Co-funded by
the European Union

Course: IT Fundamentals of Cyber Security

Project: Cyber Security 4 ALL(CS4ALL)

CS4ALL

CYBERSECURITY FOR ALL

CHAPTER V

Security Technologies and Tools

Content

- ✓ Introduction to firewall Technologies
  - ○ Types and Importance of firewall
  - ○ Best Practice for firewall configuration
- ✓ Overview of antivirus and Antimalware software
  - ○ Definition and purpose of Antivirus and antimalware Software
  - ○ Best Practices for using Antivirus and antimalware Software
- ✓ Intrusion Detection and prevention system (IDPS)
  - ○ Types and components of IDPS
  - ○ Implementing and managing IDPS
  - ○ Challenges and Best Practices of IDPS

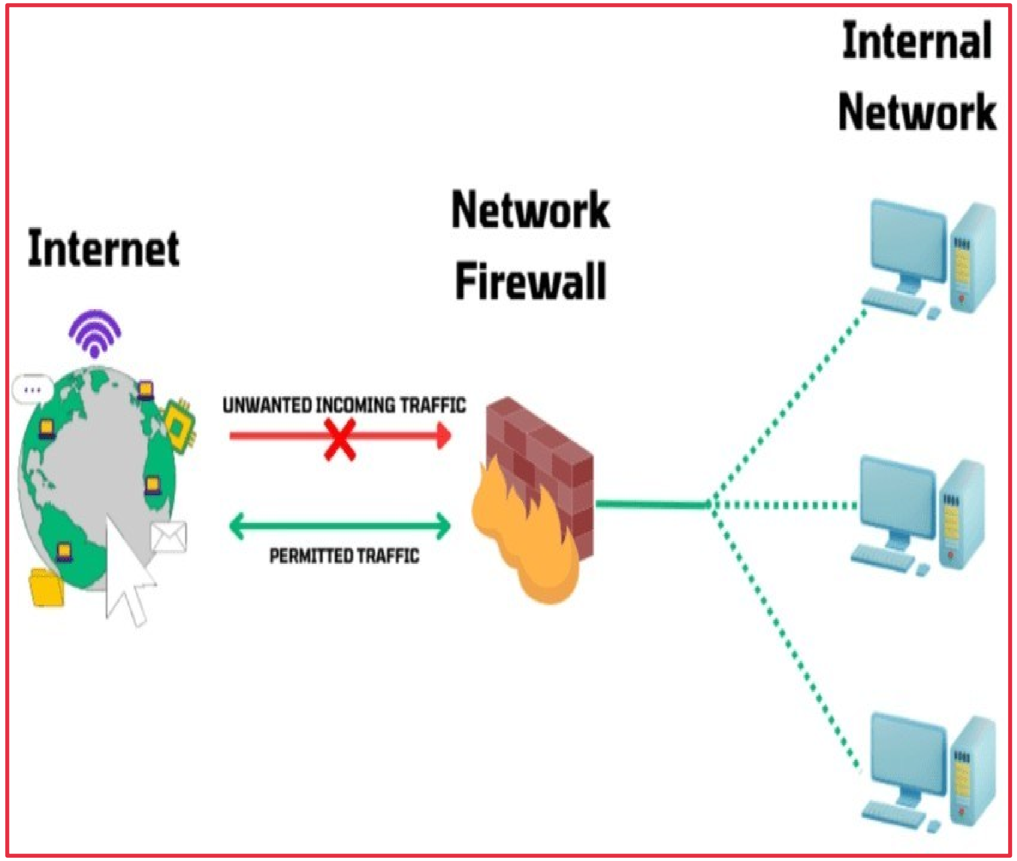
CS4ALL
CYBERSECURITY FOR ALL

Co-funded by
the European Union

Introduction to Firewall Technologies

- The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks.

- It acts as a barrier between internal private networks and external sources (such as the public Internet).



