Training Course on Endpoint Detection and Response for Threat Hunting

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's hyper-connected digital landscape, traditional perimeter defenses are no longer sufficient against sophisticated cyber adversaries. Organizations face an unprecedented volume of **advanced persistent threats (APTs)**, **ransomware attacks**, and **zero-day exploits** that bypass conventional security measures. Training Course on Endpoint Detection and Response for Threat Hunting empowers cybersecurity professionals to proactively **hunt threats**, **investigate incidents**, and **fortify organizational resilience**. By leveraging EDR platforms, participants will gain critical skills in **real-time visibility**, **behavioral analytics**, and **automated response**, transforming their security posture from reactive to proactive.

This program dives deep into the practical application of EDR in **threat hunting operations**, focusing on **actionable intelligence** and **proactive defense strategies**. Participants will learn to navigate the complexities of endpoint telemetry, identify subtle **indicators of compromise (IOCs)** and **tactics, techniques, and procedures (TTPs)**, and effectively contain and remediate evolving threats. The curriculum emphasizes **hands-on labs** and **real-world case studies** to ensure participants develop the practical expertise required to defend against the most challenging cyberattacks in the current and future threat landscape, including the rising tide of **AI-powered threats** and **supply chain vulnerabilities**.

Programme Curriculum

Training Course on Endpoint Detection and Response for Threat Hunting

Introduction

In today's hyper-connected digital landscape, traditional perimeter defenses are no longer sufficient against sophisticated cyber adversaries. Organizations face an unprecedented volume of **advanced persistent threats (APTs)**, **ransomware attacks**, and **zero-day exploits** that bypass conventional security measures. Training Course on Endpoint Detection and Response for Threat Hunting

empowers cybersecurity professionals to proactively **hunt threats**, **investigate incidents**, and **fortify organizational resilience**. By leveraging EDR platforms, participants will gain critical skills in **real-time visibility**, **behavioral analytics**, and **automated response**, transforming their security posture from reactive to proactive.

This program dives deep into the practical application of EDR in **threat hunting operations**, focusing on **actionable intelligence** and **proactive defense strategies**. Participants will learn to navigate the complexities of endpoint telemetry, identify subtle **indicators of compromise (IOCs)** and **tactics, techniques, and procedures (TTPs)**, and effectively contain and remediate evolving threats. The curriculum emphasizes **hands-on labs** and **real-world case studies** to ensure participants develop the practical expertise required to defend against the most challenging cyberattacks in the current and future threat landscape, including the rising tide of **AI-powered threats** and **supply chain vulnerabilities**.

Course Duration

10 days

Course Objectives

1. Comprehend the core architecture, capabilities, and deployment models of leading EDR solutions.
2. Develop advanced methodologies for proactively searching for dormant and active threats across enterprise endpoints, leveraging **MITRE ATT&CK Framework**.
3. Lead efficient and effective incident response lifecycles, from **detection to eradication and recovery**, utilizing EDR telemetry.
4. Analyze endpoint behavioral data to identify **anomalous activities** and **malicious patterns** indicative of advanced threats.
5. Utilize EDR platforms for in-depth **digital forensics** to reconstruct attack timelines and identify root causes.
6. Understand basic **malware analysis** techniques relevant to EDR investigations and **threat intelligence generation**.
7. Secure endpoints within **hybrid and multi-cloud environments**, addressing unique challenges and **cloud security best practices**.
8. Implement **automated containment and remediation strategies** within EDR platforms to minimize breach impact.
9. Integrate and operationalize **cyber threat intelligence (CTI)** feeds with EDR for enhanced detection and proactive defense.
10. Identify and mitigate **supply chain attack vectors** targeting endpoints, aligning with modern security operations.
11. Apply **Zero Trust security models** to endpoint protection, emphasizing continuous verification and least privilege.
12. Understand the role of **Artificial Intelligence (AI) and Machine Learning (ML)** in enhancing EDR capabilities and detecting novel threats.
13. Generate EDR-driven reports for **regulatory compliance** (e.g., GDPR, HIPAA) and audit trails.

Organizational Benefits

- Proactive identification and neutralization of advanced threats, reducing the mean time to detect (MTTD) and mean time to respond (MTTR).
- Faster containment and remediation of incidents, minimizing data loss, operational disruption, and financial repercussions.

