Training Course on Implementing and Optimizing EDR/XDR for Digital Forensics and Incident Response

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 complex **cybersecurity landscape**, organizations face an ever-increasing barrage of sophisticated **cyber threats** and targeted attacks. Traditional security measures often fall short in providing the necessary **visibility** and **response capabilities** to effectively combat these evolving threats. This is where **Endpoint Detection and Response (EDR)** and **Extended Detection and Response (XDR)** emerge as critical technologies. EDR focuses on granular monitoring and rapid response at the individual endpoint level, offering deep insights into endpoint activities, identifying suspicious behaviors, and enabling swift containment. XDR, as the evolution of EDR, transcends the endpoint, integrating and correlating security data from a wider array of sources including network, cloud, email, and identity, providing a **holistic view** of the entire **attack surface** for comprehensive threat detection and accelerated **incident response workflows**.

Training Course on Implementing and Optimizing EDR/XDR for Digital Forensics and Incident Response is meticulously designed to equip **cybersecurity professionals**, **incident responders**, and **digital forensics analysts** with the practical skills and advanced knowledge required to effectively implement, optimize, and leverage EDR/XDR platforms. Participants will gain hands-on experience with industry-leading tools, learn to conduct proactive **threat hunting**, perform in-depth **forensic investigations**, and streamline **incident remediation**. The course emphasizes **real-world scenarios** and **case studies**, ensuring participants can translate theoretical concepts into actionable strategies for enhancing their organization's **cyber resilience** and significantly reducing **mean time to detect (MTTD)** and **mean time to respond (MTTR)** to cyber incidents.

Programme Curriculum

Training Course on Implementing and Optimizing EDR/XDR for Digital Forensics and Incident Response

Introduction

In today's complex **cybersecurity landscape**, organizations face an ever-increasing barrage of sophisticated **cyber threats** and targeted attacks. Traditional security measures often fall short in providing the necessary **visibility** and **response capabilities** to effectively combat these evolving threats. This is where **Endpoint Detection and Response (EDR)** and **Extended Detection and Response (XDR)** emerge as critical technologies. EDR focuses on granular monitoring and rapid response at the individual endpoint level, offering deep insights into endpoint activities, identifying suspicious behaviors, and enabling swift containment. XDR, as the evolution of EDR, transcends the endpoint, integrating and correlating security data from a wider array of sources including network, cloud, email, and identity, providing a **holistic view** of the entire **attack surface** for comprehensive threat detection and accelerated **incident response workflows**.

Training Course on Implementing and Optimizing EDR/XDR for Digital Forensics and Incident Response is meticulously designed to equip **cybersecurity professionals**, **incident responders**, and **digital forensics analysts** with the practical skills and advanced knowledge required to effectively implement, optimize, and leverage EDR/XDR platforms. Participants will gain hands-on experience with industry-leading tools, learn to conduct proactive **threat hunting**, perform in-depth **forensic investigations**, and streamline **incident remediation**. The course emphasizes **real-world scenarios** and **case studies**, ensuring participants can translate theoretical concepts into actionable strategies for enhancing their organization's **cyber resilience** and significantly reducing **mean time to detect (MTTD)** and **mean time to respond (MTTR)** to cyber incidents.

Course Duration

10 days

Course Objectives

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

1. Grasp the core concepts, architecture, and deployment models of Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) solutions.
2. Clearly articulate the distinctions and synergistic benefits of EDR and XDR in a modern **security operations center (SOC)**.
3. Install, configure, and manage EDR/XDR agents and platforms across diverse operating systems and environments.
4. Utilize EDR/XDR capabilities for advanced **threat detection**, including **behavioral analytics**, **IOCs (Indicators of Compromise)**, and **IOAs (Indicators of Attack)**.
5. Develop and execute effective **threat hunting methodologies** using EDR/XDR data to uncover hidden threats and **advanced persistent threats (APTs)**.
6. Leverage EDR/XDR for **forensic data collection**, **memory forensics**, **file system forensics**, and **log analysis** during investigations.
7. Apply EDR/XDR for efficient **incident triage**, **containment strategies**, **eradication**, and **recovery procedures**.
8. Configure **security orchestration, automation, and response (SOAR)** capabilities within EDR/XDR for faster, more efficient responses.
9. Use EDR/XDR to analyze **malware behavior**, identify **ransomware attack chains**, and implement appropriate countermeasures.
10. Understand how EDR/XDR integrates with **Security Information and Event Management (SIEM)** and SOAR platforms for enhanced **security visibility** and automation.
11. Generate comprehensive **incident reports** and maintain proper **chain of custody** for legal and compliance purposes.

