INFOSECTRAIN
Educate. Excel. Empower.

AI-Powered

ADVANCED THREAT HUNTING

DIGITAL FORENSICS & INCIDENT RESPONSE (DFIR) TRAINING

INFOSECTRAIN

Course Highlights

- 40-Hour LIVE Instructor-led Training
- AI-Assisted Workflows Embedded Across Every Module
- Integrated Capstone: Real Enterprise Breach Simulation
- Hands-On Labs: Threat Hunting, Forensics, Malware Analysis
- Build YARA Rules, SOAR Playbooks & Detection Logic
- From Alert to Executive Report: Full Investigation Lifecycle
- Learn from Industry Experts with Real-World Experience
- Career Guidance, Mentorship, Post-Training Support
- Access to Recorded Sessions

INFOSECTRAIN

About Course

Security threats don't wait, and neither should your investigations. The Advanced Threat Hunting Digital Forensics & Incident Response (DFIR) Training from InfosecTrain is built for security professionals ready to move beyond alert triage and take full ownership of enterprise-scale investigations. Participants develop elite, hands-on skills across threat hunting, digital forensics, incident response, and detection engineering, tackling real attack scenarios from first alert to final report.

AI-assisted workflows are embedded throughout, teaching participants to accelerate investigations without compromising analytical judgment. The course culminates in an integrated capstone challenge that simulates a realistic enterprise breach, from the first alert through to containment, reporting, and post-incident detection backlog creation.

INFOSECTRAIN

Course Objectives

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

- Build and execute ATT&CK-driven threat hunting hypotheses across enterprise environments
- Detect and investigate persistence, lateral movement, and credential abuse using multi-source telemetry
- Hunt identity-based threats across endpoint, Active Directory, and cloud environments, including M365, Entra ID, and AWS
- Perform memory and disk forensics to uncover hidden threats, attacker activity, and forensic artifacts
- Analyze network traffic to identify C2 communication, beaconing, DNS tunneling, and data exfiltration
- Conduct malware triage and analyst-level reverse engineering to extract IOCs and behavioral indicators
- Write and tune production-grade detections across SIEM, EDR, and SOAR platforms
- Build and automate SOC workflows using SOAR playbooks and AI-assisted tooling
- Apply AI-assisted workflows to accelerate investigations while maintaining full analyst validation
- Produce executive-ready and technically defensible incident reports
- Manage the full incident response lifecycle from initial alert to containment and post-incident detection backlog

INFOSECTRAIN

Target Audience

This training is ideal for:

- SOC Analysts
- Tier 1 analysts who want to move into strong Tier 2 roles
- Tier 2 analysts who want to become advanced Tier 3 analysts
- Security analysts who want to move beyond alert triage into full investigation ownership
- Security professionals who are looking to equip AI-based workflows Incident Responders
- Responders who want stronger endpoint, identity, memory, disk, and network investigation skills
- Analysts who need to produce clear technical and executive reports
- Threat Hunters
- Professionals who want to build ATT&CK-based hunt hypotheses
- Detection Engineers
- Security engineers building SIEM, EDR, and SOAR detections
- Forensic analysts who want to expand into enterprise threat hunting
- Managers who want to understand what strong L2 and L3 capability should look like

INFOSECTRAIN

Pre-requisites

Participants are recommended to have:

- Basic understanding of Windows and Linux OS
- Familiarity with networking concepts, SOC operations, and common attack techniques
- Exposure to log analysis, DFIR concepts, and SIEM query writing
- Basic scripting knowledge: PowerShell, Python, or Linux command line
- Willingness to use and validate AI-assisted workflows
- At least 1 year of experience in IT, SOC, security, or equivalent hands-on lab experience

INFOSECTRAIN

Course Content

Module 1 Enterprise Threat Hunting and DFIR Operating Model

- Modern SOC L2 and L3 responsibilities
- Threat hunting vs detection engineering vs incident response
- Investigation lifecycle from alert to executive reporting
- ATT&CK-driven hypothesis building
- Evidence types in enterprise investigations
- Telemetry quality and blind spot mapping
- Analyst decision-making during uncertainty
- Common mistakes in L2 to L3 escalation
- Building an investigation notebook
- AI usage boundaries in real investigations

Hands-On Labs:

- Build the analyst investigation workspace
- Map an enterprise attack story to ATT&CK
- Convert a weak SOC alert into a full investigation plan
- Create a telemetry coverage and blind spot matrix
- Use AI to generate hypotheses, then manually validate or reject them

