ADACOM

CYBER SECURITY

When it comes to information security,

who can we actually trust?

ISO 270001 – The New Era

Enabling Security Online

ADACOM Profile

Strong Expertise

ADACOM enables security online for Financial Institutions, Telecom Operators, Government and Large Organizations, in more than 30 countries in EMEA.

ADACOM provides consulting and customised solutions from established vendors and innovative startups, leveraging international know-how and best practices to deliver tangible results for internal or external threats, and practically every security challenge.

ADACOM is certified with ISO 9001:2008, ISO 27001:2013. ISO37001:2016, ISO22301:2019, EU Clearance and eIDAS for the quality, security, anti-bribery, continuity of the provided services and solutions. ADACOM operates two Certified Processing Centers as a member of DigiCert Trust Network.

ADACOM is based in Athens, Nicosia and London

Adacom expanded its SOC & incident response services through the recent acquisition of Netbull

30
COUNTRIES IN EMEA

20
YEARS OF EXPERIENCE

20k
PROJECTS

ADACOM
CYBER SECURITY

ISO27001 History

Information Security Management Code of Practice produced by a UK government-sponsored working group.
Became British Standard BS7799

2000's
Adopted by ISO/IEC
Became ISO/IEC 17799 (later renumbered ISO/IEC 27002)
ISO/IEC 27001 published & certification scheme started

2013
Expanding into a suite of information security standards (known as "ISO27k")
Updated and reissued every few years

Now
ISO27002:2022 has been published on February 2022.
ISO27001:2022 publication is expected.

New Structure

Organizational Controls

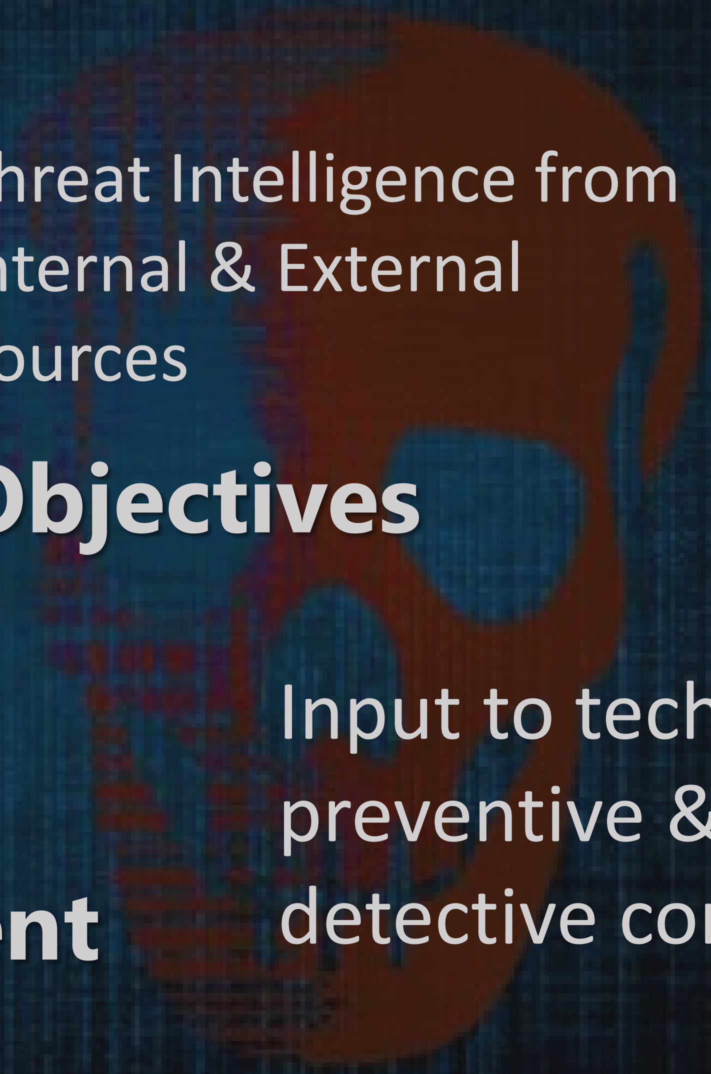
Physical Controls

People Controls

Technological Controls

ADACOM
CYBER SECURITY

Threat intelligence



Threat Intelligence from Internal & External Sources

Input to other internal processes & techniques

Objectives

Information Gathering

Input to technical preventive & detective controls

Threat Environment

Threat Intelligence

- Three layers for Threat Intelligence:
  - Strategic: threat landscape
  - Tactical: attackers' methodologies, tools
  - Operational: technical indicators
- Collaboration with other Organizations
- Facilitate decision making
- Facilitate threat prevention actions
- Reduce impact

