
GoSecure
CLOUD
MICROSOFT
SECURITY
ACADEMY
Microsoft
Partner

Cloud Fundamentals

Introduction: - A Tour to Azure	**Cloud Service types** -cloud service types	**Azure Compute Demo** -Creating a Virtual Machine (VM) -Connecting to a Virtual Machine -Creating Azure App Services / Web Apps -Azure App Services In Action -Creating Azure Functions -Kubernetes and Azure Container Instances
Describe Cloud Computing -Shared Responsibility model -public, private & Hybrid Cloud -cloud Pricing	**Core architectural components of azure** -Regions, Region Pairs, Sovereign Regions -Availability Zones and Data Centres -Resources, Resource Groups, Subscriptions, Management Groups	**Azure Storage** -Overview of Azure Storage -Create an Unmanaged Storage Account -Upload Files to a Storage Account -Azure Storage Explorer & Storage Browser -Azure File Sync -Azure Migrate

Cloud Fundamentals

Benefits of Cloud Computing -Cost Savings Benefit of Cloud Computing -High Availability, Scalability and Elasticity -Reliability and Predictability -Security, Governance and Monitoring	**Azure Compute and Networking Services** -Azure Compute services -Azure Networking services -Network Peering -Public and Private Endpoints	**Identity, access and Security** -Identity and Azure Active Directory -Benefits of Azure Active Directory (Azure AD) -Authentication vs Authorization -Azure AD Conditional Access -Multi-Factor Authentication (MFA or 2FA) -Role-Based Access Control (RBAC) -Zero-Trust Model of Security -Defense in Depth -Microsoft Defender for Cloud
Cost Management in azure -Factors that Affect Cost -Azure Pricing Calculator -Total Cost of Ownership Calculator -Azure Cost Management -Resource Tags	**Azure Governance and Compliance** -Azure Governance and Compliance	**Tools for Managing & deploying azure Resource** -Azure Portal and Command Line Tools -Create Resources Using Command Line -ARM Templates - Generate ARM Templates in the Azure Portal

Microsoft Security Family

SIEM & XDR	
Microsoft 365 Defender	This is an integrated threat protection suite for identities, endpoints(workstations, servers), cloud apps, email and documents in Microsoft 365. It combines capabilities like defender for Endpoint, Office 365 ATP, Azure ATP and more.
Microsoft Defender for Endpoint	An endpoint security solution providing comprehensive anti-virus, endpoint detection and response, auto investigation & remediation and more. Protects devices like laptops, servers, virtual machines across platforms.
Microsoft Defender for Office 365	Provides protection against threats to email and collaboration tools in Office 365. Includes features like safe attachments, safe links, anti-phishing, and more.
Microsoft Defender for Identity	Protects an organization's identities by leveraging signals from Active Directory and identifying sophisticated threats, compromised identities and malicious insider actions.
Microsoft Defender for Cloud Apps	Discovers shadow IT, protects cloud apps, and enforces data loss prevention policies. Works across platforms like Office 365, G Suite, AWS and more.
Microsoft Defender Vulnerability Management	Assesses vulnerabilities using both built-in and third party scanners, prioritizes risk based on threat intelligence, and enables patching at scale.
Microsoft Defender Threat Intelligence	Enriches security operations and hunting by providing context on adversaries, exploits, malware, and vulnerabilities being used in real-world attacks.
Microsoft Sentinel	This is Microsoft's cloud-native SIEM (security information and event management) and SOAR (security orchestration and automation response) solution. It provides intelligent threat detection, threat hunting, and automated response across an organization's on-prem and cloud environments.
Microsoft Information Protection:	Classifies and labels documents and emails based on sensitivity, applies protection (like encryption), and tracks activities. Integrates with Office apps.
Microsoft Defender for Cloud	This provides unified security management and threat protection for Azure and hybrid cloud workloads. It includes features like cloud workload protection, adaptive threat protection, unified security management, and compliance reporting.

