Start here

Tuesday, October 25, 2022 2:37 PM

Hi,

This OneNote Study Guide has been created to help you prepare for the SC-100 exam. Please note this is not an official Microsoft document.

Tabs
Overview - includes list of exam objectives and other resources. Most resources are Microsoft specific but I have included non-Microsoft links.

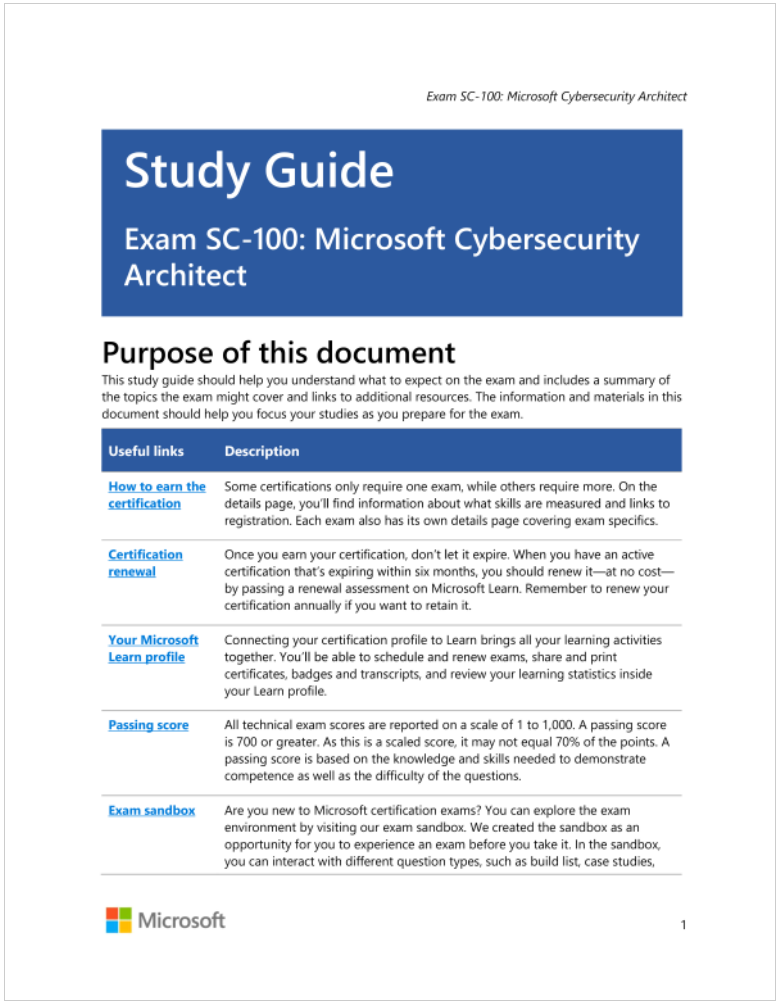
The exam domains each have a tab and each set of objectives have a page within the domain. I have included links to the Microsoft docs. Those can be found on the left side of the page. Additional links are on the right.

Please feel free to update and change this OneNote to help you prepare for SC-100.

SC-100_StudyGuide_ENU_FY23Q1.1

Tuesday, December 13, 2022 12:23 PM

SC-100_StudyGuide_ENU_FY23Q1.1



Exam SC-100: Microsoft Cybersecurity Architect

Study Guide

Exam SC-100: Microsoft Cybersecurity Architect

Purpose of this document

This study guide should help you understand what to expect on the exam and includes a summary of the topics the exam might cover and links to additional resources. The information and materials in this document should help you focus your studies as you prepare for the exam.

Useful links	Description
How to earn the certification	Some certifications only require one exam, while others require more. On the details page, you'll find information about what skills are measured and links to registration. Each exam also has its own details page covering exam specifics.
Certification renewal	Once you earn your certification, don't let it expire. When you have an active certification that's expiring within six months, you should renew it—at no cost—by passing a renewal assessment on Microsoft Learn. Remember to renew your certification annually if you want to retain it.
Your Microsoft Learn profile	Connecting your certification profile to Learn brings all your learning activities together. You'll be able to schedule and renew exams, share and print certificates, badges and transcripts, and review your learning statistics inside your Learn profile.
Passing score	All technical exam scores are reported on a scale of 1 to 1,000. A passing score is 700 or greater. As this is a scaled score, it may not equal 70% of the points. A passing score is based on the knowledge and skills needed to demonstrate competence as well as the difficulty of the questions.
Exam sandbox	Are you new to Microsoft certification exams? You can explore the exam environment by visiting our exam sandbox. We created the sandbox as an opportunity for you to experience an exam before you take it. In the sandbox, you can interact with different question types, such as build list, case studies,

Microsoft

1

Case study links on GitHub SC-100-Microsoft-Cybersecurity-Architect (microsoftlearning.github.io)

Learning Paths
https://learn.microsoft.com/en-us/training/paths/sc-100-design-zero-trust-strategy-architecture/
https://learn.microsoft.com/en-us/training/paths/sc-100-evaluate-governance-risk-compliance/
https://learn.microsoft.com/en-us/training/paths/sc-100-design-security-for-infrastructure/
https://learn.microsoft.com/en-us/training/paths/sc-100-design-strategy-for-data-applications/
https://learn.microsoft.com/en-us/training/paths/recommend-security-best-practices/

I recommend saving the learning paths to a collection in your Learn profile for easy access and tracking. For those who like "books", I send the pages to a OneNote. You can then add notes, search etc. in a OneNote notebook.

