CompTIA Security+ (SEC+)

Exam Number SY0-701

SEC+ Certification Goals

CompTIA Security+ is the first security certification a candidate should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on troubleshooting, ensuring candidates have practical security problem-solving skills required to:

- **Assess** the security posture of an enterprise environment and recommend and implement appropriate security solutions
- **Monitor and secure** hybrid environments, including cloud, mobile, and IoT
- **Operate** with an awareness of applicable laws and policies, including principles of governance, risk, and compliance
- **Identify, analyze, and respond** to security events and incidents

SEC+ Details

Current Exam Codes	SY0-701
Launch Date	November 7, 2023
Exam Description	The CompTIA Security+ certification exam will verify the successful candidate has the knowledge and skills required to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions; monitor and secure hybrid environments, including cloud, mobile, and IoT; operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents
Number of Questions	Maximum of 90 questions
Type of Questions	Multiple choice and performance-based
Length of Test	90 minutes
Passing Score	750 out of 900
Recommended Experience	CompTIA Network+ and two years of experience in IT administration with a security focus

CompTIA Security+ (SY0-701) Exam Domains

1.General Security Concepts (12%)
2.Threats, Vulnerabilities and Mitigations (22%)
3.Security Architecture (18%)
4.Security Operations (28%)
5.Security Program Management and Oversight (20%)

End of Course Exam Guidance

- 50 Questions
- 90 Minutes
- Honor System: Closed book, No Internet
- Takes place Friday from 0900 – Lunch
- Adequately study these slides and the CompTIA SEC+ book we provided and you will pass.

References

https://www.comptia.org/certifications/security

SEC+ in the DoD 8140

DoD Approved 8140 (DoD 8570) Baseline Certifications				
IA Technical				
IAT Level I		**IAT Level II**		**IAT Level III**
A+ CND Network+		CySA+ CND Security+		CASP+ CISA CCNP Security CISSP
IA Management				
IAM Level I		**IAM Level II**		**IAM Level III**
CAP Cloud+ CND Security+		CAP CISSP CASP+ CCISO CISM		CISM CISSP CCISO
IA System Architecture and Engineering				
IASAE Level I		**IASAE Level II**		**IASAE Level III**
CASP+ CISSP CSSLP		CASP+ CISSP CSSLP		CISSP-ISSAP CISSP-ISSEP
Cyber Security Service Provider				
CSSP Analyst	**CSSP Infrastructure Support**	**CSSP Incident Responder**	**CSSP Auditor**	**CSSP Manager**
CEH CFR CySA+	CEH CND CFR CHFI CySA+ Cloud+	CEH CHFI CFR CySA+	CEH Cloud+ CySA+ CFR CISA	CISM CCISO

SEC+ Chapters

16 Lessons:

Lesson 1: Summarize Fundamental Security Concepts
Lesson 2: Compare Threat Types
Lesson 3: Explain Cryptographic Solutions
Lesson 4: Implement Identity and Access Management
Lesson 5: Secure Enterprise Network Architecture
Lesson 6: Secure Cloud Network Architecture
Lesson 7: Explain Resiliency and Site Security Concepts
Lesson 8: Explain Vulnerability Management

SEC+ Chapters

16 Lessons (Cont.):

Lesson 9: Evaluate Network Security Capabilities
Lesson 10: Assess Endpoint Security Capabilities
Lesson 11: Enhance Application Security Capabilities
Lesson 12: Explain Incident Response and Monitoring Concepts
Lesson 13: Analyze Indicators of Malicious Activity
Lesson 14: Summarize Security Governance Concepts
Lesson 15: Explain Risk Management Processes
Lesson 16: Summarize Data Protection and Compliance Concepts

SEC+
Lesson 1: Summarize Fundamental Security Concept

Objectives

- Summarize information security concepts
- Compare and contrast security control types
- Describe security roles and responsibilities

