Training Course on Building a Threat Hunting Team and Program

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 **dynamic threat landscape**, traditional perimeter defenses and automated security tools are often insufficient to combat sophisticated, **stealthy adversaries** and **advanced persistent threats (APTs)**. Organizations face an urgent need to adopt a proactive **cybersecurity posture** that goes beyond reactive incident response. Training Course on Building a Threat Hunting Team and Program focuses on empowering security professionals with the **knowledge, skills, and methodologies** to establish, operate, and mature a dedicated **threat hunting team and program**. By actively searching for **undetected threats** and **anomalous behaviors** within an enterprise network, organizations can significantly reduce **dwell time**, mitigate **cyber risk**, and strengthen their overall **resilience** against **emerging threats** and **zero-day exploits**.

This comprehensive program delves into the **strategic and tactical aspects** of **threat intelligence-driven hunting**, covering everything from **hypothesis generation** and **data analysis** to **tooling**, **frameworks (MITRE ATT&CK)**, and **programmatic maturity models**. Participants will gain hands-on experience with **cutting-edge techniques** for **uncovering hidden threats**, **identifying adversarial tactics, techniques, and procedures (TTPs)**, and **proactively improving security controls**. The course emphasizes practical application through **real-world case studies** and **simulated hunting expeditions**, ensuring that participants can immediately apply their newfound expertise to **enhance their organization's security posture** and **defend against evolving cyberattacks**.

Programme Curriculum

Training Course on Building a Threat Hunting Team and Program

Introduction

In today's **dynamic threat landscape**, traditional perimeter defenses and automated security tools are often insufficient to combat sophisticated, **stealthy adversaries** and **advanced persistent threats (APTs)**. Organizations face an urgent need to adopt a proactive **cybersecurity posture** that

goes beyond reactive incident response. Training Course on Building a Threat Hunting Team and Program focuses on empowering security professionals with the **knowledge, skills, and methodologies** to establish, operate, and mature a dedicated **threat hunting team and program**. By actively searching for **undetected threats** and **anomalous behaviors** within an enterprise network, organizations can significantly reduce **dwell time**, mitigate **cyber risk**, and strengthen their overall **resilience** against **emerging threats** and **zero-day exploits**.

This comprehensive program delves into the **strategic and tactical aspects** of **threat intelligence-driven hunting**, covering everything from **hypothesis generation** and **data analysis** to **tooling**, **frameworks (MITRE ATT&CK)**, and **programmatic maturity models**. Participants will gain hands-on experience with **cutting-edge techniques** for **uncovering hidden threats**, **identifying adversarial tactics, techniques, and procedures (TTPs)**, and **proactively improving security controls**. The course emphasizes practical application through **real-world case studies** and **simulated hunting expeditions**, ensuring that participants can immediately apply their newfound expertise to **enhance their organization's security posture** and **defend against evolving cyberattacks**.

Course Duration

10 days

Course Objectives

1. Establish a Threat Hunting Program Framework aligned with organizational security goals.
2. Develop robust Threat Hunting Methodologies including hypothesis-driven, intelligence-based, and anomaly detection approaches.
3. Leverage Cyber Threat Intelligence (CTI) effectively for proactive threat detection and adversary profiling.
4. Master the use of Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) for data aggregation and analysis in threat hunts.
5. Implement the MITRE ATT&CK Framework to map adversary TTPs and develop hunt hypotheses.
6. Conduct deep dives into network forensics and log analysis to uncover hidden indicators of compromise (IoCs) and indicators of attack (IoAs).
7. Identify and mitigate sophisticated malware, ransomware, and fileless attack techniques.
8. Understand and apply User and Entity Behavior Analytics (UEBA) for detecting anomalous user activity and insider threats.
9. Develop custom scripts and automation tools to streamline threat hunting operations and reduce manual effort.
10. Measure the effectiveness of threat hunting activities using key performance indicators (KPIs) and metrics.
11. Integrate threat hunting with incident response and vulnerability management lifecycles for a holistic security approach.
12. Build and manage a skilled Threat Hunting Team, addressing talent shortages through upskilling and collaboration.
13. Stay ahead of emerging threats including AI-powered attacks, supply chain vulnerabilities, and cloud security risks.

