Read me first

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.

Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries - The Official Microsoft Blog

Introducing a new resource for all role-based Microsoft Certification exams - Microsoft Community Hub

Microsoft Certified: Cybersecurity Architect Expert - Certifications | Microsoft Learn

Study Guide As of Aug 25, 2023

Thursday, July 20, 2023 5:16 PM

- Design solutions that align with security best practices and priorities (20–25%)
- Design security operations, identity, and compliance capabilities (30–35%)
- Design security solutions for infrastructure (20–25%)
- Design security solutions for applications and data (20–25%)

From <https://learn.microsoft.com/en-us/certifications/resources/study-guides/SC-100#skills-measured-as-of-august-25-2023>

Design solutions that align with security best practices and priorities (20–25%)

Design a resiliency strategy for ransomware and other attacks based on Microsoft Security Best Practices

- Design a security strategy to support business resiliency goals, including identifying and prioritizing threats to business-critical assets
- Design solutions that align with Microsoft ransomware best practices, including backup, restore, and privileged access
- Design configurations for secure backup and restore by using Azure Backup for hybrid and multicloud environments
- Design solutions for security updates

Design solutions that align with the Microsoft Cybersecurity Reference Architectures (MCRA) and Microsoft cloud security benchmark (MCSB)

- Design solutions that align with best practices for cybersecurity capabilities and controls
- Design solutions that align with best practices for protecting against insider and external attacks
- Design solutions that align with best practices for Zero Trust security, including the Zero Trust Rapid Modernization Plan (RaMP)

Design solutions that align with the Microsoft Cloud Adoption Framework for Azure and the Microsoft Azure Well-Architected Framework

- Design a new or evaluate an existing strategy for security and governance based on the Microsoft Cloud Adoption Framework (CAF) and the Microsoft Azure Well-Architected Framework
- Recommend solutions for security and governance based on the Microsoft Cloud Adoption Framework for Azure and the Microsoft Azure Well-Architected Framework
- Design solutions for implementing and governing security by using Azure landing zones
- Design a DevSecOps process

Design security operations, identity, and compliance capabilities (30–35%)

Design solutions for security operations

- Develop security operations capabilities to support a hybrid or multicloud environment
- Design a solution for centralized logging and auditing
- Design a solution for security information and event management (SIEM), including Microsoft Sentinel
- Design a solution for detection and response that includes extended detection and response (XDR)
- Design a solution for security orchestration automated response (SOAR), including Microsoft Sentinel and Microsoft Defender
- Design and evaluate security workflows, including incident response, threat hunting, incident management, and threat intelligence
- Design and evaluate threat detection coverage by using MITRE ATT&CK

Design solutions for identity and access management

- Design a solution for access to software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), hybrid/on-premises, and multicloud resources, including identity, networking, and application controls
- Design a solution for Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra, including hybrid and multicloud environments
- Design a solution for external identities, including B2B, B2C, and Decentralized Identity
- Design a modern authentication and authorization strategy, including Conditional Access, continuous access evaluation, threat intelligence integration, and risk scoring
- Validate the alignment of Conditional Access policies with a Zero Trust strategy
- Specify requirements to secure Active Directory Domain Services (AD DS)
- Design a solution to manage secrets, keys, and certificates

Design solutions for securing privileged access

- Design a solution for assigning and delegating privileged roles by using the enterprise access model

Learn https://aka.ms/MOC_SC-100T00
GH Case Studies https://microsoftlearning.github.io/SC-100-Microsoft-Cybersecurity-Architect/

Microsoft Security Co-pilot https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-security-copilot
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/

Azure Architecture Center - Azure Architecture Center | Microsoft Learn

- Design an identity governance solution, including Privileged Identity Management (PIM), Privileged Access Management (PAM), entitlement management, and access reviews
- Design a solution for securing the administration of cloud tenants, including SaaS and multicloud infrastructure and platforms
- Design a solution for cloud infrastructure entitlement management that includes Microsoft Entra Permissions Management
- Design a solution for Privileged Access Workstation (PAW) and bastion services

Design solutions for regulatory compliance

- Translate compliance requirements into a security solution
- Design a solution to address compliance requirements by using Microsoft Purview risk and compliance solutions
- Design a solution to address privacy requirements, including Microsoft Priva
- Design Azure Policy solutions to address security and compliance requirements
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud

Design security solutions for infrastructure (20–25%)

Design solutions for security posture management in hybrid and multicloud environments

- Evaluate security posture by using MCSB
- Evaluate security posture by using Defender for Cloud
- Evaluate security posture by using Microsoft Secure Score
- Design integrated security posture management and workload protection solutions in hybrid and multicloud environments, including Defender for Cloud
- Design cloud workload protection solutions that use Defender for Cloud, such as Microsoft Defender for Servers, Microsoft Defender for App Service, and Microsoft Defender for SQL
- Design a solution for integrating hybrid and multicloud environments by using Azure Arc
- Design a solution for Microsoft Defender External Attack Surface Management (Defender EASM)

Design solutions for securing 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 security requirements for IoT devices and embedded systems
- Design a solution for securing operational technology (OT) and industrial control systems (ICS) by using Microsoft Defender for IoT
- Specify security baselines for server and client endpoints
- Design a solution for secure remote access

Specify requirements 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 web workloads, including Azure App Service
- Specify security requirements for containers
- Specify security requirements for container orchestration

Design security solutions for applications and data (20–25%)

Design solutions for securing Microsoft 365

- Evaluate security posture for productivity and collaboration workloads by using metrics, including Secure Score and Defender for Cloud secure score
- Design a Microsoft 365 Defender solution
- Design secure configurations and operational practices for Microsoft 365 workloads and data

Design solutions for securing applications

- Evaluate the security posture of existing application portfolios
- Evaluate threats to business-critical applications by using threat modeling
- Design and implement a full lifecycle strategy for application security
- Design and implement standards and practices for securing the application development process
- Map technologies to application security requirements
- Design a solution for workload identity to authenticate and access Azure cloud resources
- Design a solution for API management and security
- Design a solution for secure access to applications, including Azure Web Application Firewall (WAF) and Azure Front Door

Design solutions for securing an organization's data

- Design a solution for data discovery and classification by using Microsoft Purview data governance solutions
- Specify priorities for mitigating threats to data
- Design a solution for protection of data at rest, data in motion, and data in use
- Design a security solution for data in Azure workloads, including Azure SQL, Azure Synapse Analytics, and Azure Cosmos DB
- Design a security solution for data in Azure Storage
- Design a security solution that includes Microsoft Defender for Storage and Defender for SQL

From <https://learn.microsoft.com/en-us/certifications/resources/study-guides/SC-100#skills-measured-as-of-august-25-2023>

Old SC-100_StudyGuide_ENU_FY23Q1.1

Tuesday, December 13, 2022 12:23 PM

Learn https://aka.ms/MOC_SC-100T00
GH Case Studies https://microsoftlearning.github.io/SC-100-Microsoft-Cybersecurity-Architect/

