CompTIA Security+ (SY0-701)

This Security+ training covers essential cybersecurity skills like network security, cryptography, threat detection, risk management, and compliance. Use this CompTIA Security+ (SY0-701) certification course to prepare for the Security+ exam, and jumpstart your career as a security specialist or network administrator.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Identify Types and Categories of Security Controls — 60 min.

Security Controls Overview	9
Security Control Category: Technical Controls	12
Security Control Category: Managerial Controls	6
Security Control Category: Operational Controls	4
Security Control Category: Physical Controls	4
Validation	13

Summarize Security Concepts

Intro to summarize Security Concepts	1
CIA	23
Non-repudiation	4
AAA	8
Zero-Trust and Gap Analysis	11
Physical Security	5
Deception and Disruption Technologies	10
Validation of Security Concepts	6

Maintain Security With Change Management

Intro to Change Management	1
Change Management Overview	7
Business Processes Impacting Security Operation	11
Technical Implications and Documentation	14
Practical Example for Change Control	11

WEEK 2 — 163 min.

Validation of Change Control with Security	5

Use Symmetrical Encryption

Intro to Using Symmetrical Encryption	1
Symmetric Encryption Overview	11
Algorithm and Key Examples	6
Data at Rest Encryption Example	7
Data in Motion Encryption Examples with IPsec	14
Establishing a Shared Key	9
Reinforce and Validate	5

Use Asymmetrical Encryption

Intro to Asymmetrical Encryption	1
Asymmetrical Encryption Overview	15
Delivering Public Keys Using Digital Certificates	5
Using Digital Signatures	10
Using a Public Key to Encrypt	7
Using Keys to Authenticate	10
Validation	7

Use Certificates and PKI

Intro to PKI and Certificates	1
PKI and Certs Overview	18
Self Signed Certs	5
Adding an Internal CA to as a Trusted CA	13
Using a CSR for Requesting a Certificate	13

WEEK 3

156 min.

Reinforce and Validate What We Have Learned	5

Use Cryptography Tools and Methods

Intro to Cryptography Tools and Methods	1
Cryptography Tools and Methods Overview	18
Security Modules	11
Obfuscation	9
Salting and Key Stretching	5
Open Public Ledger	11
Validation	5

Threat Actors and Motivations

Let's compare common themes in cybersecurity threats	10
What information do we use to classify threats?	9
Where do we gain information on target systems?	13
With all this information, what do we do with it?	6
Challenge	7

Common Threat Vectors

Threat vectors	6
Threat indicators tell us more about threat vectors	13
Who's behind all this?	10
"ishing" a subcategory	11
Password Attacks	6

WEEK 4

152 min.

Challenge	4

Various Vulnerabilities

The Attack Vector	16

Authentication Vulnerabilities	10
Session Attacks	18
Cross-Site Scripting (XSS)	2
Memory Management	5
Challenge	4

Indicators of Malicious Activity

Indicators of Malicious Activity	4
Network Indicators	9
System Indications	6
Access Indicators	8
Pathways for malicious activity	7
Challenge	10

Mitigation Techniques

Identifying those indicators	11
Network Remedies	12
System Remedies	11
Access Remedies	10
Challenge	5

WEEK 5

Software Development Life Cycle — 153 min.

Software Development Life Cycle (SDLC)	13
Software Testing	12
Security Testing	7
Application Security Controls	7
Challenge	6

IDS/IPS

Introducing IDS and IPS	4
Understanding Rules	6
IDS and IPS Placement	10
Bringing all of them together	11
Challenge	11

Describe How Architecture Impacts Security

Introduction	1
Overview	5
Cloud Architectures	19
Application Architectures	9
Network Architectures	22
Segmentation Example	10

WEEK 6

152 min.

Validation	11

Use Enterprise Infrastructure Security

Intro to Enterprise Infrastructure Security	1
Enterprise Infrastructure Security Overview	21
Security Zones	10
Firewall Types and Their Uses	16
IDS and IPS	13
Load Balancer	5
Port Security and 802.1X	8
Secure Communications and Access	12
Validate and Reinforce	9

Use Strategies to Protect Data

Introduction	1
Data Protection Overview	8
Data Types	10
Data Classifications	5
General Considerations	8
Methods to Secure Data	14

WEEK 7

154 min.