Co-funded by
the European Union

Types of Firewalls

- Packet-filtering firewalls
- Circuit-level gateways
- Application-level Gateways
- Stateful Multilayer Inspection (SMLI) Firewalls
- Threat-focused NGFW
- Network Address Translation (NAT) Firewalls
- Cloud Firewalls
- Unified Threat Management (UTM) Firewalls
- Next-generation Firewalls

CS4ALL CYBERSECURITY FOR ALL

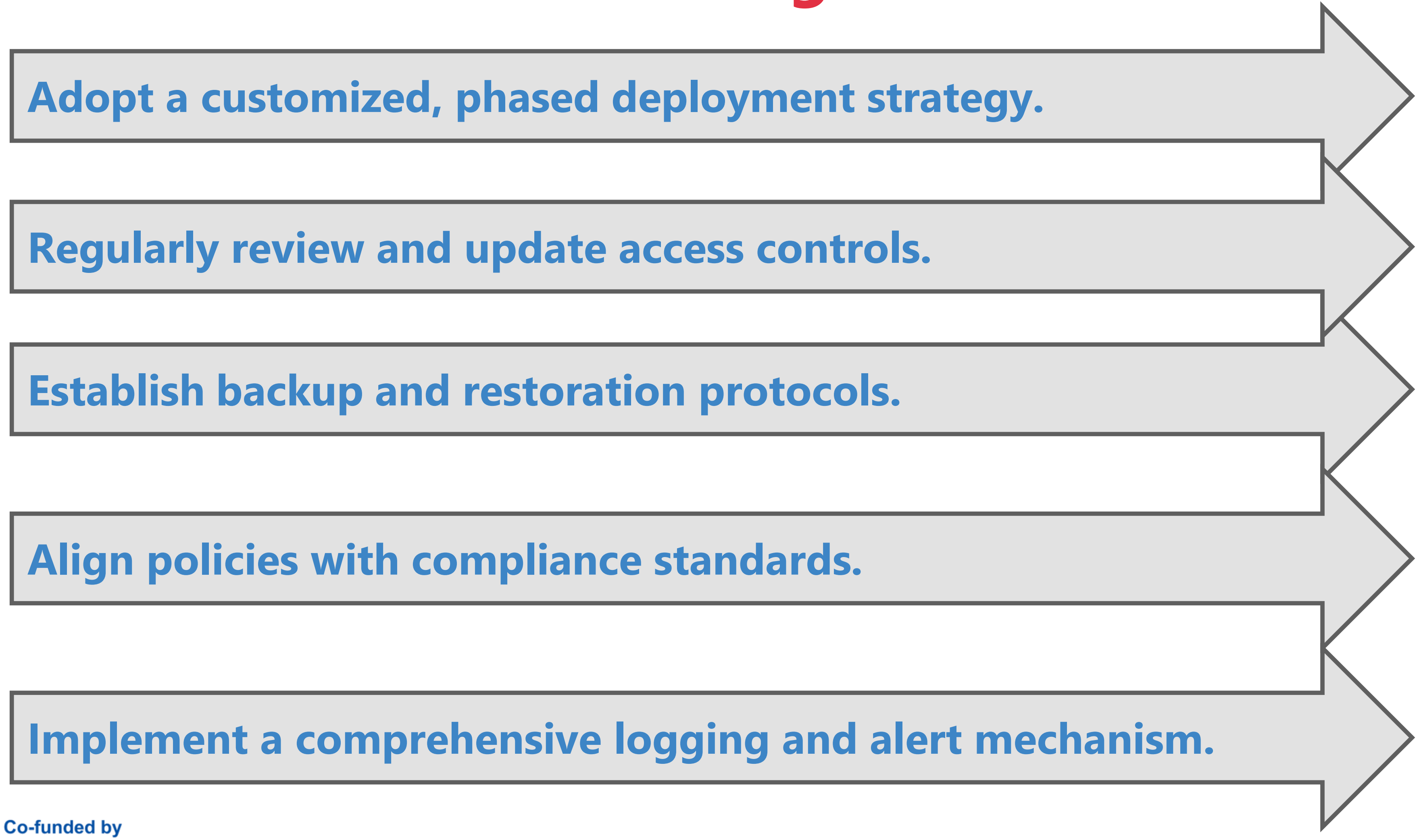
Co-funded by the European Union

Importance of Firewalls

1. Monitoring Network Traffic
2. Stops Virus Attacks Spyware
3. Preventing Hacks
4. Promotes Privacy

Co-funded by
the European Union

Best Practices for Firewall configuration



Adopt a customized, phased deployment strategy.

Regularly review and update access controls.

Establish backup and restoration protocols.

Align policies with compliance standards.