SC-100_StudyGuide_ENU_FY23Q1.1

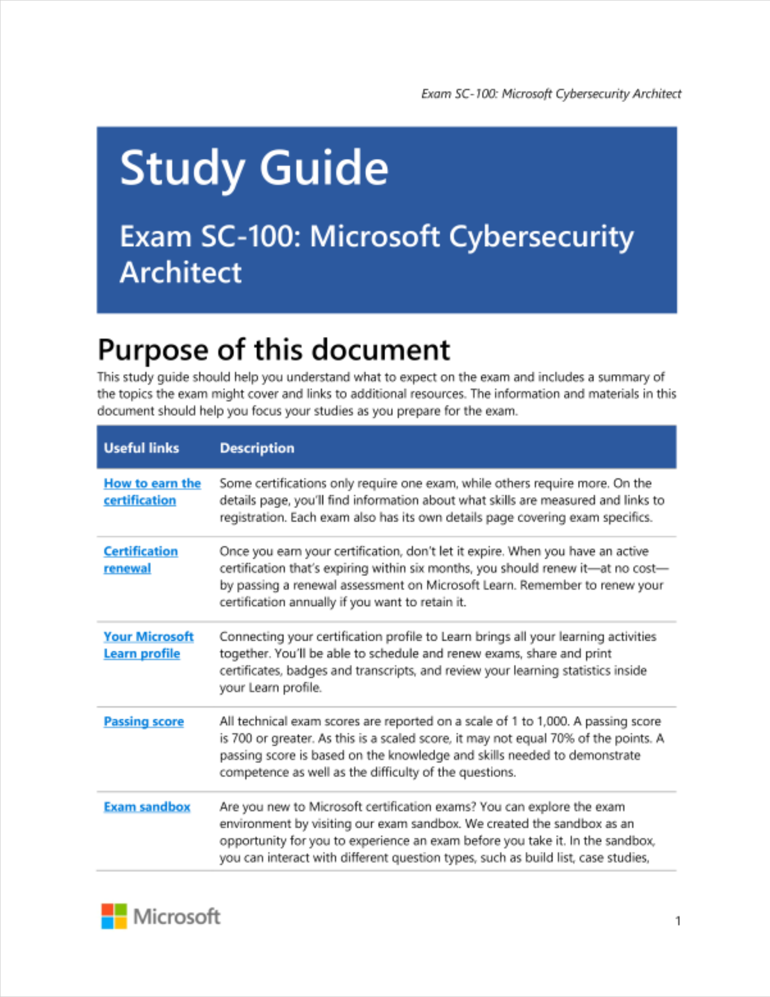
Microsoft Security Co-pilot https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-security-copilot

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



Study Guide

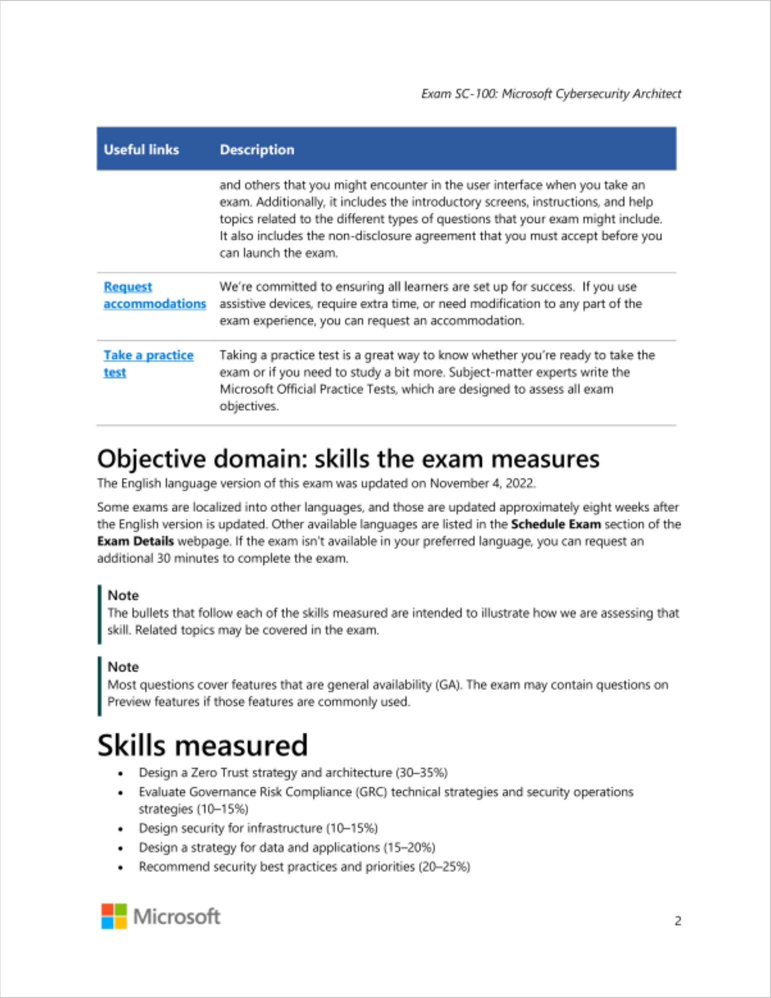
Exam SC-100: Microsoft Cybersecurity Architect

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



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.

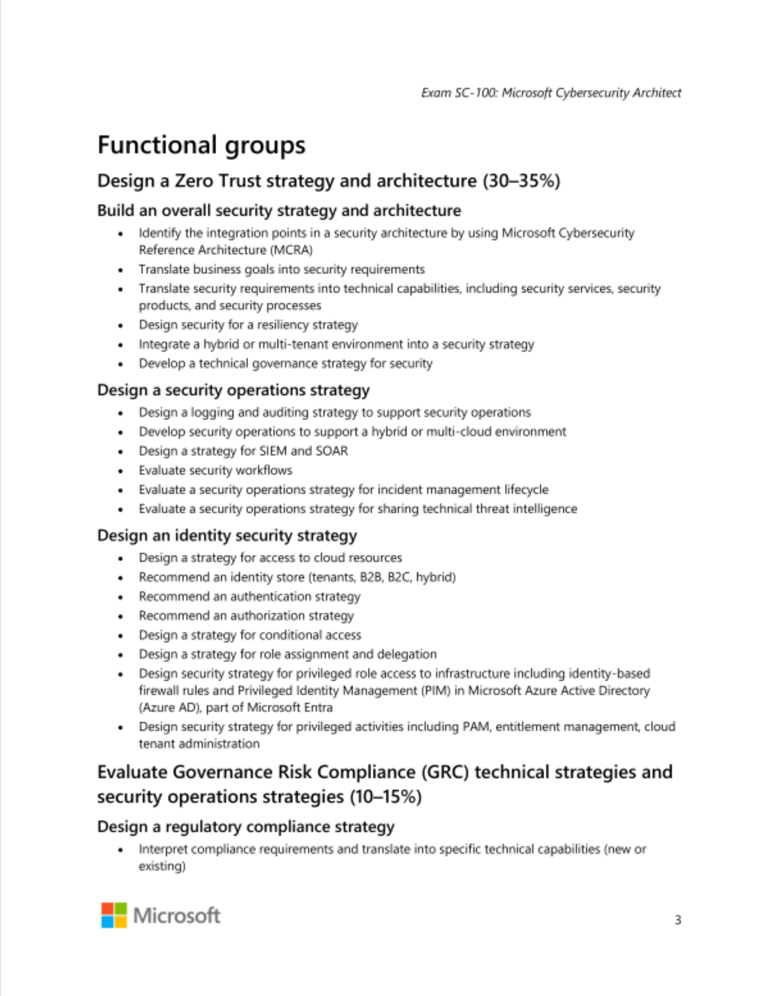
Some exams are localized into other languages, and those are updated approximately eight weeks after the English version is updated. Other available languages are listed in the **Schedule Exam** section of the **Exam Details** webpage. If the exam isn't available in your preferred language, you can request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