ADACOM
CYBER SECURITY

Information security for use of cloud services

- ✓ Scope
- ✓ Policy on the use of Cloud Services
- ✓ Architecture
- ✓ Selection Criteria
- ✓ Security Responsibilities for both Cloud Provider & Client
- ✓ Review of Cloud Service Agreements
- ✓ Risk Assessments on Cloud use
- ✓ Backups
- ✓ Access Control
- ✓ Malware protection

Information security for use of cloud services

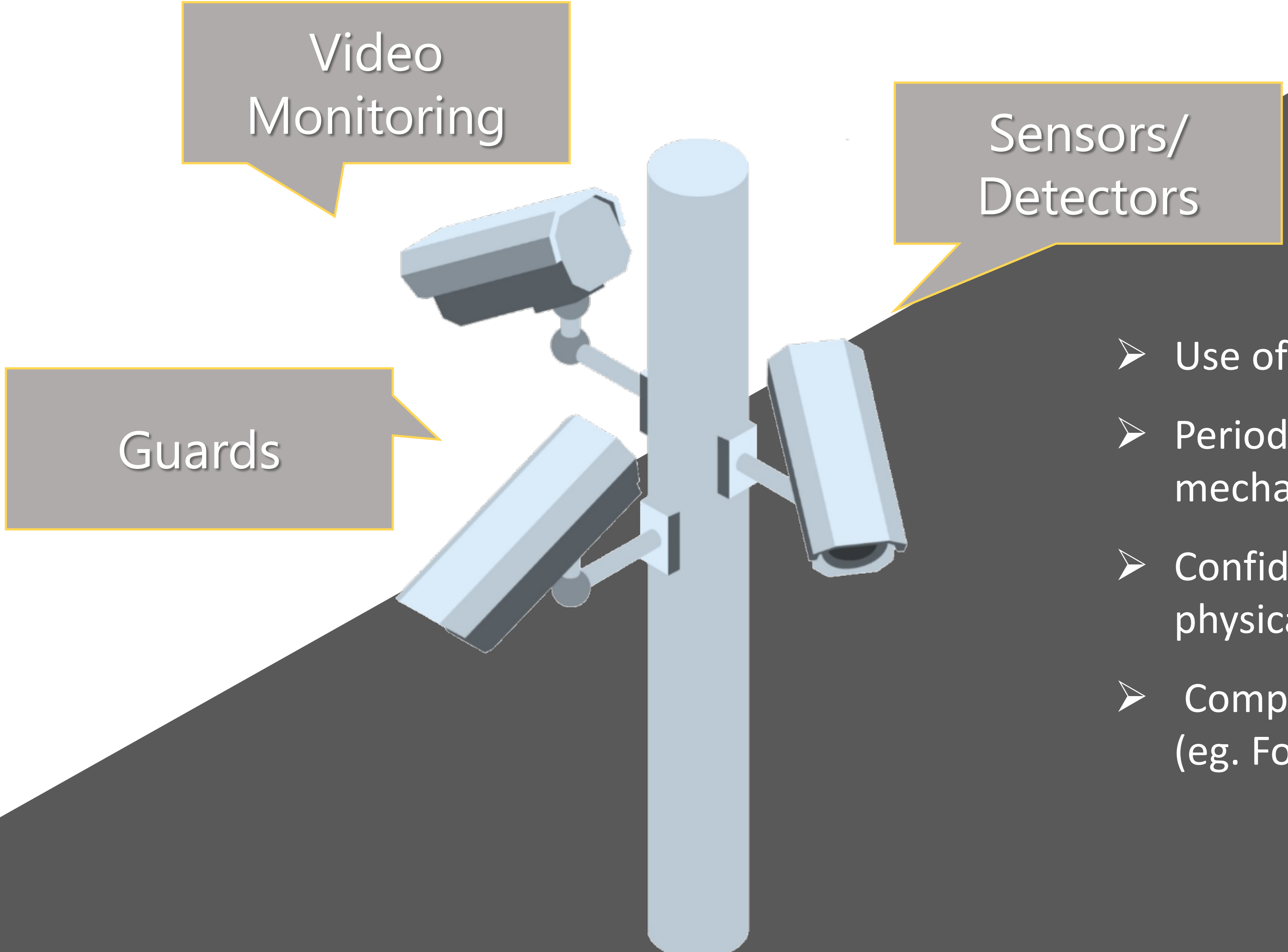
- ✓ Management & alignment of security level of different cloud services
- ✓ Exit Strategies for Cloud Providers
- ✓ Storage of sensitive information (PII or confidential)
- ✓ Identification and compliance with laws & regulations
- ✓ Incident response related to cloud services
- ✓ Notification on customer impact changes
- ✓ Contact with Cloud Providers

