Microsoft 365 for Security and Compliance Administrators
(MS-101, SC-200 and SC-400)
Duration: 4 Days

Prerequisites:

Before attending this course, students must have:

- Basic understanding of Microsoft 365 administration
- Fundamental understanding of Microsoft security, compliance, and identity products
- Basic understanding of Windows PowerShell / scripting concepts.
- Completed M365 administrator course such as Messaging, Teams, Security and Compliance, or Collaboration.
- A proficient understanding of DNS.
- A proficient understanding of general IT practices.

Content:

Module 1: Explore security metrics in Microsoft 365

Lessons

- Explore security solutions in Microsoft 365
- Examine Microsoft Secure Score
- Examine Privileged Identity Management
- Examine Azure Identity Protection

Lab:

- Tenant Setup and Privileged Identity Management
- Initialize your Microsoft 365 Tenant
- PIM Resource Workflows

Module 2: Manage your Microsoft 365 security services

Lessons

- Examine Exchange Online Protection

- Examine Microsoft Defender for Office 365
- Manage Safe Attachments
- Manage Safe Links
- Explore reporting in the Microsoft 365 security services

Lab:

- Implement a Safe Attachments policy
- Implement a Safe Links policy
- Guided demo for Microsoft defender for Office 365

Module 3: Implement threat intelligence in Microsoft 365

Lessons

- Explore the Security Dashboard
- Implement Microsoft Defender for Identity
- Implement Microsoft Cloud Application Security

Lab:

- Conduct a Spear Phishing attack using the Attack Simulator
- Conduct Password attacks using the Attack Simulator
- Prepare for Alert Policies
- Implement a Mailbox Permission Alert
- Implement a SharePoint Permission Alert
- Guided Demo for Microsoft Defender for Identity
- Guided Demo for Microsoft Cloud Application Security

Module 4: Introduction to Data Governance in Microsoft 365

Lessons

- Explore archiving in Microsoft 365
- Explore retention in Microsoft 365
- Explore Information Rights Management
- Explore Office 365 Message Encryption

Lab:

- Configure Microsoft 365 Message Encryption
- Validate Information Rights Management
- Configure Retention Tags and Policies

Module 5: Implement data governance in Microsoft 365

Lessons

- Implement compliance solutions
- Create information barriers in Microsoft 365
- Create a DLP policy from a built-in template
- Create a custom DLP policy
- Create a DLP policy to protect documents
- Implement policy tips for DLP policies

Lab:

- Manage DLP Policies
- Test MRM and DLP Policies
- Guided demo for Insider Risk Management

Module 6: Manage data governance in Microsoft 365

Lessons

- Explore sensitivity labels
- Implement sensitivity labels
- Implement Data Governance

Lab:

- Implement sensitivity labels

Module 7: Manage content search and investigations in Microsoft 365

Lessons

- Search for content in the Microsoft 365 Compliance center
- Conduct audit log investigations
- Manage Advanced eDiscovery

Lab:

- Conduct a data search
- Investigate Your Microsoft 365 Data

Module 8: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

Lessons

- Construct KQL statements for Microsoft Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with data in Microsoft Sentinel using Kusto Query Language

Lab:

- Create queries for Microsoft Sentinel using Kusto Query Language (KQL)