Information Security

This InfoSec training course explains data security best practices and threats. After finishing this Information Security training, you'll know how to mitigate vulnerabilities in web-based systems, mobile systems, and embedded devices; apply cryptography; and learn how security operations work. You'll also gain an understanding of asset security while learning about privacy protection, asset retention, data security controls.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Information Security: Security and Risk Management 153 min.

CIA Concepts	4
Cyber Crime Terms and Vocabulary	4
27000 Series Framework	6
Due Care and Due Diligence	5
Inside Threats and Ethics	5
Policies Start with Senior Management	6
Defining Risk	4
Control Types	4
Compliance Requirements	6
DR, BC, and BIA	6
Security Awareness Training	5
Intellectual Property and Licensing	6
Policy Life Cycle	6
Threat Modeling	6
Supply Chain Risk Management	5

Information Security: Asset Security

Overview	1
Classifying Assets and Information	8
Stewards and Custodians of Assets and Information	7
Protecting Privacy	4
Data Retention	4
Determining Security Controls	5
Data State and Resources for Security Control Frameworks	2
Information and Asset Handling Policies	7

Information Security: Security Architecture and Engineering

Overview	1
Designing with Security in Mind	6
Security Model Fundamentals	7
System Security Requirements	5
Hardware and Firmware Security Capabilities	6
Assessing Vulnerabilities	5
Vulnerabilities in Web-Based Systems	5

WEEK 2 **151 min.**

Vulnerabilities in Mobile Systems	4
Vulnerabilities in Embedded Devices	6
Facility Design and Controls	6
Symmetric Encryption Concepts	6
Symmetric Keys and Algorithms	4
Asymmetric Encryption Concepts	5
Digital Signature Concepts	6
Hashing for Integrity	5
Asymmetrical Encryption with Email	6
PKI and Revoking Certificates	4
Power Considerations	4

Information Security: Communication and Network Security

Overview	1
OSI and IP Models	6
IP Networking	7
Wi-Fi Security Considerations	8
Network Component Security	7
Virtualized Network Security Considerations	4
Securing Communications Channels	8

Information Security: Identity and Access Management (IAM)

Overview	1
Identity Management (IdM)	7
AAA as Part of Our Controls	6
Centralized Authentication with RADIUS	7
Using LDAP with Directory Services	4
Multi-Factor Authentication Categories	3
Biometric Acceptance and Rejection Rates	5
Options for Biometric Authentication	5
DAC, MAC, and RBAC	6
IAM Provisioning Lifecycle	8

WEEK 3 **152 min.**

Information Security: Security Assessment and Testing

Overview	1
Testing, Auditing, and Assessment Overview	6
Penetration Testing	5
Vulnerability Scans and Assessments	3
Reviewing and Testing Code	6
Security-Related Data Collection	7
Continuous Monitoring	4

Information Security: Security Operations

Overview	1

WEEK 4 **68 min.**

Information Security: Software Development Security