Microsoft 365 Licensing Compare Microsoft 365 Enterprise plans

Useful links	Description
	and others that you might encounter in the user interface when you take an exam. Additionally, it includes the introductory screens, instructions, and help topics related to the different types of questions that your exam might include. It also includes the non-disclosure agreement that you must accept before you can launch the exam.
Request accommodations	We're committed to ensuring all learners are set up for success. If you use assistive devices, require extra time, or need modification to any part of the exam experience, you can request an accommodation.
Take a practice test	Taking a practice test is a great way to know whether you're ready to take the exam or if you need to study a bit more. Subject-matter experts write the Microsoft Official Practice Tests, which are designed to assess all exam objectives.

Objective domain: skills the exam measures

The English language version of this exam was updated on November 4, 2022.

Some exams are localized into other languages, and those are updated approximately eight weeks after the English version is updated. Other available languages are listed in the **Schedule Exam** section of the **Exam Details** webpage. If the exam isn't available in your preferred language, you can request an additional 30 minutes to complete the exam.

> **Note**
> The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. Related topics may be covered in the exam.

> **Note**
> Most questions cover features that are general availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Skills measured

- Design a Zero Trust strategy and architecture (30–35%)
- Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies (10–15%)
- Design security for infrastructure (10–15%)
- Design a strategy for data and applications (15–20%)
- Recommend security best practices and priorities (20–25%)

Functional groups

Design a Zero Trust strategy and architecture (30–35%)

Build an overall security strategy and architecture

- Identify the integration points in a security architecture by using Microsoft Cybersecurity Reference Architecture (MCRA)
- Translate business goals into security requirements
- Translate security requirements into technical capabilities, including security services, security products, and security processes
- Design security for a resiliency strategy
- Integrate a hybrid or multi-tenant environment into a security strategy
- Develop a technical governance strategy for security

Design a security operations strategy

- Design a logging and auditing strategy to support security operations
- Develop security operations to support a hybrid or multi-cloud environment
- Design a strategy for SIEM and SOAR
- Evaluate security workflows
- Evaluate a security operations strategy for incident management lifecycle
- Evaluate a security operations strategy for sharing technical threat intelligence

Design an identity security strategy

- Design a strategy for access to cloud resources
- Recommend an identity store (tenants, B2B, B2C, hybrid)
- Recommend an authentication strategy
- Recommend an authorization strategy
- Design a strategy for conditional access
- Design a strategy for role assignment and delegation
- Design security strategy for privileged role access to infrastructure including identity-based firewall rules and Privileged Identity Management (PIM) in Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
- Design security strategy for privileged activities including PAM, entitlement management, cloud tenant administration

Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies (10–15%)

Design a regulatory compliance strategy

- Interpret compliance requirements and translate into specific technical capabilities (new or existing)

- Evaluate infrastructure compliance by using Microsoft Defender for Cloud
- Interpret compliance scores and recommend actions to resolve issues or improve security
- Design implementation of Azure Policy
- Design for data residency requirements
- Translate privacy requirements into requirements for security solutions

Evaluate security posture and recommend technical strategies to manage risk

- Evaluate security posture by using Azure Security Benchmark
- Evaluate security posture by using Microsoft Defender for Cloud
- Evaluate security posture by using Secure Scores
- Evaluate security posture of cloud workloads
- Design security for an Azure Landing Zone
- Interpret technical threat intelligence and recommend risk mitigations
- Recommend security capabilities or controls to mitigate identified risks

Design security for infrastructure (10–15%)

Design a strategy for securing server and client endpoints

- Specify security baselines for server and client endpoints
- Specify security requirements for servers, including multiple platforms and operating systems
- Specify security requirements for mobile devices and clients, including endpoint protection, hardening, and configuration
- Specify requirements to secure Active Directory Domain Services
- Design a strategy to manage secrets, keys, and certificates
- Design a strategy for secure remote access
- Design a strategy for securing privileged access

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

- Specify security baselines for SaaS, PaaS, and IaaS services
- Specify security requirements for IoT workloads
- Specify security requirements for data workloads, including SQL Server, Azure SQL, Azure Synapse, and Azure Cosmos DB
- Specify security requirements for web workloads, including Azure App Service
- Specify security requirements for storage workloads, including Azure Storage
- Specify security requirements for containers
- Specify security requirements for container orchestration

Design a strategy for data and applications (15–20%)

Specify security requirements for applications

- Specify priorities for mitigating threats to applications

- Specify a security standard for onboarding a new application
- Specify a security strategy for applications and APIs

Design a strategy for securing data

- Specify priorities for mitigating threats to data
- Design a strategy to identify and protect sensitive data
- Specify an encryption standard for data at rest and in motion

Recommend security best practices and priorities (20–25%)

Recommend security best practices by using the Microsoft Cybersecurity Reference Architecture (MCRA) and Azure Security Benchmarks

- Recommend best practices for cybersecurity capabilities and controls
- Recommend best practices for protecting from insider and external attacks
- Recommend best practices for Zero Trust security
- Recommend best practices for Zero Trust Rapid Modernization Plan

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

- Recommend a DevSecOps process
- Recommend a methodology for asset protection
- Recommend strategies for managing and minimizing risk

Recommend a ransomware strategy by using Microsoft Security Best Practices

- Plan for ransomware protection and extortion-based attacks (i.e., backup and recovery, limit scope)
- Protect assets from ransomware attacks
- Recommend Microsoft ransomware best practices

Start Here Page 6

Study Resources

We recommend that you train and get hands-on experience before you take the exam. We offer self-study options and classroom training as well as links to documentation, community sites, and videos.