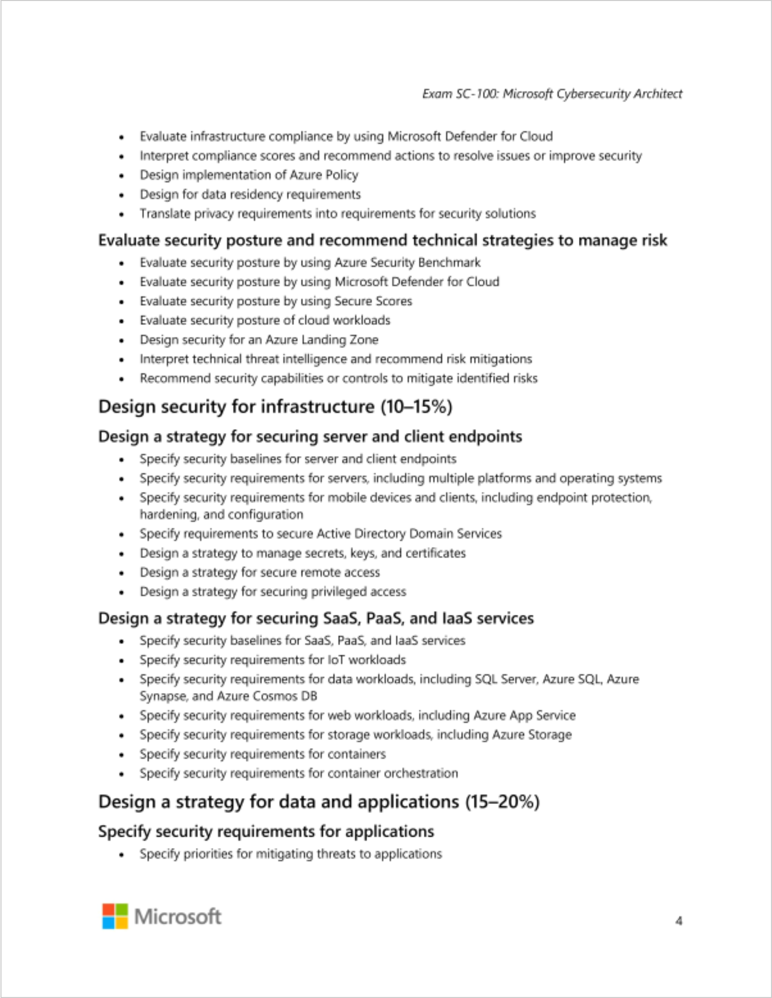
Design an identity security strategy

- 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

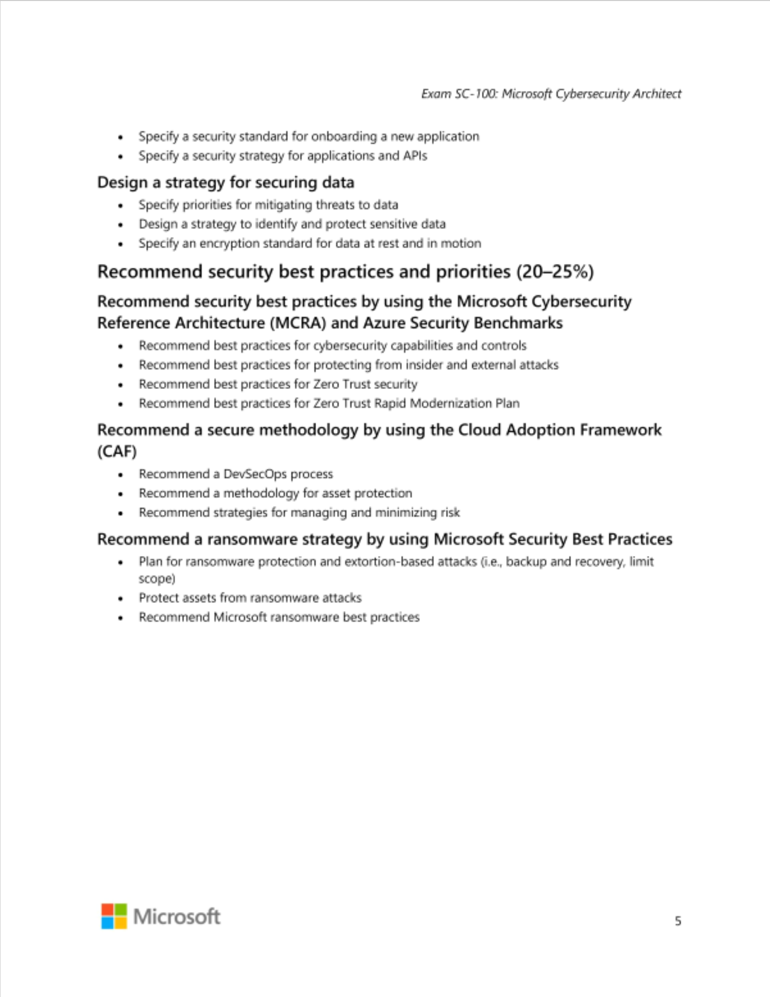
Design a strategy for securing SaaS, PaaS, and IaaS services

- 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

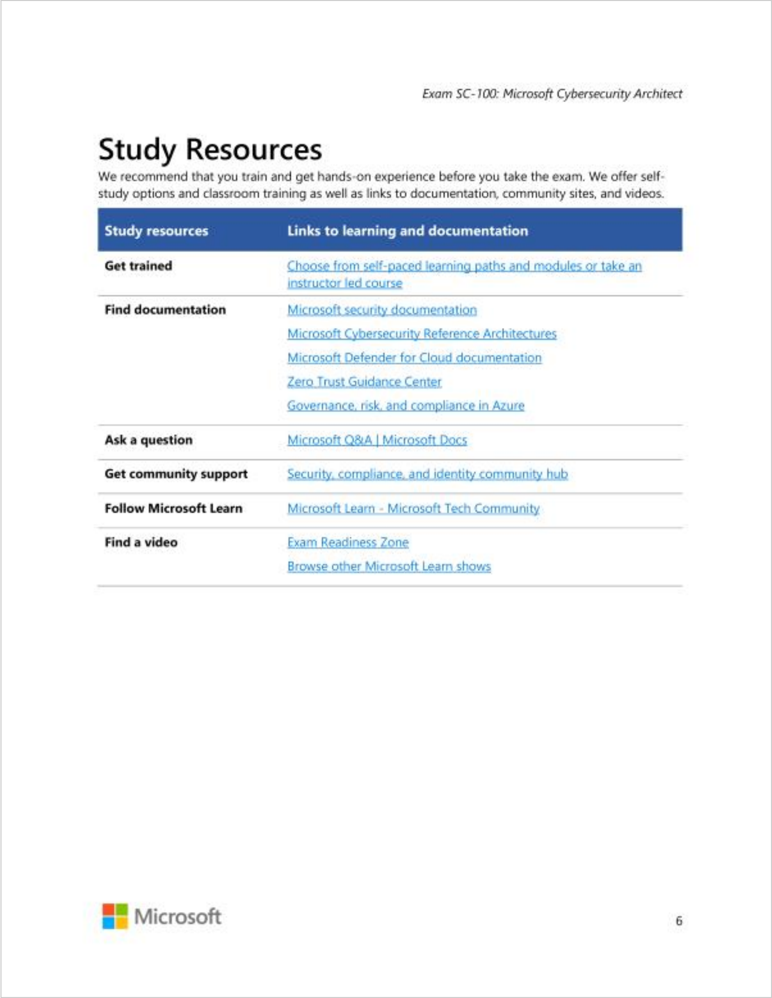
- Recommend best practices for cybersecurity capabilities and controls
- Recommend best practices for protecting from insider and external attacks
- Recommend best practices for Zero Trust security
- Recommend best practices for Zero Trust Rapid Modernization Plan

