MS-500: Microsoft 365 Security Admin, Part 3 of 4: Implement & Manage Information Protection

Meet the expert: Cristian Calinescu is a Microsoft certified Azure Solutions Architect Expert, Senior Infrastructure Engineer and Infrastructure Security Operations Manager.

Prerequisites: Candidates for this exam are familiar with Microsoft 365 workloads and have strong skills and experience with identity protection, information protection, threat protection, security management, and data governance.

Runtime: 05:04:32

Course description: Candidates for this (MS-500) exam implement, manage, and monitor security and compliance solutions for Microsoft 365 and hybrid environments.The Microsoft 365 Security Administrator proactively secures M365 enterprise environments, responds to threats, performs investigations, and enforces data governance. This course covers Domain 3 of the exam, which is 15-20% of the test. Knowledge covered includes:

Cloud Application Security, Information Protection, Rights Management and Encryption, Data Loss Prevention.

Course outline:

Deploy Cloud Application Security
- Introduction
- Deploy Cloud Application Security
- Cloud App Security
- Deploy Cloud App Security
- Control Cloud Apps with Policies
- App Connectors
- Use Cloud App Security Information
- Risk Score
- Manage Alerts
- Summary

Information Protection Concepts
- Introduction
- Information Protection Concepts
- Information Protection Lifecycle
- Digital Estate
- Classification Journey
- Sensitivity Labels
- Sensitivity Label Policies
- Create Sensitivity Labels and Policies
- Demo: Classification
- Sensitivity labels and Information Protection
- Summary

Archiving in Microsoft 365
- Introduction
- Archiving in Microsoft 365
- Archiving in 365
- Archiving in Exchange
- Records Management
- Summary

Retention in Microsoft 365
- Introduction
- Retention in Microsoft 365
- Retention Policies
- Messaging Records Management in Exchange
- Retention Tags
- Calculate Retention
- Summary

Retention Policies in Compliance Center
- Introduction
- Retention Policies in Compliance Center
- Retention Explained
- Retention Labels with Policies
- Demo: Retention
- Event Driven Retention
- Summary

Archiving and Retention in Exchange
- Introduction
- Archiving and Retention in Exchange
- Create Retention Tags
- Demo: Create Retention tags
- In-place Records Management in SharePoint
- Records Management
- Benefits of Record Management
- Demo: Records Management
- Summary

Information Rights Management (IRM)
- Introduction
- Information Rights Management (IRM)
- Information Rights Management
- Encryption Options
- Rights Management in Exchange
- Applying IRM Protection to Email
- Rights Management in Sharepoint
- Applying IRM Protection
- Summary

Secure Multi-purpose Internet Mail Extension
- Introduction
- Secure Multi-purpose Internet Mail Extension
- S-MIME Explained
- Applying Digital Signatures
- S-MIME Messages
- Digital Signatures and Encryption
- Triple Wrapped Messages
- Summary

Office 365 Message Encryption
- Introduction
- Office 365 Message Encryption
- Message Encryption Explained
- How Encryption Works
- Working with Encrypted Emails
- Summary

DLP Fundamentals
- Introduction
- DLP Fundamentals
- DLP Capabilities
- Sensitve Information
- Conditions and Actions
- Policy Tips
- Policy Templates
- Use DLP Policies
- Summary

Create a DLP Policy
- Introduction
- Create a DLP Policy
- Demo: DLP
- Customize a DLP policy
- Demo: Customize DLP
- Summary

Create a DLP Policy to protect documents
- Introduction
- Create a DLP Policy to protect documents
- Demo: Create Managed Property
- Policy Tips
- Policy Tips in Email
- Policy Tips in Office
- Summary