Endpoint Detection and Response (EDR) Tool Mastery 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

The modern cyber threat landscape is constantly evolving, with adversaries leveraging advanced persistent threats (APTs), fileless malware, and sophisticated zero-day exploits to breach enterprise networks. Traditional signature-based antivirus (AV) solutions are no longer sufficient to provide proactive defense against these highly evasive attacks. This gap has propelled Endpoint Detection and Response (EDR) from an optional tool to an essential security layer for every organization committed to cyber resilience. EDR solutions provide continuous, real-time visibility into endpoint activity laptops, desktops, servers, and mobile devices collecting rich telemetry data to detect anomalies, track suspicious processes, and rapidly facilitate incident response.

Endpoint Detection and Response (EDR) Tool Mastery Training Course is meticulously designed to transform security professionals from reactive responders to proactive threat hunters. Participants will gain hands-on experience with industry-leading EDR platforms, mastering the critical skills required for effective threat investigation, triage, and automated remediation. The curriculum emphasizes leveraging behavioral analytics, integrating with Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) systems, and applying the MITRE ATT&CK Framework for enhanced contextual awareness. By the end of this program, graduates will be equipped to significantly reduce their organization's mean time to detect (MTTD) and mean time to respond (MTTR), solidifying their role as an indispensable asset in the contemporary Security Operations Center (SOC).

Programme Curriculum

Endpoint Detection and Response (EDR) Tool Mastery Training Course

Introduction

The modern cyber threat landscape is constantly evolving, with adversaries leveraging advanced persistent threats (APTs), fileless malware, and sophisticated zero-day exploits to breach enterprise networks. Traditional signature-based antivirus (AV) solutions are no longer sufficient to provide proactive defense against these highly evasive attacks. This gap has propelled Endpoint Detection and Response (EDR) from an optional tool to an essential security layer for every organization committed to cyber resilience. EDR solutions provide continuous, real-time visibility into endpoint activity laptops, desktops, servers, and mobile devices collecting rich telemetry data to detect anomalies, track suspicious processes, and rapidly facilitate incident response.

Endpoint Detection and Response (EDR) Tool Mastery Training Course is meticulously designed to transform security professionals from reactive responders to proactive threat hunters. Participants will gain hands-on experience with industry-leading EDR platforms, mastering the critical skills required for effective threat investigation, triage, and automated remediation. The curriculum emphasizes leveraging behavioral analytics, integrating with Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) systems, and applying the MITRE ATT&CK Framework for enhanced contextual awareness. By the end of this program, graduates will be equipped to significantly reduce their organization's mean time to detect (MTTD) and mean time to respond (MTTR), solidifying their role as an indispensable asset in the contemporary Security Operations Center (SOC).

Course Duration

5 days

Course Objectives

1. Master the deployment, configuration, and daily operation of leading EDR tools
2. Develop and execute proactive threat hunting queries using EDR telemetry to discover dormant threats and IOCs
3. Effectively map detected security events to the MITRE ATT&CK Framework for standardized threat context and adversary profiling.
4. Analyze endpoint telemetry data and apply behavioral analytics to identify anomalous activity indicative of fileless malware and insider threats.
5. Lead and manage the full incident response lifecycle, from initial alert triage to final eradication and post-mortem analysis, utilizing EDR automation.
6. Conduct live digital forensics and root cause analysis on compromised endpoints using EDR's data collection and visualization capabilities.
7. Develop and fine-tune custom EDR detection rules and automated playbooks to minimize false positives and enhance security coverage.
8. Design and implement EDR strategies specifically tailored to combat sophisticated threats like ransomware and Advanced Persistent Threats (APTs).
9. Seamlessly integrate EDR data feeds with SIEM and XDR platforms for unified visibility and cross-platform correlation.
10. Apply Zero Trust concepts to endpoint security, emphasizing continuous verification and least privilege access as enforced by EDR.
11. Understand and meet regulatory compliance requirements by leveraging EDR's logging and reporting features.
12. Perform basic malware triage and sandbox analysis to understand threat characteristics and inform EDR response actions.
13. Grasp the deployment and management of Cloud-Native EDR solutions in hybrid and multi-cloud environments.