ICT readiness for business continuity

- ✓ ICT Continuity Strategies
- ✓ Business Impact Assessment
- ✓ RTO - RPO
- ✓ Tests & Exercises

ADACOM
CYBER SECURITY

Physical security monitoring



- Use of surveillance systems
- Periodically test physical monitoring mechanisms
- Confidentiality of the design of physical security system
- Compliance with laws & regulations (eg. For PII protection)

Configuration management

- Secure Configuration
- Processes & Tools
- Input from Publicly Available Guidance
- Monitoring Configurations
- Applicability to Organization’s Context
- Maintenance of Configuration Records

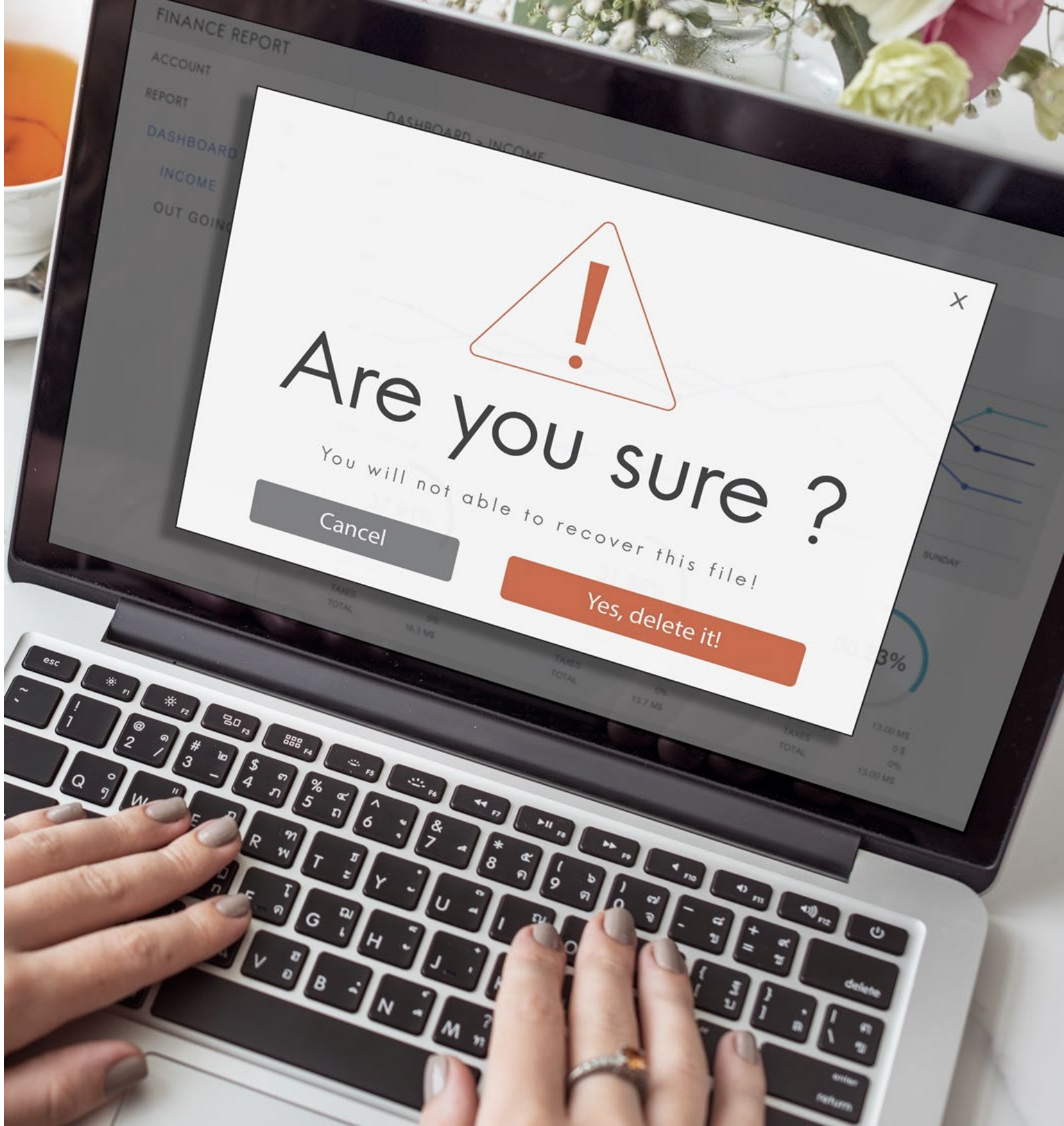
Information deletion

Select Deletion Method

