INFOSECTRAIN

Advanced Cyber Threat Hunting & DFIR Training

INFOSECTRAIN

Course Highlights

- 40-Hour LIVE Instructor-led Training
- 25+ Hands-on Labs
- Real-time Simulation
- Learn with Real-world Scenarios
- Real-world Use Cases
- Access to Recorded Sessions
- Career Guidance and Mentorship
- Guaranteed Lowest Price
- Extended Post-training Support

INFOSECTRAIN

About Course

This skill-based training is designed for cybersecurity professionals looking to master Threat Hunting and DFIR methodologies. Participants will gain hands-on experience in detecting, analyzing, and mitigating cyber threats using hybrid detection techniques, active defense strategies, and real-world case studies. The course covers MITRE ATT&CK, NIST Incident Response, malware analysis, persistence techniques, and adversary tracking, ensuring learners can respond to sophisticated cyberattacks. Participants will also explore network hunting, memory forensics, disk forensics, and anti-forensic techniques, equipping them with the ability to uncover and analyze hidden attack footprints. The training culminates in a capstone challenge, where participants reconstruct a full attack chain and produce both technical and executive reports.

INFOSECTRAIN

Target Audience

SOC Analysts (Tier 2+) seeking to advance beyond alert triage to proactive hunting

Digital Forensic Analysts expanding into threat hunting methodologies

Security Architects responsible for designing security monitoring solutions

Security Engineers responsible for building detection engineering capabilities

Penetration Testers who want to understand defensive detection techniques

Incident Responders looking to enhance investigation techniques and efficiency

INFOSECTRAIN

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)

- 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

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

INFOSECTRAIN

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

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.

INFOSECTRAIN

Course Objectives

Upon completion of the course, participants will be able to:

- Explain threat hunting workflows, DFIR lifecycle stages, and identify critical Windows artifacts.
- Create detection rules using MITRE ATT&CK (TTP mapping) and develop hypotheses for proactive hunting.
- Detect credential abuse, lateral movement, and persistence mechanisms while performing basic static/dynamic malware analysis.
- Acquire and analyze disk, memory, and registry artifacts, and use open-source tools to build artifact timelines.
- Contain threats using NIST SP 800-61 principles and document findings for handoff to DFIR teams.
- Map adversary behaviors to MITRE D3FEND mitigations and generate actionable alerts from STIX reports.
- Investigate full attack chains—from initial access to exfiltration—and produce both technical and executive reports for mock breaches.

INFOSECTRAIN

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

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
- Mul-Log Correlation for Persistence Hunting

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

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

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

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

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

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

Lab: Disk-Based Investigation and Evidence Recovery

INFOSECTRAIN

Module 9: Final Challenge

- Perform Threat Hunting, Incident Response, Malware Analysis and Forensics
- Solve and Answer Questions
- Apply what you have learnt so far
- Each module includes technical deep dives, practical demonstrations, and hands-on lab exercises.
- Participants must complete lab assignments to receive certification.

INFOSECTRAIN

Lab Contents

- Detection Engineering Lab Setup
- Hands-on writing Windows detection
- Hands-on writing complex multisource detection
- Proactive Hunt for confirming presence of adversary
- Hunt for credential abuse or malicious credential usage
- Hunt for evidence of adversary across Persistence points
- Hunt for advanced persistence techniques
- Evidence identification for Lateral Movement
- Hunt for detection of Lateral Movement
- Credential Tracking for Lateral Movement Hunting
- Malware Analysis Lab Setup
- Static Malware Analysis
- Dynamic Malware Analysis
- Hunting for Malware via YARA rules
- 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

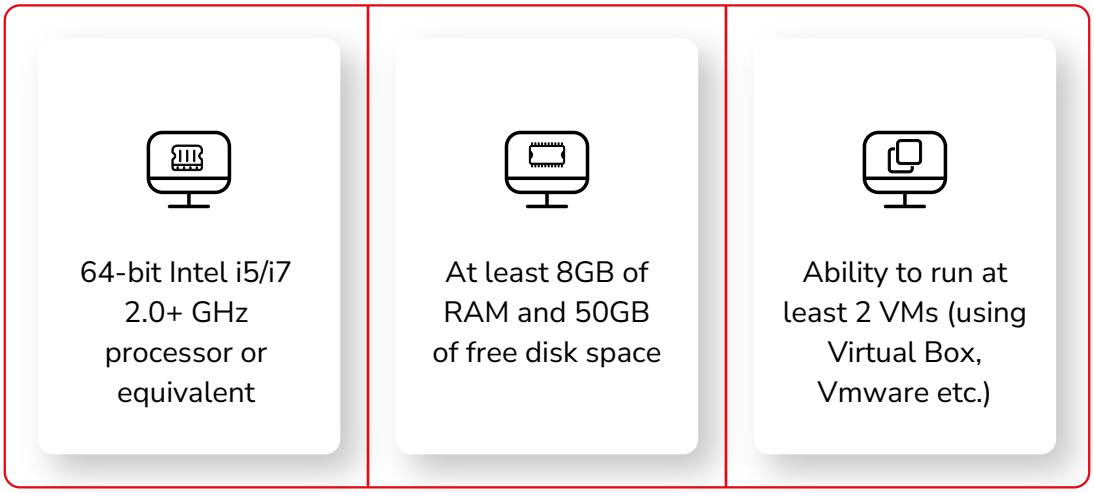
INFOSECTRAIN

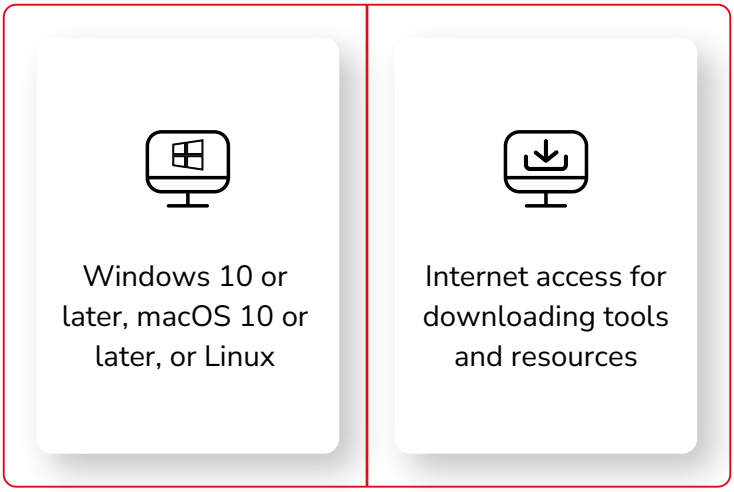
Final Exercise Challenge

To be completed by students - apply everything learnt so far and solve enterprise scale breach - write reports at the end

INFOSECTRAIN

System Requirements





INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on