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



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

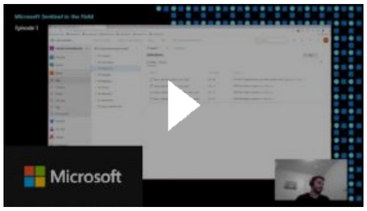
Microsoft Cybersecurity Reference Architectures
Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn

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

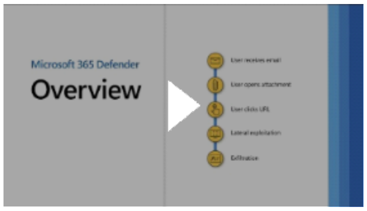
Log Analytics Demo
https://aka.ms/lademo

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

Microsoft Certified: Cybersecurity Architect Expert - Certifications | Microsoft Learn

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

Sentinel training labs
Learning with the Microsoft Sentinel Training Lab - Microsoft Community Hub

Zero Trust Illustrations for IT architects and implementers
Zero Trust illustrations for IT architects and implementers | Microsoft Learn

Organize your resources with management groups - Azure Governance - Azure governance | Microsoft Learn

Data retention and archive in Azure Monitor Logs - Azure Monitor | Microsoft Learn

OSSEM (ossemproject.com)
Normalization and the Advanced Security Information Model (ASIM) | 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

Design a resiliency strategy for ransomware and other attacks based on Microsoft Security Best Practices

Thursday, July 20, 2023 5:18 PM

- Design a security strategy to support business resiliency goals, including identifying and prioritizing threats to business-critical assets
  - Ransomware protection in Azure | Microsoft Learn
  - Improve your security defenses for ransomware attacks with Azure Firewall | Azure Blog | Microsoft Azure
  - Recommend a ransomware strategy by using Microsoft Security Best Practices - Training | Microsoft Learn
  - Business resilience - Cloud Adoption Framework | Microsoft Learn

- Design solutions that align with Microsoft ransomware best practices, including backup, restore, and privileged access

  Prepare for a ransomware attack | Microsoft Learn
  Azure backup and restore plan to protect against ransomware | Microsoft Learn
  Azure features & resources that help you protect, detect, and respond | Microsoft Learn
  https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization

- Design configurations for secure backup and restore by using Azure Backup for hybrid and multicloud environments

  What is Azure Backup? - Azure Backup | Microsoft Learn

- Design solutions for security updates
  - Manage updates and patches for your VMs in Azure Automation | Microsoft Learn

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

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

https://azure.microsoft.com/en-us/products/chaos-studio
https://en.m.wikipedia.org/wiki/Chaos_engineering

https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/overview

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/i-m-being-attacked-now-what/ba-p/3481937

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/security-operations-introduction

Design solutions that align with the Microsoft Cybersecurity Reference Architectures (MCRA) and Microsoft cloud security benchmark (MCSB)

Thursday, July 20, 2023 5:18 PM

- Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn
- Overview of the Microsoft cloud security benchmark | Microsoft Learn
-

- Design solutions that align with 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
Video: microsoft.com/en-us/videoplayer/embed/RWVECU?postJsllMsg=true

- Design solutions that align with best practices for protecting against insider and external attacks
  - Securing privileged access overview | Microsoft Learn
-
- Design solutions that align with best practices for Zero Trust security, including the Zero Trust Rapid Modernization Plan (RaMP)

  Zero Trust security in Azure | Microsoft Learn
  Zero Trust Rapid Modernization Plan | Microsoft Learn
  Conditional Access for Zero Trust - Azure Architecture Center | Microsoft Learn

Define a security strategy - Cloud Adoption Framework | Microsoft Learn

Overview of the security pillar - Microsoft Azure Well-Architected Framework | Microsoft Learn

Security in the Microsoft Cloud Adoption Framework for Azure - Cloud Adoption Framework | Microsoft Learn

Microsoft Entra Expands into Security Service Edge with Two New Offerings - Microsoft Community Hub

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

Design solutions that align with the Microsoft Cloud Adoption Framework for Azure and the Microsoft Azure Well-Architected Framework

Thursday, July 20, 2023 5:19 PM

- Design a new or evaluate an existing strategy for security and governance based on the Microsoft Cloud Adoption Framework (CAF) and the Microsoft Azure Well-Architected Framework
    - Microsoft Cloud Adoption Framework for Azure documentation - Cloud Adoption Framework | Microsoft Learn
    - Microsoft Azure Well-Architected Framework - Azure Well-Architected Framework | Microsoft Learn

- Recommend solutions for security and governance based on the Microsoft Cloud Adoption Framework for Azure and the Microsoft Azure Well-Architected Framework
    - Security in the Microsoft Cloud Adoption Framework for Azure - Cloud Adoption Framework | Microsoft Learn
    - Governance in the Microsoft Cloud Adoption Framework for Azure - Cloud Adoption Framework | Microsoft Learn
    - Security documentation - Microsoft Azure Well-Architected Framework | Microsoft Learn

- Design solutions for implementing and governing security by using Azure landing zones
    - What is an Azure landing zone? - Cloud Adoption Framework | Microsoft Learn
    - Security in the Microsoft Cloud Adoption Framework for Azure - Cloud Adoption Framework | Microsoft Learn
      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
    - Landing Zone Video microsoft.com/en-us/videoplayer/embed/RE4xdvm?postJslIMsg=true
    -

- Design a DevSecOps process
    - DevSecOps controls - Cloud Adoption Framework | Microsoft Learn

Compare Microsoft endpoint security plans | Microsoft Learn

Responsibility assignment matrix - Wikipedia

Microsoft Defender products and services | Microsoft Learn

DevSecOps Implementation Process and Road Map – Security at Every Step - DevOps.com

Azure Landing Zones | Architectural Blueprint, Tooling & Best Practices

Azure Landing Zones Overview

Design solutions for security operations

Thursday, July 20, 2023 5:19 PM

- Develop security operations capabilities to support a hybrid or multicloud environment
  Introduction to hybrid and multicloud - Cloud Adoption Framework | Microsoft Learn
  What is Microsoft Sentinel? | Microsoft Learn

- Design a solution for centralized logging and auditing
  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

- Design a solution for security information and event management (SIEM), including Microsoft Sentinel
  What is Microsoft Sentinel? | Microsoft Learn
  MITRE ATT&CK®

- Design a solution for detection and response that includes extended detection and response (XDR)

- Design a solution for security orchestration automated response (SOAR), including Microsoft Sentinel and Microsoft Defender
  Use playbooks with automation rules in Microsoft Sentinel | Microsoft Learn
  Overview - Azure Logic Apps | Microsoft Learn
    -
- Design and evaluate security workflows, including incident response, threat hunting, incident management, and threat intelligence
    -

- Design and evaluate threat detection coverage by using MITRE ATT&CK
    - MITRE ATT&CK®
    - View MITRE coverage for your organization from Microsoft Sentinel | 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?postJslIMsg=true

Workspace architecture best practices for Microsoft Sentinel | Microsoft Learn

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview

Cybercrime Module 4 Key Issues: Standards and best practices for digital forensics (unodc.org)

(PDF) Digital Forensic Analysis of Cybercrimes: Best Practices and Methodologies (researchgate.net)

Microsoft Sentinel – continuous threat monitoring for GitHub - Microsoft Community Hub