Study resources	Links to learning and documentation
Get trained	Choose from self-paced learning paths and modules or take an instructor led course
Find documentation	Microsoft security documentation Microsoft Cybersecurity Reference Architectures Microsoft Defender for Cloud documentation Zero Trust Guidance Center Governance, risk, and compliance in Azure
Ask a question	Microsoft Q&A | Microsoft Docs
Get community support	Security, compliance, and identity community hub
Follow Microsoft Learn	Microsoft Learn - Microsoft Tech Community
Find a video	Exam Readiness Zone Browse other Microsoft Learn shows

Service Mappings

Tuesday, December 13, 2022 12:31 PM

Azure AD	Cloud management. Houses tenants. B2C, B2B. Azure AD Connect. Supports SCIM.
PHS	Hash of a hash. Authentication occurs in the cloud. Password writeback keeps password changes synced Device writeback enabled conditional access in AD FS.
PTA	Authentication occurs on-premises. Requires authentication agent(s) on premises. Use when password policies, and sign-in hours are required.
Federation	Requires federated proxy server and federation servers. Required when using Smart cards.
Identity Protection	Leaked Credentials
Identity Governance aka Entra	PIM, Privileged Access Lifecycle. P2 license
Defender for Endpoint	DLP, Endpoint protection. Live response.
Defender for Cloud	Cloud Security Posture Management. Azure, AWS and GCP. Secure Score, recommendations, vulnerability assessments, file integrity monitoring.
Defender for Office 365	Phishing, training
Defender for IoT	Manage IoT resources. Asset discovery, threat detection and response. Agent or network sensor.
Defender for MS 365	Detection, prevention, investigation and response across email, endpoints, identities and applications.
Defender for Identity	Lateral movement, User Behavior and Activities. Used for on-prem, requires sensors.
Microsoft Purview	Govern, protect, manage data. Classification. Identify sensitive data i.e. credit card. Locates sensitive data. eDiscovery=Premium sku
Azure Sphere	IoT. Secure MCU, Linux OS.
Intune	Onboard devices can be used in conjunction with Configuration manager.
Configuration Manager	Onboard devices can be used in conjunction with Intune.
Azure AD App Proxy	Secure remotes access to on-prem web apps.
Azure Sentinel	SIEM/SOAR. Pulls from log analytics. Has connectors to various stores. Uses KQL for hunting, etc. Recommendations, workbooks,playbooks.
Azure ARC	Manage resources on-premises via Azure.
Azure Stack	Extends Azure services to other environments and remote locations.
Azure Lighthouse	Cross-tenant management.
Azure Bastion	Secure RDP to vms in Azure. Removes the requirement for public IP on the vms.
Azure Firewall	L3-L7 filtering and threat intelligence feeds. Known malicious Ips and FQDNs. Premium sku includes TLS filtering, IDPS, URL filtering. Traffic is denied by default.
Network Security Groups	Allows deny traffic to subnet and/or network interface.
Private Endpoint	Connect to an Azure resource directly from vnet. Uses a private IP. Services include Azure Storage, Cosmos DB, SQL DB. Requires a Private Link.
DDOS Protection	Infrastructure protection already enabled. Enhanced protection requires Azure DDoS Protection Plan $$
Azure Key Vault	Keys, secrets and certificates. Management plane = manage key vault, Data plane = manage data in the key vault.
Azure Automation Update Management	Patch management. Scheduling and managing updates.
Azure Blueprints	ARM Templates, Policies, Resource Groups, Role Assignments. Automated environment setup.
Desired State Configuration	Configuration of guest OS.
Azure Policy	Enforcing and auditing of the environment. IE location of resources, enforcing Tags, applying compliance requirements.
Virtual Machine	Secure using Azure Disk Encryption Linux=DmCrypt, Windows=Bitlocker. Backup vms. Use JIT. Protect using Defender for Cloud. Use File Integrity monitoring.
Storage	Use HTTPs over HTTP, enable Secure Transfer required. Limit access to SAS tokens. Regenerate keys (MS managed or customer managed). Uses Server Side Encryption (SSE) by default, can't be turned off.
JIT	Allow access via a port. Can time restrict and/or restrict to ip range.
Information Rights Management	Control what can be done to data. IE restrict copy, print, forward.

Other non-course Links

Monday, December 19, 2022 10:20 AM

Microsoft US OpenHack
Microsoft Virtual Training Days

MITRE ATT&CK®

Software Security Certification | CSSLP - Certified Secure Software Lifecycle Professional | (ISC)² (isc2.org)

Ninja Training

Thursday, November 17, 2022 2:11 PM

Defender Ninja Training
Microsoft Defender for Cloud Apps Ninja Training | June 2022 - Microsoft Community Hub
Microsoft Defender for Identity Ninja Training - Microsoft Community Hub
Become a Microsoft Defender for Endpoint Ninja - Microsoft Community Hub

Microsoft Cloud App Security
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/the-microsoft-cloud-app-security-mcas-ninja-training-march-2021/ba-p/1877343

Complete Sentinel Ninja Level 400 training
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/become-a-microsoft-sentinel-ninja-the-complete-level-400/ba-p/1246310

