MYTEK LAB

technology • education • knowledge

Course Title: CCST Cybersecurity Fundamentals
Grade Level: High School (Grades 10-12) / College Introductory Level
Certification Goal: Cisco Certified Support Technician (CCST) Cybersecurity

---

Scope and Sequence Outline

Unit 1: Introduction to Cybersecurity (Weeks 1-4)

- **Week 1: Course Introduction & Cybersecurity Basics**
  - Overview of cybersecurity and its importance
  - Cyber threats in everyday life
  - Cybersecurity terminology and common attack types
- **Week 2: Ethics & Cybersecurity Careers**
  - Ethical hacking vs. malicious hacking
  - Cybersecurity careers and industry trends
  - Laws and regulations (GDPR, HIPAA, CFAA)
  - The importance of ethical behavior in cybersecurity
- **Week 3: Fundamental Security Concepts**
  - CIA Triad (Confidentiality, Integrity, Availability)
  - Authentication, Authorization, and Accounting (AAA)
  - Risk management basics
  - Types of security controls: preventive, detective, corrective
- **Week 4: Cybersecurity Standards & Compliance**
  - NIST, ISO, and other frameworks
  - Role of government agencies (NSA, CISA, FBI)
  - Compliance and regulatory considerations in cybersecurity

---

Unit 2: Networking Fundamentals & Security (Weeks 5-8)

- **Week 5: Networking Basics**
  - OSI vs. TCP/IP model
  - IP addressing & subnetting
  - Network devices (routers, switches, firewalls)
  - Common network protocols (HTTP, HTTPS, DNS, FTP, SSH)
- **Week 6: Firewalls, IDS, & IPS**
  - Types of firewalls (hardware/software, stateful/stateless)
  - Intrusion Detection vs. Prevention Systems (IDS/IPS)
  - Configuring firewall rules and best practices
  - Network segmentation and access control lists (ACLs)
- **Week 7: Cryptography & VPNs**
  - Symmetric vs. asymmetric encryption
  - Hashing algorithms and digital signatures
  - VPN types and configurations (site-to-site, remote access)
  - Public Key Infrastructure (PKI) and certificate management
- **Week 8: Network Attacks & Mitigations**
  - Denial-of-Service (DoS), MitM attacks
  - SQL injection, cross-site scripting (XSS)
  - Security measures to mitigate network threats
  - Security logging and monitoring practices

Unit 3: Threats, Vulnerabilities, and Risk Management (Weeks 9-12)

- **Week 9: Malware & Social Engineering**
  - Types of malware (viruses, worms, ransomware, spyware)
  - Social engineering tactics (phishing, baiting, pretexting)
  - Recognizing and mitigating malware infections
- **Week 10: System & Application Security**
  - Secure coding practices and common vulnerabilities
  - Security patches and updates
  - Application security testing (SAST, DAST)
- **Week 11: Risk Management & Security Policies**
  - Identifying risks and vulnerabilities

  - Implementing security policies and procedures
  - Business continuity and disaster recovery planning
- **Week 12: Incident Handling & Digital Forensics**
  - Steps in incident response (preparation, detection, response, recovery)
  - Digital forensics basics (data collection, analysis, reporting)
  - Role of cybersecurity professionals in forensic investigations

---

Unit 4: Endpoint Security & Operating Systems (Weeks 13-16)

- **Week 13: Operating System Security (Windows/Linux)**
  - Hardening operating systems
  - Secure configuration management
  - File permissions and access control
- **Week 14: Secure Authentication & Access Controls**
  - Multi-Factor Authentication (MFA)
  - Role-Based Access Control (RBAC)
  - Secure password policies and enforcement
- **Week 15: Endpoint Security & Mobile Security**
  - Endpoint protection solutions (antivirus, EDR)
  - Securing mobile devices
  - BYOD security policies
- **Week 16: Midterm Review & Assessment**
  - Review of key concepts
  - Midterm exam

Unit 5: Cloud Security & Emerging Technologies (Weeks 17-22)

- **Week 17: Introduction to Cloud Security**
  - Cloud computing models (IaaS, PaaS, SaaS)
  - Cloud security risks and best practices
- **Week 18: Identity and Access Management (IAM)**
  - Identity federation and single sign-on (SSO)
  - Role of IAM in cloud security

- **Week 19: Secure Software Development & DevSecOps**
  - Secure software lifecycle (SDLC)
  - Continuous integration/continuous deployment (CI/CD) security
- **Week 20: Internet of Things (IoT) Security**
  - IoT vulnerabilities and attack vectors
  - Securing IoT devices
- **Week 21: Artificial Intelligence & Cybersecurity**
  - AI in cybersecurity threat detection
  - Ethical concerns around AI security tools
- **Week 22: Advanced Threats & Ethical Hacking**
  - Cyberwarfare and nation-state attacks
  - Introduction to penetration testing

Unit 6: Review, Labs, and Exam Preparation (Weeks 23-34)

- **Weeks 23-26: Hands-on Cybersecurity Labs**
  - Network traffic analysis with Wireshark
  - Secure system configuration
  - Simulated security incidents
- **Weeks 27-30: Cybersecurity Challenges & Case Studies**
  - Real-world attack case studies
  - Developing security response plans
- **Weeks 31-33: Exam Review & Practice Tests**
  - Practice exams and timed tests
  - Final review sessions
- **Week 34: Career Planning & Course Wrap-Up**
  - Resume building and interview preparation

Assessment & Grading

- **Projects (50%)**
- **Quizzes (20%)**
- **Midterm Exam (10%)**
- **Final Project (10%)**
- **Final Exam or CCST Certification (10%)**

***Disclaimer:** The course structure and content outlined in this scope and sequence are subject to change. MYTEK LAB reserves the right to adjust the order, pacing, and topics covered to best meet the needs of students and ensure an optimal learning experience.