

Fundamental Cloud Security Training

This course covers the fundamentals of cloud security that apply to all cloud networks. It focuses largely on the theory and concepts around cloud security, but it also covers routine solutions and has opportunities to practice a functional understanding of cloud security.

[CBT Nuggets course material](#) →

WEEK 1

Plan for Cloud Security and Compliance

170 min.

Cloud Security and Compliance	2
Threats and Vulnerabilities	9
Proactive Security Scanning	15
Data Security	17
Application and Infrastructure Security	17
Compliance Standards and Certifications	16

Plan for Cybersecurity in the Cloud

Overview	1
Plan for Cloud Cybersecurity	1
Security Patterns and Controls	21
Cloud Storage Security	19
Cloud Network Security	12
Cloud Compute Security	19
Cloud Security Solutions	20

WEEK 2

Certificates and the PKI

159 min.

Overview	1
Intro to Digital Certificates and the PKI	1
Symmetrical vs Asymmetrical Encryption	18
Digital Certificates Overview	7
Digital Signatures	14
Creating an HTTPS Session Key	9
Public Key Infrastructure	11
Quiz and Review	5

Secure Network Design

Overview	1
Intro to Secure Network Design	1
Network Segmentation	11
Network Firewalls	8
ACL Case Study	12
Load Balancing	7
Virtual private network (VPN)	6
Layer 2 Security	9
Network-based IDS/IPS	7
Quiz and Review	9

Secure Protocols

Overview	1
Intro to Secure Protocols	1
IPsec and VPNs	7
Secure Shell (SSH)	10

WEEK 3

159 min.

Domain Name System (DNS)	12
HTTPS	10
Weak Protocols	8
IP Addressing and Routing	5
Email Protocols	3
LDAP	3
SNMP, NTP, & SRTP	5
Quiz and Review	13

Host and Application Security

Overview	1
Intro to Host and App Security	1
Device Hardening	8
Boot integrity	4
Local Endpoint Protection	8
Network Based Protection	8
Secure Applications	6
Quiz and Review	14

Scanning, Monitoring, and Patching

Overview	1
Scanning, Monitoring & Patching: Scanning Overview	3
Scanning, Monitoring & Patching: Network Scanning Methodology	3
Scanning, Monitoring & Patching: Port Scanning and Discovery	4
Scanning, Monitoring & Patching: OS Discovery and Fingerprinting	6
Scanning, Monitoring & Patching: Motivators for Vulnerability Management	4
Scanning, Monitoring & Patching: Vulnerability Scanning	5
Scanning, Monitoring & Patching: Logging and Review	6
Scanning, Monitoring & Patching: Packet and Traffic Analysis	5
Scanning, Monitoring & Patching: Packet Capture and Analysis Lab	11

WEEK 4

156 min.

Scanning, Monitoring & Patching: Remediation and Patch Management	6
---	---

Scanning, Monitoring & Patching: Network Scanning with NMAP and Zenmap Lab 18

Scanning, Monitoring & Patching: Baselines 4

Plan for Cloud Policies, Procedures, and Risk Management

Overview 1

Plan for Cloud Governance 1

Risk Management 13

Resource Management 10

Vendor Lock-In and Data Portability 14

Documentation 11

Policies and Procedures 12

Regulatory and Policy-Based Incident Response

Overview 1

Regulatory and Policy-Based Incident Response - Objectives 1

Dealing with Prohibited Activities 3

Incident Response 6

The Chain of Custody 3

Software Licensing 5

Sensitive Data 6

Incident Response and Forensic Data Collection

Overview 1

Identifying an Incident 16

Containing and Mitigating an Outbreak 10

Forensic Data Collection 11

WEEK 5

Forensics In the Cloud 7

Forensic Evidence Management 6

14 min.

7

6