SKILLS GAINED

- Explain how Microsoft Defender for Endpoint can remediate risks in your environment
- Administer a Microsoft Defender for Endpoint environment
- Configure Attack Surface Reduction rules on Windows devices
- Perform actions on a device using Microsoft Defender for Endpoint
- Investigate domains and IP addresses in Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint
- Configure alert settings in Microsoft 365 Defender
- Explain how the threat landscape is evolving
- Conduct advanced hunting in Microsoft 365 Defender
- Manage incidents in Microsoft 365 Defender
- Explain how Microsoft Defender for Identity can remediate risks in your environment
- Investigate DLP alerts in Microsoft Defender for Cloud Apps
- Explain the types of actions you can take on an insider risk management case
- Configure auto-provisioning in Microsoft Defender for Cloud Apps
- Remediate alerts in Microsoft Defender for Cloud Apps
- Construct KQL statements
- Filter searches based on event time, severity, domain, and other relevant data using KQL
- Extract data from unstructured string fields using KQL
- Manage a Microsoft Sentinel workspace
- Use KQL to access the watchlist in Microsoft Sentinel
- Manage threat indicators in Microsoft Sentinel
- Explain the Common Event Format and Syslog connector differences in Microsoft Sentinel
- Connect Azure Windows Virtual Machines to Microsoft Sentinel
- Configure Log Analytics agent to collect Sysmon events
- Create new analytics rules and queries using the analytics rule wizard
- Create a playbook to automate an incident response
- Use queries to hunt for threats
- Observe threats over time with livestream