Microsoft Security Family

IDENTITY & ACCESS	
Microsoft Entra ID (Azure Active Directory)	Cloud-based identity and access management service that provides central identity and access control for users, groups and devices. Enables single sign-on (SSO) to applications and resources.
Microsoft Entra External ID	Lets organizations collaborate securely with external partners and vendors by providing controlled access to specific apps and resources.
Microsoft Entra ID Governance	Helps manage user access reviews, access requests and entitlement management across the organization
Microsoft Entra ID Protection	Provides risk-based conditional access policies, monitoring for suspicious activities, automated threat response and more.
Microsoft Entra Internet Access	Secures access to internal web apps with identity-based conditional access and protection against phishing attacks.
Microsoft Entra Private Access	Provides Zero Trust access to internal apps and resources without a VPN by using a private endpoint accessible only through Entra.
Microsoft Entra Permissions Management	Automates the assignment and management of user permissions and access across cloud apps and role-based access controls.
Microsoft Entra Verified ID	Confirms user identities by checking their phone numbers and email addresses when signing in to high value apps and resources.
Microsoft Entra Workload ID	Extends Entra identity capabilities and access controls to servers and virtual machines in the cloud or on-prem.
Azure Key Vault	Manages and secures cryptographic keys and application secrets like certificates, connection strings, passwords etc.

Microsoft Security Family

CLOUD SECURITY	
Microsoft Defender for Cloud	Unified security management, advanced threat protection, and compliance for Azure and hybrid cloud workloads.
Microsoft Defender Cloud Security Posture Mgmt	Assesses security configurations, detects misconfigurations, and provides recommendations to improve cloud workload security posture.
Microsoft Defender for DevOps	Brings security into DevOps pipelines by scanning infrastructure-as-code, generating security policies, and integrating security testing.
Microsoft Defender External Attack Surface Management	Discovers externally exposed assets, monitors for vulnerabilities and misconfigurations, and helps remediate risk.
Azure Firewall	Managed, cloud-based network security service with high availability that protects Azure Virtual Network resources.
Azure Web App Firewall	Protects web applications from common exploits and vulnerabilities through inbound protection rules.
Azure DDoS Protection	Protects Azure resources from distributed denial of service (DDoS) attacks with intelligent monitoring and mitigation.

Microsoft Security Family

M365 SERVICE MANAGEMENT	
Exchange online	Cloud-based email and calendar service that provides enterprise-grade email, shared calendars, contacts, and more. Part of Microsoft 365.
Sharepoint online	Cloud document management and collaboration platform to create sites, share files, wikis, news and more. Part of Microsoft 365.
Microsoft endpoint manager	Unified platform for managing and securing devices including desktops, laptops, mobile devices and virtual endpoints.
Microsoft power apps	Service for building custom business apps that connect to data sources and automate workflows across devices.
Microsoft power BI	Business intelligence platform for visualizing and analyzing data through interactive reports and dashboards.
Microsoft dynamics 365	Cloud-based ERP and CRM applications for managing business processes across sales, customer service, finance, operations and more.

Microsoft Security Family

SECURITY AI	
Microsoft security AI	Microsoft applies AI and machine learning across its security products and services to enhance detection, investigation, and response to threats. Key capabilities powered by AI include
	Behavioral analytics - Analyzes patterns of activity to detect anomalies and suspicious behaviors indicative of cyber threats.
	Automated investigation - Uses AI to automatically investigate security alerts and take recommended actions to resolve threats. Reduces the burden on security analysts.
	Threat hunting - Identifies advanced and previously unknown threats by continuously monitoring for indicators of attack across massive data sets.
	Risk scoring - Calculates dynamic risk scores for users, devices, and content by evaluating various risk factors using AI algorithms. Enables risk-based policies.
	Anti-phishing - Leverages AI to better identify and protect against phishing campaigns, business email compromise attacks, and other social engineering schemes.
	Vulnerability assessment - Uses machine learning to more accurately predict vulnerability severity levels and prioritize patching based on exploitability.
	Information protection - Applies intelligent classification, labeling and protection of sensitive information through automated data loss prevention and rights management.
	Secure orchestration - Employs AI to enable intelligent workflow automation for security operations and response.

