Microsoft

Microsoft Cybersecurity Architect

Exam Ref SC-100

Yuri Diogenes
Sarah Young
Mark Simos
Gladys Rodriguez

Microsoft

Exam Ref SC-100 Microsoft Cybersecurity Architect

Yuri Diogenes
Sarah Young
Mark Simos
Gladys Rodriguez

Exam Ref SC-100 Microsoft Cybersecurity Architect

Table of Contents

Cover
Title Page
Copyright Page
Contents at a glance
Contents
Introduction
- Organization of this book
- Preparing for the exam
- Microsoft certifications
- Quick access to online references
- Errata, updates, & book support
- Stay in touch

Chapter 1 Build an overall security strategy and architecture
- Security architecture
- Security architects
- Architects work across teams and roles
- Zero Trust transformation and security architects
  - Security architects are critical to Zero Trust
- Skill 1-1: Identify the integration points in an architecture by using Microsoft Cybersecurity Reference Architectures (MCRA)
  - MCRA and Cloud Adoption Framework Secure Methodology

Table of Contents

How to use the MCRA to identify integration points

Skill 1-2: Translate business goals into security requirements

Translation process

Skill 1-3: Translate security requirements into technical capabilities, including security services, security products, and security processes

Requirement: Mitigate compromise of accounts using password spray and other credential compromise

Requirement: Shorten response times to attacks across resources in the environment

Requirement: Integrate network security into Infrastructure as Code (IaC) automation

Requirement: Enable eDiscovery processes for Office 365 data

Skill 1-4: Design security for a resiliency strategy

Reducing risk by reducing critical security events

Resilience requires shifting from a network-centric to an asset- and data-centric mindset

Skill 1-5: Integrate a hybrid or multi-tenant environment into a security strategy

Skill 1-6: Develop a technical governance strategy for security

Thought experiment

Tailoring security technology to different business scenarios

Thought experiment answers

Chapter summary

Chapter 2 Design a security operations strategy

Skill 2-1: Design a logging and auditing strategy to support security operations

Centralizing log collection

Deciding which logs have security value

Designing security operations use cases

Determining log retention periods

Skill 2-2: Develop security operations to support a hybrid or multi-cloud

Table of Contents

environment

Cross-platform log collection

Cloud security posture management (CSPM)

Focus on identity

Internet of Things (IoT) / Operational Technology (OT) coverage

Skill 2-3: Design a strategy for SIEM and SOAR

Microsoft Security Operations Reference Architecture

Ingest logs into your SIEM

Automate, automate, automate

Skill 2-4: Evaluate security workflows

General incident response workflow

Automation, automation, automation (again)

Skill 2-5: Evaluate a security operations strategy for the incident management lifecycle

Microsofts approach to security incident management

Preparation

Detection and analysis

Containment

Eradication

Recovery

Post-incident activity

Skill 2-6: Evaluate a security operations strategy for sharing technical threat intelligence

Microsofts threat intelligence strategy

Sharing technical threat intelligence in your organization

Thought experiment

Security operations strategy at Contoso Ltd

Thought experiment answers

Chapter summary

Table of Contents

Chapter 3 Design an identity security strategy

Skill 3-1: Design a strategy for access to cloud resources

Identity-related access controls

Network-related access controls

Coordinated identity and network access

Interconnection and cross-service collaboration

Assume-breach and explicitly verify

People, process, and technology approach

Skill 3-2: Recommend an identity store (tenants, B2B, B2C, and hybrid)

Foundational implementations

External collaboration

Skill 3-3: Recommend an authentication strategy

Enterprise accounts

Specialized accounts

Controlling authentication sessions

Key recommendations

Skill 3-4: Recommend an authorization strategy

Configuring access to support authorization

Decentralized identities

Key recommendations

Skill 3-5: Design a strategy for conditional access

Key recommendations

Skill 3-6: Design a strategy for role assignment and delegation

Delegating to non-administrators

Delegating access to service providers

Skill 3-7: Design security strategy for privileged-role access to infrastructure, including identity-based firewall rules and Azure PIM

