Module 1: Windows Defender ATP

- The Role of Windows Defender ATP
- Windows Defender ATP Architecture
- How Windows Defender ATP helps detect sophisticated threats?
- What Else Can Windows Defender ATP Do for Us?
- Requirements and initial steps
- Manage Windows Defender ATP capabilities
- Troubleshoot Windows Defender ATP

Module 2: Threat & Vulnerability Management (LAB)

- Next-generation capabilities
- Dashboard Overview and what it means for my organization
- Configuration score
- Scenarios
- Reduce your Threat and Vulnerability Exposure Tamp
- Improve your Security Configuration

Module 3: Attack surface reduction (LAB)

- Hardware-based isolation
- Application isolation
- System requirements
- System integrity
- Application control
- Exploit protection
- Network protection
- Controlled folder access
- Credential Guard
- Attack surface reduction
- Network firewall

Module 4: Endpoint detection and response (LAB)

- Security operations dashboard
- Manage incidents
- Manage alerts
- Manage machine group and tags
- Take response actions on a machine
- Run antivirus scan
- Restrict app execution
- Check activity details in Action center
- Stop and quarantine files in your network

Module 5: Automated investigation and remediation (LAB)

• Overview of Automated investigations
• Understand the Automated investigation flow
• Details of an Automated investigation
• How an Automated investigation expands its scope
• How threats are remediated

Module 6: Advanced hunting

• Overview of advanced hunting
• Query data using Advanced hunting
• Advanced hunting reference
• Advanced hunting query language best practices
• Custom detections
• Create custom detections rules

****

****

Module 7: Intune Device Enrollment

In this module, students will examine the benefits and prerequisites for co-management and learn how to plan for it. This module will also cover Azure AD join and will be introduced to Microsoft Intune, as well as learn how to configure policies for enrolling devices. The module will conclude with an overview of device inventory in Intune and reporting using the Intune console, Power BI and Microsoft Graph.

Lessons

- Device management and Tamper Protection
- Microsoft Intune Overview
- Manage Intune device enrollment and inventory
- Managing devices with Intune

Practice Lab - Device Enrollment and Management

Module 8: Configuring Profiles

This module dives deeper into Intune device profiles including the types of device profiles and the difference between built-in and custom profiles. The student will learn about assigning profiles to Azure AD groups and monitoring devices and profiles in Intune. The module will conclude with an overview of using Windows Analytics for health and compliance reporting.

Lessons

- Configuring and controlling device by using profiles
- Managing user profiles
- Monitoring devices

Practice Lab - Managing profiles

Module 9: Managing Authentication in Azure AD

In this module, students well be introduced to the concept of directory in the cloud with Azure AD. Students will learn the similarities and differences between Azure AD and Active Directory DS and how to synchronize between the two. Students will explore identity management in Azure AD and learn about identity protection using Windows Hello for Business, as well as Azure AD Identity Protection and multi-factor authentication.

Lessons

- Azure AD Overview
- Managing identities in Azure AD
- Protecting identities in Azure AD
- Managing device authentication

Practice Lab - Managing objects and authentication in Azure AD

Module 10: Managing Device Access and Compliance

In this module, students will be introduced to managing device security. The module will cover securely accessing corporate resources and introduce concepts such as Always On VPN and remote connectivity in Windows 10. Students will learn how to create and deploy compliance policies and use compliance policies for conditional access. The module concludes with monitoring devices enrolled in Intune.

Lessons

- Microsoft Intune Overview
- Implement device compliance policies

Practice Lab - Managing Access and Compliance

Module 11: Integration with SCCM (Demo Only)

- Understanding SCCM Roles
- Understanding SCCM Agents
- Defender ATP and Intune based Policy Integration

==========END==========