CompTIA SecurityX (CAS-005)

This CompTIA SecurityX training prepares you to earn CompTIA's expert-level security architect certification. SecurityX is one of the best certifications for cybersecurity professionals, and covers asset lifecycle management, MITRE ATT&CK framework, GRC, and more. It also aligns with DoDD 8140, helping you comply with government roles and contracts. You'll learn secure system design, risk management, and compliance across complex environments. Your instructor, cybersecurity expert Erik Choron, has been in the trenches for over 20 years and knows how to make challenging material approachable, relevant, and even fun. Start studying now and pass the CAS-005 exam with confidence.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Intro to SecurityX

Policy

Hungry for some risk?

Anatomy of a Policy

Examples within the policy

Addendum

Challenge

Program/Project Management

Managing the project

RACI Matrix

This is the song that never ends...

Communication

Challenge

COBIT

Frameworks

Evaluate, Direct, and Monitor (EDM)

Align, Plan, and Organize (APO)

Build, Acquire, and Implement (BAI)

Deliver, Service, and Support (DSS)

Monitor, Evaluate, and Assess (MEA)

Check on learning

ITIL

Focused on Service Delivery

Service Strategy

Service Design

Service Transition

Service Operation

CSI Challenge

Configuration Management

Configuration Management

Configuration Management Initiation

Change accepted. Now what?

Sandboxing

Keeping track of it all

Scenario

Governance, Risk, and Compliance (GRC)

GRC - What is it?

Governance

Risk

Compliance

Monitoring GRC

Challenge

Data governance

Data governance in Staging Environments

Preventing Unauthorized Access

Maintaining Compliance

Controlling "Configuration Drift"

The Timeline

Challenge

Data Life Cycle Management

Understanding the Data Life Cycle

Data Classification Policy

Risk Reduction & Liability

Cost Optimization

Compliance & Legal Hold

Challenge

Risk Management

Understanding Risk Basics

Risk Appetite

Risk Tolerance

Risk Priorities

Transferring Risks

Challenge

Analyzing Risk

Addressing Risk Using Analysis

Quantitative Risk Analysis

Qualitative Risk Analysis

Severity Impact

Challenge

Risk From the Outside

Outside Considerations

Hope for the best, plan for the worst

Vendor Risks

Supply Chain Risks

Availability Risks

Challenge

Breach Response

Data Breach

Detection

Containment

Eradication

Recovery

Post-breach analysis

Threat Modeling

Knowing our Threat

Identifying Threats

STRIDE

Scenario

Attack Methodology Frameworks

Understanding the Attack

MITRE ATT&CK Framework

The Diamond Model

The Cyber Kill Chain

Challenge

Attack Surface

Addendum

Physical Surface

Digital Surface

Personal Surface

Why does Policy matter?

Scenario

Security Frameworks

Frameworks

NIST Cybersecurity Framework

NIST Security Controls

NIST Risk Management

NIST Vendor Compliance

Scenario

Cloud Capabilities

Cloud Access Security Brokers (CASB)

Shared Responsibility

CI/CD Pipeline

Only the Shadow knows

Scenario

Container Security

Containers

Addressing the security

Key Risks & Hardening

The "Blast Radius"

Scenario

Cloud Data Security

Data Security in the Cloud

Data Exposure and Leakage

Insecure Storage

Remanence

Learning From Others

Scenario

Encryption in the Cloud

Different States of Data

Encryption Types

Applying the Encryption in the Cloud

Encryption Compliance

Scenario

Cloud Control Strategies

Cloud Control Strategies

Protective Controls

Detective Controls

Preventive Controls

Cloud Service Integration

Scenario

Network Architecture

Network Architecture

Segmentation

Micro-segmentation

VPN

Scenario

Security Boundaries

Where does the security begin and end?

Asset Identification

Attestation

Data Perimeters

Scenario

Deperimeterization

Deperimeterization

API Integration

SASE

SD-WAN

Scenario

Executive Security Automation

Automation

Security Automation

Infrastructure as a Code

SOAR

Scenario

Vulnerability Management

Vulnerability Management

Scanning

Reporting

CVSS

Scenario

Cryptographic Techniques

Cryptographic Basics

Tokenization

Cryptographic Erase

Hashing

Scenario

Advanced Cryptography

Advanced Cryptography

Key Stretching

WEEK 2

Homomorphic Encryption

Forward Security

Scenario

Monitoring and Data Analysis

Monitoring the IT Infrastructure

Aggregate Analysis

What to look out for

Behavior Baselines

Scenario

Vulnerabilities and Attack Surface

Understanding Vulnerabilities

Attack Surfaces

Common Vulnerabilities on IT Systems

Reducing the Surface

Scenario

Threat Hunting

Know your enemy

Some enemies are already known

Here's a "TIP"

Scenario

Incident Response

Something Happened!

The Process

Preparation

Detection & Analysis

Containment, Eradication, & Recovery

Post-incident Activity

Root Cause

Scenario