Privileged Access Workstation (PAW)

Privileged Identity Management (PIM)

Table of Contents

Microsoft Entra Permissions Management

Key recommendations

Skill 3-8: Design security strategy for privileged activities, including PAM, entitlement management, and cloud tenant administration

Privileged Access Workstation (PAW)

Privileged Identity Management (PIM)

Microsoft Entra Permissions Management

Thought experiment

Thought experiment answers

Chapter summary

Chapter 4 Design a regulatory compliance strategy

Overview of security governance

Skill 4-1: Interpret compliance requirements and translate into specifi ctechnical capabilities (new or existing)

Security compliance translation process

Resolving conflicts between compliance and security

Skill 4-2: Evaluate infrastructure compliance by using Microsoft Defender for Cloud

Skill 4-3: Interpret compliance scores and recommend actions to resolve issues or improve security

Skill 4-4: Design implementation of Azure Policy

Skill 4-5: Design for data residency requirements

Skill 4-6: Translate privacy requirements into requirements for security solutions

Security and privacy

Thought experiment

Building repeatable technical patterns for security compliance

Thought experiment answers

Table of Contents

Chapter summary

Chapter 5 Evaluate security posture and recommend technical strategies to manage risk

Skill 5-1: Evaluate security posture by using benchmarks (including Azure security benchmarks for Microsoft Cloud security benchmark, ISO 27001, etc.)

Microsoft cloud security benchmark

Monitoring your MCSB compliance

Industry standards

Skill 5-2: Evaluate security posture by using Microsoft Defender for Cloud

Defender for Cloud

Security posture management

Considerations for multi-cloud

Considerations for vulnerability assessment

Skill 5-3: Evaluate security posture by using Secure Scores

Secure Score in Defender for Cloud

Skill 5-4: Evaluate security posture of cloud workloads

Workload security

Skill 5-5: Design security for an Azure Landing Zone

Design principles

Enforcing guardrails

Single management plane

Application-centric

Security considerations

Skill 5-6: Interpret technical threat intelligence and recommend risk mitigations

Threat intelligence in Defender for Cloud

Threat intelligence in Microsoft Sentinel

Skill 5-7: Recommend security capabilities or controls to mitigate

Table of Contents

identified risks
Identifying and mitigating risk
Thought experiment
Monitoring security at Fabrikam Inc
Thought experiment answers
Chapter summary
Chapter 6 Design a strategy for securing server and client endpoints
Skill 6-1: Specify security baselines for server and client endpoints
Group Policy Objects (GPO)
Security Compliance Toolkit (SCT)
Azure Security Benchmark (ASB)
Microsoft Endpoint Manager (MEM)
PowerShell DSC
Azure Automation
Azure Policy
Azure Resource Manager (ARM) templates
Blueprints
Microsoft Defender for Cloud (MDC)
Microsoft Defender for IoT (MDIoT)
Baseline configuration
Key Recommendations
Skill 6-2: Specify security requirements for servers, including multiple platforms and operating systems
Shared responsibility in the cloud
Legacy insecure protocols
Threat protection
Local Administrator Password Management (LAPS)
User rights assignments

Table of Contents

- Network-based controls
- Governance

Skill 6-3: Specify security requirements for mobile devices and clients, including endpoint protection, hardening, and configuration

- Local Administrator Password Management
- Basic Mobility and Security
- Threat protection
- Conditional access
- Microsoft Intune
- User right assignments
- Micro-segmentation
- Governance
- Other security controls

Skill 6-4: Specify requirements to secure Active Directory Domain Services

- Secure the control plane
- Privileged Access Management
- Key recommendations
- Microsoft Defender for Identity
- Active Directory Federation Services (AD FS)

Skill 6-5: Design a strategy to manage secrets, keys, and certificates

- Access control
- Configuration control
- Key management
- Key recommendations

Skill 6-6: Design a strategy for secure remote access

- Key configurations to enable secure remote access
- Remote access to desktop, applications, and data
- Remote access to on-premises web applications
- RDP/SSH connectivity

