MICROSOFT TRAINING

Microsoft Defender For Endpoint Training Course

Master Microsoft Defender for Endpoint to secure organizational devices and respond to advanced cyber threats effectively.

DURATION
2 hours

LEVEL
Intermediate

FORMAT
Instructor-Led

- Globally Recognized Certification
- Expert-Led Hands-On Training
- Flexible Scheduling

Computer Pride | 1st Floor, ICEA Building, Kenyatta Avenue, Nairobi | www.computer-pride.co.ke

COURSE OVERVIEW

Elevate your cybersecurity expertise with our intensive Microsoft Defender for Endpoint (MDE) Training Course. This intermediate-level program is meticulously designed for IT professionals aiming to master the robust capabilities of Microsoft's unified endpoint security platform. You will gain hands-on experience in deploying, configuring, and managing MDE to effectively protect an organization's endpoints from advanced threats. The course delves into the core technologies that underpin MDE, including next-generation protection, endpoint detection and response (EDR), threat and vulnerability management, and automated investigation and remediation.

Upon completion, you will possess the critical skills to enhance an organization's security posture significantly. This training will enable you to proactively identify vulnerabilities, detect sophisticated cyberattacks, investigate security incidents with precision, and automate response actions across a diverse range of devices. By mastering MDE, you will not only safeguard critical assets but also streamline security operations, making you an invaluable asset in today's threat landscape. This course is your pathway to becoming a proficient defender against modern cyber threats, bolstering your career prospects in the rapidly evolving field of cybersecurity.

Duration	2 hours
Level	Intermediate
Vendor	Microsoft

COURSE CURRICULUM

01 Module 1: Introduction to Microsoft Defender for Endpoint

- Overview of MDE architecture and components
- Understanding MDE capabilities: Prevention, Detection, Investigation, Response
- Integration with other Microsoft 365 Defender services
- Licensing and deployment considerations

02 Module 2: Deployment and Configuration

- Onboarding endpoints to MDE (GPO, SCCM, Intune, Script)
- Configuring device groups and roles
- Managing security settings with security policies
- Customizing data retention and privacy settings

03 Module 3: Threat and Vulnerability Management (TVM)

- Understanding TVM dashboard and recommendations
- Discovering and assessing software vulnerabilities
- Prioritizing and remediating security weaknesses
- Implementing attack surface reduction rules

04 Module 4: Endpoint Detection and Response (EDR)

- Analyzing MDE alerts and incidents
- Using the incident graph for investigations
- Performing advanced hunting with Kusto Query Language (KQL)
- Understanding behavioral blocking and containment

05 Module 5: Investigation and Remediation

- Automated investigation and remediation capabilities
- Manual investigation steps and tools
- Taking response actions (isolate device, run antivirus scan, collect investigation package)
- Managing exclusions and false positives

06 Module 6: Reporting and Integration

- Generating security reports and analytics
- Integrating MDE with Microsoft Sentinel and other SIEM solutions
- API integration for custom solutions
- Best practices for MDE management and maintenance

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Security Operations Center (SOC) Analyst L2/L3**

> **Cybersecurity Incident Responder**

> **Microsoft 365 Security Administrator**

FREQUENTLY ASKED QUESTIONS

Q: What foundational Microsoft security knowledge or certifications are recommended before taking this MDE training?

While not strictly mandatory, having a basic understanding of Windows operating systems, networking fundamentals, and core cybersecurity concepts is highly beneficial. Familiarity with Microsoft 365 administration or having completed the SC-900 Microsoft Security, Compliance, and Identity Fundamentals course would provide an excellent foundation for maximizing your learning in this intermediate-level MDE training.

Q: How will completing this course help me improve my organization's overall endpoint security posture directly?

This course will equip you with the practical skills to deploy and fine-tune Microsoft Defender for Endpoint, enabling you to proactively identify and remediate vulnerabilities, configure robust threat prevention policies, detect sophisticated attacks in real-time using EDR capabilities, and automate incident response. You will learn to leverage MDE's full suite of features to minimize attack surfaces, prevent breaches, and enhance your organization's resilience against evolving cyber threats.

Q: Beyond technical skills, what career opportunities does a strong understanding of Microsoft Defender for Endpoint unlock or enhance?

A strong grasp of MDE significantly enhances your profile for roles in cybersecurity operations, incident response, and security administration. It positions you as a specialist capable of managing a critical component of modern enterprise security, leading to opportunities as a Security Operations Center (SOC) Analyst, Cybersecurity Incident Responder, or a dedicated Microsoft 365 Security Administrator. This expertise is highly valued as organizations increasingly rely on Microsoft's unified security ecosystem.

ABOUT COMPUTER PRIDE

East Africa's Premier IT Training Center

With over 15 years of excellence, Computer Pride delivers globally recognized certification programs from leading technology vendors. Located on Kenyatta Avenue in Nairobi's CBD, our state-of-the-art facilities and expert instructors have empowered thousands of professionals across East Africa.

15+	10,000+	50+
Years of Excellence	Professionals Trained	Vendor Certifications

READY TO ENROL?

Take the next step in your technology career.

Location
1st Flr, ICEA Building
Kenyatta Ave, Nairobi

Email
info@computer-pride.co.ke

Phone
+254 705 900 900

www.computer-pride.co.ke