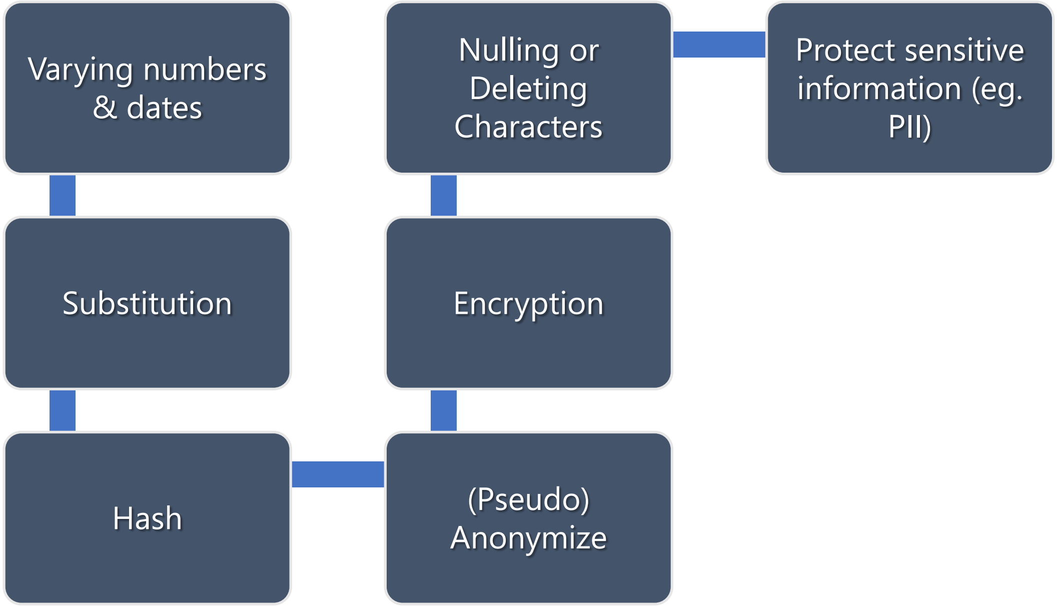
Record the Results of Deletion

Evidence of Information Deletion

ADACOM
CYBER SECURITY



Data masking



Varying numbers & dates

Substitution

Hash

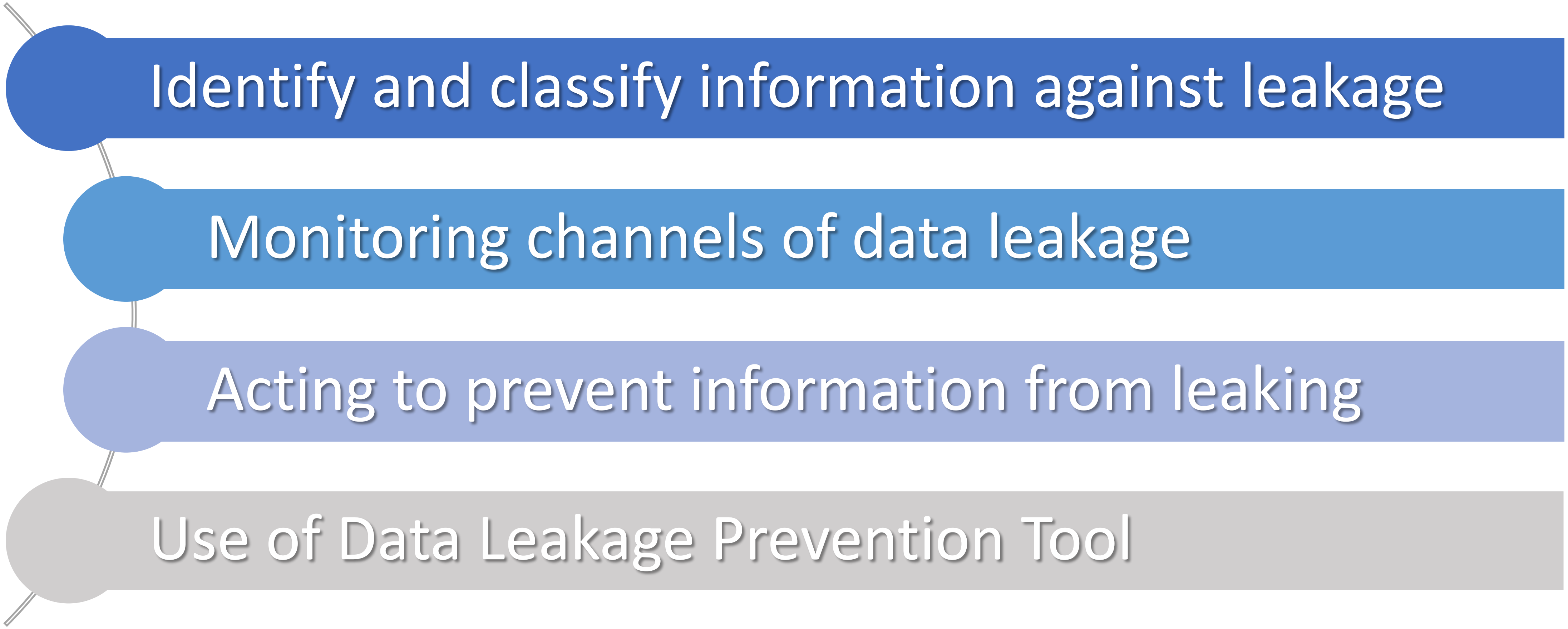
(Pseudo) Anonymize

Encryption

Nulling or Deleting Characters

Protect sensitive information (eg. PII)