Additional Links

Tuesday, October 25, 2022 10:50 AM

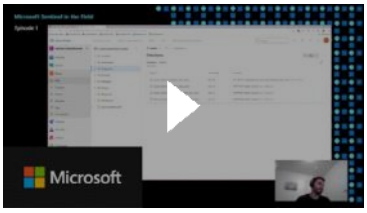
Microsoft Cybersecurity Reference Architectures
Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn

Sentinel documentation on GitHub. Fantastic Resource
azure-docs/articles/sentinel at main · MicrosoftDocs/azure-docs (github.com)

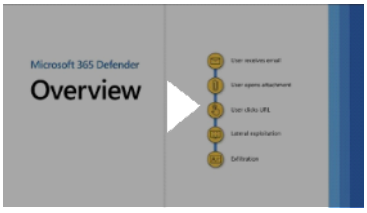
Log Analytics Demo
https://aka.ms/lademo

Microsoft Security YouTube Channel
Microsoft Security - YouTube

Microsoft Sentinel in the Field
Managing security content as code - Microsoft Sentinel in the Field #1



Microsoft 365 Defender Overview
Microsoft 365 Defender Playlist



Defender for MS 365 Playlist
Microsoft Defender for Office 365

https://github.com/Azure/Azure-Sentinel

SC-900
https://learn.microsoft.com/en-us/certifications/exams/sc-900

https://azure.microsoft.com/en-us/updates/?

Integrate Microsoft Sentinel and Microsoft Purview | Microsoft Learn

Purview
What is Microsoft Purview? | Microsoft Learn
Information Protection Administrator Microsoft Certified: Information Protection Administrator Associate - Certifications | Microsoft Learn

Logic Apps

Thursday, January 19, 2023 11:20 AM

Overview - Azure Logic Apps | Microsoft Learn

Training
Build automated workflows to integrate data and apps with Azure Logic Apps - Training | Microsoft Learn

Build an overall security strategy and architecture

Tuesday, December 13, 2022 12:23 PM

Zero Trust Guidance Center | Microsoft Learn
Zero Trust implementation guidance | Microsoft Learn
Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn

Identify the integration points in a security architecture by using Microsoft Cybersecurity Reference Architecture (MCRA)
Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn

• Translate business goals into security requirements

• Translate security requirements into technical capabilities, including security services, security products, and security processes
Security design principles - Microsoft Azure Well-Architected Framework | Microsoft Learn

• Design security for a resiliency strategy
Business resilience - Cloud Adoption Framework | Microsoft Learn
https://www.microsoft.com/en-us/videoplayer/embed/RWVECU?postJsllMsg=true
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/

• Integrate a hybrid or multi-tenant environment into a security strategy
https://learn.microsoft.com/en-us/azure/architecture/guide/multitenant/overview
Azure Arc overview - Azure Arc | Microsoft Learn
Map requests to tenants in a multitenant solution - Azure Architecture Center | Microsoft Learn
What is Azure Active Directory? - Microsoft Entra | Microsoft Learn

• Develop a technical governance strategy for security
Understand how effects work - Azure Policy | Microsoft Learn
Overview of Azure Policy - Azure Policy | Microsoft Learn
Understand how effects work - Azure Policy | Microsoft Learn

Design technical and governance strategies for traffic filtering and segmentation.
Best practices for network security - Microsoft Azure | Microsoft Learn

Benchmark tool Microsoft Cloud Adoption Framework Governance Benchmark Tool (cafbaseline.com)
Cloud Adoption Framework Microsoft Cloud Adoption Framework for Azure - Cloud Adoption Framework | Microsoft Learn
MCRA Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn
Well Architected Framework Microsoft Azure Well-Architected Framework - Azure Architecture Center | Microsoft Learn
NIST Getting Started | NIST
Microsoft Security Best Practices | Microsoft Learn
Cybersecurity Policy Framework | Microsoft Cybersecurity
National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) - Microsoft Compliance | Microsoft Learn

Zero Trust Architecture (nist.gov)
Microsoft and NIST collaborate on EO to drive Zero Trust adoption - Microsoft Security Blog

Introduction to regulatory compliance - Cloud Adoption Framework | Microsoft Learn

What is Secure Access Service Edge (SASE)? | Microsoft Security

Microsoft Defender for IoT documentation | Microsoft Learn

Azure compliance documentation | Microsoft Learn

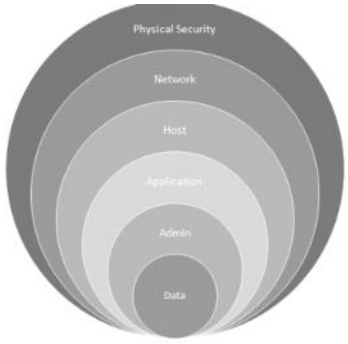


Fig. Defence in depth principles via multiple layered approach

Microsoft Economics https://azure.microsoft.com/en-us/solutions/cloud-economics/#overview

Compare Active Directory to Azure Active Directory - Microsoft Entra | Microsoft Learn
Azure application security groups overview | Microsoft Learn

Design a security operations strategy

Tuesday, December 13, 2022 12:24 PM

Design a logging and auditing strategy to support security operations
- Azure security logging and auditing | Microsoft Learn
- Overview of Log Analytics in Azure Monitor - Azure Monitor | Microsoft Learn
- Azure Monitor documentation - Azure Monitor | Microsoft Learn

Learning Kusto Query Language - A tool for performance test engineers (microsoft.com)
KQL quick reference | Microsoft Learn