Root cause analysis (preview) - Power Automate | Microsoft Learn

https://www.microsoft.com/en-us/security/blog/2023/07/19/expanding-cloud-logging-to-give-customers-deeper-security-visibility/

https://learn.microsoft.com/en-us/azure/sentinel/automation

https://learn.microsoft.com/en-us/azure/sentinel/design-your-workspace-architecture
https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide
https://learn.microsoft.com/en-us/azure/bastion/bastion-overview
https://learn.microsoft.com/en-us/azure/lighthouse/overview
https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent?pivots=portal

-[Overview of Key Management in Azure | Microsoft Learn](https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management)
-[Best practices for using Azure Key Vault | Microsoft Learn](https://learn.microsoft.com/en-us/azure/key-vault/general/best-practices)
-[What is Azure Key Vault? | Microsoft Learn](https://learn.microsoft.com/en-us/azure/key-vault/general/basic-concepts)

https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management-choose

https://en.wikipedia.org/wiki/Responsibility_assignment_matrix

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/organize/raci-alignment

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/resource-naming

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/resource-naming

Design solutions for identity and access management

Thursday, July 20, 2023 5:20 PM

- Design a solution for access to software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), hybrid/on-premises, and multicloud resources, including identity, networking, and application controls
  - Azure Active Directory and hybrid identity - Cloud Adoption Framework | Microsoft Learn
  - Architecture - Microsoft Defender for Identity | Microsoft Learn
  - Authentication methods and features - Microsoft Entra | Microsoft Learn

- Design a solution for Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra, including hybrid and multicloud environments
  - Azure security baseline for Azure Active Directory | Microsoft Learn

- Design a solution for external identities, including B2B, B2C, and Decentralized Identity

  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

- Design a modern authentication and authorization strategy, including Conditional Access, continuous access evaluation, threat intelligence integration, and risk scoring

  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

- Validate the alignment of Conditional Access policies with a Zero Trust strategy
  - Conditional Access design principles and dependencies - Azure Architecture Center | Microsoft Learn

- Specify requirements to secure Active Directory Domain Services (AD DS)
  - Overview of Azure Active Directory Domain Services | Microsoft Learn
  - Compare Active Directory-based services in Azure | Microsoft Learn

- Design a solution to manage secrets, keys, and certificates
  - Manage secrets - Cloud Adoption Framework | Microsoft Learn

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
AGDLP - Wikipedia

https://learn.microsoft.com/en-us/graph/permissions-reference

https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management?view=o365-worldwide

https://learn.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access

https://learn.microsoft.com/en-us/azure/active-directory/external-identities/customers/overview-customers-ciam

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation

From Build https://build.microsoft.com/en-US/sessions/2d3f258e-5c47-441b-9c3c-e18b993cab00

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-sso

https://fidoalliance.org/

https://learn.microsoft.com/en-us/answers/questions/86443/best-practices-on-how-to-decommission-adfs-servers

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/migrate-from-federation-to-cloud-authentication

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/whatis-phs

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/choose-ad-authn#decision-tree

https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identities-status

Design solutions for securing privileged access

Thursday, July 20, 2023 5:20 PM

- Design a solution for assigning and delegating privileged roles by using the enterprise access model
    - Delegation and roles in entitlement management - Microsoft Entra | Microsoft Learn

- Design an identity governance solution, including Privileged Identity Management (PIM), Privileged Access Management (PAM), entitlement management, and access reviews
    - Learn about privileged access management - Microsoft Purview (compliance) | Microsoft Learn
    - What is Privileged Identity Management? - Microsoft Entra | Microsoft Learn
    - What is entitlement management? - Microsoft Entra | Microsoft Learn
    - Manage access with access reviews - Microsoft Entra | Microsoft Learn

- Design a solution for securing the administration of cloud tenants, including SaaS and multicloud infrastructure and platforms
    - Delegated administration to secure with Azure Active Directory - Microsoft Entra | Microsoft Learn

- Design a solution for cloud infrastructure entitlement management that includes Microsoft Entra Permissions Management
    - What's Permissions Management? - Microsoft Entra | Microsoft Learn

- Design a solution for Privileged Access Workstation (PAW) and bastion services
    - Why are privileged access devices important | Microsoft Learn
    - About Azure Bastion | Microsoft Learn

PAM vs. PIM

Privilege access management helps organizations manage identities and makes it harder for threat actors to penetrate a network and obtain privileged account access. It adds protection to privileged groups that control access to domain-joined computers and the applications on those computers. PAM also provides monitoring, visibility, and fine-grained controls so you can see who your privileged admins are and how their accounts are being used.

Privileged identity management (PIM) provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access to sensitive resources in your organization by enforcing just-in-time access and just-enough access for these accounts. To further secure these privileged accounts, PIM enables you to enforce policy options like multifactor authentication.

While PAM and PIM have a lot of similarities, PAM uses tools and technology to control and monitor access to your resources and works on the principle of least privilege (ensuring that employees have just enough access to do their jobs) while PIM controls admins and super users with time-bound access and secures these privileged accounts.

From <https://www.microsoft.com/en-ca/security/business/security-101/what-is-privileged-access-management-pam>

https://aka.ms/SPA

Design solutions for regulatory compliance

Thursday, July 20, 2023 5:20 PM

- Translate compliance requirements into a security solution

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

  -

- Design a solution to address compliance requirements by using Microsoft Purview risk and compliance solutions
  - What is Microsoft Purview? | Microsoft Learn

- Design a solution to address privacy requirements, including Microsoft Priva
  - Learn about Microsoft Priva - Microsoft Priva | Microsoft Learn

- Design Azure Policy solutions to address security and compliance requirements

  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

- Evaluate infrastructure compliance by using Microsoft Defender for Cloud
  - The regulatory compliance dashboard - Microsoft Defender for Cloud | Microsoft Learn

Design solutions for security posture management in hybrid and multicloud environments

Thursday, July 20, 2023 5:20 PM

- Evaluate security posture by using MCSB
  - Overview of the Microsoft cloud security benchmark | Microsoft Learn
  - Microsoft cloud security benchmark introduction | Microsoft Learn

- Evaluate security posture by using 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
  - Identify and analyze risks across your environment - Microsoft Defender for Cloud | Microsoft Learn
  - Create custom Azure security policies - Microsoft Defender for Cloud | Microsoft Learn

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

- Design integrated security posture management and workload protection solutions in hybrid and multicloud environments, including Defender for Cloud
  - Workload protection dashboard and its features - Microsoft Defender for Cloud | Microsoft Learn

- Design cloud workload protection solutions that use Defender for Cloud, such as Microsoft Defender for Servers, Microsoft Defender for App Service, and Microsoft Defender for SQL
  - Plan a Defender for Servers deployment to protect on-premises and multicloud servers - Microsoft Defender for Cloud | Microsoft Learn
  - Protect your servers with Defender for Servers - Microsoft Defender for Cloud | Microsoft Learn
  - Microsoft Defender for App Service - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn
  - Microsoft Defender for Azure SQL - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn

- Design a solution for integrating hybrid and multicloud environments by using Azure Arc
  - Azure Arc overview - Azure Arc | Microsoft Learn

- Design a solution for Microsoft Defender External Attack Surface Management (Defender EASM)
  - Overview | Microsoft Learn

Browse code samples | Microsoft Learn

Azure ExpressRoute: About Encryption | Microsoft Learn

Least privileged roles by task - Microsoft Entra | Microsoft Learn

Common questions - data collection and agents - Microsoft Defender for Cloud | Microsoft Learn

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

Design solutions for securing server and client endpoints

Thursday, July 20, 2023 5:21 PM

- 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 security requirements for IoT devices and embedded systems
  - Security best practices - Azure IoT | Microsoft Learn