Target Audience

1. SOC Analysts.
2. Incident Responders.
3. Threat Hunters.
4. Security Engineers.
5. IT Security Managers.
6. Digital Forensic Investigators.
7. Red Team/Blue Team Members.
8. Mid-to-Senior IT Professionals.

Course Modules

Module 1: EDR Fundamentals and Architecture

- The evolution from traditional Antivirus to EPP, EDR, and XDR.
- Agent, Telemetry Data Collection, Cloud Console, and Analytics Engine.
- Comparing leading EDR vendors and deployment models.
- Case Study: Analyzing a successful migration from legacy AV to a modern EDR solution, highlighting key visibility gains.
- Deployment best practices, architecture sizing, and agent management across diverse operating systems

Module 2: Endpoint Telemetry and Data Analysis

- Deep dive into rich endpoint data sources.
- Mastering EDR query languages and advanced filtering for rapid data retrieval.
- Techniques for creating a baseline of "normal" endpoint behavior to spot anomalies.
- Case Study: Reconstructing a PowerShell-based fileless attack chain using EDR process and command-line logging data.
- Data retention policies, storage optimization, and performance impact on endpoints.

Module 3: Threat Detection and MITRE ATT&CK

- Understanding detection methodologies.
- Practical application of the MITRE ATT&CK Framework for threat context and reporting.
- Developing and testing custom rules to detect specific TTPs
- Case Study: Detecting a lateral movement attempt by a threat actor leveraging a valid but anomalous user account, mapped to the MITRE T1021 technique.
- Strategies for reducing Alert Fatigue and prioritizing high-fidelity alerts for triage.

Module 4: Proactive Threat Hunting with EDR

- The philosophy and methodology of proactive threat hunting and reactive incident response.
- Formulating threat hunting hypotheses based on Cyber Threat Intelligence feeds.
- Hunting for persistence mechanisms and memory injection.
- Case Study: Hunting for remnants of a targeted spear-phishing campaign by searching for specific file hashes and network connections.
- Creating a feedback loop to convert successful hunts into permanent detection rules.

Module 5: Incident Response and Containment

- The complete EDR-driven incident response workflow.
- Automating response actions
- Executing remote shell access via EDR for live system inspection during an active incident.
- Case Study: Rapidly containing a widespread ransomware outbreak using EDR's automated host isolation capabilities to prevent further encryption.
- Developing and testing SOAR playbooks for common EDR alert types

Module 6: Digital Forensics and Root Cause Analysis (RCA)

- Utilizing EDR's built-in forensic capabilities for collecting logs and memory snapshots.
- Conducting Root Cause Analysis to identify the initial access vector.
- Analyzing volatile data and creating a timeline of events leading up to the breach.
- Case Study: Performing an RCA on a data exfiltration incident to determine the affected files, user actions, and destination IP addresses.
- Evidence handling, chain of custody, and preparing EDR data for legal or regulatory reporting.

Module 7: Advanced EDR Topics and Integration

- Integrating EDR with SIEM for centralized log analysis.
- Understanding the shift to Extended Detection and Response and EDR's role within it.
- Leveraging EDR for vulnerability management and software inventory.
- Case Study: Configuring an XDR platform to correlate EDR alerts with network and email security logs, identifying a targeted supply chain attack.
- Applying Zero Trust principles to endpoint access and continuous monitoring.

Module 8: Managing Threats and EDR Optimization

- Best practices for managing and tracking advanced threats like APTs and sophisticated malware.
- Regular EDR health checks, sensor deployment auditing, and tuning for optimal performance.
- Techniques for detecting and preventing defense evasion and EDR sensor tampering.
- Case Study: Simulating an EDR bypass attempt and analyzing EDR logging to identify and patch the detection gap.
- AI/ML advancements, extended telemetry, and integration with operational technology security.

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. 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
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100
05 Oct 2026	09 Oct 2026	Online	$1,100
12 Oct 2026	16 Oct 2026	Online	$1,100
19 Oct 2026	23 Oct 2026	Online	$1,100
26 Oct 2026	30 Oct 2026	Online	$1,100

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

Register Online Now