Microsoft Certified: Cybersecurity Architect Expert (SC-100)

This Microsoft Certified: Cybersecurity Architect Expert (SC-100) training covers how to design a large network's protective security architecture, grounded in the Zero Trust strategy. For anyone who manages cybersecurity architecture training, this Azure training can be used to onboard new cybersecurity associates or as an Azure reference resource.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Examining the Microsoft Cybersecurity Reference Architecture (MCRA) — 151 min.

Intro to the Microsoft Cybersecurity Reference Architecture (MCRA)	4
Security Operations	12
SaaS & Identity Protection	6
Endpoints and Devices	5
Hybrid Infrastructure	16
Information Protection	5
IoT and Operational Technology (OT)	4
People Security	3
Other Resources	9

Translating Security Requirements

Overview	1
Guiding Principals of Zero Trust	8
Translating Requirements	12
Translating Business Goals into Security Requirements	10
Technical Solutions Basics	4
Azure Security Top 10	8
Azure Security Benchmark	9
Securing Privileged Access Using RaMP	4

Designing Security Strategies

Overview	1
Designing Security for a Resiliency Strategy	10
Hybrid Environmental Security Strategies	13
Multi-tenant Environmental Security Strategies	5

WEEK 2

156 min.

Traffic Filtering and Segmentation Strategies	9
Azure Best Practices for Network Security	13

Designing a Security Operations Strategy

Overview	1
Security Operations Strategy Overview	8
Frameworks, Processes, and Procedures	9
Logging and Auditing Strategy	8
SecOps for a Hybrid or Multi-Cloud Environment	3
SIEM/SOAR Strategy	9
Evaluating Security Workflows	7
Incident Management	4
Strategy for Sharing Technical Threat Intelligence	4

Designing an Identity Security Strategy

Overview	1
Strategy for Access to Cloud Resources	11
Identity Store Strategy	6
Authentication and Authorization Strategy	7
Strategy for Conditional Access	8
Role Assignment and Delegation	7
Privileged Role Access to Infrastructure	7
Strategy for Privileged Activities	7

Designing a Regulatory Compliance Strategy

Overview	1
Translating Compliance Requirements	10
Compliance and Defender for Cloud	7
Compliance Scores and Recommendations	6

WEEK 3

158 min.

Implementing Azure Policy	11
Data Residency Requirements	5
Translating Privacy Requirements	11

Evaluating and Managing Security Postures

Overview	1
Evaluating Security Postures by Using Benchmarks	6
Evaluating Security Postures by Using Defender for Cloud	5
Evaluate Security Posture of Cloud Workloads	5
Designing Security for an Azure Landing Zone	10
Interpret Technical Threat Intelligence	8
Mitigating Identified Risks	12

Designing a Strategy for Securing Server and Client Endpoints

Overview	1
Security Baselines for Servers and Client Endpoints	9
Security Requirements for Servers	10
Security Requirements for Mobile Devices and Clients	10
Requirements to Secure Active Directory Domain Services	10
Strategy to Manage Secrets, Keys, and Certificates	10
Strategy for Securing Remote Access	6

Designing a Strategy for Securing SaaS, PaaS, and IaaS Services

Overview	1
Security Baselines for SaaS, PaaS, and IaaS services	8
Security Requirements for IoT Workloads	7
Security Requirements for Data Workloads	9

WEEK 4

94 min.

Security Requirements for Web Workloads	6
Security Requirements for Storage Workloads	8
Security Requirements for Containers and Orchestration	8

Design a security strategy for data and applications

Overview	1
Specify Priorities for Mitigating Threats to Apps	13
Onboarding New Applications	10
Security Strategy for Applications and APIs	10
Priorities For Mitigating Threats To Data	12
Identify and Protect Sensitive Data	9
Encryption Standards for Data at Rest and In Motion	10
Azure Data Security and Encryption Best Practices	5