# CompTIA Security+ (SY0-701) Exam Prep 2026

CompTIA Security+ SY0-701 2026. Threat analysis, cryptography, and network defense.

IT Certifications Instructor: Brian Taylor • 5 sections • 45 lessons • 15.25h total

View this course online Browse all courses

## About this course

Preparing for the CompTIA Security+ certification can feel overwhelming with so much ground to cover. This course cuts through the noise, focusing on the practical skills and knowledge areas you will face on the SY0-701 exam and in your first security role.

You will get a step-by-step guide through core security concepts, from threat analysis to cryptography and network defense. We use real case studies, problem-solving sessions, and downloadable checklists. This is your roadmap to passing the exam and building a foundation for your career.

## Course curriculum

### Foundations and Preparation

- How the Security+ Exam Works in 2026 (12m)
  We'll break down the exam structure, question types, and scoring so you know exactly what to expect on test day.
- Setting Up Your Study Environment (8m)
  Learn how to build a practical study plan and organize your resources for efficient learning from day one.
- Core Security Principles: CIA Triad (18m)
  Get a real-world understanding of Confidentiality, Integrity, and Availability and how they apply to every security decision.
- Understanding Governance and Compliance (15m)
  We'll show you how policies, standards, and laws like GDPR actually impact day-to-day IT operations.
- Risk Management Fundamentals (22m)
  A step-by-step guide to identifying, assessing, and treating risk using common frameworks you'll see on the exam.
- Data Privacy Concepts Explained (10m)
  Learn the difference between PII, PHI, and other data types, and why protecting them is a core security function.
- Building a Security Mindset (9m)
  A practical look at the thinking patterns and problem-solving skills that separate successful security professionals.

### Threats, Attacks, and Vulnerabilities

- Identifying Social Engineering Attacks (25m)
  A deep dive into phishing, vishing, and other human-based attacks with real case study analysis of recent breaches.
- How Malware Works: From Viruses to Ransomware (28m)
  We'll analyze different types of malware, their delivery methods, and the specific damage they cause to organizations.
- Network Attack Strategies: Reconnaissance to Exploitation (32m)
  Walk through the attacker's lifecycle step-by-step, learning how to spot and defend against each phase.
- Wireless and Mobile Device Attacks (18m)
  Understand the unique vulnerabilities of Wi-Fi, Bluetooth, and mobile devices with practical defense strategies.
- Password Attacks and Credential Stuffing (14m)
  A problem-solving session on how attackers crack passwords and the multi-layered defense you need to implement.

- Application and Web Vulnerabilities (26m)
  Learn to spot common flaws like SQL injection and XSS with a downloadable vulnerability checklist for quick reference.
- Cloud and Virtualization Threats (20m)
  We'll explore the shared responsibility model and the specific security challenges in cloud environments like AWS and Azure.
- Analyzing Attack Indicators with SIEM (23m)
  Get hands-on with the basics of using Security Information and Event Management tools to spot malicious activity.
- Understanding Advanced Persistent Threats (19m)
  A real-world case study on how sophisticated, long-term attacks operate and how to build a defense-in-depth strategy.

## Security Architecture and Design

- Designing Secure Network Topologies (24m)
  Learn how to implement secure network designs, including DMZs, segmentation, and proper firewall placement.
- Secure Systems and Host Baseline Configuration (21m)
  A step-by-step guide to hardening operating systems and applications to reduce your attack surface.
- Cryptography: Symmetric vs. Asymmetric (29m)
  Demystifying encryption, hashing, and digital signatures with practical examples of how they're used to protect data.
- Implementing Public Key Infrastructure (PKI) (27m)
  We'll show you how certificates, CAs, and keys work together to secure communications and prove identity.
- Authentication and Access Control Models (22m)
  A deep dive into RBAC, MAC, and DAC, with a downloadable template for mapping permissions to job roles.
- Secure Cloud and Hybrid Architecture (19m)
  Explore secure design patterns for IaaS, PaaS, and SaaS, focusing on container security and API protection.
- Applying the Zero Trust Security Model (16m)
  A practical problem-solving session on how to implement 'never trust, always verify' in a real-world network.

## Operations and Incident Response

- The Incident Response Process: Step-by-Step (25m)
  Learn the six key phases of IR, from preparation to lessons learned, with a downloadable IR plan template.
- Digital Forensics Basics for Security Pros (20m)
  We'll cover the fundamentals of evidence collection, chain of custody, and forensic imaging techniques.

- Disaster Recovery and Business Continuity Planning (31m)
  A real case study analysis of how companies recover from major incidents and how to calculate RTO and RPO.
- Data Backup and Restoration Strategies (15m)
  Learn the 3-2-1 backup rule and how to test your restoration process to ensure your data is truly safe.
- Configuring and Managing Firewalls (26m)
  A hands-on guide to setting up firewall rules, understanding stateful vs. stateless inspection, and logging.
- Intrusion Detection and Prevention Systems (22m)
  We'll compare IDS and IPS, and show you how to tune them to reduce false positives and catch real threats.
- Vulnerability Scanning and Penetration Testing (28m)
  Understand the difference between scanning for known flaws and ethical hacking, with a sample test plan.
- Patch Management and Secure Configuration (17m)
  A practical look at prioritizing patches and using configuration baselines to maintain a secure environment.
- User and Administrator Account Management (19m)
  Learn best practices for creating, managing, and de-provisioning user accounts to prevent privilege creep.
- Secure Protocols and Services: SSH, TLS, and More (23m)
  We'll break down which protocols to use (and which to disable) to protect data in transit across your network.

## Implementation and Next Steps

- Implementing Endpoint Security Solutions (24m)
  A step-by-step guide to deploying and managing antivirus, anti-malware, and EDR solutions on user devices.
- Securing Mobile and IoT Devices with MDM (18m)
  Learn how Mobile Device Management policies can enforce encryption, passcodes, and app control.
- Deploying Secure Wireless Networks (21m)
  We'll show you how to configure WPA3, set up a secure guest network, and implement rogue AP detection.
- Implementing Secure Remote Access with VPNs (22m)
  A practical look at VPN protocols, split tunneling, and ensuring secure connections for remote workers.
- Securing Email and Collaboration Tools (16m)
  Learn to implement SPF, DKIM, and DMARC to prevent spoofing and protect your organization's communication.
- Identity and Access Management (IAM) in Practice (29m)
  A deep dive into SSO, MFA, and federated identities with a real-world implementation checklist.
- Automation and Scripting for Security Tasks (15m)
  A problem-solving session on using simple scripts to automate log reviews and security checks.

- Hands-On Lab: Simulating a Security Audit (35m)
  We'll walk through a simulated audit, from gathering evidence to identifying gaps and writing a report.
- Creating Your CompTIA Security+ Study Plan (12m)
  A downloadable template and guide to build your final study schedule, focusing on your weak areas.
- Final Exam Review: Key Concepts and Acronyms (25m)
  We'll review the most critical concepts and exam acronyms to ensure you're ready for test day.
- Career Paths After Security+ (10m)
  Explore common job roles like SOC Analyst and Penetration Tester, and what to learn next to advance.
- Test Day Strategy and Tips (8m)
  Final advice on managing your time, handling tricky questions, and staying calm to perform your best.

## Discover our blog

Learn more with free articles written by our professors and guest experts.

Latest article: **Flight Attendant Preparation: What to Study Before You Apply**

Visit the blog  All courses  This course