Lesson 1

Comparing Security Roles and Security Controls

CompTIA®

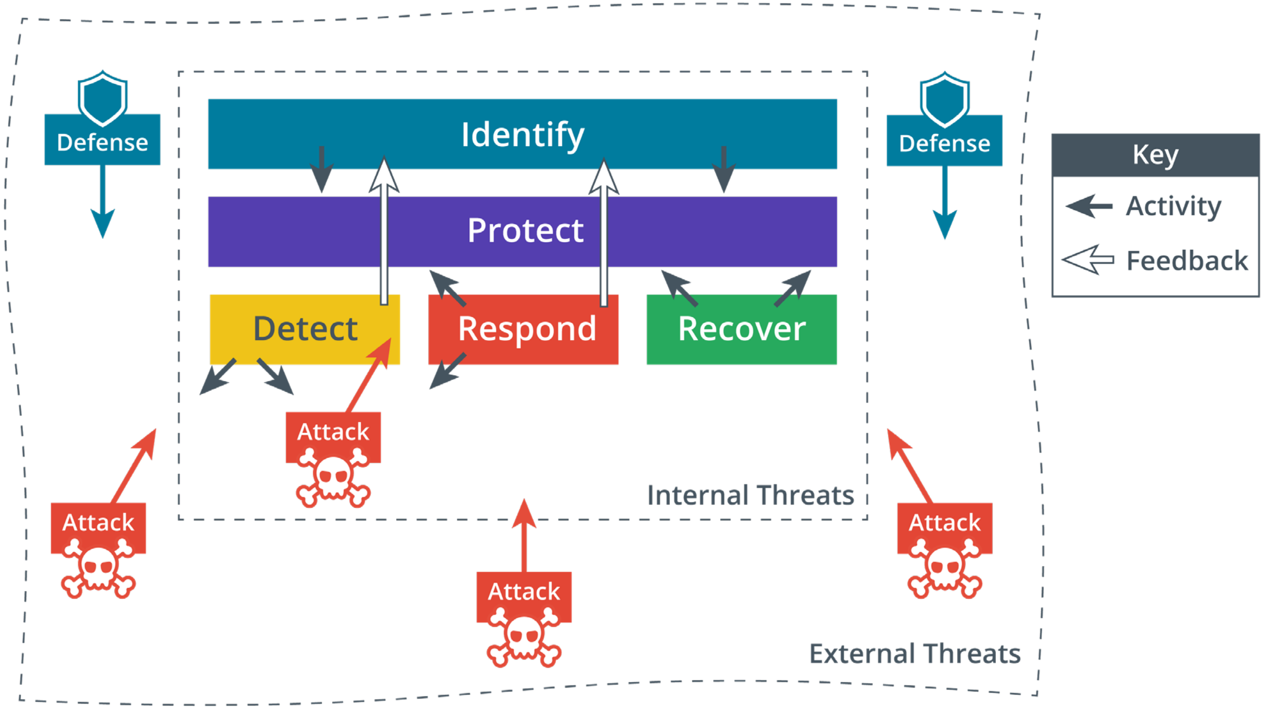
Topic 1A

Compare and Contrast Information Security Roles

Information Security

- CIA Triad
- Confidentiality
  - Information should only be known to certain people
- Integrity
  - Data is stored and transferred as intended and that any modification is authorized
- Availability
  - Information is accessible to those authorized to view or modify it
- Non-repudiation
  - Subjects cannot deny creating or modifying data

Cybersecurity Framework



Information Security Competencies

- Risk assessments and testing
- Specifying, sourcing, installing, and configuring secure devices and software
- Access control and user privileges
- Auditing logs and events
- Incident reporting and response
- Business continuity and disaster recovery
- Security training and education programs

Information Security Roles and Responsibilities

Image credit: Shannon Fagan © 123rf.com.

- Overall responsibility
  - Chief Security Officer (CSO)
  - Chief Information Security Officer (CISO)
- Managerial
- Technical
  - Information Systems Security Officer (ISSO)
- Non-technical
- Due care/liability

Information Security Business Units

- Security Operations Center (SOC)
- DevSecOps
  - Development, security, and operations
- Incident response
  - Cyber incident response team (CIRT)
  - Computer security incident response team (CSIRT)
  - Computer emergency response team (CERT)

Image credit: John Mattern/Feature Photo Service for IBM

Topic 1B

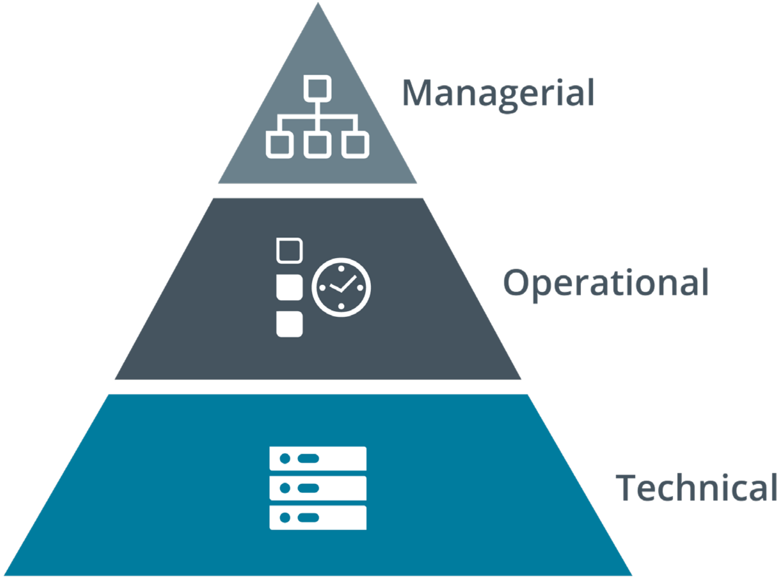
Compare and Contrast Security Control and Framework Types

