Training Course on Network Threat Hunting Techniques and Tools

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$2,200 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's volatile cybersecurity landscape, organizations face persistent and evolving threats that often bypass traditional perimeter defenses. **Network Threat Hunting** has emerged as a critical, proactive cybersecurity discipline focused on actively searching for hidden, undetected, and advanced persistent threats (APTs) lurking within network infrastructures. Training Course on Network Threat Hunting Techniques and Tools provides security professionals with the essential methodologies, cutting-edge tools, and strategic mindset required to move beyond reactive defense, enabling them to identify subtle indicators of compromise (IOCs) and adversary tactics, techniques, and procedures (TTPs) before significant damage occurs.

This comprehensive program delves deep into the practical application of **threat intelligence**, **network forensics**, and **behavioral analytics** to uncover sophisticated threats. Participants will gain hands-on experience with industry-leading **network security monitoring** platforms and data analysis techniques. The course emphasizes building a robust **threat hunting program** capable of minimizing dwell time and enhancing overall organizational **cyber resilience** against both known and unknown threats.

Programme Curriculum

Training Course on Network Threat Hunting Techniques and Tools

Introduction

In today's volatile cybersecurity landscape, organizations face persistent and evolving threats that often bypass traditional perimeter defenses. **Network Threat Hunting** has emerged as a critical, proactive cybersecurity discipline focused on actively searching for hidden, undetected, and advanced persistent threats (APTs) lurking within network infrastructures. Training Course on Network Threat Hunting Techniques and Tools provides security professionals with the essential

methodologies, cutting-edge tools, and strategic mindset required to move beyond reactive defense, enabling them to identify subtle indicators of compromise (IOCs) and adversary tactics, techniques, and procedures (TTPs) before significant damage occurs.

This comprehensive program delves deep into the practical application of **threat intelligence**, **network forensics**, and **behavioral analytics** to uncover sophisticated threats. Participants will gain hands-on experience with industry-leading **network security monitoring** platforms and data analysis techniques. The course emphasizes building a robust **threat hunting program** capable of minimizing dwell time and enhancing overall organizational **cyber resilience** against both known and unknown threats.

Course Duration

10 days

Course Objectives

1. Master **Proactive Defense** strategies against advanced cyber threats.
2. Develop and implement effective **Threat Hunting Methodologies**.
3. Utilize **Network Forensics** for in-depth incident investigation and root cause analysis.
4. Apply **Cyber Threat Intelligence (CTI)** to inform hunting hypotheses.
5. Leverage **Behavioral Analytics** to detect anomalies and suspicious network activities.
6. Operate and configure key **Network Security Monitoring (NSM)** tools.
7. Understand and apply the **MITRE ATT&CK Framework** for adversary emulation.
8. Conduct effective **Packet Analysis** and traffic reconstruction.
9. Implement **Endpoint Detection and Response (EDR)** integration for comprehensive visibility.
10. Develop **Hunting Playbooks** and automation scripts for repeatable processes.
11. Strengthen **Incident Response** capabilities through proactive threat discovery.
12. Build a sustainable **Threat Hunting Program** within an organizational context.
13. Enhance overall **Organizational Cyber Resilience** and security posture.

Organizational Benefits

- Significantly decrease the time malicious actors remain undetected within the network, minimizing potential damage and data exfiltration.
- Identify and neutralize threats before they escalate into major security incidents, reducing financial losses and reputational damage.
- Improve the overall security strength by identifying weaknesses and validating existing security controls through real-world hunting exercises.
- Streamline incident response processes with early detection and richer contextual information gleaned from threat hunting activities.
- Maximize the value of existing security tools by integrating them into a comprehensive threat hunting strategy.
- Cultivate an internal team of highly skilled threat hunters capable of addressing complex and evolving cyber threats.
- Strengthen compliance with industry regulations and data protection mandates by demonstrating proactive security measures.

