

AI-Powered

Advanced Cyber Threat Hunting & DFIR Training

Digital Forensics & Incident Response



Course Highlights



40-Hour
Instructor-Led
Training



Learn from
Industry Experts



Highly Interactive
and Dynamic
Sessions



20+ AI-driven
Hands-On
Labs



Capstone
Challenges



Learn with
Real-World
Scenarios



Access to Recorded
Sessions



Extended Post
Training Support



Career Guidance
and Mentorship

About Course

The AI-powered Advanced Threat Hunting, Digital Forensics, and Incident Response (DFIR) Training equips security professionals with elite skills to detect, investigate, and respond to sophisticated cyber threats across enterprise environments. Participants learn core DFIR competencies, including persistence, lateral movement, and credential abuse hunting, memory and disk forensics, malware analysis, and network-based C2 detection.

What sets this course apart is the integration of AI-accelerated workflows, enabling analysts to handle massive datasets, automate repetitive tasks, and generate actionable reports faster, while retaining full control over investigative judgment, hypothesis testing, and evidence interpretation. By combining hands-on labs, real-world scenarios, and portable AI techniques, learners gain practical experience that applies to any enterprise environment, preparing them to deliver precise, executive-ready investigations efficiently and confidently.



Course Objectives

Upon successful completion of the training, participants will be able to:

- ✔ Hunt persistence, lateral movement, and credential abuse
- ✔ Perform memory, disk, and malware forensics effectively
- ✔ Analyze network traffic for C2 and anomalies
- ✔ Apply AI to accelerate investigative workflows
- ✔ Generate executive-ready and legally defensible incident reports
- ✔ Correlate multi-source logs for advanced threat detection
- ✔ Design and execute enterprise-scale threat hunting exercises
- ✔ Develop portable DFIR skills across tools and environments

Target Audience

This training is ideal for:

- ✔ **SOC Analysts (Tier 2+)** seeking to advance beyond alert triage to proactive hunting
- ✔ **Incident Responders** looking to enhance investigation techniques and efficiency
- ✔ **Security Engineers** responsible for building detection engineering capabilities
- ✔ **Digital Forensic Analysts** expanding into threat hunting methodologies
- ✔ **Penetration Testers** who want to understand defensive detection techniques
- ✔ **Security Architects** responsible for designing security monitoring solutions



Pre-requisites

Required Technical Knowledge

Windows Systems (Essential)

- ✓ Windows Event Log analysis (Security, System, Application logs)
- ✓ Registry structure and common keys related to security
- ✓ Windows authentication mechanisms and security tokens
- ✓ PowerShell fundamentals and security-related cmdlets
- ✓ Windows services, scheduled tasks, and startup mechanisms

Networking Fundamentals (Essential)

- ✓ TCP/IP protocol stack operations
- ✓ Common protocols and their security implications (HTTP/S, DNS, SMB, RDP)
- ✓ Basic packet analysis concepts
- ✓ Network traffic patterns and anomaly identification

Security Concepts (Essential)

- ✓ Common attack vectors and techniques
- ✓ Basic log analysis and correlation
- ✓ Security monitoring principles
- ✓ Malware behavior fundamentals

Additional Skills (Highly Recommended)

- ✓ Basic Linux command-line operations (can use an OS without GUI)
- ✓ Virtualization experience (VMware/VirtualBox/Hyper-V/Docker)
- ✓ Basic scripting and decent programming abilities (PowerShell/Bash/Python/C/C++)
- ✓ Understanding of Applied Statistical Analysis (Maths and Stats)
- ✓ Familiarity with MITRE ATT&CK framework
- ✓ Willingness to experiment with AI tools during hands-on labs (we teach this from scratch - no prior LLM experience required)

Required Experience Level

- ✓ **Professional:** Minimum 1 year in an IT security role OR
- ✓ **Hands-on:** Demonstrable equivalent experience through labs, CTFs, or personal projects

Note : This is a technically rigorous course. Participants without these prerequisites will struggle significantly with the pace and depth of the material.

Technical Requirements

- ✓ Laptop with 8GB+ RAM (16GB recommended) for running VMs and analysis tools AI Setup (choose one):
 - ✓ **Local-only (Free):** Ollama + local models on your laptop (slower but private)
 - ✓ **API-based (~\$5-20 total):** OpenAI/Groq/Gemini credits for faster responses
- ✓ All course materials, datasets, and setup guides provided
- ✓ Labs work with either setup - you choose based on your

Course Content

Module 1

Advanced Security Operations

- ✓ SOC Metrics and KPIs
- ✓ Purple Team Integration
- ✓ Detection Engineering Methodology
- ✓ SIEM and SOAR Optimization
- ✓ Implementing MITRE ATT&CK Framework

AI for DFIR: realistic use cases, limitations, and validation requirements

Lab: Set up your AI workflow environment (Ollama OR API keys + basic CLI/integration)

Module 2

Persistence Threat Hunting

- ✓ Advanced Registry Analysis Techniques
- ✓ WMI Event Subscription Detection
- ✓ COM Hijacking and DLL Search Order
- ✓ Scheduled Task Analysis and Anomaly Detection
- ✓ Multi-Log Correlation for Persistence Hunting

