Training Course on Proactive Threat Hunting Methodologies

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 cyber threat landscape**, traditional perimeter defenses and reactive security measures are no longer sufficient. **Sophisticated threat actors**, including **Advanced Persistent Threats (APTs)** and **ransomware groups**, consistently evade conventional security tools, leaving organizations vulnerable to devastating breaches. Training Course on Proactive Threat Hunting Methodologies equips **cybersecurity professionals** with the **cutting-edge skills** and **strategic mindset** required to **proactively detect, analyze, and neutralize hidden threats** before they escalate into major incidents. By embracing an **adversary-centric approach** and leveraging **advanced analytics**, participants will learn to go beyond automated alerts, significantly reducing **dwell time** and strengthening their organization's overall **security posture**.

This intensive program delves deep into the **tactics, techniques, and procedures (TTPs)** of modern adversaries, empowering participants to develop and execute **hypothesis-driven threat hunts**. Through **hands-on labs, real-world case studies, and practical exercises**, attendees will gain proficiency in **data analysis, forensic investigation, and incident response integration**. The course emphasizes building a **proactive defense strategy**, enabling security teams to **identify anomalies, uncover stealthy attacks, and develop robust detection engineering capabilities**. This vital shift from reactive to **proactive cybersecurity** is essential for any organization seeking to maintain **cyber resilience** in the face of evolving and increasingly complex digital threats.

Programme Curriculum

Training Course on Proactive Threat Hunting Methodologies

Introduction

In today's **dynamic cyber threat landscape**, traditional perimeter defenses and reactive security measures are no longer sufficient. **Sophisticated threat actors**, including **Advanced Persistent Threats (APTs)** and **ransomware groups**, consistently evade conventional security tools, leaving

organizations vulnerable to devastating breaches. Training Course on Proactive Threat Hunting Methodologies equips **cybersecurity professionals** with the **cutting-edge skills** and **strategic mindset** required to **proactively detect, analyze, and neutralize hidden threats** before they escalate into major incidents. By embracing an **adversary-centric approach** and leveraging **advanced analytics**, participants will learn to go beyond automated alerts, significantly reducing **dwell time** and strengthening their organization's overall **security posture**.

This intensive program delves deep into the **tactics, techniques, and procedures (TTPs)** of modern adversaries, empowering participants to develop and execute **hypothesis-driven threat hunts**. Through **hands-on labs, real-world case studies, and practical exercises**, attendees will gain proficiency in **data analysis, forensic investigation, and incident response integration**. The course emphasizes building a **proactive defense strategy**, enabling security teams to **identify anomalies, uncover stealthy attacks, and develop robust detection engineering capabilities**. This vital shift from reactive to **proactive cybersecurity** is essential for any organization seeking to maintain **cyber resilience** in the face of evolving and increasingly complex digital threats.

Course Duration

10 days

Course Objectives

1. Develop advanced skills in leveraging **actionable threat intelligence (CTI)** to inform and prioritize proactive threat hunting efforts.
2. Formulate and execute robust **hypothesis-driven threat hunts** based on current **adversary TTPs** and organizational risk profiles.
3. Optimize the use of **EDR solutions** for deep forensic analysis and effective threat detection across endpoints.
4. Gain expertise in analyzing **network telemetry** to identify suspicious patterns, **command and control (C2)** communications, and data exfiltration attempts.
5. Proficiently analyze vast volumes of **security information and event management (SIEM)** logs to uncover subtle indicators of compromise (IoCs) and anomalies.
6. Understand fundamental **malware analysis** techniques to identify malicious binaries, understand their functionality, and extract critical intelligence.
7. Implement effective threat hunting strategies specifically tailored for **cloud environments** and **cloud-native security** challenges.
8. Develop methodologies for **proactively detecting insider threats** and malicious activities originating from within the organization.
9. Design, implement, and continuously refine **custom detection rules** and **YARA signatures** to improve automated threat detection.
10. Effectively utilize the **MITRE ATT&CK framework** to map adversary behaviors, understand attack methodologies, and build comprehensive hunting playbooks.
11. Seamlessly integrate threat hunting findings into the broader **incident response lifecycle** for rapid containment and remediation.
12. Apply **User and Entity Behavior Analytics (UEBA)** principles to identify deviations from baseline behaviors indicating potential threats.
13. Leverage **scripting (e.g., Python)** and automation tools to enhance the efficiency and scalability of threat hunting operations.

