SC-5004: Defend against cyberthreats with Microsoft Defender XDR

Course Outline

1. **Mitigate incidents using Microsoft Defender**
   - Manage incidents in Microsoft Defender
   - Investigate incidents in Microsoft Defender
   - Conduct advanced hunting in Microsoft Defender

2. **Deploy the Microsoft Defender for Endpoint environment**
   - Create a Microsoft Defender for Endpoint environment
   - Onboard devices to be monitored by Microsoft Defender for Endpoint
   - Configure Microsoft Defender for Endpoint environment settings

3. **Configure for alerts and detections in Microsoft Defender for Endpoint**
   - Configure alert settings in Microsoft Defender for Endpoint
   - Manage indicators in Microsoft Defender for Endpoint

4. **Configure and manage automation using Microsoft Defender for Endpoint**
   - Configure advanced features of Microsoft Defender for Endpoint
   - Manage automation settings in Microsoft Defender for Endpoint

5. **Perform device investigations in Microsoft Defender for Endpoint**
   - Use the device page in Microsoft Defender for Endpoint
   - Describe device forensics information collected by Microsoft Defender for Endpoint
   - Describe behavioral blocking by Microsoft Defender for Endpoint

6. **Defend against Cyberthreats with Microsoft Defender XDR lab exercises**
   - Configure the Microsoft Defender XDR environment
   - Deploy Microsoft Defender for Endpoint
   - Mitigate threats using Microsoft Defender for Endpoint
   - Investigate and respond to incidents using Microsoft Defender XDR

SpireTec Solutions