Implement a comprehensive logging and alert mechanism.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by
the European Union

Overview of Antivirus and Antimalware software

Benefits of Antivirus

- ❖ Spam and advertisements are blocked.
- ❖ Virus protection and transmission prevention.
- ❖ Hackers and data thieves are a threat.
- ❖ Protected against devices that can be detached.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by
the European Union

Drawbacks of Antivirus

- Slows down system’s speed.
- Security Holes.
- No customer care service.

Co-funded by
the European Union

Definition and Purpose of Anti Malware

Benefits of Antimalware

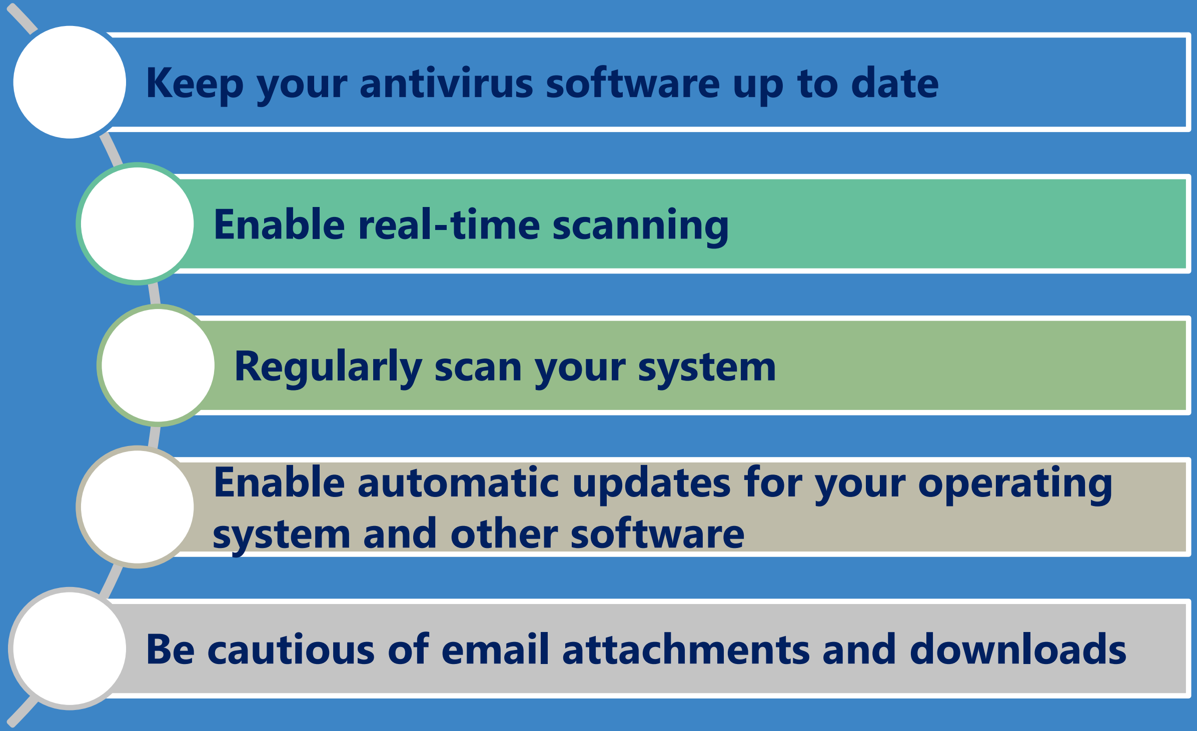
- ❖ Protection Against Malware.
- ❖ Improved System Performance.
- ❖ Data Protection.
- ❖ System Maintenance and Updates.

Drawbacks of Antimalware

- ❖ Resource Consumption.
- ❖ Subscription Fees.
- ❖ Complexity and Maintenance.
- ❖ Security Vulnerabilities.

Co-funded by
the European Union

Best Practices for using Antivirus and Anti Malware Software



- Keep your antivirus software up to date
- Enable real-time scanning
- Regularly scan your system
- Enable automatic updates for your operating system and other software
- Be cautious of email attachments and downloads

- Use strong, unique passwords
- Be wary of phishing attempts
- Keep backups of your important data
- Practice safe browsing habits
- Educate yourself about security best practices

Co-funded by
the European Union

Intrusion Detection and Prevention System(IDPS)

An intrusion detection and prevention system (IDPS) is a solution that monitors a network for threats and then takes action to stop any threats that are detected.

