CompTIA Security+ (Exam SY0-701), Videos & Skill Labs Set

Course Specifications

Course Number: ACI77-001VL_rev1.0
Video and Lab Length: Approximately 48 hours, 19 minutes

Course Introduction

This course is designed to equip you with the knowledge and skills required to excel in the dynamic field of cybersecurity and achieve the **CompTIA Security+** certification. In this course, you will learn how to assess the security posture of an enterprise environment, enabling you to recommend and implement appropriate security solutions. You will delve into the intricacies of monitoring and securing hybrid environments, covering cloud, mobile, and Internet of Things (IoT) technologies. Our expert instructors will guide you through the essential principles of governance, risk, and compliance, ensuring you operate with a keen awareness of applicable regulations and policies. Moreover, you will gain proficiency in identifying, analyzing, and responding to security events and incidents, a crucial skillset in the ever-evolving world of cybersecurity. By the end of this course, you will not only be prepared to ace the **CompTIA Security+** certification exam but also be well-equipped to tackle real-world security challenges and secure vital systems and data. Join us on this educational journey, and take the first step toward a fulfilling career in cybersecurity.

Video Enhanced Learning

(30h 19m * 6 Modules * 110 Episodes)

We've enhanced select lab sets with targeted video content to strengthen student readiness and improve lab success. With focused video learning, students get reinforcement of core concepts before they enter the lab, giving them the confidence and context needed to apply skills effectively. Support diverse learning styles, improve lab readiness, and drive stronger outcomes across today's most in-demand skills.

Video Topics

1. Course Overview
2. Examining Security Control Categories
3. Examining Security Control Types
4. Examining the Principles of Security
5. Examining Authentication Factors
6. Examining Authorization and Access Control Models

7. Examining Authentication, Authorization, and Accounting (AAA)
8. Examining the Principles of Zero Trust
9. Examining Physical Security
10. Examining Deception and Disruption Technology
11. Business Processes and Security Operations
12. Change Management Implications & Documentation
13. Examining Encryption Solutions
14. Examining Public Key Infrastructure (PKI)
15. Examining Digital Certificates
16. Examining Asymmetric Encryption
17. Examining Symmetric Encryption
18. Examining Hashing and Obfuscation
19. Threat Actors
20. Social Engineering
21. Business Email Compromise
22. Digital System Threats
23. Network Based Threats
24. Removable Media Threats
25. Supply Chain Attacks
26. Application Vulnerabilities
27. Operating System Vulnerabilities
28. Web Based Vulnerabilities
29. Hardware Vulnerabilities
30. Cloud Vulnerabilities
31. Virtualization Vulnerabilities
32. Cryptographic Vulnerabilities
33. Mobile Device Vulnerabilities
34. Zero Day Vulnerabilities
35. Indicators of Malware Attacks
36. Indicators of Physical Attacks
37. Indicators of Network Attacks
38. Indicators of Application Attacks
39. Indicators of Crypographic Attacks
40. Indicators of Password Attacks

41. Cybersecurity Mitigation Techniques
42. Cloud-Related Concepts
43. Network Infrastructure Concepts
44. Virtualization Concepts
45. IoT and SCADA
46. Architectural Model Considerations
47. Security Infrastructure Considerations
48. Network Appliances
49. Port Security
50. Firewall Types
51. Secure Communication and Access
52. Selecting Effective Controls
53. Data Types
54. Data Classifications
55. Data Considerations
56. Methods to Secure Data
57. HA and Site Considerations
58. Platform Diversity and Multi-Cloud Systems
59. Continuity of Operations and Capacity Planning
60. Testing
61. Backups
62. Power
63. Examining Security Baselines and Hardening
64. Examining Security for Mobile Devices
65. Examining Wireless Security
66. Examining Application Security
67. Examining Asset Management
68. Identifying Vulnerabilities
69. Examining Vulnerability Analysis
70. Vulnerability Response, Remediation and Reporting
71. Examining Security Monitoring and Alerting
72. Examining Firewalls and Intrusion Detection Devices
73. Examining Web Filtering
74. Examining Email Security

75. Examining Endpoint Detection and Response (EDR)
76. Examining Secure Network Protocols and Services
77. Examining Operating System Security
78. Examining Password Security
79. Examining Single Sign-on
80. Examining User Onboarding and Offboarding
81. Examining Identity and Access Management
82. Examining Privileged Identity Management
83. Examining Automation and Scripting Uses
84. Examining the Incident Response Process and Activities
85. Examining Digital Forensics Activities
86. Examining Investigation Data Sources and Log Data
87. Guidelines and Policies
88. Standards and Procedures
89. External Considerations and Revisions
90. Governance Structures
91. Roles and Responsibilities
92. Risk Identification and Assessment
93. Risk Analysis
94. Risk Register, Tolerance, and Appetite
95. Risk Management Strategies
96. Risk Reporting And BIA
97. Vendor Assessment and Selection
98. Agreement Types
99. Additional Vendor Considerations
100. Compliance
101. Compliance Monitoring
102. Privacy
103. Attestation
104. Audits
105. Penetration Testing
106. Phishing
107. Anomalous Behavior Recognition
108. User Guidance and Training

109. Reporting and Monitoring
110. Development and Execution

Skill Labs

(18h * 18 Labs)

A **skills lab** is a guided, hands-on learning environment that allows students to practice real-world tasks in a safe, virtual setting. Instead of simply reading or watching videos, learners actively do the work—navigating realistic scenarios, applying concepts, troubleshooting issues, and building confidence through practical experience. This ensures that theory becomes usable skill. Skill labs are essential for developing true workplace readiness because they mirror real systems, tools, and challenges, helping learners bridge the gap between knowledge and performance. By completing a skills lab, students gain the hands-on competence employers expect and are better prepared for both assessments and real job responsibilities.

Skill Labs Topics

1. Security Concept Fundamentals
2. Cryptographic Solutions
3. Threat Vectors and Attack Surfaces
4. Identifying Security Vulnerabilities
5. Analyze Malicious Activity
6. Security Architecture Models
7. Securing Enterprise Infrastructures
8. Data Protection Strategies
9. Resilience in Security Architecture
10. Securing Computing Resources
11. Asset Management Techniques
12. Vulnerability Management
13. Monitoring Computing Resources
14. Enhancing Enterprise Security
15. Implement Identity & Access Management
16. Implementation of Automation & Orchestration for Security Operations
17. Investigative Data Sources
18. Mitigation Techniques