SecurityX (CAS-005) Exam Preparation

CompTIA SecurityX CAS-005. Advanced security architecture, hands-on labs, and enterprise case studies.

IT Certifications Instructor: Brian Taylor • 5 sections • 46 lessons • 18.50h total

View this course online Browse all courses

About this course

This course addresses preparing for the CAS-005 SecurityX exam by focusing on practical application rather than just memorization. We will work through real scenarios that mirror the complexity you will face in advanced security architecture roles and on the certification exam.

You will learn how to apply advanced security concepts through hands-on labs, step-by-step configuration guides, and detailed problem-solving sessions. The course includes downloadable study materials, practice question walkthroughs, and analysis of enterprise-level security cases.

Course curriculum

Foundations and Exam Overview

- Understanding SecurityX CAS-005 Exam Structure (12m)
  Learn the exam domains, question types, and scoring methodology with a breakdown of what to expect on test day.
- Setting Up Your Security Lab Environment (28m)
  Step-by-step guide to configuring virtual machines, security tools, and network simulators for hands-on practice.
- Advanced Security Architecture Fundamentals (18m)
  Review core concepts including zero trust models, defense in depth, and secure design principles with practical examples.
- Risk Management Framework Deep Dive (22m)
  Walk through NIST RMF steps and learn how to apply them in enterprise environments with downloadable templates.
- Cryptographic Concepts for SecurityX (15m)
  Understand modern cryptography, PKI implementation, and cryptographic attacks with real-world case examples.
- Identity and Access Management Review (20m)
  Master SSO, MFA, RBAC, and ABAC configurations with practical implementation scenarios.
- Network Security Architecture Patterns (25m)
  Analyze secure network design, segmentation strategies, and protocol security with configuration walkthroughs.

Core Security Engineering Concepts

- Cloud Security Architecture Strategies (32m)
  Explore AWS, Azure, and GCP security controls with hands-on lab exercises for secure cloud deployments.
- Secure Software Development Lifecycle (19m)
  Implement DevSecOps practices, secure coding standards, and automated security testing pipelines.
- Advanced Threat Detection and Response (26m)
  Build SIEM queries, analyze threat intelligence feeds, and create incident response playbooks.
- Virtualization and Container Security (23m)
  Secure Docker, Kubernetes, and hypervisor environments with practical hardening techniques.
- Mobile and IoT Security Challenges (16m)
  Address device management, app security, and IoT vulnerabilities with enterprise case studies.
- Database Security Configuration (21m)
  Apply encryption, access controls, and auditing to SQL and NoSQL databases with step-by-step guides.
- Wireless Security Implementation (14m)
  Configure secure wireless networks, assess WPA3 deployments, and mitigate rogue access points.

- Security Assessment Tools and Techniques (27m)
  Use vulnerability scanners, penetration testing tools, and security assessment frameworks in lab environments.
- Business Continuity and Disaster Recovery (24m)
  Design BCDR plans, conduct tabletop exercises, and evaluate backup strategies with real scenarios.

Advanced Security Operations

- Security Operations Center (SOC) Workflows (29m)
  Analyze SOC processes, escalation procedures, and threat hunting methodologies with practical examples.
- Forensic Investigation Techniques (31m)
  Learn disk imaging, memory analysis, and network forensics using industry-standard tools.
- Advanced Malware Analysis (35m)
  Reverse engineering basics, sandbox analysis, and behavioral assessment of suspicious files.
- Secure Remote Access Implementation (17m)
  Configure VPNs, zero trust network access, and secure administrative access with best practices.
- Email Security and Anti-Phishing (20m)
  Deploy SPF, DKIM, DMARC, and advanced email filtering with configuration examples.
- Web Application Security Testing (33m)
  OWASP Top 10 review, manual testing techniques, and automated scanning with hands-on practice.
- Data Loss Prevention Strategies (18m)
  Implement DLP policies, content inspection, and endpoint protection with real enterprise cases.
- Security Metrics and Reporting (15m)
  Create meaningful security dashboards, KPIs, and executive reports using downloadable templates.

Complex Security Scenarios and Solutions

- Mergers and Acquisitions Security Planning (28m)
  Address security integration challenges, due diligence, and risk assessment in M&A scenarios.
- Third-Party Risk Management (22m)
  Vendor assessments, supply chain security, and contractual security requirements walkthrough.
- Security for Hybrid Work Environments (24m)
  Secure remote workers, BYOD policies, and distributed infrastructure with practical implementations.
- Advanced Compliance and Auditing (26m)
  Navigate SOC 2, ISO 27001, and regulatory requirements with audit preparation checklists.
- Security Automation and Orchestration (34m)
  Build SOAR playbooks, automate incident response, and integrate security tools with step-by-step guides.
- Cryptocurrency and Blockchain Security (19m)
  Understand wallet security, smart contract vulnerabilities, and blockchain threat analysis.
- OT and ICS Security Fundamentals (21m)
  Secure industrial control systems, SCADA networks, and operational technology environments.
- Security for Mergers and Acquisitions (27m)
  Real case study analysis of security integration challenges and successful remediation strategies.

- Advanced Incident Response Scenarios (36m)
  Problem-solving session for complex breaches including ransomware, APTs, and insider threats.

Exam Strategy and Implementation

- Practice Exam 1: Architecture Domain (38m)
  Timed practice questions with detailed explanations and strategy for the security architecture section.
- Practice Exam 2: Operations Domain (35m)
  Scenario-based questions covering SOC operations, incident response, and threat management.
- Practice Exam 3: Engineering Domain (40m)
  Technical problem-solving questions on security engineering, cryptography, and secure design.
- Practice Exam 4: Risk Management Domain (32m)
  Risk assessment, compliance, and governance questions with step-by-step solution walkthroughs.
- Time Management and Question Strategy (13m)
  Learn how to pace yourself, identify key information in scenarios, and eliminate wrong answers efficiently.
- Memorization Techniques for SecurityX (16m)
  Proven methods for retaining complex concepts, port numbers, encryption standards, and frameworks.
- Final Exam Day Preparation (11m)
  Checklist for exam day, what to bring, testing center procedures, and online proctoring tips.
- Troubleshooting Common Exam Pitfalls (18m)
  Address tricky question types, ambiguous scenarios, and how to handle questions you're unsure about.
- Building Your Post-Certification Career Plan (20m)
  Leverage SecurityX for career advancement, job roles, and continuing education opportunities.
- Downloadable Resources and Templates (8m)
  Access study guides, lab configurations, checklists, and practice question banks for final review.
- Full Practice Exam: Simulated Test Environment (40m)
  Complete timed practice exam replicating real CAS-005 conditions with immediate feedback.
- Review Session: Weak Areas and Retake Strategy (25m)
  Personalized review approach, identifying knowledge gaps, and creating your final study plan.
- Q&A: Real Exam Experiences and Tips (30m)
  Student questions answered, sharing of exam experiences, and last-minute preparation advice.
