01- Summarize Fundamental Security Concepts

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

1.1- Security Concepts

1.2- Security Controls

1.1- Security Concepts

1.2- Security Controls

INFORMATION SECURITY

- **Information Security (infosec)** refers to the protection of data resources from unauthorized access, attack, theft, or damage.
- Data may be vulnerable because of the way it is **stored**, **transferred**, or **processed**.
- The systems used to store, transmit, and process data must demonstrate the properties of security.

INFORMATION SECURITY (cont.)

- Secure information has **three** properties, often referred to as the **CIA Triad**:
  - ✓**Confidentiality** - means that information can only be read by people who have been explicitly authorized to access it.
  - ✓**Integrity** - means that the data is stored and transferred as intended and that any modification is authorized.
  - ✓**Availability** - means that information is readily accessible to those authorized to view or modify.

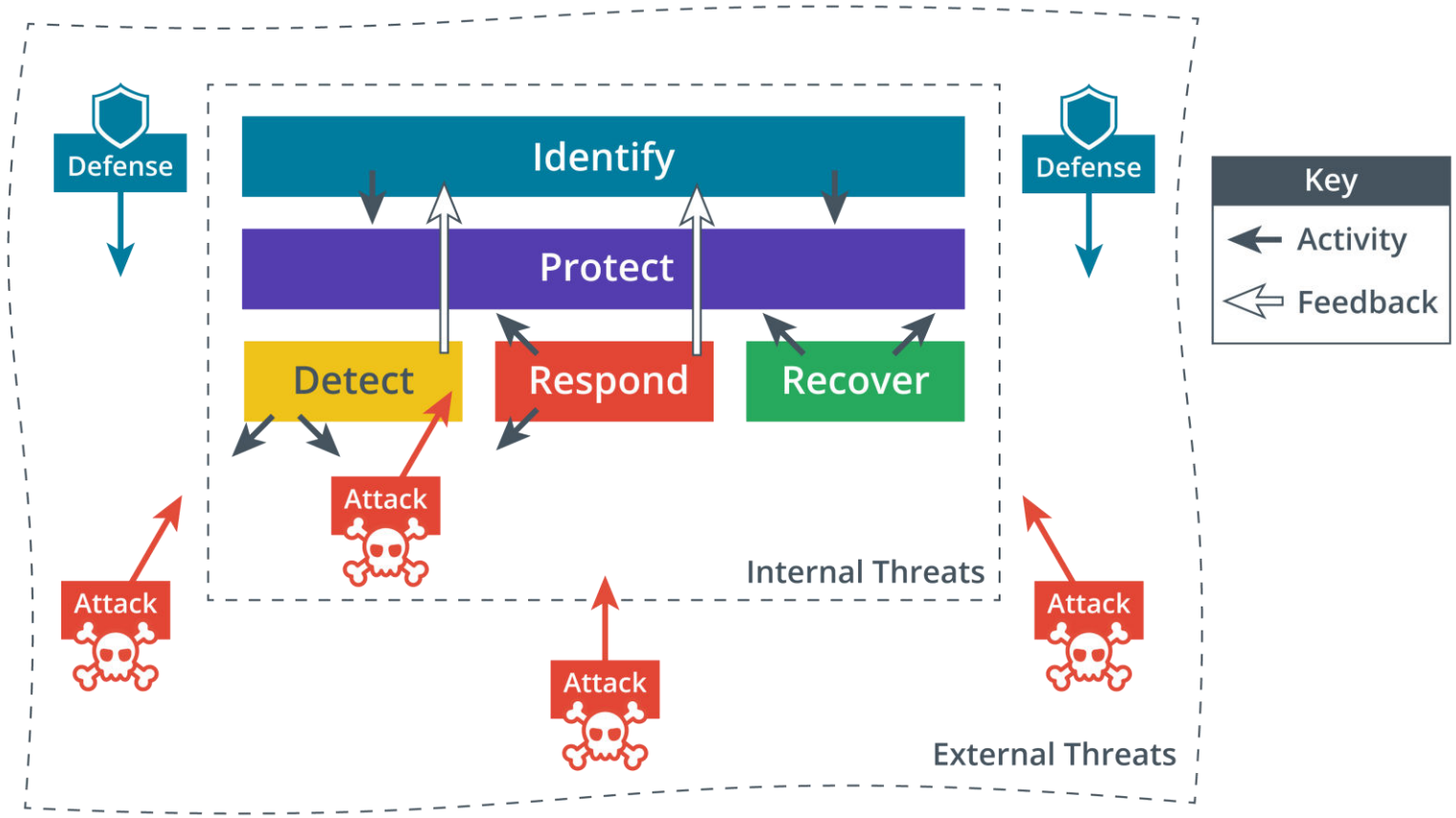
INFORMATION SECURITY (cont.)