Module 2 Production Telemetry, Log Normalization, and SIEM Hunting

- Windows event logs that actually matter
- Sysmon and EDR-style telemetry
- Authentication telemetry from endpoints and domain controllers
- DNS, proxy, firewall, VPN, and web logs
- Cloud and identity log concepts
- OCSF style normalization thinking
- Time synchronization and timestamp issues
- Field mapping across SIEM platforms
- Detection logic portability
- Query writing strategy for SPL, KQL, EQL, Sigma, and SQL style syntax

Hands-On Labs:

- Ingest or load the prebuilt enterprise telemetry pack
- Normalize raw logs into investigation-ready fields
- Write the same hunt across SPL, KQL, EQL, and Sigma
- Use AI to translate queries, then test for logic drift
- Build a reusable hunt notebook

Module 3 Detection Engineering in Production

- Detection engineering lifecycle
- Detection objective and data requirement
- Behavior-based vs IOC-based detection
- Atomic detection vs correlation detection
- Thresholds, baselines, and suppression logic
- False positive analysis
- Detection testing with replayed attack data
- Detection tuning without killing visibility
- Detection documentation
- Converting hunts into production detections

Hands-On Labs:

- Write a detection from an ATT&CK technique
- Test detection against clean and malicious telemetry
- Tune noisy detection without losing true positives
- Convert detection into Sigma and SIEM-specific logic
- Use AI to draft detection logic, then perform analyst QA

Module 4 Advanced Persistence Hunting

- Registry run keys and autoruns
- Services and drivers
- Scheduled tasks
- WMI event subscriptions
- DLL search order hijacking
- COM hijacking
- Startup folders and logon scripts
- PowerShell profile abuse
- Living off the land persistence
- Persistence timeline reconstruction

Hands-On Labs:

- Hunt registry persistence using endpoint telemetry
- Investigate suspicious scheduled tasks
- Detect WMI event subscription persistence
- Identify COM hijacking indicators
- Build a persistence timeline from multiple artifacts
- Use AI to cluster persistence evidence, then verify manually

Module 5 Identity Threat Hunting (Endpoint and Cloud)

- Windows authentication essentials for hunters
- LSASS access and credential dumping indicators
- Credential theft via LOLBins
- DPAPI and browser credential theft indicators
- Reading AD attack signatures without a range: Kerberoasting (4769 RC4), AS-REP roasting (4768 no preauth), Pass-the-Hash (4624 type 3 NTLM anomalies), DCSync (4662 replication GUIDs), Golden and Silver Ticket
- Service account and privileged account abuse hunting
- Cloud identity attacks: OAuth illicit consent grant, device code phishing, AiTM session and token theft, MFA fatigue, PRT abuse, Golden SAML

Hands-On Labs:

- Analyze failed and successful authentication chains
- Investigate LSASS access from endpoint telemetry
- Identify Kerberoasting and DCSync signatures in prebuilt DC logs
- Hunt OAuth consent abuse and malicious inbox rules in M365
- Detect AiTM token theft and MFA fatigue in sign-in logs
- Use AI to suggest pivots & then validate using raw evidence

INFOSECTRAIN

Module 6 Lateral Movement and Remote Execution Hunting

- Admin share abuse
- PsExec style execution
- WMI remote execution
- PowerShell remoting
- RDP abuse
- SMB lateral movement patterns
- WinRM activity
- Remote service creation
- VPN and jump server investigations
- Lateral movement chain reconstruction
- Source host, target host, and user mapping

Hands-On Labs:

- Hunt remote service creation
- Investigate WMI-based lateral movement
- Trace RDP movement through logs
- Identify suspicious SMB admin share activity
- Use AI to build an ATT&CK Flow Graph

INFOSECTRAIN

Module 7 Network Threat Hunting and C2 Detection

- Network hunting methodology
- DNS hunting
- HTTP and HTTPS beaconing
- TLS and certificate indicators
- Domain fronting concepts
- Suspicious user agents
- Long connection and low-and-slow patterns
- DNS tunneling
- Data exfiltration signals
- PCAP to SIEM workflow
- Network timeline reconstruction
- Statistical hunting without overcomplication

Hands-On Labs:

- Detect beaconing using proxy and DNS logs
- Hunt DNS tunneling from noisy traffic
- Analyze PCAP for C2 behavior
- Detect suspicious TLS patterns

INFOSECTRAIN

Module 8 Malware Triage and Analyst-Level Reverse Engineering

- Safe malware handling workflow
- Static triage
- Strings, imports, and sections
- Packer and obfuscation indicators
- Dynamic behavior analysis
- Process, file, registry, and network behavior
- YARA rule development
- Disassembly and decompilation basics in Ghidra
- Anti-analysis recognition as hunting signals
- Injection and shellcode technique identification