Organizational Benefits

- Significantly decrease the time attackers remain undetected within the network, minimizing potential damage and data loss.

- Identify and neutralize advanced threats before they escalate into full-blown breaches, preventing costly incidents.
- Strengthen overall cybersecurity defenses by uncovering blind spots and vulnerabilities that traditional tools miss.
- Provide richer, more actionable intelligence to incident response teams, leading to faster and more effective remediation.
- Maximize the value of existing security tools and technologies by leveraging them for proactive hunting.
- Demonstrate a commitment to robust and proactive security measures, aiding in regulatory compliance.
- Safeguard sensitive data, intellectual property, and critical infrastructure from sophisticated cyberattacks.
- Minimize financial losses associated with data breaches, downtime, legal fees, and reputational damage.

Target Audience

1. Security Operations Center (SOC) Analysts
2. Incident Responders
3. Threat Intelligence Analysts
4. Digital Forensics Professionals
5. Security Architects
6. Penetration Testers (looking to enhance defensive skills)
7. IT Security Managers
8. Cybersecurity Consultants

Course Outline

Module 1: Introduction to Proactive Threat Hunting

- Defining Threat Hunting: Proactive vs. Reactive Cybersecurity.
- The Evolving Threat Landscape: Understanding modern adversary motivations and capabilities.
- Key Principles of Threat Hunting: Hypothesis-driven, intelligence-led, iterative.
- Integrating Threat Hunting into the Security Ecosystem: SOC, Incident Response, Vulnerability Management.
- **Case Study:** The "SolarWinds Supply Chain Attack" - How proactive hunting could have identified early indicators of compromise.

Module 2: Cyber Threat Intelligence (CTI) for Hunters

- Sources and Types of Threat Intelligence: Strategic, Operational, Tactical.
- Leveraging OSINT and Commercial Feeds for Hunting Hypotheses.
- Understanding Adversary Profiles, TTPs, and Kill Chains.
- Structuring and Prioritizing Threat Intelligence for Actionable Hunts.
- **Case Study:** Analyzing a specific APT group's TTPs (e.g., Fancy Bear) and developing hunt queries based on their known methods.

Module 3: Building Hunting Hypotheses

- Methodologies for Hypothesis Generation: Data-driven, Intelligence-driven, Anomaly-driven.
- Translating Threat Intelligence into Testable Hypotheses.
- Developing Hunting Scenarios based on Industry-Specific Threats.
- Quantifying Risk and Prioritizing Hunting Efforts.

- **Case Study:** Formulating a hypothesis to detect "living off the land" attacks after a recent vulnerability disclosure.

Module 4: Endpoint Threat Hunting

- Deep Dive into Endpoint Detection and Response (EDR) Tools and Capabilities.
- Analyzing Endpoint Logs: Process creation, file modifications, registry changes.
- Identifying Malicious Process Behavior and DLL Injections.
- Memory Forensics for Advanced Endpoint Analysis.
- **Case Study:** Hunting for remnants of fileless malware on compromised endpoints.

Module 5: Network Threat Hunting

- Fundamentals of Network Traffic Analysis (NTA) and NetFlow.
- Identifying Anomalous Network Connections and Data Exfiltration.
- Analyzing DNS Traffic for Malicious Lookups and Domain Generation Algorithms (DGAs).
- Hunting for Command and Control (C2) Channels and Lateral Movement.
- **Case Study:** Using network flow data to identify an attacker's lateral movement across segmented networks.

Module 6: Log Management and SIEM Optimization for Hunting

- Critical Log Sources for Threat Hunting: Windows Event Logs, Linux Logs, Application Logs.
- Advanced SIEM Querying and Correlation Techniques (e.g., Splunk SPL, Elastic Stack KQL).
- Establishing Baselines and Identifying Deviations.
- Data Enrichment and Contextualization for Improved Analysis.
- **Case Study:** Correlating disparate log entries from multiple systems to uncover a multi-stage attack.

Module 7: Malware Analysis for Threat Hunters

- Introduction to Static and Dynamic Malware Analysis Techniques.
- Identifying Malware Persistence Mechanisms.
- Extracting Indicators of Compromise (IoCs) from Malware Samples.
- Leveraging Sandboxes and Threat Intelligence Platforms for Analysis.
- **Case Study:** Analyzing a ransomware sample to understand its infection vector and recovery mechanisms for improved hunting.