- Some security models and researchers identify other properties of secure systems.
- The most important of these is **Non-Repudiation**.
- **Non-Repudiation** means that a person cannot deny doing something, such as creating, modifying, or sending a resource.
- **For Example:** a legal document, such as a **will**, must usually be witnessed when it is signed, If there is a dispute about whether the document was correctly executed, the witness can provide evidence that it was.

CYBERSECURITY FRAMEWORK

- Within the goal of ensuring information security, **Cybersecurity** refers specifically to provisioning secure processing hardware and software.
- **Information Security** and **Cybersecurity** tasks can be classified as five functions, following the framework developed by the **National Institute of Standards and Technology (NIST)** (nist.gov/cyberframework/online-learning/five-functions):
  - ✓Identify
  - ✓Protect
  - ✓Detect
  - ✓Respond
  - ✓Recover

CYBERSECURITY FRAMEWORK (cont.)



CYBERSECURITY FRAMEWORK (cont.)

1. **Identify—** develop security policies and capabilities, Evaluate risks, threats, and vulnerabilities and recommend security controls to mitigate them.
2. **Protect—** develop, install, operate IT hardware and software assets with security as an embedded requirement of every stage of this operation's lifecycle.
3. **Detect—** perform ongoing, proactive monitoring to ensure that controls are effective and capable of protecting against new types of threats.
4. **Respond—** identify, analyze, contain, and eradicate threats to systems and data security.
5. **Recover—** implement cybersecurity resilience to restore systems and data if other controls are unable to prevent attacks.

GAP ANALYSIS

- **Gap Analysis** is a process that identifies how an organization's security systems deviate from those required or recommended by a framework.
- This will be performed when first adopting a framework or when meeting a new industry or legal compliance requirement.
- The analysis might be repeated every few years to meet compliance requirements or to validate any changes that have been made to the framework.
- For each section of the framework, a gap analysis report will provide an overall score, a detailed list of missing or poorly configured controls associated with that section, and recommendations for remediation.

GAP ANALYSIS (cont.)

Function	Controls (Actual/Required)	CIA Triad Risk Levels	Target Remediation
Identify (10/16)	Asset Management (4/6)	C : 6 I : 6 A : 6	Q4
	Governance (3/4)	C : 6 I : 6 A : 1	Q3
	Risk Assessment (3/6)	C : 6 I : 6 A : 3	Q3
Protect (8/16)	Identity and Access Management (5/8)	C : 9 I : 9 A : 4	Q1
	Data Security (3/8)	C : 9 I : 9 A : 4	Q1

- Advanced capability
- Intermediate capability
- No/basic capability

ACCESS CONTROL

- An access control system ensures that an information system meets the goals of the **CIA triad**.
- Access control governs how **subjects** may interact with **objects**.
- **Subjects** are people, devices, software processes, or any other system that can request and be granted access to a resource.
- **Objects** are the resources, An object could be a network, server, database, app, or file.

Subjects** are assigned rights or permissions on **Objects

ACCESS CONTROL (cont.)

- Modern access control is typically implemented as an **Identity and Access Management (IAM)** system.
- **IAM** comprises **four** main processes:
  - ✓Identification
  - ✓Authentication
  - ✓Authorization
  - ✓Accounting

ACCESS CONTROL (cont.)

- **IAM** comprises **four** main processes (cont.)

1. **Identification—**creating an account or ID that uniquely represents the user, device, or process on the network.

