CompTIA Security+ (SY0-701) Exam Prep

CompTIA Security+ SY0-701. Threat scenarios, security architecture, and risk management.

IT Certifications Instructor: Brian Taylor • 5 sections • 42 lessons • 13.00h total

View this course online Browse all courses

About this course

Many people preparing for the CompTIA Security+ (SY0-701) exam feel overwhelmed by the breadth of topics. This course cuts through the noise to give you a clear, structured path to exam readiness. We focus on the actual exam objectives.

You will learn how to tackle threat scenarios, security architecture, and risk management with practical, step-by-step methods. The course includes video lessons, downloadable study guides, and real case studies.

Course curriculum

Section 1: Foundations and Exam Overview

- Understanding the SY0-701 Exam Structure (12m)
  Learn how the exam is scored and what to expect on test day, so you can plan your study time effectively.
- Core Security Concepts You Must Know (18m)
  We'll break down confidentiality, integrity, and availability with real-world examples to build your foundational knowledge.
- Threats and Vulnerabilities in Plain English (15m)
  A step-by-step guide to identifying common threats and vulnerabilities in a typical business environment.
- Setting Up Your Study Plan (8m)
  Downloadable template to create a personalized study schedule that fits your life and learning style.
- How to Use Practice Tests Effectively (10m)
  Discover strategies for taking practice exams to identify weak areas and improve your score over time.
- Ethical Hacking Basics for Security+ (20m)
  Learn the ethical hacking process and how it relates to the Security+ exam objectives, with a simple case study.
- Introduction to Security Policies (14m)
  Understand the role of security policies and procedures in an organization, with examples of effective documents.

Section 2: Core Security Domains

- Threat Intelligence (22m)
  Learn how to gather and analyze threat intelligence using practical tools and techniques for the exam.
- Network Security Protocols Explained (19m)
  We'll show you how SSL, TLS, and IPsec work in real scenarios, with a problem-solving session on configuration.
- Wireless Security Best Practices (16m)
  A step-by-step guide to securing Wi-Fi networks, including WPA3 and common misconfigurations to avoid.
- Identity and Access Management Fundamentals (25m)
  Deep dive into MFA, SSO, and role-based access control with downloadable checklists for implementation.
- Cryptography for Security+ Exam (28m)
  Learn symmetric and asymmetric encryption, hashing, and digital signatures with real case study analysis.

- Securing Cloud Environments (20m)
  Understand shared responsibility models and cloud security controls with examples from AWS and Azure.
- Incident Response Process (23m)
  Follow the step-by-step incident response lifecycle and learn how to document your actions for the exam.
- Vulnerability Management Strategies (17m)
  Learn how to scan, prioritize, and remediate vulnerabilities using practical tools and templates.
- Disaster Recovery and Business Continuity (21m)
  We'll cover RTO, RPO, and backup strategies with a real-world case from a small business scenario.

Section 3: Security Operations and Monitoring

- Using SIEM for Threat Detection (26m)
  Learn how Security Information and Event Management systems work, with a hands-on lab walkthrough.
- Intrusion Detection vs. Prevention Systems (14m)
  A clear comparison of IDS and IPS, including how to configure them for optimal protection.
- Log Management and Analysis (19m)
  Discover best practices for collecting and analyzing logs to spot security incidents early.
- Endpoint Security Solutions (22m)
  Step-by-step guide to antivirus, EDR, and endpoint management tools for protecting devices.
- Data Loss Prevention Techniques (18m)
  Learn how to prevent data breaches with DLP tools and policies, including a downloadable template.
- Email Security and Phishing Defense (15m)
  Real case study analysis of phishing attacks and how to defend against them with email security tools.
- Web Application Security Basics (24m)
  Understand OWASP Top 10 vulnerabilities and how to mitigate them in a practical problem-solving session.

Section 4: Advanced Security Topics

- Advanced Threat Hunting Techniques (30m)
  Learn proactive threat hunting methods with real-world scenarios and a step-by-step guide.
- Zero Trust Architecture for Security+ (27m)
  We'll explore Zero Trust principles and how to apply them in modern IT environments.
- Secure Software Development Lifecycle (23m)
  Understand DevSecOps and how to integrate security into the SDLC with practical examples.
- Industrial Control Systems Security (20m)
  Learn about SCADA and ICS security challenges, with a case study on critical infrastructure.
- Mobile Device Management Security (18m)
  Step-by-step guide to securing mobile devices and BYOD policies for corporate environments.
- Virtualization and Container Security (25m)
  Learn how to secure VMs and containers, including Docker and Kubernetes best practices.

- Forensic Investigation Basics (22m)
  Understand the forensic process and tools used in security investigations, with a real case study.
- Compliance and Legal Considerations (16m)
  We'll cover GDPR, HIPAA, and PCI DSS requirements, with a downloadable compliance checklist.
- Security in IoT Environments (21m)
  Learn about IoT security risks and mitigation strategies, including a problem-solving session.

Section 5: Exam Strategy and Final Preparation

- Reviewing Key Exam Objectives (12m)
  A focused review of the SY0-701 objectives with tips on what to prioritize in your final study.
- Time Management During the Exam (10m)
  Learn how to pace yourself and manage time effectively to complete all questions.
- Handling Performance-Based Questions (28m)
  Step-by-step walkthrough of PBQs with practice scenarios and downloadable templates.
- Common Exam Pitfalls to Avoid (15m)
  We'll discuss frequent mistakes and how to avoid them, with real examples from past exams.
- Final Practice Exam Walkthrough (35m)
  A complete practice test analysis with explanations for each answer to reinforce learning.
- Creating Your Personal Exam Cheat Sheet (13m)
  Downloadable template to build a concise reference sheet for last-minute review.
- Stress Management and Confidence Building (11m)
  Practical tips to stay calm and focused during the exam, with a real case study from a successful candidate.
- What to Do After Passing Security+ (9m)
  Learn about next steps in your cybersecurity career, including advanced certifications and job paths.
- Resources for Continued Learning (8m)
  A curated list of books, forums, and tools to keep your skills sharp after the exam.
- Course Wrap-Up and Q&A (14m)
  We'll summarize key takeaways and answer common questions from students about the exam process.