Lesson 1

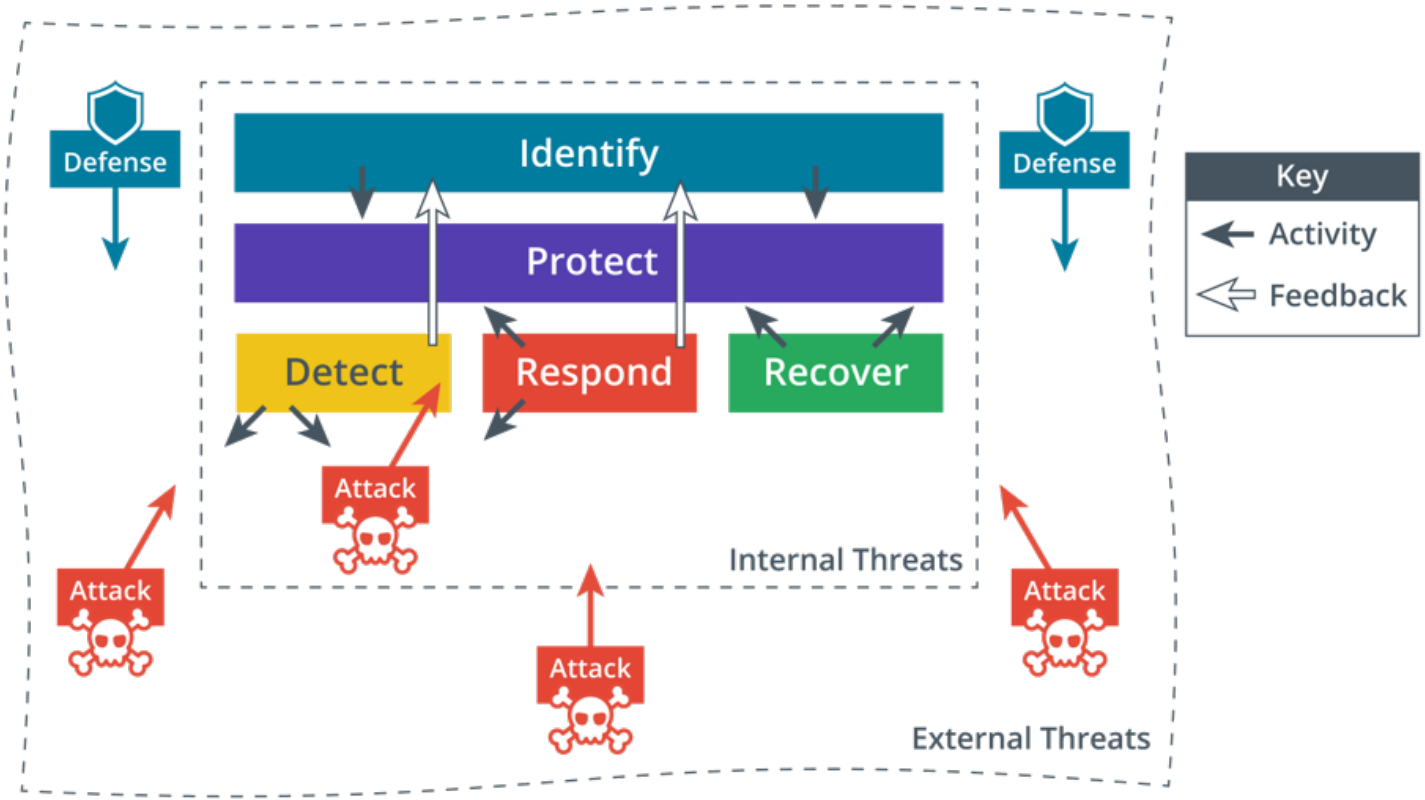
Topic 1A

Security Concepts

Information Security

- Confidentiality
  - Information should only be read by authorized persons
- Integrity
  - Data is stored and transferred as intended and any modification is authorized
- Availability
  - Information is accessible to those authorized to view or modify it
- Non-repudiation
  - Persons cannot deny creating or modifying data