AI for query generation (natural language → platform-specific syntax)

Lab: Detecting Advanced Persistence Mechanisms

Module 3 Lateral Movement Analysis

- ✓ Pass-the-Hash and Pass-the-Ticket Detection
- ✓ Detecting Authenticated Remote Execution
- ✓ RDP/VPN Access Analysis
- ✓ WMI and PowerShell Remoting Abuse
- ✓ Kerberos Protocol Analysis

AI for evidence mapping (correlate events across systems, analyst validates chains)

Lab: Lateral Movement Investigation

Module 4 Network-Based Threat Hunting

- ✓ Statistical Approaches to Traffic Analysis
- ✓ Beacon Pattern Detection in Network Traffic
- ✓ DNS and HTTP Tunneling Identification
- ✓ TLS/SSL Inspection Strategies
- ✓ Network Timeline Reconstruction

AI to generate Python anomaly detection code (you review, run, interpret results)

Lab: Network Traffic Analysis for C2 Detection

Module 5 Credential Theft Investigation

- ✓ Windows Authentication Mechanisms (In-depth)
- ✓ Detecting Credential Dumping Operations
- ✓ Kerberoasting and AS-REP Roasting Detection
- ✓ DPAPI Analysis for Credential Extraction
- ✓ Domain Controller Authentication Log Analysis

AI-assisted log correlation for credential abuse

Lab: Credential Abuse Incident Response

Module 6 Malware Analysis Techniques

- ✓ Static Analysis with Binary Analysis Tools
- ✓ Dynamic Analysis in Isolated Environments
- ✓ Memory Dumping and Analysis for Malware
- ✓ Anti-Analysis Technique Identification
- ✓ Process Injection and Hollowing Detection
- ✓ Natural-language malware analysis with GHIDRA / IDA /
- ✓ Radare2 (extract IOCs, behaviors, key functions, configs)

Lab: Analyzing Real-World Malicious Samples

Module 7

Memory Forensics

- ✓ Memory Acquisition Methods and Challenges
- ✓ Process, DLL, and Driver Analysis
- ✓ Detecting Rootkits and Bootkits
- ✓ Finding Injected Code and Hidden Processes
- ✓ Analyzing Malware Artifacts in Memory

AI to rank suspicious entries from Volatility output (you validate and extract)

Lab: Memory Analysis for Hidden Threats

Module 8

Disk Forensics

- ✓ Analysis for Proof of Execution
- ✓ Analysis for Proof of File / Folder Access
- ✓ Extracting Windows Event Logs for Offline Analysis
- ✓ Extracting Windows Registry for Offline Analysis
- ✓ MFT Analysis for File System Artifacts
- ✓ Advanced File System Artifact Analysis
- ✓ Timeline Creation and Analysis
- ✓ Super Timeline Creation and Analysis

AI to filter timeline noise and draft incident narrative (you verify against artifacts)

Lab: Disk-Based Investigation and Evidence Recovery

Module 9 Final Challenge

- ✓ Perform Threat Hunting, Incident Response, Malware
- ✓ Analysis and Forensics, and Solve and Answer Questions
- ✓ Apply what you learnt so far
- ✓ Optional: build your personal AI-assisted DFIR workflow (portable stack + report deliverable)



Lab Contents

Core DFIR Labs (Traditional Skills + AI-Accelerated Options)

- ✓ Detection Engineering Lab Setup
- ✓ Hands-on writing windows detection (traditional + AI query generation comparison)
- ✓ Hands-on writing complex multi-source detection
- ✓ Proactive Hunt for confirming the presence of adversary
- ✓ Hunt for credential abuse (manual correlation + AI-assisted pivot suggestions)
- ✓ Hunt for evidence of adversary across Persistence points
- ✓ Hunt for advanced persistence techniques
- ✓ Evidence identification for Lateral Movement
- ✓ Hunt for the detection of Lateral Movement
- ✓ Credential Tracking for Lateral Movement Hunting

Malware Analysis Labs (AI-Driven Investigation)

- ✓ Malware Analysis Lab Setup (radare2 + MCP integration, safe workflow, structured output capture) Static Malware Analysis (natural language → functions/strings/IOCs extraction)
Natural-language reverse engineering lab (radare2 MCP tool calls: triage sample → extract IOCs/behaviors → draft capability report)
- ✓ Dynamic Malware Analysis (behavior capture → LLM-assisted IOC + behavior summary, analyst validated)
- ✓ Hunting for Malware via YARA rules (LLM-assisted rule drafting + false-positive review)

Network & Forensics Investigation Labs

- ✓ Network Hunting for Malware Beacons
- ✓ Network Hunting for DNS Exfiltration
- ✓ Network Hunting for Domain Fronting Techniques
- ✓ Hands-on Hunting Report Writing with Hand off to Incident Response Teams
- ✓ Forensics Evidence Acquisition
- ✓ Analysing Disk Image
- ✓ Analysing Memory Image
- ✓ Analysing Filesystem Image
- ✓ Writing Threat Intel Reports

Capstone Challenge

Final Exercise Challenge: To be completed by students, apply everything learnt so far and solve enterprise scale breach, write reports at the end



Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on