Validation	6

Use Resilience and Recovery

Introduction	1
Resilience and Recovery Overview	5
High Availability and Fault Tolerance	10
Continuity of Operations (COOP)	9
Testing	8
Backups	14
Power	7
Validation	7

Apply Device, Network, & Server Security

Introduction	1
Security Techniques Overview	11
Security Baselines	19
Hardening Targets (Examples)	14
Mobile Solutions	6
Wireless Security	12
Application Security	10
Validation	14

WEEK 8

153 min.

Use H/W, S/W, and Data Asset Mgmt.

Intro	1
Overview of H/W, S/W, and Data Asset Mgmt.	6
Acquisition/Procurement Process	7
Assignment and Accounting	4
Monitoring/Asset Tracking	6
Disposal - Decommissioning	13
Validation	5

Understand Vulnerability Mgmt

Intro to Vulnerability Management	1
Vulnerability Mgmt. Overview	6
Identifying Vulnerabilities	20
Analyze and Categorize Vulnerabilities	12
Correcting or Compensating for Vulnerabilities	8
Confirm the Remediation	3
Validation	6

Explain Security Alerting and Monitoring

Intro to Security Monitoring and Alerting	1
Alerting and Monitoring Overview	13
Monitoring Computer Resources	11
Security Monitoring Activities	11
Tools for Security Monitoring and Alerting	14
Validation	5

WEEK 9

Use NGFWs to Enhance Security — 151 min.

Intro to NGFWs to Enhance Security	1
Overview of NGFW Features	14
Basic NGFW Rules	11
HTTPS Decryption and Proxy	6
NGFW Web Filtering	9
NGFW Anti-Virus	6
Validation	5

OS, Email, and Endpoint Security

Intro	1
OS Security	14
Email Security	14
Endpoint Security	8
Using Secure Protocols	11
Validation	5

Use Identity and Access Management

Intro	1
Multifactor Authentication	12
Single Sign-On (SSO)	15
Authorization and Access Control	12
Validation	5

Response, Automation, and Investigations

Introduction	1
Overview of Response, Automation, and Investigation	6
Incident Response Activities	15
Automation and Orchestration	17
Use Data Sources to Support and Investigation	8
Validation Scenario	5

Effective Security Governance

Effective Security Governance	7
Employing Effective Security Governance	7
Stakeholders	4
More Than Just the IT Systems	9
Things to Consider	11
Common Policies	4
Challenge	3

Elements of Risk Management

Elements of Risk Management	9
Risk Assessment	5
Risk Mitigation	5
Risk Transfer and Avoidance	7
Risk Monitoring and Review	4
Risk Communication	4
Incident Response Planning	4
Risk Documentation	7

Third-party Risk Assessment

Vendor Selection	8
Vendor Assessment	8

WEEK 10 — 157 min.

WEEK 11

	152 min.
Supply Chain Analysis	7
Vendor Agreements	9
Vendor Monitoring	6
Check on Learning	3

Standard Areas within Security Compliance

Standard Areas within Security Compliance	3
Health Insurance Portability and Accountability Act (HIPAA)	2
Payment Card Industry Data Security Standard (PCI DSS)	2
Gramm-Leach-Bliley Act (GLBA)	2
Sarbanes-Oxley (SOX)	3
Family Educational Rights and Privacy Act (FERPA)	4
General Data Protection Regulation (GDPR)	3
What About Cloud Data?	8
Data Inventory	3
Check on Learning	10

Elements of Security Compliance

Elements of Security Compliance	6
NIST Cybersecurity Framework	6
Awareness and Training	7
Compliance Reporting	8
What if we don't do it?	7
Check on Learning	6

Audits and Assessments

Audits and Assessments	15
Security Tests	9
Security Audits	10
Security Assessments	4
Disclosure	7
Check on Learning	2