2. **Authentication—**proving that a subject is who or what it claims to be when it attempts to access the resource, An authentication factor determines what sort of credential the subject can use, For example, people might be authenticated by providing a password; a computer system could be authenticated using a token such as a digital certificate.

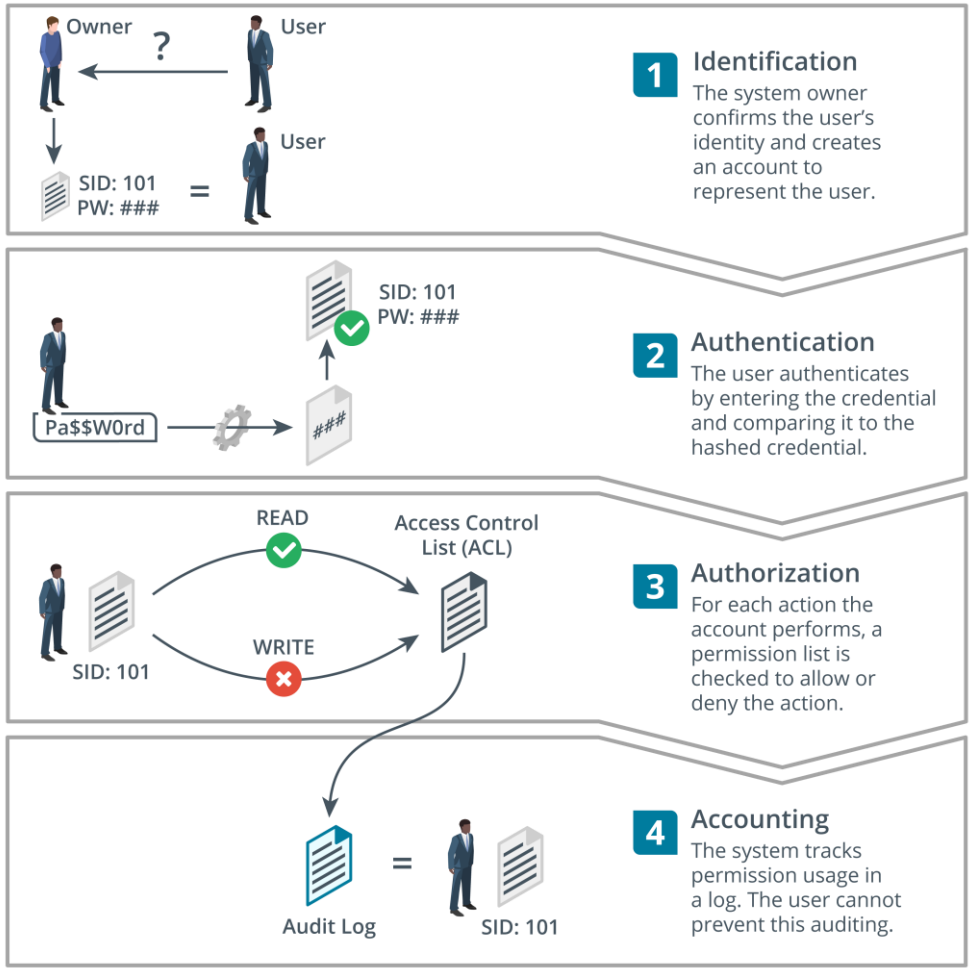
ACCESS CONTROL (cont.)

- **IAM** comprises **four** main processes (cont.)

3. **Authorization—**determining what rights subjects should have on each resource, and enforcing those rights, An authorization model determines how these rights are granted, For example, in a discretionary model, the object owner can allocate rights, In a mandatory model, rights are predetermined by system-enforced rules and cannot be changed by any user within the system.

4. **Accounting—**tracking authorized usage of a resource or use of rights by a subject and alerting when unauthorized use is detected or attempted.

ACCESS CONTROL (cont.)



1.1- Security Concepts

1.2- Security Controls

SECURITY CONTROL

- Implementation of cybersecurity functions is often the responsibility of the IT department.
- Some organizations have developed IT service frameworks to provide best practice guides to implementing IT and cybersecurity.
- These frameworks can shape company policies and provide checklists of procedures, activities, and technologies that represent best practice.
- These procedures, activities, and tools can be referred to as **Security Controls**.

