CompTIA CASP+ (CAS-004)

This expert CompTIA CASP+ training prepares security analysts to take the CAS-004 exam, which is the one exam required to earn the CASP+ certification. Learn the skills you need to configure and implement enterprise security strategies.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Secure Network Architecture Services — 162 min.

DoS Protection, Load Balancers and Proxies	17
Intrusion Prevention/Detection Systems	13
Application Security	5
NACs and VPNs	7
Securing DNS and Email	10
Routers and NAT Gateways	8
Firewalls, UTMs and NGFWs	12

Secure Network Architecture Practices

Overview	1
Traffic Monitoring	8
Security Sensors	15
Network Segmentation	15
Deperimeterization / Zero Trust	3
Merging Networks	7
Defense In Depth	4

Security Infrastructure Design

Overview	1
Software Defined Networking (SDN)	9
Scalability and Automation	10
Resiliency In Infrastructure Design	15

WEEK 2

159 min.

Virtuailzation and Containerization	17
CDNs and Caching	7

Secure Software Integration

Overview	1
Baselines and Templates	8
APIs and Middleware	13
Software Assurance	11
Integrating Enterprise Applications	6
Application Development Security	10
Web Application Security	7

Data Security Techniques

Overview	1
Data Loss Prevention and Detection	6
Data Classification, Labeling and Tagging	7
Obfuscation and Anonymization of Data	7
Data Lifecycle Management	13
Data Inventory and Mapping	7
Data Integrity Management	13

Authentication and Authorization Controls

Overview	1
Managing Credentials	10
Password Policies	11

Cloud and Virtualization Solutions

Overview	1
Virtualization Technologies	8
Virtualization Strategies	9
Cloud Deployment Models	9
Cloud Computing Characteristics	8
Cloud Provider Limitations	10
Extending On-premise Security Controls	9

Cryptography and PKI

Overview	1
The CIA Triad	7
Non-repudiation and Compliance Requirements	10
Cryptography and PKI	7
Hashes and Digital Signatures	10
Cryptography Use Cases	10

Enterprise Security and Emerging Technologies

Overview	1
AI and ML	5
Quantum Computing and Nano Technology	6
Homomorphic Encryption and SMC	8

WEEK 3

152 min.

Access Control	7
AAA Protocols	13
MFA, OTP and SSO	5
Authenticating Hardware and People	5

WEEK 4

156 min.

Blockchain and Distributed Consensus	8
Big Data and Passwordless Authentication	8
Virtual Reality and 3D Printing	7
Deepfakes and Biometric Impersonation	6

Threat Management Activities

Overview	1
Threat Intelligence	14
Threat Intel Collection Methods	7
Types of Threat Actors	7
Threat Management Frameworks	10
Using MITRE ATT&CK	9
IOCs and Responses	6

Vulnerability Management Activities

Overview	1
Vulnerability Scans	11
Security Content Automation Protocol (SCAP)	12
Assessments	14
Patch Management	8
Information Sources	4

Vulnerability Assessments and Pentesting

Overview	1
Vulnerability Assessment vs Pentesting	7
Testing Methods	12

WEEK 5

152 min.

Pentesting: Post Exploit	7
Vulnerability Assessment Tools	7
Some Pentesting Tools	9
Vulnerability Assessments and Pentesting Requirements	5

Vulnerability Analysis and Mitigation

Overview	1
Common Software Vulnerabilities	13
Race Conditions	7
Cryptographic Vulnerabilities	5
Software Development Vulnerabilities	7
Web Application Attacks	8
VM and Network-Based Attacks	13

Using Processes to Reduce Risk

Overview	1
Being Proactive	13
Using Data Analysis	9
Preventative Measures	8
Application Control	6
Security Automation	4
Physical .Security	8

Incidents and Their Responses

Overview	1
Intro	3
Event Classification	7
Event Triage	7

WEEK 6

153 min.

Incident Response Process	8
Incident Response Playbooks	16
Automated Response	4
Communications Plans & Stakeholder Management	3

Forensic Concepts and Analysis

Overview	1
Intro	1
Forensic Process: Identification	9
Digital Forensics	5
Forensic Process: Evidence Collection	15
Forensic Process: Evidence Preservation	5
Forensic Process: Analysis	6
Forensic Process: Verification and Presentation	3

Configuring Enterprise Mobility and Endpoint Security

Overview	1
Intro	2
Enterprise Mobility Management	6
Windows Information Protection	14
Configuring Endpoint Security Controls	9
Hardening Techniques	12
Compensation Controls	4

Cloud Adoption And Operational Technology Security Impacts

Overview	1
Intro	1
Cloud Deployment Models	8
Impacts of Cloud Technology Adoption	8
Securing Specialized Technologies	8

WEEK 7 **157 min.**

Cloud Threats And Vulnerabilities	4
Monitoring Logs Using Azure AD Audit.	5
Emerging Technologies	13

Implementing PKI Solutions and Cryptography

Overview	1
Introduction To Public Key Infrastructure	1
The Role Of Public Key Infrastructure	8
Private And Public Key Encryption	7
Certificate Lifecycle	12
Certificate Types And Usage	8
Understanding Trust Concepts	11

Implementing Cryptographic Protocols and Algorithms

Overview	1
Hashing	11
SSL/TLS	8
Symmetric And Asymmetric Algorithm	4
S/MIME and SSH	14
Internet Protocol Security (IPSec)	9

Risk Strategies

Overview	1
Risk Analysis Methods	7
Responding To Risk	11
Types of Risk	7
Risk Management Lifecycle and Frameworks	11

WEEK 8 **152 min.**

Tracking Risk	4
Risk Appetite, Tolerance, and Capacity	8
Policies and Security Practices	9

Managing and Mitigating Third Party Risk

Overview	1
Third Party Risk Management	17
Vendor Lock-In/Out and Viability	6
Meeting Obligations	7
Third Party Dependencies	6
Technical Considerations	7
Additional Vendor Considerations	8

Compliance Frameworks and Legal Considerations

Overview	1
Data Considerations	12
Location, Location, Location	8
Regulations, Accreditations and Standards	12
Legal Considerations	9
Contract and Agreement Types	9

Business Continuity and Disaster Recovery Planning

Overview	1
BC and DR Planning	4
BC/DR Planning Process	12
Creating a BC Plan	8
DR Planning	15
Resiliency Technologies	8
Testing BC/DR Plans	6

WEEK 9 **30 min.**