Organizational Benefits

- Uncover hidden threats and advanced persistent threats (APTs) before they cause significant damage, dramatically reducing dwell time.
- Minimize the likelihood and impact of successful cyberattacks by identifying and neutralizing threats early in the kill chain.

- Accelerate incident detection, investigation, and containment by providing richer context and insights from proactive hunts.
- Continuously strengthen defenses by identifying security gaps, misconfigurations, and vulnerabilities.
- Maximize the value of existing security tools (SIEM, EDR, XDR) through targeted data analysis.
- Demonstrate robust security practices and proactive threat management to meet regulatory requirements and internal audits.
- Safeguard intellectual property, sensitive data, and critical infrastructure from targeted attacks.
- Prevent costly data breaches, business disruption, and reputational damage.
- Generate valuable, tailored threat intelligence specific to the organization's environment and risk profile.

Target Audience

- Security Analysts and SOC (Security Operations Center) Analysts.
- Incident Responders.
- Cybersecurity Engineers
- IT Security Professionals.
- Network Security Engineers.
- Security Architects.
- Security Consultants.
- Managers overseeing cybersecurity teams and aiming to establish a threat hunting capability.

Course Outline

Module 1: Introduction to Threat Hunting & Its Importance

- Defining Threat Hunting: Proactive vs. Reactive Security
- The Evolving Threat Landscape: APTs, Zero-Days, and Ransomware
- Key Benefits of a Mature Threat Hunting Program
- Core Principles and Mindset of a Threat Hunter
- **Case Study:** The NotPetya attack and how proactive hunting could have minimized impact.

Module 2: Building the Threat Hunting Foundation

- Establishing a Threat Hunting Vision and Mission
- Defining Scope, Objectives, and Success Metrics
- Team Roles, Responsibilities, and Skillsets for a Hunting Team
- Integrating Threat Hunting with Existing Security Operations (SOC, Incident Response)
- **Case Study:** Staffing models for small, medium, and large enterprises and their challenges.

Module 3: Threat Intelligence for Hunters

- Understanding Different Types of Threat Intelligence (Strategic, Operational, Tactical)
- Leveraging OSINT, Commercial Feeds, and Internal Intelligence
- Indicators of Compromise (IoCs) vs. Indicators of Attack (IoAs)
- Threat Actor Profiling and Attribution
- **Case Study:** Using a specific APT group's TTPs from a threat intelligence report to formulate hunt hypotheses.

Module 4: Threat Hunting Methodologies

- Hypothesis-Driven Hunting: Formulation and Refinement

- Analytics-Driven Hunting: Anomaly Detection and Baselines
- Intelligence-Driven Hunting: Adapting to Known Threats
- Situational Awareness-Driven Hunting: Responding to Current Events
- **Case Study:** Developing a hypothesis based on recent phishing campaign intelligence and outlining the hunt steps.

Module 5: Data Sources for Threat Hunting

- Network Logs: Flow Data (NetFlow, IPFIX), DNS, Proxy, Firewall Logs
- Endpoint Data: Process Creation, Registry Changes, File System Activity
- Authentication Logs: Active Directory, Identity Provider Logs
- Cloud Logs and APIs for Cloud Environments
- **Case Study:** Analyzing web proxy logs to identify suspicious outbound connections to rare or newly registered domains.

Module 6: SIEM and EDR for Threat Hunting

- Optimizing SIEM for Threat Hunting: Data Ingestion and Correlation
- Advanced EDR Capabilities for Deep Endpoint Visibility
- Leveraging XDR for Unified Data Analysis across Domains
- Building Custom Search Queries and Dashboards in SIEM/EDR
- **Case Study:** Using a SIEM to correlate EDR alerts with network flow data to uncover lateral movement.

Module 7: Introduction to MITRE ATT&CK Framework

- Understanding the ATT&CK Matrix: Tactics, Techniques, Procedures
- Mapping Internal Data Sources to ATT&CK Techniques
- Using ATT&CK Navigator for Threat Coverage Analysis
- Developing Hunt Playbooks based on ATT&CK
- **Case Study:** Mapping observed suspicious PowerShell activity to specific ATT&CK techniques (e.g., T1059.001 - PowerShell).