SECURITY CONTROL CATEGORIES

- A **Security Control** is designed to give a system or data asset the properties of **Confidentiality**, **Integrity**, **Availability**, and **Non-Repudiation**.
- Controls can be divided into **four** broad categories based on the way the control is implemented:
  - ✓Managerial
  - ✓Operational
  - ✓Technical
  - ✓Physical

SECURITY CONTROL CATEGORIES (cont.)

- Controls can be divided into **four** broad categories (cont.)

1. **Managerial—** the control gives oversight of the information system, Examples could include risk identification or a tool allowing the evaluation and selection of other security controls.

2. **Operational—** the control is implemented primarily by people, For example, security guards and training programs are operational controls.

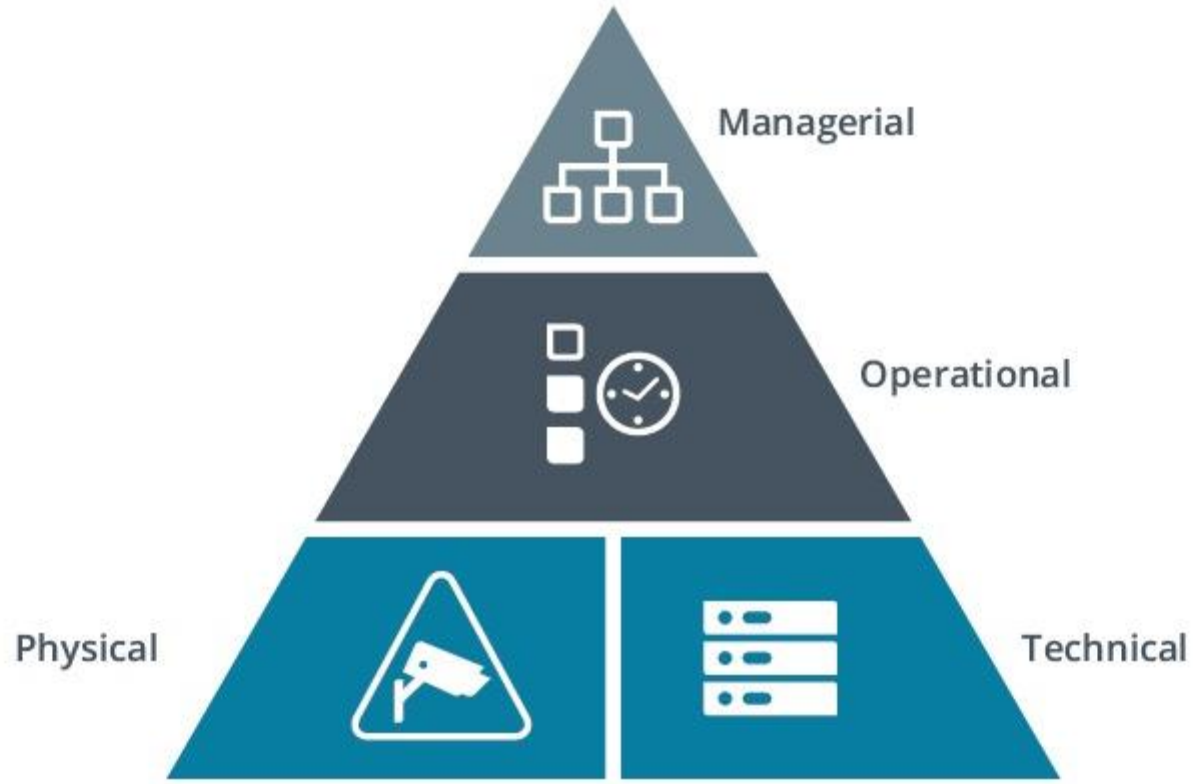
SECURITY CONTROL CATEGORIES (cont.)

- Controls can be divided into **four** broad categories (cont.)