Hands-On Labs:

- Perform static triage of a suspicious binary
- Identify process injection or hollowing indicators
- Draft and test a YARA rule from RE findings
- Ghidra: locate the C2 config and decode obfuscated strings
- Manually unpack a simple packed sample
- Identify the injection technique in a given binary
- Use AI to summarize functions and behaviors from tool output

Module 9 Memory Forensics & Cloud Threat Hunting

- Memory acquisition considerations
- Volatility workflow
- Process analysis
- DLL and handle analysis
- M365 Unified Audit Log hunting
- Entra ID sign-in and audit hunting
- AWS CloudTrail fundamentals
- Cloud privilege escalation and lateral movement signals

Hands-On Labs:

- Triage a memory image
- Identify suspicious processes and parent-child anomalies
- Extract command line and network indicators
- Use AI to rank suspicious Volatility output
- Hunt a malicious OAuth app plus exfil inbox rule in M365
- Detect service principal credential addition in Entra audit
- AWS EC2 Analysis & Forensics

INFOSECTRAIN

Module 10 Disk Forensics and Enterprise Evidence Recovery

- Evidence handling and forensic soundness
- Disk image triage
- MFT analysis
- Prefetch
- Amcache
- ShimCache
- UserAssist
- Jump Lists
- LNK files
- ShellBags
- Browser artifacts
- Recycle Bin artifacts
- Event log extraction
- Registry hive analysis
- Proving execution, file access, and data staging

Hands-On Labs:

- Analyze a disk image for attacker activity
- Prove execution using multiple artifacts
- Prove file and folder access
- Recover deleted or staged evidence
- Use AI to reduce timeline noise, then manually validate key events

Module 11 Incident Response, Containment, and Case Management

- Incident classification
- Scoping the incident
- Evidence priority
- Containment decision making
- Eradication planning
- Communication during an active incident
- Legal and compliance considerations
- Case notes and chain of custody
- Executive reporting vs technical reporting
- Detection backlog creation after incident closure

Hands-On Labs:

- Convert investigation findings into an incident scope
- Build containment and eradication plan
- Write an executive incident brief
- Write a technical incident report
- Create post-incident detection backlog
- Use AI to draft the first report version

Module 12 AI-Assisted SOC Workflows

- Where AI helps in DFIR
- Where AI fails in DFIR
- Evidence summarization
- Query generation
- Report drafting
- IOC extraction
- Detection explanation
- Local LLM vs API-based workflow
- Prompt injection risks in evidence
- Hallucination control
- Analyst validation loop

Hands-On Labs:

- Build an AI-assisted investigation promptbook
- Convert natural language questions into SIEM queries
- Summarize noisy logs without losing evidence
- Extract IOCs from malware and network notes
- Build a case-specific AI evidence assistant using local files

INFOSECTRAIN

Module 13 SOAR & Automation

- SOAR fundamentals and playbook as code
- Auto-triage and enrichment (VirusTotal, AbuseIPDB, OTX free APIs)
- Alert to case automation

Hands-On Labs:

- Build an enrichment and auto-triage playbook in n8n
- Run a phishing alert through triage end-to-end
- Using AI to draft playbook logic

Module 14 Integrated Capstone - Enterprise Breach Investigation

Scenario: A user endpoint is compromised through phishing. The attacker establishes persistence, steals credentials, moves laterally, accesses sensitive files, uses C2, and attempts data exfiltration.

Hands-On Challenge:

- Start with a limited alert context
- Identify initial access evidence
- Confirm persistence
- investigate credential theft
- Trace lateral movement
- Scope affected users and hosts
- Build incident timeline
- Prepare containment plan
- Write executive and technical reports

INFOSECTRAIN

Lab Requirements

To get the most out of this training, participants are recommended to have the following system configuration:

- Laptop or desktop with 8 GB RAM (16 GB recommended)
- 350–500 GB free disk space
- Windows 10/11, macOS, or Ubuntu
- Admin rights to install tools
- Stable internet connection
- Virtualization support enabled

Hardware

A prebuilt lab environment is provided, including memory images, disk images, network captures, and malware samples. No prior setup is required; all datasets, tools, and lab files are ready from Day 1.

Lab Environment

All required DFIR, network analysis, and forensics tools are covered during the course. Software installation is guided by the instructor as part of the training.

Tools

Supports both local and API-based AI setups, giving participants flexibility based on their hardware. Full guidance is provided during the course; no prior AI tool experience required.

AI Setup

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on