12. Recommend and implement best practices for optimizing EDR/XDR deployments to improve overall **cybersecurity posture**.
13. Understand how EDR/XDR evolves to address new and emerging **cyber threats** and attack techniques.

Organizational Benefits

- Proactive identification and faster detection of sophisticated cyber threats, including zero-day attacks and advanced persistent threats (APTs).
- Reduced **mean time to detect (MTTD)** and **mean time to respond (MTTR)**, minimizing the impact of security incidents.
- Strengthened overall cybersecurity defenses through comprehensive endpoint and extended visibility.
- Lowered likelihood of successful data breaches and associated financial and reputational damage.
- Streamlined security workflows, automation of repetitive tasks, and more efficient use of security team resources.
- Better adherence to industry regulations and compliance frameworks requiring robust incident response capabilities.
- Empowering internal teams to actively hunt for threats before they cause significant damage.
- Enhanced ability to conduct thorough digital forensic investigations to understand attack vectors and prevent future occurrences.
- Maximized return on investment in existing and new security tools through effective integration and utilization of EDR/XDR.

Target Audience

1. Security Analysts
2. Incident Responders
3. Digital Forensics Investigators
4. SOC Analysts
5. Cybersecurity Engineers
6. IT Security Professionals
7. Threat Hunters
8. Security Consultants

Course Outline

Module 1: Introduction to EDR/XDR and the Modern Threat Landscape

- Understanding the Evolving Cyber Threat Landscape
- Limitations of Traditional Security Solutions.
- Introduction to EDR
- Introduction to XDR
- The Role of EDR/XDR in Digital Forensics and Incident Response (DFIR).
- **Case Study**: Analyzing a targeted phishing campaign that bypassed traditional defenses, demonstrating the need for behavioral detection.

Module 2: EDR Architecture and Deployment

- EDR Agent Deployment Strategies
- Endpoint Data Collection:
- Centralized EDR Platforms.
- Policy Management and Configuration.

- Integrating EDR with IT Infrastructure
- **Case Study**: Deploying EDR across a large enterprise network to gain initial visibility and identifying rogue endpoints.

Module 3: XDR Framework and Data Correlation

- Extending Beyond the Endpoint
- Data Ingestion and Normalization
- Cross-Domain Correlation
- XDR Use Cases.
- Building a Unified Security Picture
- **Case Study**: Tracing a multi-stage attack from an email phishing attempt, through a compromised endpoint, to cloud resource exfiltration using XDR's correlation capabilities.

Module 4: Threat Detection with EDR/XDR

- Indicators of Compromise (IOCs)
- Indicators of Attack (IOAs)
- Machine Learning and AI in Threat Detection
- Alert Triage and Prioritization
- Custom Detection Rules and YARA Signatures.
- **Case Study**: Detecting a sophisticated fileless malware attack that leveraged PowerShell and WMI, highlighting EDR's behavioral analysis.

Module 5: Proactive Threat Hunting with EDR/XDR

- Principles of Threat Hunting
- Threat Hunting Queries and Techniques
- Common Hunting Scenarios.
- Leveraging Threat Intelligence.
- Documenting Hunting Findings and Remediation.
- **Case Study**: Proactively hunting for signs of a known APT group's presence within the network using EDR/XDR telemetry and uncovering dormant backdoors.

