|  |  |
| --- | --- |
| **Exam SC-900: Microsoft Security, Compliance, and Identity Fundamentals – Skills Measured** | |
| **Domain 1: Describe the concepts of security, compliance, and identity (10-15%)** [**https://docs.microsoft.com/en-us/learn/modules/describe-security-concepts-methodologies/**](https://docs.microsoft.com/en-us/learn/modules/describe-security-concepts-methodologies/) | |
| Describe security and compliance concepts | |
| • describe the shared responsibility model  The Shared responsibility model responsibilities by type. | * Identifies the security tasks that are handled by the cloud provider and the end user * Information and Data, Devices, and Accounts and identities are always responsible by the customer * IaaS: Not responsible for physical hosts, networks, or datacenters * PaaS: Not responsible for Physical and Operating System * SaaS: Least amount of management |
| • describe defense in depth  Defense in depth uses multiple layers of security to protect sensitive data. | * A layered approach to security * A series of mechanisms to slow the advance of an attack * Physical: limiting access to a datacenter * Identity and access: MFA or condition based access for control access * Perimeter: DdoS protection * Network: Network segmentation and network access controls * Compute: Securing access to virtual machines * Application: Apps do not have vulnerabilities * Data: Access to data and encryption |
| • describe confidentiality, integrity, availability (CIA) | * Confidentiality: The need to keep confidential sensitive data (passwords, financial data, etc) * Integrity: Keeping data or messages correct, confidence that data was not tampered * Availability: Refers to making data available to those who need it when needed. |
| • describe the Zero-Trust model  “trust no one, verify everything” | * Assumes that everything is on an open and untrusted network * Principles   + Verify explicitly: authenticate and authorize based on available datapoints   + Least privileged access: limit use access with JIT/JEA   + Assume breach: segment access by network, user, devices, and application * Foundational pillars   + Identities: must verity   + Devices: monitor for health and compliance   + Applications: managing permissions and access   + Data: classified, labeled, and encrypted   + Infrastructures:   + Networks: segmented and deep in-network microsegmentation |
| • describe encryption and hashing | * Encryption: making data unreadable and unusable to unauthorized users   + Symmetric Encryption: The same key to encrypt and decrypt data   + Asymmetric Encryption: Uses a public and private key   + Encrypt data at rest, data in transit, and data in use * Hashing: An algorithm to convert text to a fixed length value called a hash   + Functions are deterministic   + Passwords are salted to prevent brute-force attacks |
| • describe compliance concepts | * Regulations to protect and govern the use of data * Data residency: Where data is stored, how and when it can be transferred, processed, or accessed internationally * Data sovereignty: Personal data is subject to the laws and regulations of the country and region it is physical collected, held or processed * Data privacy: providing notice and being transparent about collection, processing use and sharigng |
| Define identity concepts | |
| • define identity as the primary security perimeter | * Includes the on-premises network, SaaS applications, personal devices, unmanaged devices, IoT * **Identity is the new security perimeter** * Four pillars of identity infrastructure:   + Administration: creation and management of identities of users, devices, and services   + Authentication: How much an IT system needs to know about an identity   + Authorization: process the incoming identity data to determine the level of access an authenticated person or service has within the application   + Auditing: tracking of actions |
| • define authentication | * Proving that a person is who they say they are * AuthN |
| • define authorization | * What an authenticated user can do and access * The level of access or the permissions an authenticated person has to data and resources * AuthZ |
| • describe identity providers are | * Provides a security token for accessing a server |
| • describe Active Directory | * AzureAD: Stores information about members of a domain; including devices, users, creds, access rights |
| • describe the concept of Federation  Simplifed view of how federation works | * A single account can be used to access multiple services * There is a trust relationship between the different services |
| **Domain 2: Describe the capabilities of Microsoft identity and access management solutions (25-30%)** | |
| Describe the basic identity services and identity types of Azure AD | |
| • describe Azure Active Directory (AD) | * Cloud based identity and access management service * Used to allow access to internal and external resources * Simplifies the way organizations manage authorization and access |
| • describe Azure AD identities | * Free, Office 365 Apps, Premium P1, Premium P2 * Free: administer users and groups, sync with on-site AD, basic reports, self-service password change, SSO, included with subscriptions * Office 365: Self-service password reset, device write-back * P1: Advanced administration, Microsoft Identity Manager, cloud write-back * P2: Azure AD identity protection, conditional based access, identity management |
| • describe what hybrid identity | * Hybrid identity: A common user identity for authentication and authorization to all resources, regardless of location * Password hash synchronization: sign into azure AD using the same user and pass on the on-premises AD, the hashing algorithm is shared * Pass-through authentication: sends the authentication to a local server, not to Azure server * Federated authentication: The sign in process is passed on to another Federated server, hash sync is then used as a backup |
| • describe the different external identity types | * External identity types: allow external users access * B2B Collaboration: share apps and resources, while maintaining own data   + Self-service   + Invitation and redemption process * B2C access management: customer identity access management solution, sign in using social external or local account identities |
| Describe the authentication capabilities of Azure AD | |