Table of Contents

Remotely provisioning new devices

B2B collaboration

Key recommendations

Thought experiment

Thought experiment answers

Chapter summary

Chapter 7 Design a strategy for securing SaaS, PaaS, and IaaS services

Skill 7-1: Specify security baselines for SaaS, PaaS, and IaaS services

Specify security baselines for SaaS services

Skill 7-2: Specify security requirements for IoT workloads

Security requirements

Security posture and threat detection

Skill 7-3: Specify security requirements for data workloads, including SQL, Azure SQL Database, Azure Synapse, and Azure Cosmos DB

Security considerations for Azure Cosmos DB

Skill 7-4: Specify security requirements for web workloads, including Azure App Service

Network communication

Authentication and authorization

Security posture and threat protection

Skill 7-5: Specify security requirements for storage workloads, including Azure Storage

Data protection

Identity and access management

Networking

Logging and monitoring

Table of Contents

Skill 7-6: Specify security requirements for containers

Hardening access to Azure Container Registry

Skill 7-7: Specify security requirements for container orchestration

Threat detection

Thought experiment

Design a strategy for securing PaaS and IaaS services at Fabrikam, Inc

Thought experiment answers

Chapter summary

Chapter 8 Specify security requirements for applications

Skill 8-1: Specify priorities for mitigating threats to applications

Classifying applications

Application threat modeling

Microsoft Security Development Lifecycle (SDL)

Skill 8-2: Specify a security standard for onboarding a new application

Old versus new

Security standards for onboarding applications

Skill 8-3: Specify a security strategy for applications and APIs

Waterfall to Agile/DevOps

Security in DevOps (DevSecOps)

Thought experiment

Application migration and modernization at Fabrikam, Inc

Thought experiment answers

Chapter summary

Chapter 9 Design a strategy for securing data

Skill 9-1: Specify priorities for mitigating threats to data

Common threats

Prioritization

Skill 9-2: Design a strategy to identify and protect sensitive data

Table of Contents

Know your data

Protect your data

Prevent data loss

Govern your data

Skill 9-3: Specify an encryption standard for data at rest and in motion

Encryption at rest

Encryption in motion

Thought experiment

Design a strategy for securing data

Thought experiment answers

Chapter summary

Chapter 10 Microsoft Cybersecurity Reference Architectures and Microsoft cloud security benchmark best practices

What are best practices?

Antipatterns are the opposites of best practices

Microsoft Cybersecurity Reference Architectures (MCRA)

Microsoft cloud security benchmark (MCSB)

Skill 10-1: Recommend best practices for cybersecurity capabilities and controls

Skill 10-2: Recommend best practices for protecting from insider and external attacks

Skill 10-3: Recommend best practices for Zero Trust security

Skill 10-4: Recommend best practices for the Zero Trust Rapid Modernization Plan

Thought experiment

Identifying applicable best practices

Thought experiment answers

Chapter summary

Table of Contents

Chapter 11 Recommend a secure methodology by using the Cloud Adoption Framework (CAF)

Skill 11-1: Recommend a DevSecOps process

DevSecOps Controls

Plan and develop

Commit the code

Build and test

Go to production and operate

Skill 11-2: Recommend a methodology for asset protection

Getting secure

Staying secure

Key recommendations for an asset protection program

Skill 11-3: Recommend strategies for managing and minimizing risk

Measuring risk

Managing security risk

Thought experiment

Using the CAF for secure methodologies at Tailwind Traders

Thought experiment answers

Chapter summary

Chapter 12 Recommend a ransomware strategy by using Microsoft Security Best Practices

Skill 12-1: Plan for ransomware protection and extortion-based attacks

Preparation

Security hygiene and damage control

Skill 12-2: Protect assets from ransomware attacks

Enter environment

Traverse and spread

Execute objective

Table of Contents

- Skill 12-3: Recommend Microsoft ransomware best practices
  - Best practices
- Thought experiment
  - Developing a strategy to protect against ransomware
- Thought experiment answers
- Chapter summary

Index

Pearson