Data leakage prevention



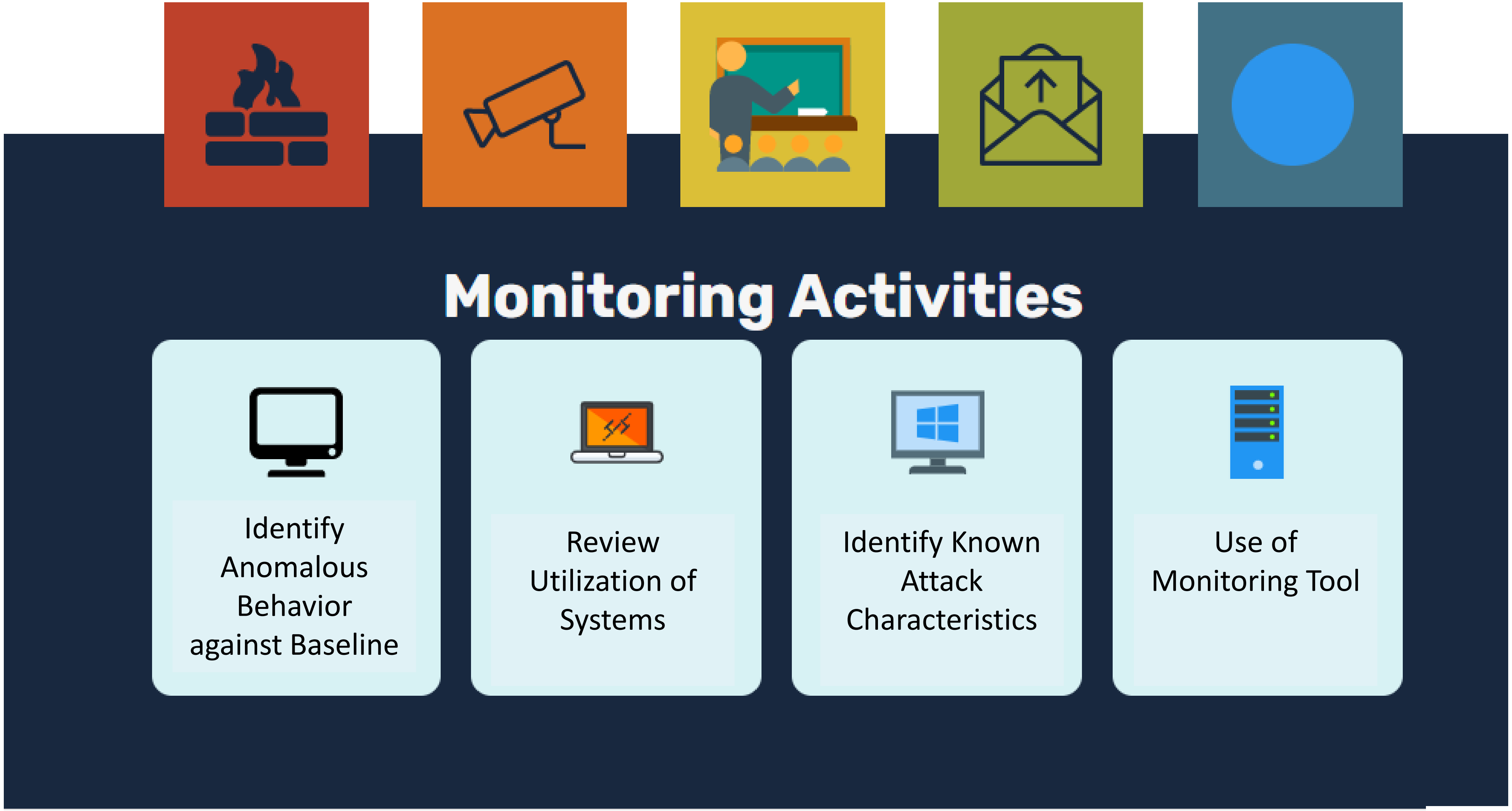
Identify and classify information against leakage