- Design a solution for securing operational technology (OT) and industrial control systems (ICS) by using Microsoft Defender for IoT
  - Overview - Microsoft Defender for IoT for organizations - Microsoft Defender for IoT | Microsoft Learn

- 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

- Design a solution 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
  Azure application security groups overview | Microsoft Learn
  Azure network security groups overview | Microsoft Learn
  Virtual networks and virtual machines in Azure | Microsoft Learn
  Azure Virtual Network - Concepts and best practices | Microsoft Learn
  Microsoft Defender for DNS - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn

  Azure ExpressRoute: About Encryption | Microsoft Learn

Microsoft Defender for DNS - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn

Azure Network Watcher overview | Microsoft Learn

Specify requirements 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
- Introduction to Azure Advisor - Azure Advisor | 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
- Overview - Azure App Service | Microsoft Learn
- Application Insights overview - Azure Monitor | 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
- Introduction to Azure Kubernetes Service - 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

Microsoft Cloud Penetration Testing Rules of Engagement

Coding best practices - Wikipedia

Diagnostic settings in Azure Monitor - Azure Monitor | Microsoft Learn

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

Enable end-to-end encryption using encryption at host - Azure portal - managed disks - Azure Virtual Machines | Microsoft Learn

Design solutions for securing Microsoft 365

Thursday, July 20, 2023 5:22 PM

- Evaluate security posture for productivity and collaboration workloads by using metrics, including Secure Score and Defender for Cloud secure score
  - Microsoft Secure Score | Microsoft Learn
  - Assess your security posture through Microsoft Secure Score | Microsoft Learn
  - Track your Microsoft Secure Score history and meet goals | Microsoft Learn

- Design a Microsoft 365 Defender solution
  - Microsoft 365 Defender prerequisites | Microsoft Learn
  - Turn on Microsoft 365 Defender | Microsoft Learn
  - Zero Trust with Microsoft 365 Defender | Microsoft Learn

- Design secure configurations and operational practices for Microsoft 365 workloads and data
  - Microsoft Defender for Endpoint documentation | Microsoft Learn
  - Microsoft Defender for Office 365 security documentation | Microsoft Learn
  - Microsoft Defender for Identity sensor health and settings in Microsoft 365 Defender | Microsoft Learn

Customer Lockbox requests - Microsoft Purview (compliance) | Microsoft Learn

Office 365 Security including Microsoft Defender for Office 365 and Exchange Online Protection | Microsoft Learn
Assess your security posture through Microsoft Secure Score | Microsoft Learn
Zero Trust identity and device access configurations - Microsoft 365 for enterprise | Microsoft Learn

Design solutions for securing applications

Thursday, July 20, 2023 5:22 PM

- Evaluate the security posture of existing application portfolios
  - Overview - Microsoft Defender for Cloud Apps | Microsoft Learn

- Evaluate threats to business-critical applications by using threat modeling
  - Microsoft Threat Modeling Tool overview - Azure | Microsoft Learn

- Design and implement a full lifecycle strategy for application security
  - Microsoft Security Development Lifecycle Practices

- Design and implement standards and practices for securing the application development process

- Map technologies to application security requirements

- Design a solution for workload identity to authenticate and access Azure cloud resources
  - Workload identities - Microsoft Entra | Microsoft Learn

- Design a solution for API management and security

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
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 solution for secure access to applications, including Azure Web Application Firewall (WAF) and Azure Front Door
  - Web Application Firewall documentation | Microsoft Learn
  - What is Azure web application firewall on Azure Front Door? | Microsoft Learn

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

https://learn.microsoft.com/en-us/azure/frontdoor/standard-premium/tier-comparison
https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview
https://learn.microsoft.com/en-us/azure/cdn/cdn-overview
Azure Monitor Insights Overview - Azure Monitor | Microsoft Learn
https://learn.microsoft.com/en-us/azure/architecture/solution-ideas/articles/devsecops-infrastructure-as-code

https://learn.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code
and
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-devops-introduction
https://learn.microsoft.com/en-us/azure/security/fundamentals/operational-checklist
https://owasp.org/www-community/Threat_Modeling#:~:text=The%20following%20four%20question%20framework%20can%20help%20to,it%3F%204%20Did%20we%20do%20a%20good%20job%3F

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

Overview of the Microsoft Defender for APIs plan - Microsoft Defender for Cloud | Microsoft Learn
Common questions - Defender for APIs - Microsoft Defender for Cloud | Microsoft Learn

Workload identities - Microsoft Entra | Microsoft Learn

New name for Azure Active Directory - Microsoft Entra | Microsoft Learn

Mitre Corporation - Wikipedia

Announcing Microsoft Sentinel All-in-One v2 - Microsoft Community Hub
Azure-Sentinel/Solutions/Training/Azure-Sentinel-Training-Lab at master · Azure/Azure-Sentinel (github.com)

Azure-Sentinel/Solutions/Training/Azure-Sentinel-Training-Lab at master · Azure/Azure-Sentinel (github.com)

Design solutions for securing an organization's data

Thursday, July 20, 2023 5:22 PM

- Design a solution for data discovery and classification by using Microsoft Purview data governance solutions
  - Introduction to Microsoft Purview governance solutions - Microsoft Purview | Microsoft Learn
  - Use the Microsoft Purview governance portal - Microsoft Purview | Microsoft Learn

- Specify priorities for mitigating threats to data

- Design a solution for protection of data at rest, data in motion, and data in use
  - Azure Data Encryption-at-Rest - Azure Security | Microsoft Learn
  - Data security and encryption best practices - Microsoft Azure | Microsoft Learn
  - Customer Lockbox for Microsoft Azure | Microsoft Learn
  - Azure encryption overview | Microsoft Learn

- Design a security solution for data in Azure workloads, including Azure SQL, Azure Synapse Analytics, and Azure Cosmos DB
  - Overview of Defender for Azure Cosmos DB - Microsoft Defender for Cloud | Microsoft Learn
  - Azure SQL Database security features | Microsoft Learn
  - Azure Synapse Analytics security white paper - Azure Synapse Analytics | Microsoft Learn
  - Database security overview - Azure Cosmos DB | Microsoft Learn

- Design a security solution for data in Azure Storage
  - Storage Accounts and security - Microsoft Azure Well-Architected Framework | Microsoft Learn

- Design a security solution that includes Microsoft Defender for Storage and Defender for SQL
  - Microsoft Defender for Storage - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn
  - Microsoft Defender for Azure SQL - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn

What is Azure Web Application Firewall on Azure Application Gateway? - Azure Web Application Firewall | Microsoft Learn

Azure Front Door | Microsoft Learn

Data retention and archive in Azure Monitor Logs - Azure Monitor | Microsoft Learn

StorSimple documentation | Microsoft Learn
Microsoft Azure Data Box overview | Microsoft Learn
Hybrid file services - Azure Architecture Center | Microsoft Learn

Organize your resources with management groups - Azure Governance - Azure governance | Microsoft Learn

Design a resiliency strategy for ransomware and other attacks based on Microsoft Security Best Practices

Thursday, July 20, 2023 5:18 PM

- Design a security strategy to support business resiliency goals, including identifying and prioritizing threats to business-critical assets
  - Ransomware protection in Azure | Microsoft Learn
  - Improve your security defenses for ransomware attacks with Azure Firewall | Azure Blog | Microsoft Azure

- Design solutions that align with Microsoft ransomware best practices, including backup, restore, and privileged access

  Prepare for a ransomware attack | Microsoft Learn
  Azure backup and restore plan to protect against ransomware | Microsoft Learn
  Azure features & resources that help you protect, detect, and respond | Microsoft Learn
  https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization

