stealthy infiltration with advanced techniques
8. C) ICMP ping flood

Co-funded by
the European Union

Resources

List the resources you used for your research:

- https://blog.invgate.com/enterprise-network
- https://www.liquidweb.com/blog/enterprise-network-security/
- https://www.pomerium.com/blog/the-perimeter-problem
- https://www.royalholloway.ac.uk/media/20188/techreport-2022-5.pdf.pdf
- https://www.theweek.in/theweek/cover/2022/01/06/inside-story-of-cyber-attacks-on-india-banks-airlines-railways-and-the-fightback.html
- https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
- https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/
- https://www.cloudflare.com/learning/ddos/application-layer-ddos-attack/

Co-funded by the European Union

Resources

List the resources you used for your research:

- https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/
- https://www.cloudflare.com/learning/network-layer/internet-protocol/
- https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/
- https://www.akamai.com/blog/security/record-breaking-ddos-in-apac
- https://www.indusface.com/blog/what-is-slowloris/
- https://www.a10networks.com/blog/5-most-famous-ddos-attacks/
- https://www.marketsandmarkets.com/Market-Reports/network-security-market-151632343.html
- https://www.skyquestt.com/report/network-security-market

Co-funded by the European Union