Endpoint Security and Device Management Basics Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Endpoint Security and Device Management Basics Training Course offers a foundational understanding of Endpoint Security and Unified Device Management (UDM), which are critical disciplines in the current climate of sophisticated cyber threats and dispersed workforces. Endpoints from laptops and mobile devices to servers and IoT represent the new security perimeter, making their protection paramount. The program dives into Zero Trust principles, Endpoint Detection and Response (EDR), and Mobile Device Management (MDM), equipping IT professionals with the practical, hands-on skills needed to implement, configure, and maintain a robust, modern security posture against evolving risks like Ransomware and Insider Threats. This knowledge is essential for ensuring regulatory compliance and business continuity in any enterprise environment.

The curriculum is engineered for immediate applicability, focusing on real-time threat hunting, security automation, and adherence to industry best practices like the MITRE ATT&CK Framework. Participants will gain expertise in asset inventory, patch management, and configuration baselining across diverse operating systems, culminating in the ability to design and manage a cohesive Security Operations Center (SOC) strategy for endpoints. By mastering these core competencies, IT and security teams can effectively reduce the organizational attack surface, improve incident response time, and leverage cloud-native tools to provide seamless, secure access for a hybrid workforce, ultimately becoming vital protectors of critical enterprise data and infrastructure.

Programme Curriculum

Endpoint Security and Device Management Basics Training Course

Introduction

Endpoint Security and Device Management Basics Training Course offers a foundational understanding of Endpoint Security and Unified Device Management (UDM), which are critical disciplines in the current climate of sophisticated cyber threats and dispersed workforces. Endpoints from laptops and mobile devices to servers and IoT represent the new security perimeter, making their protection paramount. The program dives into Zero Trust principles, Endpoint Detection and Response (EDR), and Mobile Device Management (MDM), equipping IT professionals with the practical, hands-on skills needed to implement, configure, and maintain a robust, modern security posture against evolving risks like Ransomware and Insider Threats. This knowledge is essential for ensuring regulatory compliance and business continuity in any enterprise environment.

The curriculum is engineered for immediate applicability, focusing on real-time threat hunting, security automation, and adherence to industry best practices like the MITRE ATT&CK Framework. Participants will gain expertise in asset inventory, patch management, and configuration baselining across diverse operating systems, culminating in the ability to design and manage a cohesive Security Operations Center (SOC) strategy for endpoints. By mastering these core competencies, IT and security teams can effectively reduce the organizational attack surface, improve incident response time, and leverage cloud-native tools to provide seamless, secure access for a hybrid workforce, ultimately becoming vital protectors of critical enterprise data and infrastructure.

Course Duration

5 days

Course Objectives

1. Implement a Zero Trust Architecture (ZTA) framework for endpoint access and data protection.
2. Configure Next-Generation Endpoint Detection and Response (NG-EDR) solutions for advanced threat visibility.
3. Perform Threat Hunting and analysis using the MITRE ATT&CK Framework and security telemetry.
4. Master Unified Endpoint Management (UEM) platforms for seamless policy enforcement across diverse OSs.
5. Develop robust Mobile Device Management (MDM) and Mobile Application Management (MAM) policies.
6. Execute proactive Vulnerability Management and automated Patch Management workflows.
7. Harden Windows, macOS, and Linux endpoints using industry-standard Security Baselines and GPOs.
8. Analyze endpoint security alerts and logs in a Security Information and Event Management (SIEM) system.
9. Formulate effective Ransomware Protection and Data Loss Prevention (DLP) strategies for endpoints.
10. Apply Cloud-Native Security principles for protecting remote and hybrid workforce devices.
11. Differentiate between, and implement, various Authentication and Access Control mechanisms like MFA and Conditional Access.
12. Investigate and respond to common Insider Threats and fileless malware attacks.
13. Ensure ongoing Security Compliance through audited device configuration.