Monitoring channels of data leakage

Acting to prevent information from leaking

Use of Data Leakage Prevention Tool

Monitoring activities



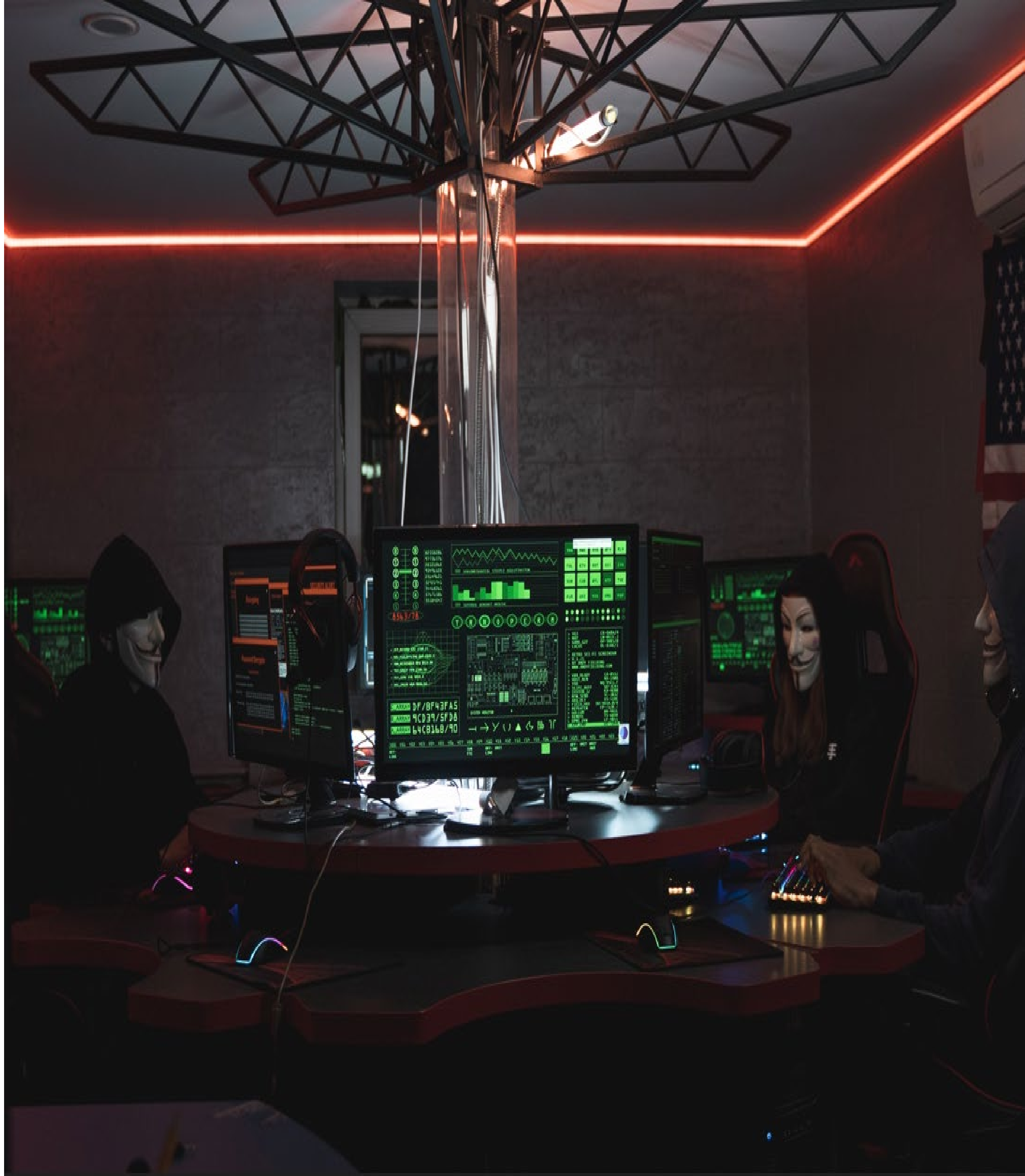
Monitoring Activities

- Identify Anomalous Behavior against Baseline
- Review Utilization of Systems
- Identify Known Attack Characteristics
- Use of Monitoring Tool

Web filtering

Blocking access to types of websites:

- ✓ Information Upload Function
- ✓ Known or suspected malicious websites
- ✓ Command & Control Servers
- ✓ Malicious websites identified by threat intelligence
- ✓ Illegal content



Secure Coding

Planning and before coding

- Expectations & approved principles
- Controlled environments
- Secure design & architecture
- Coding standards
- Developers’ qualifications
- Secure coding practices

During coding

- Structured programming techniques
- Secure coding practices
- Documenting code and removing programming defects
- Prohibit the use of insecure design techniques

Review & maintenance

- Updates should be securely packaged and deployed
- Reported vulnerabilities should be addressed
- Protection of code from unauthorized access & tampering

ADACOM
CYBER SECURITY

New Era

- Emphasis on Protection of **PII**
- Identification of need for specific security controls for **Cloud environments**
- Introduction of **Technological Solutions** (eg. DLP, secure deletion tools)
- Introduction of **new processes** (secure coding, configuration management)
- Higher **cybersecurity baseline**

ADACOM

CYBER SECURITY

United Kingdom
88 Wood Street,
Barbican EC2V 7RS,
London
+44 (0) 203 126 4590

Greece
Kreontos St. 25,
104 42
Athens
+30 210 5193740

Cyprus
10 Katsoni Str.,
1082,Nicosia
+357 22 444 071

info@adacom.com