SC-5004 Defend against cyberthreats with Microsoft Defender XDR

Category: Networking & Security | **Vendor:** Microsoft Technical

Duration: 8.00 hours (1 days) **6.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Microsoft Applied Skills: Defend against cyberthreats with Microsoft Defender XDR
Related Exam:	SC-5004

Course Overview

Implement the Microsoft Defender for Endpoint environment to manage devices, perform investigations on endpoints, manage incidents in Defender XDR, and use Advanced Hunting with Kusto Query Language (KQL) to detect unique threats.

About This Course

Implement the Microsoft Defender for Endpoint environment to manage devices, perform investigations on endpoints, manage incidents in Defender XDR, and use Advanced Hunting with Kusto Query Language (KQL) to detect unique threats.

Who Should Attend

Prerequisites & Entry Requirements

General Prerequisites:

- Experience using the Microsoft Defender portal
- Basic understanding of Microsoft Defender for Endpoint
- Basic understanding of Microsoft Sentinel
- Experience using Kusto Query Language (KQL) in Microsoft Sentinel

Learning Outcomes

Upon successful completion of this course, participants will be able to:

Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender

XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's

advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint

monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with

advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender

XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution., Course ObjectivesMitigate security incidents using Microsoft Defender.Investigate and manage incidents with advanced hunting tools.Deploy and configure Microsoft Defender for Endpoint environments.Onboard devices and manage endpoint monitoring.Configure alert settings and manage indicators in Microsoft Defender.Automate security responses using Microsoft Defender's advanced features.Perform device investigations and analyze forensic data.Conduct lab exercises to implement a full Microsoft Defender XDR solution.

Detailed Course Outline

1 - Mitigate incidents using Microsoft Defender

- Use the Microsoft Defender portal
- Manage incidents
- Investigate incidents
- Manage and investigate alerts
- Manage automated investigations
- Use the action center
- Explore advanced hunting
- Investigate Microsoft Entra sign-in logs
- Understand Microsoft Secure Score
- Analyze threat analytics
- Analyze reports
- Configure the Microsoft Defender portal

2 - Deploy the Microsoft Defender for Endpoint environment

- Create your environment
- Understand operating systems compatibility and features
- Onboard devices
- Manage access
- Create and manage roles for role-based access control
- Configure device groups
- Configure environment advanced features

3 - Configure for alerts and detections in Microsoft Defender for Endpoint

- Configure advanced features
- Configure alert notifications
- Manage alert suppression
- Manage indicators

4 - Configure and manage automation using Microsoft Defender for Endpoint

- Configure advanced features
- Manage automation upload and folder settings
- Configure automated investigation and remediation capabilities
- Block at risk devices

5 - Perform device investigations in Microsoft Defender for Endpoint

- Use the device inventory list
- Investigate the device
- Use behavioral blocking
- Detect devices with device discovery

6 - Defend against Cyberthreats with Microsoft Defender XDR lab exercises

- Configure the Microsoft Defender XDR environment
- Deploy Microsoft Defender for Endpoint
- Mitigate Attacks with Microsoft Defender for Endpoint

, Mitigate incidents using Microsoft Defender, Deploy the Microsoft Defender for Endpoint environment, Configure for alerts and detections in Microsoft Defender for Endpoint, Configure and manage automation using Microsoft Defender for Endpoint, Perform device investigations in Microsoft Defender for Endpoint, Defend against Cyberthreats with Microsoft Defender XDR lab exercises

□□ Certification Path

Microsoft Applied Skills: Defend against cyberthreats with Microsoft Defender XDR

Exam: SC-5004

Upcoming Schedule

Available training dates for SC-5004 Defend against cyberthreats with Microsoft Defender XDR:

Start Date	End Date	Location	Delivery	Price
21 Dec 2026	21 Dec 2026	Online	Virtual	€695.00

Frequently Asked Questions

Q: What delivery options are available for SC-5004 Defend against cyberthreats with Microsoft Defender XDR?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The SC-5004 Defend against cyberthreats with Microsoft Defender XDR course helps prepare you for the Microsoft Applied Skills: Defend against cyberthreats with Microsoft Defender XDR certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the SC-5004 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 1-day SC-5004 Defend against cyberthreats with Microsoft Defender XDR course provides up to 6.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the SC-5004 Defend against cyberthreats with Microsoft Defender XDR training?

The training takes place over 1 day(s), with each day lasting approximately 8.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for SC-5004 Defend against cyberthreats with Microsoft Defender XDR?

Yes, we provide corporate training, dedicated training, and closed classes for SC-5004 Defend against cyberthreats with Microsoft Defender XDR. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: SC-5004: Defend against cyberthreats with Microsoft Defender XDR, Microsoft, vILT, SC-5004

Q: Why choose Nexus Human for SC-5004 Defend against cyberthreats with Microsoft Defender XDR?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your SC-5004 Defend against cyberthreats with Microsoft Defender XDR training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)