Video https://www.microsoft.com/en-us/videoplayer/embed/RWVECU?postJsllMsg=true

• Develop security operations to support a hybrid or multi-cloud environment
- Introduction to hybrid and multicloud - Cloud Adoption Framework | Microsoft Learn

• Design a strategy for SIEM and SOAR
- What is Microsoft Sentinel? | Microsoft Learn
- MITRE ATT&CK®

• Evaluate security workflows
- Use playbooks with automation rules in Microsoft Sentinel | Microsoft Learn
- Overview - Azure Logic Apps | Microsoft Learn

• Evaluate a security operations strategy for incident management lifecycle

• Evaluate a security operations strategy for sharing technical threat intelligence

Design an identity security strategy

Tuesday, December 13, 2022 12:24 PM

Design a strategy for access to cloud resources	

Publisher verification overview - Microsoft Entra | Microsoft Learn
What is Azure Active Directory? - Microsoft Entra | Microsoft Learn
Azure Active Directory Pricing | Microsoft Security
Secure access practices for administrators in Azure AD - Microsoft Entra | Microsoft Learn

- Recommend an identity store (tenants, B2B, B2C, hybrid)
  - What is Azure Active Directory B2C? | Microsoft Learn
  - B2B collaboration overview - Azure AD - Microsoft Entra | Microsoft Learn
  - What is hybrid identity with Azure Active Directory? - Microsoft Entra | Microsoft Learn
  - Continuous access evaluation in Azure AD - Microsoft Entra | Microsoft Learn
  - SCIM synchronization with Azure Active Directory - Microsoft Entra | Microsoft Learn

- Recommend an authentication strategy
  - What is password hash synchronization with Azure AD? - Microsoft Entra | Microsoft Learn
  - Azure AD Connect: Pass-through Authentication - Microsoft Entra | Microsoft Learn
  - What is federation with Azure AD? - Microsoft Entra | Microsoft Learn

  - What is Azure AD Connect cloud sync? - Microsoft Entra | Microsoft Learn
  - What is Azure AD Connect and Connect Health. - Microsoft Entra | Microsoft Learn

- Recommend an authorization strategy
  - About security, authentication, authorization, and security policies - Azure DevOps | Microsoft Learn

- Design a strategy for conditional access
  - What is Conditional Access in Azure Active Directory? - Microsoft Entra | Microsoft Learn
  - What is risk? Azure AD Identity Protection - Microsoft Entra | Microsoft Learn
  - Azure: How to create a Conditional Access Policy - TechNet Articles - United States (English) - TechNet Wiki (microsoft.com)
  - Plan an Azure Active Directory Conditional Access deployment - Microsoft Entra | Microsoft Learn

- Design a strategy for role assignment and delegation
  - Assign Azure AD roles to users - Azure Active Directory - Microsoft Entra | Microsoft Learn
  - Delegation and roles in entitlement management - Azure AD - Microsoft Entra | Microsoft Learn

- Design security strategy for privileged role access to infrastructure including identity-based firewall rules and Privileged Identity Management (PIM) in Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
  - Least privileged roles by task - Azure Active Directory - Microsoft Entra | Microsoft Learn
  - What is Privileged Identity Management? - Azure AD - Microsoft Entra | Microsoft Learn

- Design security strategy for privileged activities including PAM, entitlement management, cloud tenant administration
  - What is Privileged Access Management (PAM) | Microsoft Security
  - Privileged access management - Microsoft Purview (compliance) | Microsoft Learn
  - What is entitlement management? - Microsoft Entra | Microsoft Learn
  - Create a new access package in entitlement management - Microsoft Entra | Microsoft Learn
  - Create an access review of Azure resource and Azure AD roles in PIM - Azure AD - Microsoft Entra | Microsoft Learn

  - Understanding just-in-time virtual machine access in Microsoft Defender for Cloud | Microsoft Learn

Azure Management Overview - Azure Governance | Microsoft Learn
Organize your resources with management groups - Azure Governance - Azure governance | Microsoft Learn
Overview of Azure Policy - Azure Policy | Microsoft Learn
Mark an app as publisher verified - Microsoft Entra | Microsoft Learn

Not a MS resource but a glossary of Security Terms PAM and Cybersecurity Glossary and Vocabulary (delinea.com)

Exploiting MFA Inconsistencies on Microsoft Services - Black Hills Information Security (blackhillsinfosec.com)

Azure AD and data residency - Microsoft Entra | Microsoft Learn

Securing identity with Zero Trust | Microsoft Learn

Secure hybrid access, protect legacy apps with Azure Active Directory - Microsoft Entra | Microsoft Learn

Microsoft identity platform access tokens - Microsoft Entra | Microsoft Learn

What's the difference between Azure roles and Azure AD roles? - Microsoft Community Hub

Azure Active Directory Identity Protection security overview - Microsoft Entra | Microsoft Learn

Managed identities for Azure resources frequently asked questions - Azure AD" - Microsoft Entra | Microsoft Learn

Overview of federated identity credentials in Azure Active Directory - Microsoft Graph v1.0 | Microsoft Learn

Microsoft Entra - Secure Identities and Access | Microsoft Security

Design a regulatory compliance strategy

Tuesday, December 13, 2022 12:24 PM

Interpret compliance requirements and translate into specific technical capabilities (new or existing)