Module 8: Hunting for Initial Access and Execution

- Common Initial Access Vectors: Phishing, Exploited Public-Facing Applications
- Detecting Execution Techniques: PowerShell, WMI, Scheduled Tasks
- Hunting for Persistence Mechanisms: Run Keys, Services, Scheduled Tasks
- Analyzing PE Files and Suspicious Processes
- **Case Study:** Hunting for unusual new services or scheduled tasks created by non-standard users after a suspected phishing compromise.

Module 9: Hunting for Lateral Movement and Privilege Escalation

- Techniques for Lateral Movement: PsExec, SMB, RDP, Pass-the-Hash
- Identifying Privilege Escalation Attempts: UAC Bypass, Exploited Vulnerabilities
- Analyzing Authentication Logs for Credential Theft Indicators
- Detecting Network Reconnaissance and Internal Scanning
- **Case Study:** Tracing suspicious RDP connections from a compromised workstation to other high-value assets.

Module 10: Hunting for Command and Control (C2) & Exfiltration

- Common C2 Channels: DNS Tunneling, HTTP/S Anomalies, Encrypted Traffic
- Detecting Data Staging and Exfiltration Attempts

- Analyzing Data Volumes and Unusual Destinations
- Identifying Cloud Storage Syncing Anomalies
- **Case Study:** Uncovering DNS tunneling activity used for C2 by analyzing high-frequency, low-entropy DNS queries.

Module 11: Malware and Ransomware Hunting

- Understanding Malware Families and Their Characteristics
- Hunting for Fileless Malware and Living-off-the-Land Binaries
- Behavioral Analysis of Ransomware Attacks
- Using Sandbox Environments for Malware Analysis
- **Case Study:** Analyzing a suspicious macro-enabled document in a sandbox to observe its behavior and identify potential ransomware indicators.

Module 12: Automation and Tooling for Threat Hunting

- Scripting for Data Collection and Analysis (Python, PowerShell)
- Leveraging Open-Source Hunting Tools (Velociraptor, KQL, Sigma Rules)
- Building Custom Automation for Repetitive Hunt Tasks
- Integration with SOAR (Security Orchestration, Automation, and Response)
- **Case Study:** Automating the collection and analysis of specific registry keys across endpoints to hunt for known persistence mechanisms.

Module 13: Measuring and Maturing the Threat Hunting Program

- Defining Key Performance Indicators (KPIs) for Threat Hunting Success
- Reporting on Hunt Findings and Impact to Stakeholders
- Continuous Improvement and Feedback Loops
- Building a Threat Hunting Playbook Library and Knowledge Base
- **Case Study:** Presenting a quarterly report on threat hunt findings, highlighting a reduction in average dwell time and identifying new detection opportunities.

Module 14: Advanced Threat Hunting Techniques

- Anomaly Detection with Machine Learning and Behavioral Analytics
- Hunting in Cloud-Native Environments (Container Security, Serverless)
- Supply Chain Threat Hunting and Third-Party Risk Assessment
- Dark Web and Deep Web Monitoring for Threat Intelligence
- **Case Study:** Utilizing UEBA to detect anomalous user behavior indicative of an insider threat, such as unusual data access patterns.

Module 15: Future of Threat Hunting & Career Paths

- The Impact of AI on Threat Hunting: AI for Defense and Offense
- Quantum Computing and its Implications for Cybersecurity
- The Role of Threat Hunting in a Zero Trust Architecture
- Career Paths and Professional Development for Threat Hunters
- **Case Study:** Discussing the evolving role of a threat hunter in an organization adopting advanced AI-driven security platforms.

Training Methodology

This course employs a **blended learning approach** to maximize participant engagement and knowledge retention:

- **Interactive Lectures:** Core concepts and theoretical foundations delivered through engaging presentations.
- **Hands-on Labs:** Practical exercises and simulated scenarios using industry-standard tools and realistic datasets.
- **Real-World Case Studies:** In-depth analysis of actual cyber incidents to illustrate threat hunting principles and techniques.
- **Group Discussions:** Collaborative problem-solving and sharing of best practices among participants.
- **Q&A Sessions:** Opportunities for direct interaction with experienced instructors.
- **Demonstrations:** Live showcases of tools and techniques in action.
- **Capstone Project:** A comprehensive, scenario-based project where participants apply all learned skills to build a mini-threat hunting program or conduct a simulated hunt.

Register as a group from 3 participants for a Discount

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

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

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