SC - 401T00 : Information Security Administrator

Course Outline

Implement Information Protection

- **Protect sensitive data in a digital world**
  - Describe challenges in protecting sensitive data across cloud and AI environments
  - Explain how Microsoft Purview enables data classification, labeling, and protection
  - Identify how data loss prevention (DLP) prevents unauthorized data sharing
  - Understand how Insider Risk Management helps detect potential threats
  - Explore security monitoring tools for detecting and responding to data risks
- **Classify data for protection and governance**
  - Explain the importance of data classification for protection and governance
  - Describe how sensitive information types (SITs) classify structured data
  - Explain how trainable classifiers identify unstructured data
  - Create a custom trainable classifier to detect organization-specific content
- **Review and analyze data classification and protection**
  - Interpret Information Protection Reports to assess classification and protection trends
  - Investigate labeled content using Data explorer and Content explorer to identify classification patterns
  - Analyze user activity in Activity explorer to detect policy violations and potential security risks
  - Use Microsoft Purview tools to improve data security, maintain compliance, and refine protection strategies
- **Create and manage sensitive information types**
  - Recognize the difference between built-in and custom sensitivity labels
  - Configure sensitive information types with exact data match-based classification
  - Implement document fingerprinting
  - Create custom keyword dictionaries
- **Create and configure sensitivity labels with Microsoft Purview**
  - Understand the basics of Microsoft Purview sensitivity labels in Microsoft 365
  - Create and publish sensitivity labels to classify and safeguard data
  - Configure encryption settings with sensitivity labels for improved data security
  - Implement auto-labeling for consistent data classification and protection
  - Use the Microsoft Purview data classification dashboard to monitor sensitivity label usage
- **Apply sensitivity labels for data protection**
  - Understand the foundations of sensitivity label integration in Microsoft 365
  - Manage sensitivity label use in Office apps for security compliance
  - Secure Outlook and Teams meetings with sensitivity labels
  - Apply labels to Microsoft 365 Groups, SharePoint, and OneDrive for data

protection

- **Understand Microsoft 365 encryption**
  - Explain how encryption mitigates the risk of unauthorized data disclosure
  - Describe Microsoft data-at-rest and data-in-transit encryption solutions
  - Explain how Microsoft 365 implements service encryption to protect customer data at the application layer
  - Understand the differences between Microsoft managed keys and customer managed keys for use with service encryption
- **Deploy Microsoft Purview Message Encryption**
  - Configure Microsoft Purview Message Encryption for end users
  - Implement Microsoft Purview Advanced Message Encryption

Implement and manage data loss prevention

- **Prevent data loss in Microsoft Purview**
  - Understand the purpose and benefits of Microsoft Purview DLP
  - Plan, design, simulate, and deploy DLP policies
  - Apply Adaptive Protection for dynamic, risk-based data controls
  - Use DLP analytics to improve policy effectiveness
  - Monitor, investigate, and refine policies using alerts and activity tracking
- **Implement endpoint data loss prevention (DLP) with Microsoft Purview**
  - Understand the benefits of endpoint DLP
  - Onboard devices for endpoint DLP
  - Configure endpoint DLP settings
  - Create and manage endpoint DLP policies
- **Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform**
  - Describe the integration of DLP with Microsoft Defender for Cloud Apps
  - Configure policies in Microsoft Defender for Cloud Apps

Implement and manage Microsoft Purview Insider Risk Management

- **Understand Microsoft Purview Insider Risk Management**
  - Define insider risks and their effect on organizations
  - Understand the purpose of Microsoft Purview Insider Risk Management
  - Identify key features like policies, signals, analytics, dashboards, and investigative tools
  - Recognize how these tools detect and address potential risks
  - Explore scenarios that demonstrate effective risk management strategies
- **Prepare for Microsoft Purview Insider Risk Management**
  - Collaborate with stakeholders to prepare for insider risk management
  - Understand what's needed to meet prerequisites for implementation
  - Configure settings to align with compliance and privacy needs
  - Explore how connecting tools and data sources enhances risk management
- **Create and manage Insider Risk Management policies**
  - Explain the purpose of policy templates
  - Identify when to use quick or custom policies
  - Create quick policies for common scenarios
  - Build and configure custom policies for specific risks

  - Update and manage policies as organizational needs change
- **Implement Adaptive Protection in Insider Risk Management**
  - Describe Adaptive Protection and its role in dynamically mitigating risks
  - Configure risk level settings and customize risk levels based on your organization's needs
  - Set up Adaptive Protection with quick or custom setup
  - Manage Adaptive Protection to review policy metrics, track in-scope users, and assess risk levels

Protect data in AI environments

- **Manage AI data security challenges with Microsoft Purview**
  - Understand sensitivity labels in Microsoft 365 Copilot
  - Secure against generative AI data exposure with endpoint DLP
  - Detect generative AI usage with Insider Risk Management
  - Dynamically protect sensitive data with Adaptive Protection
- **Manage compliance with Microsoft Purview for Microsoft 365 Copilot**
  - Audit Copilot interactions within Microsoft 365 using Microsoft Purview
  - Investigate Copilot interactions using Microsoft Purview eDiscovery
  - Manage Copilot data retention with Microsoft Purview Data Lifecycle Management
  - Monitor and mitigate risks in Copilot interactions using Microsoft Purview Communication Compliance
- **Identify and mitigate AI data security risks**
  - Explain the purpose and benefits of Microsoft Purview DSPM for AI
  - Set up and configure DSPM for AI to monitor AI interactions
  - Identify and analyze AI security risks using reports and insights
  - Run and review AI data assessments to detect oversharing risks
  - Apply security policies, such as DLP and sensitivity labels, to protect AI-referenced data

Implement and manage retention in Microsoft Purview

- **Introduction to information security and compliance in Microsoft Purview**
  - Understand the importance of data security and compliance
  - Discuss Microsoft's approach to protecting and managing sensitive data using Microsoft Purview
  - Define key concepts related to data protection, lifecycle management, and compliance
  - Identify Microsoft Purview tools and solutions that support data protection and governance strategies
- **Implement and manage retention with Microsoft Purview**
  - Understand the differences between retention policies and retention labels
  - Configure retention policies
  - Create, publish, and automate retention labels
  - Implement event-based retention
  - Configure adaptive and static scopes
  - Declare items as records and manage them through disposition reviews