Module 8: Detection Engineering & YARA Rule Development

- Principles of Effective Detection Engineering.
- Developing Custom YARA Rules for Malware and Threat Actor Detection.
- Testing and Validating YARA Rules to Minimize False Positives.
- Automating Rule Deployment and Integration with Security Tools.
- **Case Study:** Writing a YARA rule to detect a newly identified variant of a common banking Trojan.

Module 9: Applying the MITRE ATT&CK Framework

- Navigating and Understanding the MITRE ATT&CK Matrix.
- Mapping Adversary TTPs to ATT&CK Techniques and Sub-Techniques.
- Developing ATT&CK-Aligned Hunting Playbooks.
- Assessing Detection Coverage against ATT&CK.

- **Case Study:** Using ATT&CK to build a hunt around a specific phishing campaign's post-exploitation activities.

Module 10: Cloud Environment Threat Hunting

- Understanding Cloud Security Models and Shared Responsibility.
- Hunting for Threats in IaaS, PaaS, and SaaS Environments.
- Analyzing CloudTrail, Azure Activity Logs, and other Cloud-Native Logs.
- Identifying Misconfigurations and Vulnerabilities in Cloud Resources.
- **Case Study:** Hunting for suspicious API calls and unauthorized access in an AWS environment.

Module 11: Insider Threat Hunting

- Identifying Indicators of Insider Threat Behavior (Malicious and Accidental).
- Leveraging User and Entity Behavior Analytics (UEBA) for Anomaly Detection.
- Monitoring Data Exfiltration Channels and Privileged Access.
- Legal and Ethical Considerations in Insider Threat Investigations.
- **Case Study:** Detecting an employee attempting to exfiltrate sensitive intellectual property using unusual file access patterns.

Module 12: Automation and Orchestration in Threat Hunting

- Introduction to Security Automation and Orchestration (SOAR).
- Scripting for Automated Data Collection and Analysis (e.g., Python for forensic tasks).
- Building Automated Hunt Workflows and Playbooks.
- Integrating Automation with Existing Security Tools.
- **Case Study:** Automating the collection and initial analysis of suspicious network flows to reduce manual effort.

Module 13: Communicating Hunt Findings & Reporting

- Effective Communication of Technical Findings to Stakeholders.
- Developing Clear and Concise Threat Hunt Reports.
- Actionable Recommendations for Remediation and Prevention.
- Post-Hunt Analysis and Lessons Learned.
- **Case Study:** Presenting a threat hunt discovery to executive leadership, emphasizing business impact and mitigation strategies.

Module 14: Advanced Threat Hunting Techniques

- Threat Hunting for Zero-Day Exploits (Hypothetical Scenarios).
- Hunting in Encrypted Traffic (When Permissible and Possible).
- Leveraging Machine Learning for Predictive Threat Hunting.
- Red Team/Blue Team Exercises for Skill Enhancement.
- **Case Study:** Simulating a sophisticated phishing attack and conducting a hunt to identify the simulated adversary's actions.

Module 15: Building and Sustaining a Threat Hunting Program

- Staffing and Training a Dedicated Threat Hunting Team.
- Developing a Threat Hunting Maturity Model.
- Establishing Metrics for Success and ROI.
- Continuous Improvement and Adaptation to New Threats.

- **Case Study:** Designing a phased implementation plan for a new threat hunting program within a large enterprise.

Training Methodology

This training course employs a highly **interactive and practical methodology** designed to maximize learning and skill acquisition. It combines:

- **Instructor-Led Presentations:** Engaging lectures providing theoretical foundations and conceptual understanding.
- **Hands-on Labs:** Extensive practical exercises using industry-standard tools and realistic simulated environments.
- **Real-World Case Studies:** In-depth analysis of actual cyber incidents to illustrate threat hunting principles and techniques.
- **Interactive Discussions:** Fostering knowledge sharing and problem-solving among participants.
- **Group Activities & Scenarios:** Collaborative exercises to apply learned concepts in team-based hunting scenarios.
- **Q&A Sessions:** Dedicated time for addressing participant queries and clarifying complex topics.
- **Tool Demonstrations:** Live demonstrations of popular threat hunting tools and platforms.
- **Capstone Project:** A comprehensive practical project to consolidate all learned skills.

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. Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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