Microsoft Security Family

AZURE
Introduction to Cloud Computing Models (IaaS, PaaS, SaaS)
Azure Infrastructure as a Service (IaaS) - 1 hr
Overview of Azure IaaS and key components like Virtual machines, Azure Virtual Network, Storage, Azure Backup
Azure Platform as a Service (PaaS) - 1 hr
Overview of Azure PaaS services like App Services, Functions, Logic Apps,Network watcher, Azure firewall
Azure security and management tools - 1hr Azure Portal, CLI, PowerShell, ARM Templates, Azure Advisor ,Azure monitor, Azure policy for governance and compliance

Microsoft 365 Defender

Microsoft 365 Defender
In processing Into Defender 365 Defender, Access to Microsoft365 Defender portal
Overview of Microsoft 365 Defender, Microsoft 365 Defender advanced features
Investigate, respond, and remediate threats to email by using Microsoft 365 Defender
Investigate and respond to alerts generated from insider risk policies
Microsoft Defender for Endpoints (End devices)
Onboarding/Offboarding Devices to Microsoft 365 Defender
Manage data retention, alert notification, and advanced features
Respond to incidents and alerts
Manage automated investigations and remediations
Remediate vulnerabilities by using the Microsoft's threat and vulnerability management solution
Manage endpoint threat indicators

Microsoft 365 Defender

Microsoft Defender for Office (Emails)
Overview of Microsoft Defender for office
Define threat-protection policies to set the appropriate level of protection for your organization
Threat investigation and response capabilities
Configuration of policies: anti-malware, anti-phishing, anti-spam
Threat investigation and response capabilities
Defender for Identity threats (Identity protection for hybrid environment)
Describing the architecture of defender for Identity
Configuring of Defender for Identity
Identify and remediate security risks related to events for Microsoft Azure Active Directory
Identify and remediate security risks related to Azure AD Identity Protection events

Microsoft 365 Defender

Defender for Cloud Apps (SaaS apps)
Describing the architecture of defender for Cloud Apps
Configure Microsoft Defender for Cloud Apps
generate alerts and reports to detect threats
Identify, investigate, and remediate security risks by using Microsoft Defender for Cloud Apps

Microsoft 365 Management

365 Admin Portal
Microsoft admin portal
Difference between Microsoft admin portal and azure portal
Creating object using M365 admin portal
Microsoft support request creation
Handeling Microsoft tickets
Subscription and billing of azure and M365
Configure azure resources
Use the Azure portal
Use Azure Cloud Shell
Use Azure PowerShell
Office 365 suite configurations
Creating sharepoint sites
Managing sharepoint sites with permissions
Creating onedrive
Creating one note and managing permissions on it

Managing Objects in azure
Creating users in azure AD
Assiging licences to users
Creating Groups
Different types of Groups
Creating App registration
Managing objects
Azure Resource manager
Review Azure Resource Manager benefits
Review Azure resource terminology
Creating resource groups
Create Azure Resource Manager locks
Reorganize Azure resources
Remove resources and resource groups
Determine resource limits

Microsoft Information Protection

Introduction to information protection and data lifecycle management in Microsoft Purview -Know your data -Protect your data -Prevent data loss -Govern your data -Summary and knowledge check
Prevent data loss -Introduction to Microsoft Purview Data Loss Prevention -Define the sensitive data you want to protect -Use data loss prevention (DLP) policies to protect your data -Summary and knowledge check

Microsoft Information Protection

Classify data for protection and governance

-Data classification overview
-Classify data using sensitive information types
-Classify data using trainable classifiers
-Review sensitive information and label usage
-Explore labeled and sensitive content
-Understand activities related to your data
-Summary and knowledge check

Create and manage sensitive information types

-Compare built-in versus custom sensitive information types
-Create and manage custom sensitive information types
-Describe custom sensitive information types with exact data match
-Implement document fingerprinting
-Create keyword dictionary
-Knowledge check
-Summary and resources

Microsoft Sentinel

Overview -Other learning and support options -Get started with Microsoft Sentinel -How is Microsoft Sentinel used?
Architecting and deploying -Workspace and tenant architecture -Data collection -Log management -Enrichment: Threat intelligence, watchlists, and more -Log transformation -Migration -Advanced SIEM information model and normalization

Microsoft Sentinel

Creating content -Kusto Query Language -Analytics -Implementing SOAR -Workbooks, reporting, and visualization -Notebooks -Use cases and solutions
Operating A day in a SOC analyst's life, incident management, and investigation Hunting User and Entity Behavior Analytics (UEBA) Monitoring Microsoft Sentinel's health
Workspace manager centrally manage multiple Microsoft Sentinel workspaces within one or more Azure tenants with workspace manager