| • describe the authentication methods available in Azure AD | * Passwords: should be used in conjunction with other authentication methods * Phone: SMS authentication, Voice call verification * OATH (Open authentication): One-time password codes   + Tokens are generated and inputted into the application * Passwordless Authentication: Biometrics * Windows Hello Business: Pin and Biometrics * FIDO2: A external security key or a platform key built into a device |
| • describe multi-factor authentication | * Using more than one form of verification * Administrator can require certain verification methods |
| • describe self-service password reset | * Allows users to change or reset their password without need for help * Used for password change, reset, unlock |
| • describe password protection and management capabilities available in Azure AD | * A feature of AAD that reduces the risk of having a weak password * Default global banned password lists are applied to all users * Custom banned password lists * Protection against password spray |
| Describe access management capabilities of Azure AD | |
| • describe what conditional access is. | * Analyzes signals such as the user, location, device, application, to automate decisions for authorizing access to resources, require MFA, or block access * Signals:   + User or group membership   + Named location information   + Device   + Application   + Real-time sign in risk detection   + Cloud apps or actions   + User Risk * Access Controls:   + Block access   + Grant access   + MFA before access |
| • describe the benefits of Azure AD roles | * Convenient to manage identity across Microsoft 365 services |
| • describe the benefits of Azure AD role-based access control | * RBAC: roles control access to resources * Built-in roles:   + Global Admin: access to all admin rights in the AD   + User admin: Create and manage all aspects of users and groups   + Billing admin: make purchases, manage subscriptions and support tickets, and monitor service health * Custom Roles: collection of permissions that you choose from a preset list; create the definition of the role, then assign roles to users. * Only grant access users need * Categories of AD roles:   + Azure AD roles: manage resource within the AD only   + Service specific roles: roles for services i.e. teams, sharepoint, etc.   + Cross service roles: span services |
| Describe the identity protection & governance capabilities of Azure AD | |
| • describe identity governance in Azure AD | * Identity governance: govern the identity lifecycle, govern access lifecycle, secure privileged access for administration * Identity lifecycle: join, move, leave * Access lifecycle: process of managing access throughout organizational life   + Dynamic groups: attribute-based rules to determine membership of groups * Privileged access lifecycle: monitoring privileged access   + Privileged Identity Management (PIM): extra controls tailored to securing access rights   + A P2 feature |
| • describe entitlement management and access reviews | * Identity governance feature that enables organizations to manage the identity and access lifecycle at scale * AD reviews: efficiently mange group memberships, access to applications, and role assignment |
| • describe the capabilities of PIM | * Just in time, only providing access when needed * Time-bound * Appro9val based * Visible * Auditable * PIM: reduces the change of malicious actor getting access to resources by limiting access |
| • describe Azure AD Identity Protection | * Automates the detection and remediation of identity-based risks * Investigate risks using data in the portal * Export risk detection data to third part utilities for further analysis |
| **Describe the capabilities of Microsoft Security solutions (25-30%)** | |
| Describe basic security capabilities in Azure | |
| • describe Azure DDoS protection |  |
| • describe Azure Firewall |  |
| • describe Web Application Firewall |  |
| • describe Network Segmentation with Azure VNet |  |
| • describe Azure Network Security groups |  |
| • describe Azure Bastion and JIT Access |  |
| • describe the ways Azure encrypts data |  |
| Describe security management capabilities of Azure |  |
| • describe Cloud security posture management (CSPM) |  |
| • describe Microsoft Defender for Cloud |  |
| • describe enhanced security features of Microsoft Defender for Cloud |  |
| • describe security baselines for Azure |  |
| Describe security capabilities of Microsoft Sentinel |  |
| • define the concepts of SIEM and SOAR |  |
| • describe how Microsoft Sentinel provides integrated threat management |  |
| Describe threat protection with Microsoft 365 Defender |  |
| • describe Microsoft 365 Defender services |  |
| • describe Microsoft Defender for Office 365 |  |
| • describe Microsoft Defender for Endpoint |  |
| • describe Microsoft Defender for Cloud Apps |  |
| • describe Microsoft Defender for Identity |  |
| • describe the Microsoft 365 Defender portal |  |
| **Describe the capabilities of Microsoft compliance solutions (25-30%)** | |
| Describe the compliance management capabilities of Microsoft | |
| • describe the offerings of the Service Trust portal | * Compliance Manager: Compliance in Microsoft Purview compliance portal * Trust Documents: security implementation and design information |
| • describe Microsoft’s privacy principles |  |
| Describe the compliance management capabilities of Microsoft 365 |  |
| • describe Microsoft 365 compliance center |  |
| • describe compliance manager |  |
| • describe the use of benefits of compliance score |  |
| Describe information protection and governance capabilities of Microsoft 365 |  |
| • describe data classification capabilities |  |
| • describe the benefits of content and activity explorer |  |
| • describe sensitivity labels |  |
| • describe Data Loss Prevention (DLP) |  |
| • describe Records Management |  |
| • describe Retention Polices and Retention Labels |  |
| Describe insider risk capabilities in Microsoft 365 |  |
| • describe Insider Risk Management |  |
| • describe communication compliance |  |
| • describe information barriers |  |
| Describe resource governance capabilities in Azure |  |
| • describe what Azure Blueprints is |  |
| • describe Azure Policy |  |
| • describe Azure Blueprint |  |
| • describe Azure Purview |  |