- Design configurations for secure backup and restore by using Azure Backup for hybrid and multicloud environments

  What is Azure Backup? - Azure Backup | Microsoft Learn

- Design solutions for security updates
  - Manage updates and patches for your VMs in Azure Automation | Microsoft Learn

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

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

https://azure.microsoft.com/en-us/products/chaos-studio
https://en.m.wikipedia.org/wiki/Chaos_engineering

https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/overview

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/i-m-being-attacked-now-what/ba-p/3481937

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/security-operations-introduction

Design solutions that align with the Microsoft Cybersecurity Reference Architectures (MCRA) and Microsoft cloud security benchmark (MCSB)

Thursday, July 20, 2023 5:18 PM

- Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn
- Overview of the Microsoft cloud security benchmark | Microsoft Learn

Define a security strategy - Cloud Adoption Framework | Microsoft Learn

- Design solutions that align with 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
Video: microsoft.com/en-us/videoplayer/embed/RWVECU?postJslIMsg=true

- Design solutions that align with best practices for protecting against insider and external attacks
    - Securing privileged access overview | Microsoft Learn
-
- Design solutions that align with best practices for Zero Trust security, including the Zero Trust Rapid Modernization Plan (RaMP)

  Zero Trust security in Azure | Microsoft Learn
  Zero Trust Rapid Modernization Plan | Microsoft Learn

Design solutions that align with the Microsoft Cloud Adoption Framework for Azure and the Microsoft Azure Well-Architected Framework

Thursday, July 20, 2023 5:19 PM

- Design a new or evaluate an existing strategy for security and governance based on the Microsoft Cloud Adoption Framework (CAF) and the Microsoft Azure Well-Architected Framework
  - Microsoft Cloud Adoption Framework for Azure documentation - Cloud Adoption Framework | Microsoft Learn
  - Microsoft Azure Well-Architected Framework - Azure Well-Architected Framework | Microsoft Learn

- Recommend solutions for security and governance based on the Microsoft Cloud Adoption Framework for Azure and the Microsoft Azure Well-Architected Framework
  - Security in the Microsoft Cloud Adoption Framework for Azure - Cloud Adoption Framework | Microsoft Learn
  - Governance in the Microsoft Cloud Adoption Framework for Azure - Cloud Adoption Framework | Microsoft Learn
  - Security documentation - Microsoft Azure Well-Architected Framework | Microsoft Learn

- Design solutions for implementing and governing security by using Azure landing zones
  - What is an Azure landing zone? - Cloud Adoption Framework | Microsoft Learn
  - Security in the Microsoft Cloud Adoption Framework for Azure - Cloud Adoption Framework | Microsoft Learn
    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
  - Landing Zone Video microsoft.com/en-us/videoplayer/embed/RE4xdvm?postJsllMsg=true
  -

- Design a DevSecOps process
  - DevSecOps controls - Cloud Adoption Framework | Microsoft Learn

DevSecOps Implementation Process and Road Map – Security at Every Step - DevOps.com

Design solutions for security operations

Thursday, July 20, 2023 5:19 PM

- Develop security operations capabilities to support a hybrid or multicloud environment

  Introduction to hybrid and multicloud - Cloud Adoption Framework | Microsoft Learn
  What is Microsoft Sentinel? | Microsoft Learn

- Design a solution for centralized logging and auditing

  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

- Design a solution for security information and event management (SIEM), including Microsoft Sentinel

  What is Microsoft Sentinel? | Microsoft Learn
  MITRE ATT&CK®

- Design a solution for detection and response that includes extended detection and response (XDR)

- Design a solution for security orchestration automated response (SOAR), including Microsoft Sentinel and Microsoft Defender

  Use playbooks with automation rules in Microsoft Sentinel | Microsoft Learn
  Overview - Azure Logic Apps | Microsoft Learn
  -

- Design and evaluate security workflows, including incident response, threat hunting, incident management, and threat intelligence
  -

- Design and evaluate threat detection coverage by using MITRE ATT&CK
  - MITRE ATT&CK®
  - View MITRE coverage for your organization from Microsoft Sentinel | 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

Workspace architecture best practices for Microsoft Sentinel | Microsoft Learn

https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview

Cybercrime Module 4 Key Issues: Standards and best practices for digital forensics (unodc.org)

(PDF) Digital Forensic Analysis of Cybercrimes: Best Practices and Methodologies (researchgate.net)

Microsoft Sentinel – continuous threat monitoring for GitHub - Microsoft Community Hub

Root cause analysis (preview) - Power Automate | Microsoft Learn

Design solutions for identity and access management

Thursday, July 20, 2023 5:20 PM

- Design a solution for access to software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), hybrid/on-premises, and multicloud resources, including identity, networking, and application controls
  - Azure Active Directory and hybrid identity - Cloud Adoption Framework | Microsoft Learn

- Design a solution for Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra, including hybrid and multicloud environments
  - Azure security baseline for Azure Active Directory | Microsoft Learn

- Design a solution for external identities, including B2B, B2C, and Decentralized Identity

  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

- Design a modern authentication and authorization strategy, including Conditional Access, continuous access evaluation, threat intelligence integration, and risk scoring

  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

- Validate the alignment of Conditional Access policies with a Zero Trust strategy
  - Conditional Access design principles and dependencies - Azure Architecture Center | Microsoft Learn

- Specify requirements to secure Active Directory Domain Services (AD DS)
  - Overview of Azure Active Directory Domain Services | Microsoft Learn
  - Compare Active Directory-based services in Azure | Microsoft Learn

- Design a solution to manage secrets, keys, and certificates
  - Manage secrets - Cloud Adoption Framework | Microsoft Learn

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

Design solutions for securing privileged access

Thursday, July 20, 2023 5:20 PM

- Design a solution for assigning and delegating privileged roles by using the enterprise access model
    - Delegation and roles in entitlement management - Microsoft Entra | Microsoft Learn

- Design an identity governance solution, including Privileged Identity Management (PIM), Privileged Access Management (PAM), entitlement management, and access reviews
    - Learn about privileged access management - Microsoft Purview (compliance) | Microsoft Learn
    - What is Privileged Identity Management? - Microsoft Entra | Microsoft Learn
    - What is entitlement management? - Microsoft Entra | Microsoft Learn
    - Manage access with access reviews - Microsoft Entra | Microsoft Learn

- Design a solution for securing the administration of cloud tenants, including SaaS and multicloud infrastructure and platforms
    - Delegated administration to secure with Azure Active Directory - Microsoft Entra | Microsoft Learn

- Design a solution for cloud infrastructure entitlement management that includes Microsoft Entra Permissions Management
    - What's Permissions Management? - Microsoft Entra | Microsoft Learn

- Design a solution for Privileged Access Workstation (PAW) and bastion services
    - Why are privileged access devices important | Microsoft Learn
    - About Azure Bastion | Microsoft Learn

PAM vs. PIM

Privilege access management helps organizations manage identities and makes it harder for threat actors to penetrate a network and obtain privileged account access. It adds protection to privileged groups that control access to domain-joined computers and the applications on those computers. PAM also provides monitoring, visibility, and fine-grained controls so you can see who your privileged admins are and how their accounts are being used.

Privileged identity management (PIM) provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access to sensitive resources in your organization by enforcing just-in-time access and just-enough access for these accounts. To further secure these privileged accounts, PIM enables you to enforce policy options like multifactor authentication.

