MICROSOFT SECURITY, COMPLIANCE, AND IDENTITY

Describe security and compliance concepts & methodologies

- describe the Zero-Trust methodology
- describe the shared responsibilitymodel
- define defense in depth
- describe common threats
- describe encryption
- describe cloud adoption framework

Define identity concepts

- **define identity as the primary security perimeter**
- **define authentication**
- **define authorization**
- **describe what identity providersare**
- **describe what Active Directoryis**
- **describe the concept of Federated services**
- **define common Identity Attacks**

ATS
ATS Learning Solutions

Describe the basic identity services and identity types of Azure AD

- describe what Azure Active Directory is
- describeAzureAD identities (users, devices, groups, serviceprincipals/applications)
- describe what hybrid identity is
- describe the different external identity types (Guest Users)

Describe the authentication capabilities of Azure AD

- **describe the different authentication methods**
- **describe self-service password reset**
- **describe password protection and management capabilities**
- **describe Multi-factor Authentication**
- **describe Windows Hello for Business**

Describe access management capabilities of Azure AD

- describe what conditional accessis
- describe uses and benefits of conditional access
- describe the benefits of Azure AD roles

Describe the identity protection & governance capabilities of Azure AD

- describe what identity governanceis
- describe what entitlement management and access reviews is
- describe the capabilities of PIM
- describe Azure AD IdentityProtection

Describe basic security capabilities in Azure

- describe Azure Network Securitygroups
- describe Azure DDoS protection
- describe what Azure Firewall is
- describe what Azure Bastion is
- describe what Web Application Firewall is
- describe ways Azure encryptsdata

Describe security management capabilities of Azure

- **describe the Azure Securitycenter**
- **describe Azure Secure score**
- **describethebenefitandusecasesofAzureDefender - previouslythecloudworkload protection platform (CWPP)**
- **describe Cloud security posture management (CSPM)**
- **describe security baselines forAzure**

Describe security capabilities of Azure Sentinel

- define the concepts of SIEM, SOAR, XDR
- describe the role and value of Azure Sentinel to provide integrated threat protection

Describe threat protection with Microsoft 365 Defender

- describe Microsoft 365 Defenderservices
- describe Microsoft Defender for Identity (formerly Azure ATP)
- describe Microsoft Defender for Office 365 (formerly Office 365 ATP)
- describe Microsoft Defender for Endpoint (formerly Microsoft Defender ATP)
- describe Microsoft Cloud AppSecurity

Describe security management capabilities of Microsoft 365

- **describe the Microsoft 365 Defender portal**
- **describe how to use Microsoft Secure Score**
- **describe security reports and dashboards**
- **describe incidents and incident management capabilities**

Describe endpoint security with Microsoft Intune

- **describe what Intune is**
- **describe endpoint security with Intune**
- **describe the end point security with the Microsoft End point Manager admin center**

Describe the compliance management capabilities in Microsoft

- **describe the offerings of the Service Trust portal**
- **describe Microsoft's privacy principles**
- **describe the compliance center**
- **describe compliance manager**
- **describe use and benefits of compliance score**

Describe information protection and governance capabilities of Microsoft 365

- **describe data classification capabilities**
- **describe the value of content and activity explorer**
- **describe sensitivity labels**
- **describe Retention Polices and Retention Labels**
- **describe Records Management**
- **describe Data Loss Prevention**

Describe insider risk capabilities in Microsoft 365

- **describe Insider risk managementsolution**
- **describe communication compliance**
- **describe information barriers**
- **describe privileged access management**
- **describe customer lockbox**

Describe the eDiscovery and audit capabilities of Microsoft 365
- **describe the purpose ofeDiscovery**
- **describe the capabilities of the content search tool**
- **describe the core eDiscoveryworkflow**
- **describe the advanced eDiscoveryworkflow**
- **describe the core audit capabilities of M365**
- **describe purpose and value of Advanced Auditing**

Describe resource governance capabilities in Azure
- **describe the use of Azure Resource locks**
- **describe what Azure Blueprintsis**
- **define Azure Policy and describe its use cases**