Module 6: Digital Forensics Fundamentals with EDR/XDR

- The Digital Forensics Incident Response (DFIR) Lifecycle.
- Forensic Soundness and Chain of Custody.
- Endpoint Data Acquisition
- Memory Forensics with EDR/XDR.
- File System and Registry Forensics
- **Case Study**: Conducting a rapid forensic analysis on a workstation suspected of being compromised by ransomware, using EDR to gather critical artifacts.

Module 7: Network Forensics and Log Analysis with XDR

- Network Data Collection in XDR
- Traffic Analysis and Anomaly Detection
- DNS and HTTP Log Analysis
- Cloud Log Forensics.
- Correlating Network and Endpoint Data
- **Case Study**: Investigating an insider threat where sensitive data was exfiltrated via unusual network protocols, identified through XDR's network visibility.

Module 8: Incident Response Strategies with EDR/XDR

- Incident Triage and Prioritization
- Containment Techniques
- Eradication and Remediation
- Recovery Planning.
- Post-Incident Analysis and Lessons Learned
- **Case Study**: Responding to a widespread malware outbreak where EDR/XDR was used to quickly identify patient zero, contain the spread, and automate remediation across affected systems.

Module 9: Automated Incident Response and SOAR Integration

- Benefits of Security Orchestration, Automation, and Response (SOAR)
- Playbooks and Automated Workflows.
- Integrating EDR/XDR with SOAR Platforms.
- Automated Containment and Remediation Actions
- Building Custom Automation Rules
- **Case Study**: Implementing an automated response playbook for phishing incidents, where XDR detects malicious attachments, isolates affected endpoints, and creates a help desk ticket.

Module 10: Malware and Ransomware Analysis with EDR/XDR

- Malware Analysis Techniques.
- Identifying Malware Characteristics
- Ransomware Attack Kill Chain
- EDR/XDR for Ransomware Detection and Prevention
- Post-Ransomware Forensics.
- **Case Study**: Analyzing a new variant of ransomware that targeted a critical server, using EDR to understand its execution flow and identify the encryption process.

Module 11: Cloud EDR/XDR and Cloud Forensics

- Challenges of Cloud Security
- Cloud EDR/XDR Capabilities.
- Cloud Logging and Monitoring.
- Investigating Cloud Incidents.
- Securing Cloud Configurations with XDR
- **Case Study**: Investigating a breach in an AWS environment where an exposed S3 bucket led to data compromise, leveraging cloud EDR/XDR for visibility and remediation.

Module 12: Advanced EDR/XDR Features and Best Practices

- Threat Intelligence Integration
- Vulnerability Management with EDR/XDR.
- Compliance Reporting and Auditing.
- Managed Detection and Response (MDR) Services.
- Optimizing EDR/XDR Performance
- **Case Study**: Implementing an EDR/XDR platform across a global organization, focusing on optimizing policies for various regional compliance requirements.

Module 13: Purple Teaming with EDR/XDR

- Introduction to Purple Teaming.
- Using EDR/XDR for Red Team Emulation.
- Blue Team Response Validation effective.
- Improving Detection Engineering exercises.
- Continuous Improvement of DFIR Processes
- **Case Study**: A purple team exercise where a simulated insider threat activity was used to test the EDR/XDR's ability to detect anomalous user behavior and trigger automated alerts.

Module 14: Legal and Ethical Considerations in DFIR

- Legal Frameworks and Regulations.
- Data Privacy and Confidentiality.
- Ethics in Digital Forensics.
- Reporting Requirements and Notifications
- Working with Law Enforcement and Legal Counsel
- **Case Study**: Navigating a data breach where sensitive customer data was exposed, focusing on the legal reporting obligations and proper evidence preservation for potential litigation.

Module 15: Future Trends in EDR/XDR and Cybersecurity

- AI and Machine Learning Advancements.
- Zero Trust Architecture and EDR/XDR
- Convergence of Security Tools.
- Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

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

Register Online Now