- Building a robust, adaptive security framework capable of defending against evolving cyber threats and sophisticated attack campaigns.
- Streamlined incident response workflows, reduced alert fatigue, and efficient resource allocation for security teams.
- Comprehensive audit trails and reporting capabilities to meet stringent regulatory requirements and demonstrate due diligence.
- Shifting from a reactive "fix-it" mentality to a proactive "hunt and prevent" strategy, identifying vulnerabilities before exploitation.
- Gaining unparalleled insight into endpoint activity, user behavior, and potential insider threats.
- Maximizing the return on investment (ROI) from EDR solutions by leveraging their full capabilities for advanced threat hunting.

Target Audience

1. Security Operations Center (SOC) Analysts (Tier I, II, & III).
2. Incident Responders.
3. Threat Hunters
4. Security Engineers.
5. Digital Forensics Professionals.
6. Cybersecurity Consultants.
7. IT Security Managers.
8. Network Security Professionals

Course Outline

Module 1: EDR Foundations & Architecture

- Introduction to Endpoint Detection and Response (EDR) and its evolution in modern cybersecurity.
- Core components of EDR solutions: agents, data collection, cloud backend, analytics engine.
- Comparing EDR with traditional antivirus (AV) and Endpoint Protection Platforms (EPP).
- Deployment strategies and considerations for EDR in various enterprise environments.
- **Case Study:** Analyzing a successful EDR deployment in a financial institution, highlighting initial challenges and measurable improvements in threat visibility.

Module 2: Endpoint Telemetry & Data Collection

- Understanding key endpoint data sources: process activity, network connections, file system events, registry modifications.
- Deep dive into Windows Event Logs, Sysmon, and PowerShell logging for security investigations.
- Leveraging EDR for comprehensive telemetry collection and centralized data aggregation.
- Data normalization, enrichment, and correlation for effective analysis.
- **Case Study:** Investigating a sophisticated fileless malware attack by correlating multiple endpoint telemetry sources captured by EDR.

Module 3: Introduction to Threat Hunting Methodologies

- Defining threat hunting: proactive vs. reactive security.
- Developing threat hunting hypotheses based on threat intelligence and adversary TTPs.
- Structured, unstructured, and entity-driven threat hunting approaches.
- The Pyramid of Pain and its relevance to threat hunting strategies.

- **Case Study:** A threat hunt initiated by a low-fidelity alert, leading to the discovery of a long-standing compromise using an unstructured hunting approach.

Module 4: MITRE ATT&CK Framework for EDR & Hunting

- In-depth exploration of the MITRE ATT&CK Framework: Tactics, Techniques, and Procedures (TTPs).
- Mapping EDR capabilities to ATT&CK techniques for improved detection coverage.
- Using ATT&CK to develop targeted threat hunting queries and enrich incident data.
- Adversary emulation and red teaming exercises integrated with ATT&CK.
- **Case Study:** Applying ATT&CK to analyze a simulated ransomware attack, identifying the specific TTPs used and how EDR could have detected each stage.

Module 5: EDR for Initial Access & Execution Detection

- Hunting for common initial access vectors: phishing, vulnerable public-facing applications.
- Detecting execution techniques: PowerShell, WMI, scheduled tasks, malicious services.
- Analyzing process trees and parent-child relationships for suspicious execution.
- Unusual process behavior and living-off-the-land binaries (LOLBINs) detection.
- **Case Study:** Identifying a spear-phishing campaign that led to initial compromise through an EDR alert on an unusual process execution.

Module 6: Persistence & Privilege Escalation Hunting

- Techniques for establishing persistence: registry run keys, startup folders, WMI event subscriptions.
- Hunting for common privilege escalation methods: UAC bypass, vulnerable services, unpatched software.
- Detecting credential dumping and sensitive data access attempts.
- Analyzing user and system account activity for signs of compromise.
- **Case Study:** Uncovering a lateral movement attempt within an organization through the detection of suspicious account activity and privilege escalation attempts on an endpoint.