While PAM and PIM have a lot of similarities, PAM uses tools and technology to control and monitor access to your resources and works on the principle of least privilege (ensuring that employees have just enough access to do their jobs) while PIM controls admins and super users with time-bound access and secures these privileged accounts.

From <https://www.microsoft.com/en-ca/security/business/security-101/what-is-privileged-access-management-pam>

Design solutions for regulatory compliance

Thursday, July 20, 2023 5:20 PM

- Translate compliance requirements into a security solution

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

  -

- Design a solution to address compliance requirements by using Microsoft Purview risk and compliance solutions
  - What is Microsoft Purview? | Microsoft Learn

- Design a solution to address privacy requirements, including Microsoft Priva
  - Learn about Microsoft Priva - Microsoft Priva | Microsoft Learn

- Design Azure Policy solutions to address security and compliance requirements

  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

- Evaluate infrastructure compliance by using Microsoft Defender for Cloud
  - The regulatory compliance dashboard - Microsoft Defender for Cloud | Microsoft Learn

Design solutions for security posture management in hybrid and multicloud environments

Thursday, July 20, 2023 5:20 PM

- Evaluate security posture by using MCSB

  Overview of the Microsoft cloud security benchmark | Microsoft Learn
  Microsoft cloud security benchmark introduction | Microsoft Learn

- Evaluate security posture by using 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 Microsoft Secure Score

  Tracking your secure score in Microsoft Defender for Cloud | Microsoft Learn
  Workflow automation in Microsoft Defender for Cloud | Microsoft Learn

- Design integrated security posture management and workload protection solutions in hybrid and multicloud environments, including Defender for Cloud
  - Workload protection dashboard and its features - Microsoft Defender for Cloud | Microsoft Learn

- Design cloud workload protection solutions that use Defender for Cloud, such as Microsoft Defender for Servers, Microsoft Defender for App Service, and Microsoft Defender for SQL
  - Plan a Defender for Servers deployment to protect on-premises and multicloud servers - Microsoft Defender for Cloud | Microsoft Learn
  - Protect your servers with Defender for Servers - Microsoft Defender for Cloud | Microsoft Learn
  - Microsoft Defender for App Service - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn
  - Microsoft Defender for Azure SQL - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn

- Design a solution for integrating hybrid and multicloud environments by using Azure Arc
  - Azure Arc overview - Azure Arc | Microsoft Learn

- Design a solution for Microsoft Defender External Attack Surface Management (Defender EASM)
  - Overview | Microsoft Learn

Design solutions for securing server and client endpoints

Thursday, July 20, 2023 5:21 PM

- 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 security requirements for IoT devices and embedded systems
  - Security best practices - Azure IoT | Microsoft Learn

- Design a solution for securing operational technology (OT) and industrial control systems (ICS) by using Microsoft Defender for IoT
  - Overview - Microsoft Defender for IoT for organizations - Microsoft Defender for IoT | Microsoft Learn

- 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

- Design a solution 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

Specify requirements 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

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

Zero Trust illustrations for IT architects and implementers | Microsoft Learn

Using Microsoft Defender for Endpoint in Microsoft Defender for Cloud to protect native, on-premises, and AWS machines. | Microsoft Learn

Traffic mirroring methods - Microsoft Defender for IoT | Microsoft Learn

New Microsoft Intune Suite with Privilege Management, Advanced Analytics, Remote Help & App VPN

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 solutions for securing Microsoft 365

Thursday, July 20, 2023 5:22 PM

- Evaluate security posture for productivity and collaboration workloads by using metrics, including Secure Score and Defender for Cloud secure score
  - Microsoft Secure Score | Microsoft Learn
  - Assess your security posture through Microsoft Secure Score | Microsoft Learn
  - Track your Microsoft Secure Score history and meet goals | Microsoft Learn

- Design a Microsoft 365 Defender solution
  - Microsoft 365 Defender prerequisites | Microsoft Learn
  - Turn on Microsoft 365 Defender | Microsoft Learn
  - Zero Trust with Microsoft 365 Defender | Microsoft Learn

- Design secure configurations and operational practices for Microsoft 365 workloads and data
  - Microsoft Defender for Endpoint documentation | Microsoft Learn
  - Microsoft Defender for Office 365 security documentation | Microsoft Learn
  - Microsoft Defender for Identity sensor health and settings in Microsoft 365 Defender | Microsoft Learn

Customer Lockbox requests - Microsoft Purview (compliance) | Microsoft Learn

Office 365 Security including Microsoft Defender for Office 365 and Exchange Online Protection | Microsoft Learn
Assess your security posture through Microsoft Secure Score | Microsoft Learn
Zero Trust identity and device access configurations - Microsoft 365 for enterprise | Microsoft Learn

Design solutions for securing applications

Thursday, July 20, 2023 5:22 PM

- Evaluate the security posture of existing application portfolios
  - Overview - Microsoft Defender for Cloud Apps | Microsoft Learn

- Evaluate threats to business-critical applications by using threat modeling
  - Microsoft Threat Modeling Tool overview - Azure | Microsoft Learn

- Design and implement a full lifecycle strategy for application security
  - Microsoft Security Development Lifecycle Practices

- Design and implement standards and practices for securing the application development process

- Map technologies to application security requirements

- Design a solution for workload identity to authenticate and access Azure cloud resources
  - Workload identities - Microsoft Entra | Microsoft Learn

- Design a solution for API management and security

  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

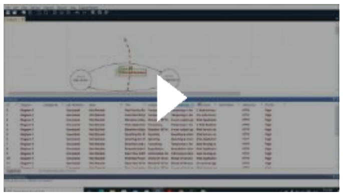
About GitHub Advanced Security - GitHub Docs
Scan container images using GitHub Actions - Azure Container Registry | Microsoft Learn
Introduction to Azure Web Application Firewall | Microsoft Learn
Microsoft Threat Modeling Tool overview - Azure | Microsoft Learn

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

- Design a solution for secure access to applications, including Azure Web Application Firewall (WAF) and Azure Front Door
  - Web Application Firewall documentation | Microsoft Learn
  - What is Azure web application firewall on Azure Front Door? | Microsoft Learn

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 solutions for securing an organization's data

Thursday, July 20, 2023 5:22 PM

- Design a solution for data discovery and classification by using Microsoft Purview data governance solutions
  - Introduction to Microsoft Purview governance solutions - Microsoft Purview | Microsoft Learn
  - Use the Microsoft Purview governance portal - Microsoft Purview | Microsoft Learn

- Specify priorities for mitigating threats to data

- Design a solution for protection of data at rest, data in motion, and data in use
  - Azure Data Encryption-at-Rest - Azure Security | Microsoft Learn
  - Data security and encryption best practices - Microsoft Azure | Microsoft Learn
  - Customer Lockbox for Microsoft Azure | Microsoft Learn
  - Azure encryption overview | Microsoft Learn

- Design a security solution for data in Azure workloads, including Azure SQL, Azure Synapse Analytics, and Azure Cosmos DB
  - Overview of Defender for Azure Cosmos DB - Microsoft Defender for Cloud | Microsoft Learn
  - Azure SQL Database security features | Microsoft Learn
  - Azure Synapse Analytics security white paper - Azure Synapse Analytics | Microsoft Learn
  - Database security overview - Azure Cosmos DB | Microsoft Learn

- Design a security solution for data in Azure Storage
  - Storage Accounts and security - Microsoft Azure Well-Architected Framework | Microsoft Learn

- Design a security solution that includes Microsoft Defender for Storage and Defender for SQL
  - Microsoft Defender for Storage - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn
  - Microsoft Defender for Azure SQL - the benefits and features - Microsoft Defender for Cloud | Microsoft Learn