Target Audience

1. IT Administrators and System Engineers responsible for device maintenance.
2. Security Analysts and SOC Team Members new to endpoint defense.
3. Cybersecurity Professionals looking to specialize in endpoint and device management.
4. Network Administrators and Operations staff involved in corporate device connectivity.
5. Compliance and Audit Officers needing to understand device security controls.
6. Help Desk/Support Staff who troubleshoot endpoint security issues.

7. Cloud Architects implementing security for hybrid work environments.
8. Security Managers overseeing endpoint protection strategy and tool selection.

Course Modules

Module 1: Foundational Concepts and the Evolving Perimeter

- Defining the Modern Endpoint.
- The CIA Triad and the New Security Perimeter
- Endpoint Threats.
- Introduction to the Zero Trust Architecture Model.
- Case Study: Analysis of a major corporate Ransomware attack that exploited a single unmanaged remote laptop, detailing the initial access and lateral movement.

Module 2: Device Hardening and Security Baselines

- Implementing Security Baselines for Windows, macOS, and Linux.
- Configuring Host-based Firewalls, Disk Encryption
- Disabling unnecessary services and enforcing least-privilege access.
- Advanced settings like Windows Attack Surface Reduction Rules.
- Case Study: The successful hardening project of a Financial Services Firm that used a standardized security baseline rollout to achieve PCI DSS compliance across 5,000 corporate endpoints.

Module 3: Unified Endpoint Management (UEM) Essentials

- Overview of UEM platforms
- Device Enrollment, Inventory, and Configuration Profile Management.
- Policy Creation and Enforcement
- Remote Wipe, Lock, and Data Segregation techniques.
- Case Study: A Global Retailer's implementation of a UEM solution to centrally manage 10,000+ Point-of-Sale devices, corporate laptops, and employee BYOD assets from a single console.

Module 4: Mobile Device Security

- Distinction between Mobile Device Management and Mobile Application Management (MAM).
- Securing BYOD and Corporate-Owned devices.
- App Wrapping, Containerization, and Conditional Access for mobile apps.
- Secure Mobile Gateways and establishing mobile VPNs.
- Case Study: A Healthcare Provider's use of MAM to secure protected health information accessed via employee personal smartphones, ensuring HIPAA compliance without taking full device control.

Module 5: Endpoint Detection and Response

- Understanding the shift from traditional Antivirus to NG-EDR.
- Core EDR capabilities.
- Utilizing MITRE ATT&CK techniques for analyzing threat actor behavior.
- Automated Incident Response
- Case Study: How a Tech Startup utilized an EDR platform to detect and neutralize a sophisticated, multi-stage fileless malware attack that bypassed their legacy perimeter defenses.

Module 6: Threat Hunting and Advanced Analysis

- Developing proactive Threat Hunting hypotheses and playbooks.
- Analyzing endpoint telemetry data
- Using YARA rules and Sigma rules for custom threat signature creation.
- Integrating EDR data with SIEM systems for correlation and alerting.
- Case Study: A Cybersecurity Firm's successful Threat Hunting engagement where they uncovered a long-term Insider Threat using anomalous process execution data and logon history.

Module 7: Vulnerability and Patch Management

- The importance of a coordinated Vulnerability Management program.
- Automating the Patch Management lifecycle
- Handling unpatchable or legacy "Shadow IT" devices.
- Strategies for rapid patching of zero-day vulnerabilities.
- Case Study: A large University's rapid response to a critical zero-day vulnerability using automated patch deployment to secure thousands of diverse endpoints within a 48-hour window.

Module 8: Compliance, Governance, and Future Trends

- Aligning endpoint security with Data Loss Prevention strategy.
- Reporting and Auditing for Regulatory Compliance
- The rise of Extended Detection and Response and AI/ML in security.
- Developing a mature Incident Response Plan for endpoint breaches.
- Case Study: A global Manufacturing Company that successfully passed a demanding compliance audit by demonstrating full, verifiable control and encryption of all its engineering and employee endpoints.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com