Target Audience

1. SOC Analysts and Tier 2/3 Security Analysts
2. Incident Responders and Digital Forensics Professionals

3. Security Engineers and Architects
4. Threat Intelligence Analysts
5. Network Administrators and IT Security Professionals
6. Cybersecurity Consultants
7. Penetration Testers and Red Teamers looking to understand defender techniques
8. Anyone seeking to advance their skills in proactive cybersecurity defense

Course Outline

Module 1: Introduction to Network Threat Hunting

- Defining Threat Hunting: Proactive vs. Reactive Security
- The Threat Hunting Loop: Hypothesis, Investigation, Discovery, Enrichment, Action
- Key Principles: "Assume Breach," Human-driven, Data-centric
- Differentiating Threat Hunting from SIEM/IDS Alerts
- **Case Study:** The NotPetya Ransomware: How early network anomaly detection could have mitigated widespread impact.

Module 2: Building a Threat Hunting Program

- Assessing Organizational Maturity (Hunting Maturity Model)
- Defining Scope, Goals, and Metrics for a Hunt Program
- Team Roles and Responsibilities within a Threat Hunting Unit
- Integrating Threat Hunting with Incident Response and SOC Operations
- **Case Study:** Establishing a New Threat Hunting Team: A financial institution's journey from reactive to proactive defense, highlighting initial challenges and successes.

Module 3: Threat Intelligence and Hypothesis Generation

- Sources of Threat Intelligence (OSINT, Commercial Feeds, ISACs)
- Leveraging CTI to Formulate Hunting Hypotheses
- Understanding Adversary Profiles and Threat Actors
- Mapping Threat Intelligence to MITRE ATT&CK
- **Case Study:** Utilizing CTI on a new ransomware family to develop hypotheses for a targeted hunt within a healthcare network.

Module 4: Network Data Sources for Hunting

- Understanding Network Telemetry: Flow Data (NetFlow, IPFIX), Packet Captures (PCAPs)
- DNS Logs, Proxy Logs, Firewall Logs, VPN Logs
- Authentication Logs and Identity Provider Data
- Selecting and Prioritizing Data Sources for Effective Hunts
- **Case Study:** Using DNS exfiltration patterns from internal logs to detect a C2 channel missed by traditional IDS.

Module 5: Network Security Monitoring (NSM) Platforms

- Overview of SIEM Solutions (Splunk, Elastic SIEM, QRadar) for Hunting
- Network Packet Brokers and Network Taps for Data Acquisition
- Open-Source NSM Tools (Zeek, Suricata, Moloch)
- Log Management and Centralized Data Aggregation Strategies
- **Case Study:** A company transitioning from limited log collection to a full NSM platform, showcasing the increase in visibility and hunt capabilities.

Module 6: Packet Analysis and Wireshark for Hunters

- Fundamentals of TCP/IP and Network Protocols
- Advanced Wireshark Filters and Display Options
- Protocol Analysis for Malicious Activity Detection
- Reconstructing Network Sessions and File Transfers from PCAPs
- **Case Study:** Analyzing a suspicious HTTP request in Wireshark to uncover a credential phishing attempt targeting internal users.

Module 7: Flow Data Analysis (NetFlow, IPFIX) for Hunting

- Understanding Flow Records and Their Components
- Tools for Flow Data Analysis (Elastiflow, SiLK, Commercial Platforms)
- Identifying Anomalous Traffic Patterns and Volume Shifts
- Hunting for Command and Control (C2) Traffic via Flow Data
- **Case Study:** Detecting a low-and-slow data exfiltration attempt by analyzing unusual flow data patterns over several weeks.

Module 8: Hunting for Malware and C2 Activity

- Indicators of Compromise (IOCs) vs. Indicators of Attack (IOAs)
- Hunting for Malware Beaconing and DNS Tunneling
- Identifying Common C2 Frameworks (Cobalt Strike, Metasploit)
- Detecting Lateral Movement Techniques over the Network
- **Case Study:** Uncovering a sophisticated multi-stage APT attack by correlating network C2 traffic with endpoint behavior.

Module 9: Behavioral Analytics for Network Hunting

- Establishing Baselines of Normal Network Behavior
- User and Entity Behavior Analytics (UEBA) for Insider Threats
- Anomaly Detection Techniques and Machine Learning in Hunting
- Identifying Deviations from Expected Network Patterns
- **Case Study:** Anomaly detection flagging unusual access to a sensitive file share by a regular user, revealing an insider threat.

Module 10: Applying MITRE ATT&CK in Network Hunts

- Understanding the MITRE ATT&CK Framework
- Mapping Network Hunting Techniques to ATT&CK Tactics and Techniques
- Developing ATT&CK-aligned Hunting Hypotheses
- Using ATT&CK to Communicate Findings and Improve Defenses
- **Case Study:** Simulating an ATT&CK-based adversary scenario to test and refine network detection capabilities.

Module 11: Hunting for Web-Based Threats and Exfiltration

- Analyzing HTTP/HTTPS Traffic for Malicious Payloads
- Hunting for Web Shells and Compromised Web Servers
- Detecting Data Exfiltration over HTTP/S, DNS, and ICMP
- Leveraging Proxy Logs for Web Threat Hunting
- **Case Study:** Using proxy logs and content analysis to identify successful data exfiltration through a seemingly innocuous web application.

Module 12: Cloud Network Threat Hunting

- Unique Challenges of Cloud Network Visibility (IaaS, PaaS, SaaS)
- Leveraging Cloud Provider Logs (VPC Flow Logs, CloudTrail, Azure Monitor)
- Hunting for Misconfigurations and Unauthorized Access in Cloud Environments
- Container and Serverless Security Hunting
- **Case Study:** Identifying unauthorized resource provisioning in an AWS environment through vigilant analysis of CloudTrail logs.

Module 13: Automation and Orchestration in Threat Hunting

- Scripting for Data Collection and Analysis (Python, PowerShell)
- SOAR (Security Orchestration, Automation, and Response) in Hunting
- Developing Automated Hunt Playbooks and Workflows
- Integrating Hunting with Ticketing and Case Management Systems
- **Case Study:** Automating the collection and initial analysis of suspicious network flows to reduce manual effort and speed up investigations.

Module 14: Post-Hunt Activities and Reporting

- Documenting Hunt Findings and Lessons Learned
- Developing New Detections and Signatures from Hunts
- Communicating Threat Hunt Outcomes to Stakeholders
- Measuring the Effectiveness of the Threat Hunting Program
- **Case Study:** Presenting findings from a successful hunt to executive management, leading to increased investment in security tools and personnel.

Module 15: Advanced Network Threat Hunting Scenarios

- Hunting in Encrypted Traffic (SSL/TLS Inspection, Metadata Analysis)
- Hunting for Living-off-the-Land (LotL) Attacks
- Supply Chain Attack Hunting
- Red Team/Blue Team Engagements for Hunt Validation
- **Case Study:** A simulated Red Team exercise reveals a sophisticated LotL attack, challenging the Blue Team's network hunting capabilities and leading to significant improvements.

Training Methodology

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

- **Instructor-Led Presentations:** Clear explanations of core concepts, theories, and best practices.
- **Hands-on Labs:** Extensive practical exercises using real-world tools and simulated network environments. Participants will perform actual hunts on provided datasets.
- **Case Studies and Scenarios:** In-depth analysis of real-world breach scenarios and successful threat hunts to illustrate concepts and techniques.
- **Group Discussions and Collaborative Exercises:** Fostering peer-to-peer learning and problem-solving.
- **Live Demonstrations:** Expert instructors showcasing advanced techniques and tool functionalities.
- **Capstone Project:** A comprehensive threat hunting exercise that integrates all learned concepts and skills.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254724527104*

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
10 Aug 2026	21 Aug 2026	Online	$2,200
17 Aug 2026	28 Aug 2026	Online	$2,200
24 Aug 2026	04 Sep 2026	Online	$2,200
31 Aug 2026	11 Sep 2026	Online	$2,200
07 Sep 2026	18 Sep 2026	Online	$2,200

Start Date	End Date	Location	Price
14 Sep 2026	25 Sep 2026	Online	$2,200
21 Sep 2026	02 Oct 2026	Online	$2,200
28 Sep 2026	09 Oct 2026	Online	$2,200

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

Register Online Now

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