- The Five Disciplines of Cloud Governance - Cloud Adoption Framework | Microsoft Learn

https://www.techtarget.com/searchitoperations/tip/Compare-runbooks-vs-playbooks-for-IT-process-documentation

Evaluate infrastructure compliance by using Microsoft Defender for Cloud

- What is Microsoft Defender for Cloud? - Microsoft Defender for Cloud | Microsoft Learn
- Workbooks gallery in Microsoft Defender for Cloud | Microsoft Learn
- Workbooks gallery in Microsoft Defender for Cloud | Microsoft Learn

• Interpret compliance scores and recommend actions to resolve issues or improve security

- Compliance score calculation - Microsoft Purview (compliance) | Microsoft Learn
- Tutorial: Regulatory compliance checks - Microsoft Defender for Cloud | Microsoft Learn

• Design implementation of Azure Policy

- Overview of Azure Policy - Azure Policy | Microsoft Learn
- Regulatory Compliance in initiative definitions - Azure Policy | Microsoft Learn
- https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects

• Design for data residency requirements

- Azure Products by Region | Microsoft Azure

Microsoft announces the phased rollout of the EU Data Boundary for the Microsoft Cloud begins January 1, 2023 - EU Policy Blog

Schrems II a summary - all you need to know - GDPR Summary

• Translate privacy requirements into requirements for security solutions

- Microsoft Purview compliance documentation - Microsoft Purview (compliance) | Microsoft Learn
- Microsoft Purview compliance portal - Microsoft Purview (compliance) | Microsoft Learn
- Overview of Azure Blueprints - Azure Blueprints | Microsoft Learn
- Message encryption version comparison - Microsoft Purview (compliance) | Microsoft Learn

Evaluate security posture and recommend technical strategies to manage risk

Tuesday, December 13, 2022 12:25 PM

Rapidly modernize your security infrastructure | Microsoft Learn
Zero Trust Rapid Modernization Plan | Microsoft Learn

Evaluate security posture by using Azure Security Benchmark
- Overview of the Microsoft cloud security benchmark | Microsoft Learn
- Microsoft cloud security benchmark introduction | Microsoft Learn

• Evaluate security posture by using Microsoft Defender for Cloud
- MITRE ATT&CK®
- Investigate threat detection alerts - Microsoft Defender for Cloud Apps | Microsoft Learn
- Security Posture Management Improvements | Microsoft Learn (video)
- Security posture for Microsoft Defender for Cloud | Microsoft Learn

• Evaluate security posture by using Secure Scores
- Tracking your secure score in Microsoft Defender for Cloud | Microsoft Learn
- Workflow automation in Microsoft Defender for Cloud | Microsoft Learn

• Evaluate security posture of cloud workloads

• Design security for an Azure Landing Zone
- What is an Azure landing zone? - Cloud Adoption Framework | Microsoft Learn
- Azure landing zone design principles - Cloud Adoption Framework | Microsoft Learn
- Resource organization design area overview - Cloud Adoption Framework | Microsoft Learn

- Plan for inbound and outbound internet connectivity - Cloud Adoption Framework | Microsoft Learn
- Plan for landing zone network segmentation - Cloud Adoption Framework | Microsoft Learn
- Define network encryption requirements - Cloud Adoption Framework | Microsoft Learn
- Plan for traffic inspection - Cloud Adoption Framework | Microsoft Learn
- Security design in Azure - Cloud Adoption Framework | Microsoft Learn
- What is an Azure landing zone? - Cloud Adoption Framework | Microsoft Learn - Accelerator

• Interpret technical threat intelligence and recommend risk mitigations
- https://learn.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports

• Recommend security capabilities or controls to mitigate identified risks

The Five Disciplines of Cloud Governance - Cloud Adoption Framework | Microsoft Learn
Azure Virtual WAN Overview | Microsoft Learn

Video on Security Posture Management:
https://docs.microsoft.com/en-us/shows/mdc-in-the-field/security-posture-management

Landing zone video
https://www.microsoft.com/en-us/videoplayer/embed/RE4xdvm?postJsllMsg=true

Design a strategy for securing server and client endpoints

Tuesday, December 13, 2022 12:25 PM

Specify security baselines for server and client endpoints
- Learn about Windows security baselines you can deploy with Microsoft Intune | Microsoft Learn
- Overview of the Microsoft cloud security benchmark | Microsoft Learn

• Specify security requirements for servers, including multiple platforms and operating systems
- Security baselines guide | Microsoft Learn
- Microsoft Security Compliance Toolkit 1.0 Guide | Microsoft Learn
- Secure Boot and Trusted Boot | Microsoft Learn
- Zero Trust and Windows device health | Microsoft Learn
- Understand Windows Defender Application Control (WDAC) policy rules and file rules (Windows) | Microsoft Learn
- Windows LAPS overview | Microsoft Learn
- Key concepts in Windows LAPS | Microsoft Learn

• Specify security requirements for mobile devices and clients, including endpoint protection, hardening, and configuration
- Device compliance policies in Microsoft Intune | Microsoft Learn
- Windows Server Security documentation | Microsoft Learn

• Specify requirements to secure Active Directory Domain Services
- Secure Azure AD Domain Services | Microsoft Learn
- Windows Security overview - Windows Server | Microsoft Learn
- What is Microsoft Defender for Identity? - Microsoft Defender for Identity | Microsoft Learn
- Microsoft Defender for Identity security alert guide - Microsoft Defender for Identity | Microsoft Learn