3. **Technical—** the control is implemented as a system (hardware, software, or firmware), For example, firewalls, antivirus software, and OS access control models are technical controls.

4. **Physical—** controls such as alarms, gateways, locks, lighting, and security cameras that deter and detect access to premises and hardware are often placed in a separate category to technical controls.

SECURITY CONTROL CATEGORIES (cont.)



SECURITY CONTROL FUNCTIONAL TYPES

- As well as a category, a security control can be defined according to the **goal** or **function** it performs:

  ✓**Preventive—** the control acts to eliminate or reduce the likelihood that an attack can succeed. A preventive control operates **before** an attack can take place, Access control lists (ACL) configured on firewalls and file system objects are preventive-type technical controls, Antimalware software acts as a preventive control by blocking malicious processes from executing.

  ✓**Detective—** the control may not prevent access, but it will identify and record an attempted or successful intrusion, A detective control operates **during** an attack, Logs provide one of the best examples of detective-type controls.

SECURITY CONTROL FUNCTIONAL TYPES (cont.)

- As well as a category, a security control can be defined according to the **goal** or **function** it performs (cont.)

  ✓**Corrective—** the control eliminates or reduces the impact of a security policy violation. A corrective control is used **after** an attack, A good example is a backup system that restores data that was damaged during an intrusion, Another example is a patch management system that eliminates the vulnerability exploited during the attack.

SECURITY CONTROL FUNCTIONAL TYPES (cont.)

- As well as a category, a security control can be defined according to the **goal** or **function** it performs (cont.)

  ✓**Directive—** the control enforces a rule of behavior, such as a policy, best practice standard, or standard operating procedure (SOP), For example, an employee's contract will set out disciplinary procedures or causes for dismissal if they do not comply with policies and procedures, Training and awareness programs can also be considered as directive controls.

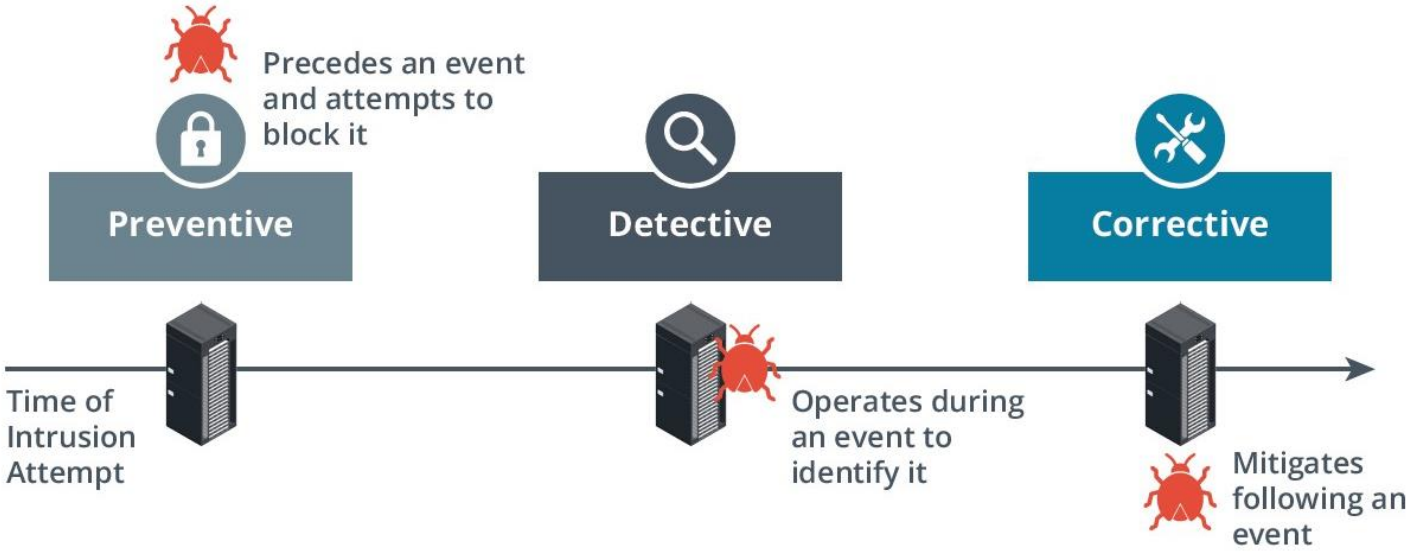
SECURITY CONTROL FUNCTIONAL TYPES (cont.)