Cybersecurity Framework

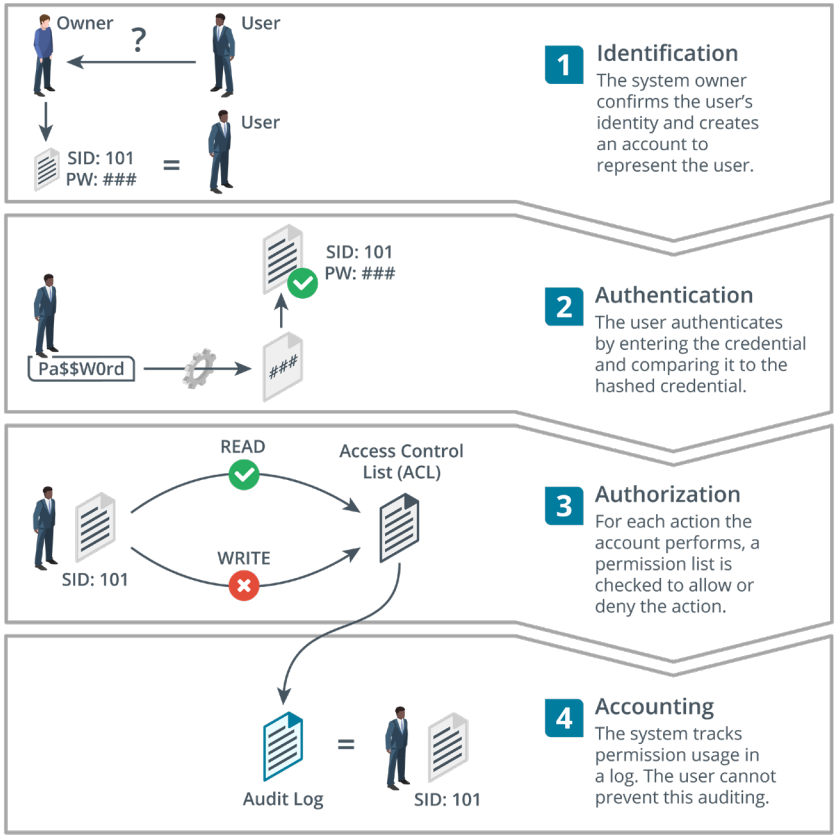


Gap Analysis

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

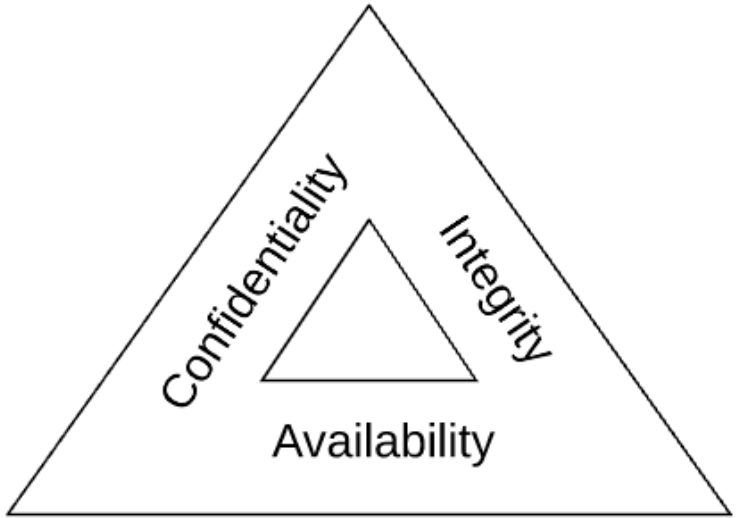
- Advanced capability
- Intermediate capability
- No/basic capability

Access Control



REVIEW: SECURITY CONCEPTS

- Information security
  - CIA triad
- Cybersecurity Framework
- Gap analysis
- Access control
  - IAM and AAA