• Design a strategy to manage secrets, keys, and certificates
- What is Azure Key Vault? | Microsoft Learn
- Best practices for using Azure Key Vault | Microsoft Learn
- Azure Key Vault security overview | Microsoft Learn
- Azure encryption overview | Microsoft Learn
- Overview of Key Management in Azure | Microsoft Learn
- Azure Managed HSM Overview - Azure Managed HSM | Microsoft Learn
- Frequently asked questions - Azure Dedicated HSM | Microsoft Learn

• Design a strategy for secure remote access
- About Azure VPN Gateway | Microsoft Learn
- Azure ExpressRoute Overview: Connect over a private connection | Microsoft Learn
- About Azure VPN Gateway | Microsoft Learn
- Azure Virtual Network - Concepts and best practices | Microsoft Learn

• Design a strategy for securing privileged access
- Data security and encryption best practices - Microsoft Azure | Microsoft Learn
- Investigate entities on devices using live response in Microsoft Defender for Endpoint | Microsoft Learn
- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

Not MS products for visibility into Azure
Welcome to Tenable for Microsoft Azure
Wiz | Secure Everything You Build and Run in the Cloud

Microsoft Cloud Adoption Framework video
https://www.microsoft.com/en-us/videoplayer/embed/RWVBXs?postJsllMsg=true

Understand the basic and extended security features of Microsoft Defender for Cloud | Microsoft Learn

How to manage local administrators on Azure AD joined devices - Microsoft Entra | Microsoft Learn

Microsoft Identity Manager | Microsoft Learn

Understanding just-in-time virtual machine access in Microsoft Defender for Cloud | Microsoft Learn

DevSecOps controls - Cloud Adoption Framework | Microsoft Learn

Security considerations for container instances - Azure Container Instances | Microsoft Learn

Learn how to secure access to data in Azure Cosmos DB | Microsoft Learn

Cloud security functions - Cloud Adoption Framework | Microsoft Learn

https://www.microsoft.com/en-us/videoplayer/embed/RWVBXs?postJsllMsg=true

Password policy recommendations - Microsoft 365 admin | Microsoft Learn

Windows LAPS overview | Microsoft Learn

Awesome link - Security best practices and patterns - Microsoft Azure | Microsoft Learn

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

Tuesday, December 13, 2022 12:25 PM

Security best practices and patterns - Microsoft Azure | Microsoft Learn

Specify security baselines for SaaS, PaaS, and IaaS services

Overview of the Microsoft cloud security benchmark | Microsoft Learn

• Specify security requirements for IoT workloads

Security recommendations for Azure IoT | Microsoft Learn
Internet of Things (IoT) security best practices | Microsoft Learn

• Specify security requirements for data workloads, including SQL Server, Azure SQL, Azure Synapse, and Azure Cosmos DB

Playbook for addressing common security requirements - Azure SQL Database & Azure SQL Managed Instance | Microsoft Learn
Azure Policy Regulatory Compliance controls for Azure SQL Database - Azure SQL Database | Microsoft Learn
Azure security baseline for Azure SQL Database | Microsoft Learn
Transparent data encryption - Azure SQL Database & SQL Managed Instance & Azure Synapse Analytics | Microsoft Learn
Always Encrypted documentation - Azure SQL | Microsoft Learn
Business Critical service tier - Azure SQL Database & Azure SQL Managed Instance | Microsoft Learn
Database security overview - Azure Cosmos DB | Microsoft Learn
Learn how to secure access to data in Azure Cosmos DB | Microsoft Learn
Encryption at rest in Azure Cosmos DB | Microsoft Learn
Azure security baseline for Synapse Analytics Workspace | Microsoft Learn
Azure Synapse Analytics security white paper - Azure Synapse Analytics | Microsoft Learn

• Specify security requirements for web workloads, including Azure App Service

Security - Azure App Service | Microsoft Learn

• Specify security requirements for storage workloads, including Azure Storage

Azure security baseline for Storage | Microsoft Learn
Security recommendations for Blob storage - Azure Storage | Microsoft Learn
Azure Storage encryption for data at rest | Microsoft Learn
Use private endpoints - Azure Storage | Microsoft Learn

• Specify security requirements for containers

Security considerations for container instances - Azure Container Instances | Microsoft Learn
Azure security baseline for Container Instances | Microsoft Learn
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-vulnerability-assessment-azure
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-architecture?tabs=defender-for-container-arch-aks

Video https://learn.microsoft.com/_themes/docs.theme/master/en-us/_themes/global/video-embed.html?id=b8624912-ef9e-4fc6-8c0c-ea65e86d9128

• Specify security requirements for container orchestration

Concepts - Security in Azure Kubernetes Services (AKS) - Azure Kubernetes Service | Microsoft Learn
Azure security baseline for Azure Kubernetes Service | Microsoft Learn
Learn Azure Policy for Kubernetes - Azure Policy | Microsoft Learn
Use Azure Policy to secure your cluster - Azure Kubernetes Service | Microsoft Learn

Password policy recommendations - Microsoft 365 admin | Microsoft Learn
Security baselines for Azure overview | Microsoft Learn

Azure Virtual Network - Concepts and best practices | Microsoft Learn

About GitHub Advanced Security - GitHub Docs

Azure Security product name changes – Microsoft Ignite November 2021

https://learn.microsoft.com/en-us/azure/external-attack-surface-management/

Create custom Azure security policies in Microsoft Defender for Cloud | Microsoft Learn

