MS-500: Microsoft 365 Security Admin, Part 2 of 4: Implement and Manage Threat 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: 05:32:50

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 2 of the exam, which is 20-25% of the test. The knowledge covered include: Security in Microsoft 365, Threat Protection, Threat Management and Mobility.

Course outline:

Threat Vectors and Data Breaches
- Introduction
- Threat Vectors and Data Breaches
- The Workplace and Threat Landscape
- Phishing
- Spoofing
- Spam and Malware
- Account Breach
- Data Exfiltration
- Data Deletion
- Coin Mining
- Other Attacks
- Summary

Security Strategy and Principles
- Introduction
- Security Strategy and Principles
- Security Principles
- Measuring Security Success
- Defenders Dilemma
- Raise Attackers Cost
- Microsoft Security Solutions
- Security Center
- Demo: Security Center
- Exchange Online Protection
- Cloud Application Security
- Summary

Secure Score
- Introduction
- Secure Score
- Secure Score Explained
- Demo: Secure Score Dashboard
- Secure Score API
- Improve Scurity Posture
- Summary

Exchange Online Protection (EOP)
- Introduction
- Exchange Online Protection (EOP)
- Anti-Malware Pipeline
- Zero-Hour Auto Purge
- Spoof Intelligence
- Manage Spoof Intelligence
- Demo: Spoof
- Summary

Office 365 Advanced Threat Protection
- Introduction
- Office 365 Advanced Threat Protection
- ATP Expands on Exchange Online Protection
- Safe Attachments
- Safe Links
- ATP for SharePoint and OneDrive
- Manage Safe Attachments
- Safe Attachment Policies
- Demo: Create Safe Attachment Policy
- Create with PowerShell
- Demo: Modify policy
- End-user Experience with Safe Attachments
- Summary

Manage Safe Links
- Introduction
- Manage Safe Links
- Demo: Create Safe Links
- Create Safe Link Policies with PowerShell
- Demo: Modify Safe Links
- End-User Experience with Safe Links
- Summary

Azure Advanced Threat Protection
- Introduction
- Azure Advanced Threat Protection
- Azure ATP Explained
- Demo: Azure ATP
- Summary

Microsoft Defender Advanced Threat Protection
- Introduction
- Microsoft Defender Advanced Threat Protection
- Defender ATP Explained
- Configure Defender ATP
- Defender ATP with security Center
- Defender Application Control
- Demo: Windows Defender
- Security Configuration Framework
- Summary

Security Dashboard
- Introduction
- Security Dashboard
- Threat Dashboard
- Demo: Threats
- More Insights
- Demo: Alert
- Threat Investigation and Response
- Threat Explorer
- Demo: threat Explorer
- Automated Investigation Response
- Demo: Automated Investigation Response
- Graph Security API
- Summary

Azure Sentinel
- Introduction
- Azure Sentinel
- Sentinel Overview
- Connect Data Sources
- Analytics
- Demo: Sentinel
- Summary

Mobile Application Management (MAM)
- Introduction
- Mobile Application Management (MAM)
- Mobile Application Management
- Using Configuration Manager
- Application Considerations
- Mobile Device Management (MDM)
- Compare MDM and Intune
- Policy Settings for Mobile Devices
- Control Email and Document Access
- Demo: Control Access
- Summary

Deploy Mobile Device Services
- Introduction
- Deploy Mobile Device Services
- Activate MDM Services

(Continued on page 2)

MS-500: Microsoft 365 Security Admin, Part 2 of 4: Implement and Manage Threat Protection

- Deploy MDM
- Configure APN Certificate for IOS
- Define Corporate Device Enrollment Policy
- Enroll Devices to MDM
- Enroll Windows 10 and Android Devices
- Demo: Enrollment
- Enrollment Rules
- Multi-Factor Authentication Considerations
- Summary