Types and Components of IDPS

Co-funded by the European Union

Types of IDPS

- ❖ Network-Based
- ❖ Wireless
- ❖ Network Behavior Analysis (NBA)
- ❖ Host-Based

Components of IDPS

- ❖ Sensor or Agent
- ❖ Management Server
- ❖ Database Server
- ❖ Console

Implementing and Managing IDPS

Step1: Define Your Network Segmentation

Identifying Critical Assets

Creating Segmentation Zones

Step 2: Selecting the Right Hardware and Software

Hardware Requirements

Software Requirements

Compatibility Checks

Step 3: Installation and Configuration

Deploying IDS/IPS Sensors

Configuring Network Taps or SPAN Ports

Step 4: Rule and Signature Management

Fine-tuning Detection Rules

Updating Signatures and Rules

Step 5: Monitoring and Alerts

Real-time Monitoring

Alert Management

Step 6: Regular Updates and Maintenance

Patch Management

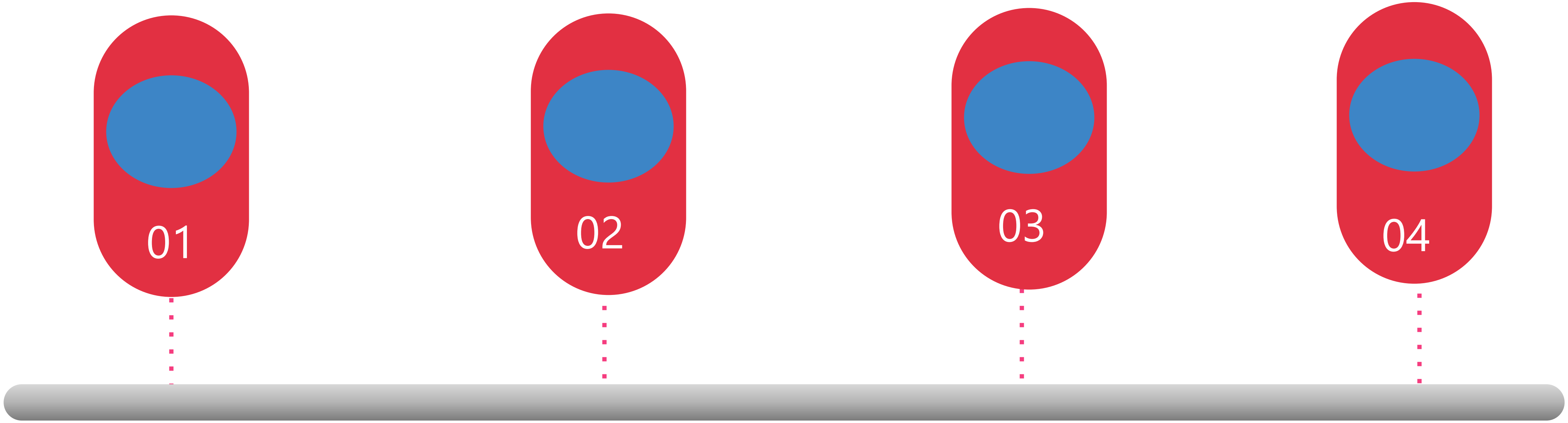
Performance Optimization

Periodic Auditing and Testing

CS4ALL CYBERSECURITY FOR ALL

Co-funded by
the European Union

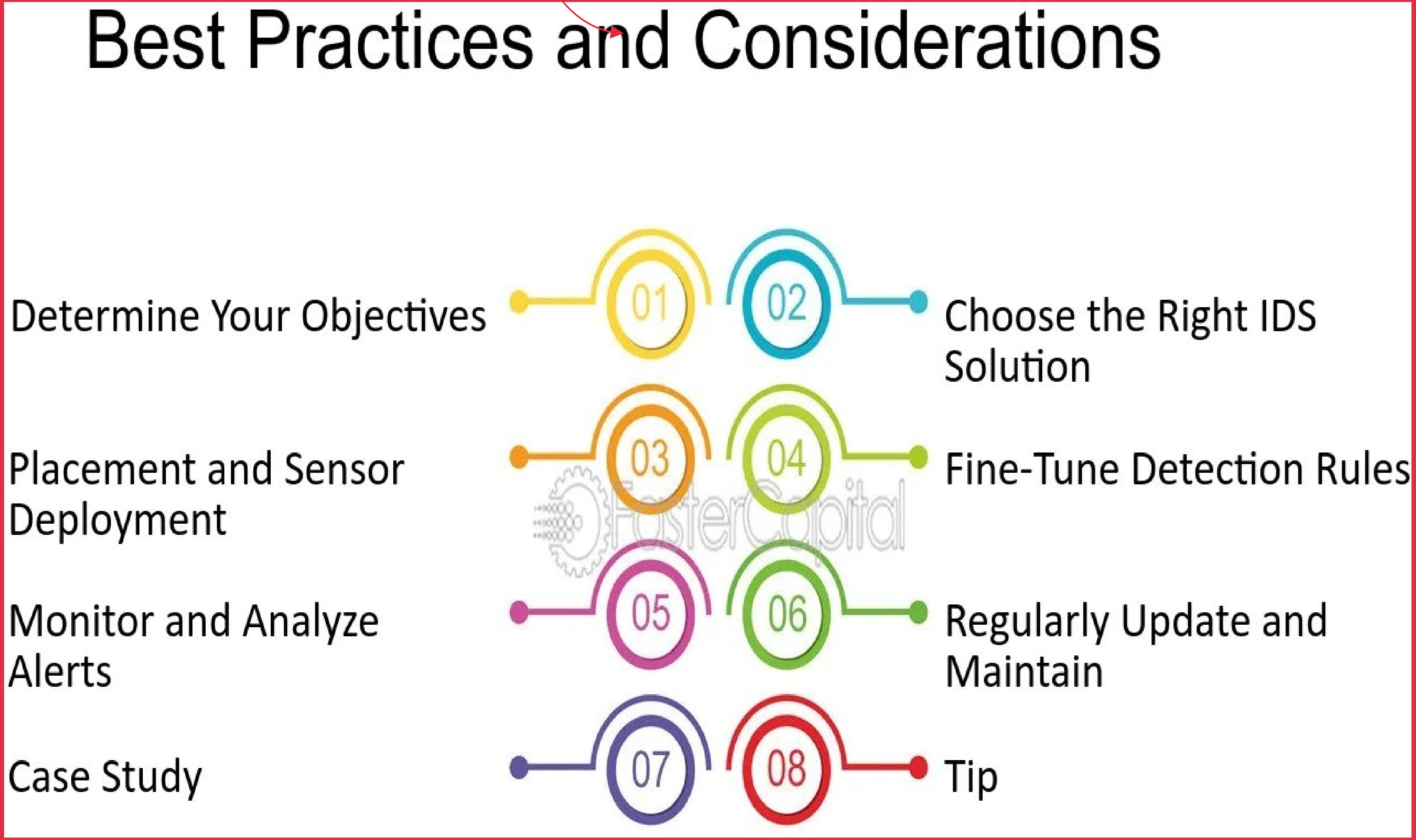
Challenges and Best Practices of IDPS



1. Ensuring an effective deployment
2. Managing the high volume of alerts
3. Understanding and investigating alerts
4. Knowing how to respond to threats

Co-funded by
the European Union

Best Practices of IDPS



Best Practices and Considerations

01 Determine Your Objectives

02 Choose the Right IDS Solution

03 Placement and Sensor Deployment

04 Fine-Tune Detection Rules

05 Monitor and Analyze Alerts

06 Regularly Update and Maintain

07 Case Study

08 Tip

Conclusion

In conclusion, security technologies, particularly firewalls, play a critical role in safeguarding networks and sensitive data from unauthorized access and cyber threats. As cyberattacks become increasingly sophisticated, integrating firewalls with other security measures—like antivirus software and intrusion prevention systems—becomes essential for a comprehensive security strategy. Ultimately, investing in and maintaining effective firewall solutions is vital for organizations aiming to protect their assets and maintain trust in a digital landscape.

Thank You

Co-funded by
the European Union

Questions & answers

Invite questions from the audience.

Co-funded by
the European Union

Resources

Reference Books:

1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
2. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.
3. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
4. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J.David Irwin.CRC Press T & F Group

Reference Links:

1. https://www.researchgate.net/publication/281148436_Security_Technologies
2. https://www.researchgate.net/publication/376600966_CYBER_SECURITY_TOOLS_AND_THEIR_USES
3. https://www.tandfonline.com/journals/tsec20

Co-funded by
the European Union