- As well as a category, a security control can be defined according to the **goal** or **function** it performs (cont.)

  ✓**Deterrent—** the control may not physically or logically prevent access, but it psychologically discourages an attacker from attempting an intrusion, This could include signs and warnings of legal penalties against trespass or intrusion.

  ✓**Compensating—** the control is a substitute for a principal control, as recommended by a security standard, and affords the same (or better) level of protection but uses a different methodology or technology.

SECURITY CONTROL FUNCTIONAL TYPES (cont.)



Other Control Functional Types:

Directive	Deterrent	Compensating

INFORMATION SECURITY ROLES AND RESPONSIBILITIES

- A **Security Policy** is a formalized statement that defines how security will be implemented within an organization.
- It describes the means the organization will take to protect the **Confidentiality**, **Availability**, and **Integrity** of sensitive data and resources.
- The implementation of a security policy to support the goals of the CIA triad might be very different for a school, a multinational accountancy firm, or a machine tool manufacturer.
- However, each of these organizations, or any other organization should have the same interest in ensuring that its employees, equipment, and data are secure against attack or damage.

INFORMATION SECURITY ROLES AND RESPONSIBILITIES (cont.)

- An organization that develops security policies and uses framework-based security controls has a strong security posture.
- As part of the process of adopting an effective organizational security posture, employees must be aware of their responsibilities.
- The structure of security responsibilities will depend on the size and hierarchy of an organization, but these roles are typical.

INFORMATION SECURITY ROLES AND RESPONSIBILITIES (cont.)

CIO, CTO, CSO and CISO

- Overall responsibility for the IT function lies with a **Chief Information Officer (CIO)**.
- This role might also have direct responsibility for security.
- Some organizations will also appoint a **Chief Technology Officer (CTO)** , with more specific responsibility for ensuring effective use of new and emerging IT products and solutions to achieve business goals.
- In larger organizations, internal responsibility for security might be allocated to a dedicated department, run by a **Chief Security Officer (CSO)** or **Chief Information Security Officer (CISO)**.

INFORMATION SECURITY BUSINESS UNITS

Security Operations Center (SOC)

- A **Security Operations Center (SOC)** is a location where security professionals monitor and protect critical information assets across other business functions, such as finance, operations, sales/marketing, and so on.
- Because **SOCs** can be difficult to establish, maintain, and finance, they are usually employed by larger corporations, like a government agency or a healthcare company.

INFORMATION SECURITY BUSINESS UNITS (cont.)

DevSecOps

- Network operations and use of cloud computing make ever-increasing use of automation through software code.
- Traditionally, software code would be the responsibility of a programming or development team.
- Separate development and operations departments or teams can lead to silos, where each team does not work effectively with the other.

INFORMATION SECURITY BUSINESS UNITS (cont.)

DevSecOps (cont.)

- **Development and Operations (DevOps)** is a cultural shift within an organization to encourage much more collaboration between developers and system s administrators.
- By creating a highly orchestrated environment, IT personnel and developers can build, test, and release software faster and more reliably.

INFORMATION SECURITY BUSINESS UNITS (cont.)

DevSecOps (cont.)

- **DevSecOps** extends the boundary to security specialists and personnel, reflecting the principle that security is a primary consideration at every stage of software development and deployment.
- The principle of **DevSecOps** recognizes this and shows that security expertise must be embedded into any development project.
- Security tools can be automated through code.
- Consequently, security operations need to take on developer expertise to improve detection and monitoring.

INFORMATION SECURITY BUSINESS UNITS (cont.)

Incident Response

- A dedicated **Computer Incident Response Team (CIRT) /Computer Security Incident Response Team (CSIRT)/Computer Emergency Response Team (CERT)** is a single point of contact for the notification of security incidents.
- This function might be handled by the **SOC** or it might be established as an independent business unit.