Specify security requirements for applications

Tuesday, December 13, 2022 12:26 PM

Specify priorities for mitigating threats to applications
- Securing PaaS web & mobile applications - Azure App Service | Microsoft Learn

Specify a security standard for onboarding a new application
- Application security in Azure | Microsoft Learn

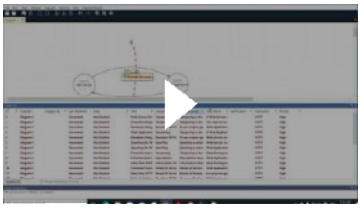
• Specify a security strategy for applications and APIs
- Protect APIs with Azure Application Gateway and Azure API Management - Azure Reference Architectures | Microsoft Learn
- Apps & service principals in Azure AD - Microsoft Entra | Microsoft Learn
- What is Azure App Configuration? | Microsoft Learn

Additional Information on App and API Security

https://docs.microsoft.com/en-us/devops/plan/what-is-agile-development
https://docs.microsoft.com/en-us/devops/plan/what-is-scrum
https://docs.microsoft.com/en-us/devops/plan/what-is-kanban
Security in DevOps (DevSecOps) - Azure DevOps | Microsoft Learn
https://docs.microsoft.com/en-us/azure/architecture/best-practices/api-design

About GitHub Advanced Security - GitHub Docs
Scan container images using GitHub Actions - Azure Container Registry | Microsoft Learn
Introduction to Azure Web Application Firewall | Microsoft Learn
Microsoft Threat Modeling Tool overview - Azure | Microsoft Learn

Quick video on using the Threat Modeling Tool 2. Microsoft Threat Modeling Practical session | UCSC, STRIDE+MS_TMT



Design a strategy for securing data

Tuesday, December 13, 2022 12:26 PM

Specify priorities for mitigating threats to data

Azure threat protection | Microsoft Learn

• Design a strategy to identify and protect sensitive data

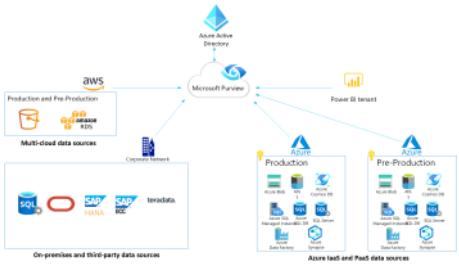
Data security and encryption best practices - Microsoft Azure | Microsoft Learn
Microsoft Purview Information Protection - Microsoft Purview (compliance) | Microsoft Learn
https://learn.microsoft.com/en-us/azure/information-protection/what-is-information-protection
Get started with exact data match based sensitive information types - Microsoft Purview (compliance) | Microsoft Learn

https://learn.microsoft.com/en-us/azure/purview/concept-best-practices-accounts

• Specify an encryption standard for data at rest and in motion

Data encryption in Azure - Microsoft Azure Well-Architected Framework | Microsoft Learn
https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption-overview
Server-side encryption of Azure managed disks - Azure Virtual Machines | Microsoft Learn

Always Encrypted - SQL Server | Microsoft Learn
Azure Key Vault soft-delete | Microsoft Learn



https://learn.microsoft.com/en-us/azure/dedicated-hsm/overview

https://learn.microsoft.com/en-us/azure/purview/register-scan-azure-multiple-sources

Azure ExpressRoute Overview: Connect over a private connection | Microsoft Learn

(MCRA) and Azure Security Benchmarks

Tuesday, December 13, 2022 12:26 PM

Recommend best practices for cybersecurity capabilities and controls

Azure security best practices - Cloud Adoption Framework | Microsoft Learn
Define a security strategy - Cloud Adoption Framework | Microsoft Learn
https://aka.ms/benchmarkdocs

- Recommend best practices for protecting from insider and external attacks

Insider Threat Monitoring for Zero Trust with Microsoft Azure (5 of 6) - Azure Government
What is Microsoft Defender for Identity? - Microsoft Defender for Identity | Microsoft Learn

- Recommend best practices for Zero Trust security

Zero Trust security in Azure | Microsoft Learn

- Recommend best practices for Zero Trust Rapid Modernization Plan

Zero Trust Rapid Modernization Plan | Microsoft Learn

Cloud Adoption Framework (CAF)

Tuesday, December 13, 2022 12:27 PM

Recommend a DevSecOps process

Development security strategy - Cloud Adoption Framework | Microsoft Learn

• Recommend a methodology for asset protection

Align assets to prioritized workloads - Cloud Adoption Framework | Microsoft Learn

• Recommend strategies for managing and minimizing risk

Ransomware strategy by using Microsoft Security Best Practices

Tuesday, December 13, 2022 12:27 PM

Improve your security defenses for ransomware attacks with Azure Firewall | Azure Blog and Updates | Microsoft Azure

Ransomware protection in Azure | Microsoft Learn

Plan for ransomware protection and extortion-based attacks (i.e., backup and recovery, limit scope)

- Prepare for a ransomware attack | Microsoft Learn
- Azure backup and restore plan to protect against ransomware | Microsoft Learn

• Protect assets from ransomware attacks

- Azure features & resources that help you protect, detect, and respond | Microsoft Learn

• Recommend Microsoft ransomware best practices

Malware and ransomware protection in Microsoft 365 - Microsoft Service Assurance | Microsoft Learn

https://learn.microsoft.com/en-us/azure/active-directory/develop/active-directory-configurable-token-lifetimes

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime