Training Course on Threat Hunting with Sysmon and Windows Event Logs

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 landscape, traditional perimeter defenses and signature-based antivirus solutions are often insufficient to combat sophisticated adversaries and **Advanced Persistent Threats (APTs)**. Organizations face a critical need for proactive strategies to detect and neutralize stealthy attacks that bypass conventional security controls. Training Course on Threat Hunting with Sysmon and Windows Event Logs empowers cybersecurity professionals with the essential skills and methodologies to **proactively hunt for malicious activity**, **minimize dwell time**, and significantly **bolster their organizational security posture**. Participants will gain hands-on expertise in leveraging granular telemetry from Sysmon and the rich data within Windows Event Logs, transforming raw log data into actionable **threat intelligence**.

This program delves deep into the art and science of **adversary detection**, focusing on real-world scenarios and practical application. By mastering the configuration and analysis of **Sysmon events** and critical **Windows Event IDs**, attendees will learn to identify subtle indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with advanced threats, including **insider threats**, **ransomware**, and **living-off-the-land attacks**. The course emphasizes a **hypothesis-driven threat hunting methodology**, integrating **MITRE ATT&CK framework** mapping for comprehensive threat coverage. Participants will acquire the ability to build effective detection rules, conduct in-depth investigations, and contribute to a robust **Security Operations Center (SOC)** environment, ultimately enhancing their organization's ability to **respond to cyber incidents** with greater speed and precision.

Programme Curriculum

Training Course on Threat Hunting with Sysmon and Windows Event Logs

Introduction

In today's dynamic cyber landscape, traditional perimeter defenses and signature-based antivirus solutions are often insufficient to combat sophisticated adversaries and **Advanced Persistent Threats (APTs)**. Organizations face a critical need for proactive strategies to detect and neutralize stealthy attacks that bypass conventional security controls. Training Course on Threat Hunting with Sysmon and Windows Event Logs empowers cybersecurity professionals with the essential skills and methodologies to **proactively hunt for malicious activity**, **minimize dwell time**, and significantly **bolster their organizational security posture**. Participants will gain hands-on expertise in leveraging granular telemetry from Sysmon and the rich data within Windows Event Logs, transforming raw log data into actionable **threat intelligence**.

This program delves deep into the art and science of **adversary detection**, focusing on real-world scenarios and practical application. By mastering the configuration and analysis of **Sysmon events** and critical **Windows Event IDs**, attendees will learn to identify subtle indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with advanced threats, including **insider threats**, **ransomware**, and **living-off-the-land attacks**. The course emphasizes a **hypothesis-driven threat hunting methodology**, integrating **MITRE ATT&CK framework** mapping for comprehensive threat coverage. Participants will acquire the ability to build effective detection rules, conduct in-depth investigations, and contribute to a robust **Security Operations Center (SOC)** environment, ultimately enhancing their organization's ability to **respond to cyber incidents** with greater speed and precision.

Course Duration

10 days

Course Objectives

1. Learn to deploy and optimize Sysmon for maximum **endpoint telemetry** and **behavioral anomaly detection**.
2. Develop expert-level skills in parsing, filtering, and correlating critical **Windows Event IDs** for **forensic investigations** and **incident response**.
3. Implement **hypothesis-driven threat hunting** and **intelligence-led hunting** techniques to uncover hidden threats.
4. Map observed adversary TTPs to the **MITRE ATT&CK knowledge base** for comprehensive threat understanding and improved detection engineering.
5. Identify and analyze common LotL techniques leveraging legitimate system tools as observed in **Sysmon** and **Event Logs**.
6. Hunt for and analyze various **persistence techniques** utilized by adversaries, including **registry modifications**, **scheduled tasks**, and **service creation**.
7. Detect and track **lateral movement** activities across Windows networks using **authentication logs**, **process creation events**, and **network connections**.
8. Analyze **Sysmon Event ID 1** and related logs to detect and understand **malware execution**, **process injection**, and **anti-forensic techniques**.
9. Identify indicators of **credential dumping**, **pass-the-hash**, and other **credential theft** techniques.
10. Utilize **Sysmon Event ID 3** and **DNS queries** to identify suspicious **command and control (C2)** communications and **data exfiltration**.
11. Learn to create and implement effective **detection rules** for SIEM and EDR platforms based on Sysmon and Windows Event Log data.
12. Understand how threat hunting findings feed into and enhance the **incident response lifecycle** and **digital forensics investigations**.

13. Integrate **threat intelligence feeds** to enrich hunting activities and contextualize suspicious behaviors.

Organizational Benefits

- Proactively identify and neutralize threats before they cause significant damage, dramatically shortening the time adversaries remain undetected within the network.
- Strengthen overall organizational security by uncovering hidden vulnerabilities and gaps in existing defenses, leading to more robust detection and prevention capabilities.
- Provide richer, more accurate **threat intelligence** and **forensic artifacts** to accelerate incident detection, containment, eradication, and recovery.
- Validate the effectiveness of current security tools and processes, guiding future investments in **security technologies** and **detection engineering**.
- Shift from a reactive to a proactive security stance, anticipating and preventing future attacks by understanding adversary TTPs.
- Equip security analysts and incident responders with advanced skills in **log analysis**, **behavioral analytics**, and **threat intelligence** utilization.
- Generate comprehensive audit trails and evidence for regulatory compliance and internal security audits.

Target Audience

1. SOC Analysts
2. Incident Responders.
3. Security Engineers.
4. Digital Forensic Analysts.
5. System Administrators with Security Responsibilities
6. Red Teamers / Penetration Testers.
7. Cybersecurity Consultants
8. Security Architects.

Course Outline

Module 1: Introduction to Threat Hunting and Windows Logging Fundamentals

- Understanding the Threat Landscape
- Defining Threat Hunting
- Windows Logging Ecosystem
- Introduction to Sysmon.
- Setting Up a Lab Environment
- **Case Study:** Analyzing a "noisy" network segment and developing an initial hypothesis for potential insider threat activity.

Module 2: Deep Dive into Sysmon Configuration and Event IDs

- Sysmon Installation and Configuration
- Understanding Key Sysmon Event IDs
- Understanding Key Sysmon Event IDs
- Advanced Sysmon Filtering and Rules
- Sysmon Event Log Structure and Correlation.
- **Case Study:** Detecting a suspicious process creation linked to a known malware family and tracing its network connections

Module 3: Windows Event Log Analysis for Security

- Windows Event Viewer Mastery.
- Essential Security Event IDs
- Essential Security Event IDs
- System and Application Event Logs
- Log Retention and Forwarding Strategies.
- **Case Study:** Investigating failed logon attempts (Event ID 4625) and successful administrative logons (Event ID 4624, 4672) to identify potential brute-force attacks or privilege escalation.

Module 4: Threat Hunting with MITRE ATT&CK Framework

- Introduction to MITRE ATT&CK.
- Mapping Sysmon and Event Logs to ATT&CK
- Developing ATT&CK-Aligned Hunting Hypotheses
- Using ATT&CK Navigator for Visualization and Analysis.
- Hunting for Initial Access and Execution Techniques
- **Case Study:** Hunting for "Phishing" (T1566) by analyzing email client logs and subsequent process creation events related to suspicious attachments.

Module 5: Detecting Persistence Mechanisms

- Hunting for Scheduled Tasks.
- Registry Run Keys / Startup Folder.
- Service Creation and Modification.
- WMI Persistence
- DLL Search Order Hijacking.
- **Case Study:** Discovering a backdoor established through a malicious scheduled task, using correlated Sysmon and Security Event logs.

Module 6: Uncovering Lateral Movement

- Remote Services
- Lateral Tool Transfer.
- Credential Dumping (T1003) for Lateral Movement.
- Pass the Hash / Pass the Ticket
- Lateral Movement with PsExec and PowerShell Remoting.
- **Case Study:** Tracing an attacker's lateral movement from a compromised workstation to a domain controller using successful network logons (Event ID 4624) and subsequent credential access attempts.

Module 7: Command and Control (C2) Detection

- DNS Tunneling
- Uncommon Network Protocols.
- Web Protocols.
- Named Pipes (T1021.005) and C2
- Detecting Domain Fronting and Cloud-Based C2
- **Case Study:** Identifying a suspicious outbound network connection (Sysmon Event ID 3) to an unusual IP address, followed by abnormal DNS queries, indicating a C2 channel.

Module 8: Malware and Process Analysis

- Process Injection
- Process Hollowing / Herpaderping.

- Reflective Code Loading.
- Analyzing Parent-Child Process Relationships
- DLL Loading and Module Events.
- **Case Study:** Uncovering a process injection attack by correlating Sysmon Event ID 8 (CreateRemoteThread) with a suspicious parent process that spawned a seemingly legitimate child process.

Module 9: Hunting for Data Exfiltration and Collection

- Archive Collected Data
- Data Compressed
- Exfiltration Over C2 Channel.
- Exfiltration to Cloud Storage
- Removable Media (T1091) and Data Staging
- **Case Study:** Detecting the archival of sensitive documents into a password-protected zip file, followed by an outbound network connection to a public file-sharing service.

Module 10: Advanced PowerShell and Scripting Attacks

- PowerShell Logging and Script Block Logging.
- Hunting for Obfuscated PowerShell.
- PowerShell Downgrade Attacks.
- Abuse of Built-in PowerShell Cmdlets
- Hunting for Living-Off-The-Land Binaries (LOLBins) and Scripts
- **Case Study:** Uncovering a malicious PowerShell script executed via a WMI event consumer, bypassing traditional antivirus by using system binaries.

Module 11: Insider Threat Hunting with Logs

- User Behavior Analytics (UBA) with Logs
- Accessing Sensitive Data.
- Privilege Escalation Attempts analysis.
- Unusual Logons and Account Usage
- Data Staging and Exfiltration by Insiders
- **Case Study:** Detecting an insider attempting to access highly restricted financial documents outside their normal working hours, followed by attempts to copy them to removable media.

Module 12: Building Custom Detections and SIEM Integration

- Leveraging Sysmon and Event Logs for SIEM Rules.
- Correlation Rules and Use Cases
- Threat Intelligence Feed Integration
- Baselines and Anomaly Detection.
- Alert Triage and Prioritization.
- **Case Study:** Building a SIEM correlation rule to detect a sequence of events: a failed logon, followed by a suspicious process creation, then an outbound connection to an untrusted IP.

Module 13: Digital Forensics & Incident Response with Logs

- Log Collection and Preservation
- Timeline Reconstruction
- Evidence Correlation and Analysis
- Reporting and Documentation.
- Post-Incident Hardening and Remediation

- **Case Study:** Reconstructing a ransomware attack chain, from initial compromise to file encryption, using log data.

Module 14: Automation and Orchestration for Threat Hunting

- Scripting for Log Analysis.
- Using Open-Source Tools for Log Analysis
- Introduction to SOAR Concepts
- Automated Response Actions based on Hunting Findings.
- Developing Playbooks for Specific Hunting Scenarios
- **Case Study:** Developing a PowerShell script to automatically parse Sysmon network connection events and cross-reference destination IPs against a blacklist.

Module 15: Advanced Hunting Techniques and Future Trends

- Memory Forensics for Advanced Persistence
- Endpoint Detection & Response (EDR) in Threat Hunting.
- Machine Learning and AI in Threat Hunting.
- Cloud Environment Log Analysis
- Zero Trust Architecture and Threat Hunting
- **Case Study:** Using EDR telemetry to hunt for specific behavioral patterns associated with a novel zero-day exploit, augmenting traditional log analysis.

Training Methodology

This course adopts a highly **interactive and hands-on methodology**, combining theoretical concepts with practical application.

- **Instructor-Led Presentations:** Clear and concise explanations of core concepts.
- **Live Demonstrations:** Real-time walkthroughs of tools and techniques.
- **Extensive Lab Exercises:** Practical, scenario-based labs designed to reinforce learning and build muscle memory, conducted in a dedicated virtual lab environment.
- **Case Studies & Real-World Scenarios:** Analysis of actual cyberattack patterns and how Sysmon and Event Logs were used for detection.
- **Group Discussions & Collaboration:** Fostering knowledge sharing and problem-solving among participants.
- **Q&A Sessions:** Dedicated time for addressing participant queries and clarifying concepts.
- **Capstone Hunting Exercise:** A comprehensive, multi-stage exercise where participants apply learned skills to hunt for an adversary in a simulated environment.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.orgUpcoming 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

Start Date	End Date	Location	Price
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