Syllabus Objectives Covered

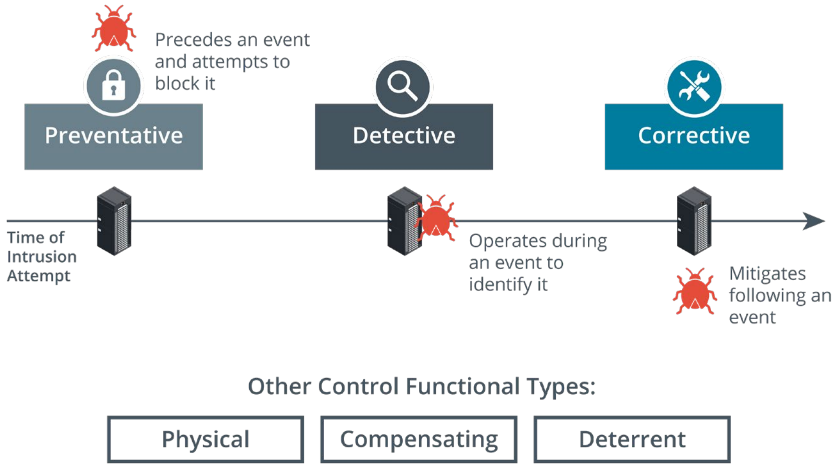
- 5.1 Compare and contrast various types of controls
- 5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture

Security Control Categories

- Technical
  - Controls implemented in operating systems, software, and security appliances
- Operational
  - Controls that depend on a person for implementation
- Managerial
  - Controls that give oversight of the system



Security Control Functional Types (1)


Precedes an event and attempts to block it
Preventative
Detective
Corrective
Time of Intrusion Attempt
Operates during an event to identify it
Mitigates following an event
Other Control Functional Types:
Physical
Compensating
Deterrent

Images © 123rf.com.

- Preventive
  - Physically or logically restricts unauthorized access
  - Operates before an attack
- Detective
  - May not prevent or deter access, but it will identify and record any attempted or successful intrusion
  - Operates during an attack
- Corrective
  - Responds to and fixes an incident and may also prevent its reoccurrence
  - Operates after an attack

Security Control Functional Types (2)

- Physical
  - Controls such as alarms, gateways, and locks that deter access to premises and hardware
- Deterrent
  - May not physically or logically prevent access, but psychologically discourages an attacker from attempting an intrusion
- Compensating
  - Substitutes for a principal control

NIST Cybersecurity Framework

- Importance of frameworks
  - Objective statement of current capabilities
  - Measure progress towards a target capability
  - Verifiable statement for regulatory compliance reporting
- National Institute of Standards and Technology (NIST)
  - Cybersecurity Framework (CSF)
  - Risk Management Framework (RMF)
  - Federal Information Processing Standards (FIPS)
  - Special Publications

ISO and Cloud Frameworks

- International Organization for Standardization (ISO)
  - 27K information security standards
  - 31K enterprise risk management (ERM)
- Cloud Security Alliance
  - Security guidance for cloud service providers (CSPs)
  - Enterprise reference architecture
  - Cloud controls matrix
- Statements on Standards for Attestation Engagements (SSAE) Service Organization Control (SOC)
  - SOC2 evaluates service provider
    - Type I report assesses system design
    - Type II report assesses ongoing effectiveness
  - SOC3 public compliance report

Benchmarks and Secure Configuration Guides

- Center for Internet Security (CIS)
  - The 20 CIS Controls
  - CIS-RAM (Risk Assessment Method)
- OS/network platform/vendor-specific guides and benchmarks
  - Vendor guides and templates
  - CIS benchmarks
  - Department of Defense Cyber Exchange
  - NIST National Checklist Program (NCP)
- Application servers and web server applications
  - Client/server
  - Multi-tier—front-end, middleware (business logic), and back-end (data)
  - Open Web Application Security Project (OWASP)

Regulations, Standards, and Legislation

- Due diligence
  - Sarbanes-Oxley Act (SOX)
  - Computer Security Act (1987)
  - Federal Information Security Management Act (FISMA)
- General Data Protection Regulation (GDPR)
- National, territory, or state laws
  - Gramm–Leach–Bliley Act (GLBA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - California Consumer Privacy Act (CCPA)
- Payment Card Industry Data Security Standard (PCI DSS)

Lesson 1

Summary