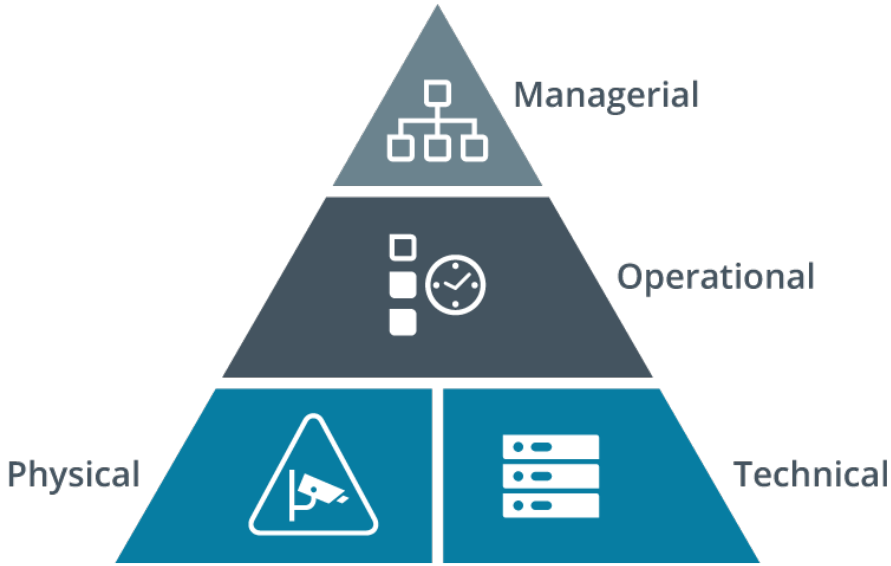
Lesson 1

Topic 1B

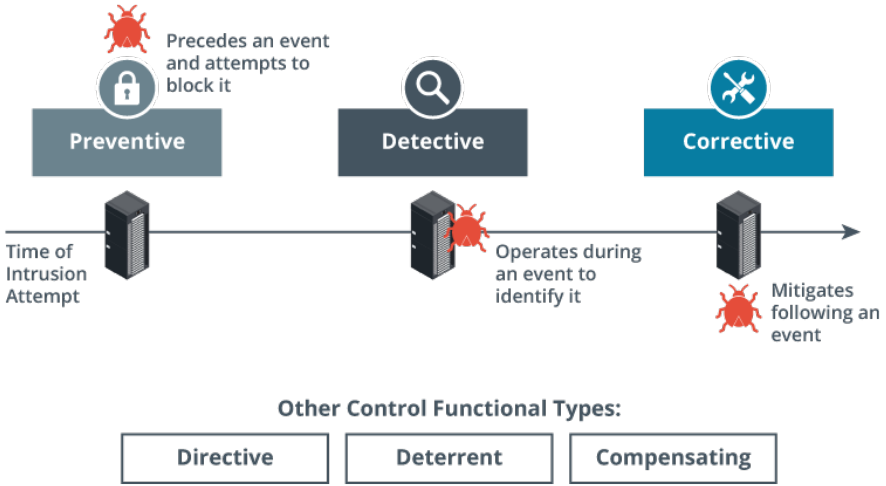
Security Controls

Security Control Categories

- Managerial
  - Give oversight of system
- Operational
  - Relies on a person for implementation
- Technical
  - Implemented in operating systems, software, and security appliances
- Physical
  - Devices that mediate access to premises and hardware



Security Control Functional Types (1)



Images © 123rf.com.

- Preventive
  - Physically or logically restricts unauthorized access
  - Operates before an attack
- Detective
  - Identifies attempted or successful intrusions
  - Operates during an attack
- Corrective
  - Responds to and fixes an incident and may prevent its reoccurrence
  - Operates after an attack

Security Control Functional Types (2)

- Directive
  - Enforces a rule of behavior
- Deterrent
  - Psychologically discourages intrusions
- Compensating
  - Substitutes for a principal control
  - Associated with framework compliance measures

Information Security Roles and Responsibilities

Image credit: Shannon Fagan © 123rf.com.

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

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 response and reporting
- Business continuity and disaster recovery
- Security training and education programs

Information Security Business Units

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

Image © gorodenkoff 123RF.com

Review: Security Controls

- Security control categories
  - Managerial, operational, technical, physical
- Security control functional types
  - Preventive, detective, corrective plus directive, deterrent, compensating
- Information security roles and responsibilities
- Information security competencies
- Information security business units
  - SOC, DevSecOps, and CIRT

Lesson 1

Summary