Module 7: Lateral Movement & Command and Control (C2) Detection

- Identifying lateral movement techniques: PsExec, WMI, RDP abuse, SMB exploitation.
- Hunting for C2 communication channels: DNS tunneling, HTTP/S beacons, non-standard protocols.
- Network connections analysis via EDR: anomalous destination, volume, and frequency.
- Detecting beaconing activity and data exfiltration patterns.
- **Case Study:** Tracing the lateral movement of an attacker across multiple machines using EDR network logs and identifying the C2 server.

Module 8: Data Exfiltration & Impact Hunting

- Techniques for data exfiltration: cloud storage, encrypted archives, network shares.
- Hunting for data staging and compression activities prior to exfiltration.
- Detecting impact activities: data destruction, ransomware encryption, system manipulation.
- Analyzing unusual file access patterns and large data transfers.
- **Case Study:** Responding to a ransomware attack by utilizing EDR to identify encrypted files, pinpoint the initial infection vector, and contain the spread.

Module 9: Advanced EDR Querying & Analytics

- Developing sophisticated EDR queries using boolean logic, regular expressions, and statistical functions.
- Leveraging EDR's built-in analytical capabilities: dashboards, visualizations, reporting.
- Creating custom detection rules and alerts based on specific TTPs.
- Integrating EDR with SIEM and SOAR platforms for enhanced correlation and automation.
- **Case Study:** Building a custom EDR query to hunt for a specific nation-state actor's known TTPs, leading to the discovery of previously undetected activity.

Module 10: Digital Forensics with EDR

- Forensic artifact collection using EDR: memory dumps, disk images, specific file acquisition.
- Analyzing EDR data for forensic purposes: timeline analysis, event reconstruction.
- Utilizing EDR to assist in compromise assessment and scope determination.
- Anti-forensics techniques and how EDR can help detect them.
- **Case Study:** Using EDR's forensic capabilities to reconstruct the full attack chain of a sophisticated breach, providing evidence for legal and internal review.

Module 11: Threat Intelligence & EDR Integration

- Sources of threat intelligence: open-source, commercial, and proprietary.
- Operationalizing CTI within EDR: IOC matching, TTP detection.
- Creating custom intelligence feeds and integrating them into EDR workflows.
- Building a feedback loop between threat hunting, incident response, and threat intelligence.
- **Case Study:** Implementing a new threat intelligence feed into an EDR solution, resulting in the proactive detection of a new variant of malware targeting the organization's industry.

Module 12: Automated Response & Orchestration with EDR

- Automated containment actions: process termination, file quarantine, network isolation.
- Orchestration with SOAR platforms for automated incident response playbooks.
- Developing custom automated response rules within EDR.
- Best practices for implementing and testing automated responses.
- **Case Study:** Demonstrating the effectiveness of automated response by containing a rapidly spreading worm before it could impact critical systems.

Module 13: EDR for Cloud & Containerized Environments

- Challenges of EDR in cloud-native and containerized environments.
- Specific EDR capabilities for cloud workloads, serverless functions, and Kubernetes.
- Integrating EDR with cloud security posture management (CSPM) and cloud workload protection platforms (CWPP).
- Securing hybrid cloud deployments with unified EDR visibility.
- **Case Study:** Extending EDR coverage to a newly deployed cloud environment, successfully detecting misconfigurations and unauthorized access attempts.

Module 14: AI, Machine Learning & Future of EDR

- The role of AI and ML in enhancing EDR's detection capabilities (behavioral analytics, predictive analysis).
- Understanding AI-driven attacks and how EDR can defend against them.
- Emerging trends in EDR: XDR (Extended Detection and Response) and its benefits.
- Future outlook for endpoint security and threat hunting.
- **Case Study:** Exploring how an EDR solution's AI algorithms flagged a subtle, multi-stage attack that bypassed traditional rule-based detections.

Module 15: Building a Mature Threat Hunting Program

- Establishing a dedicated threat hunting team: roles, skills, and organizational structure.
- Metrics and KPIs for measuring the effectiveness of a threat hunting program.
- Developing a continuous improvement cycle for threat hunting and EDR operations.
- Legal and ethical considerations in threat hunting.
- **Case Study:** Developing a roadmap for an organization to mature its threat hunting capabilities from ad-hoc activities to a full-fledged, intelligence-driven program.

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.com 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. Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$3,000
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

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

Register Online Now

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