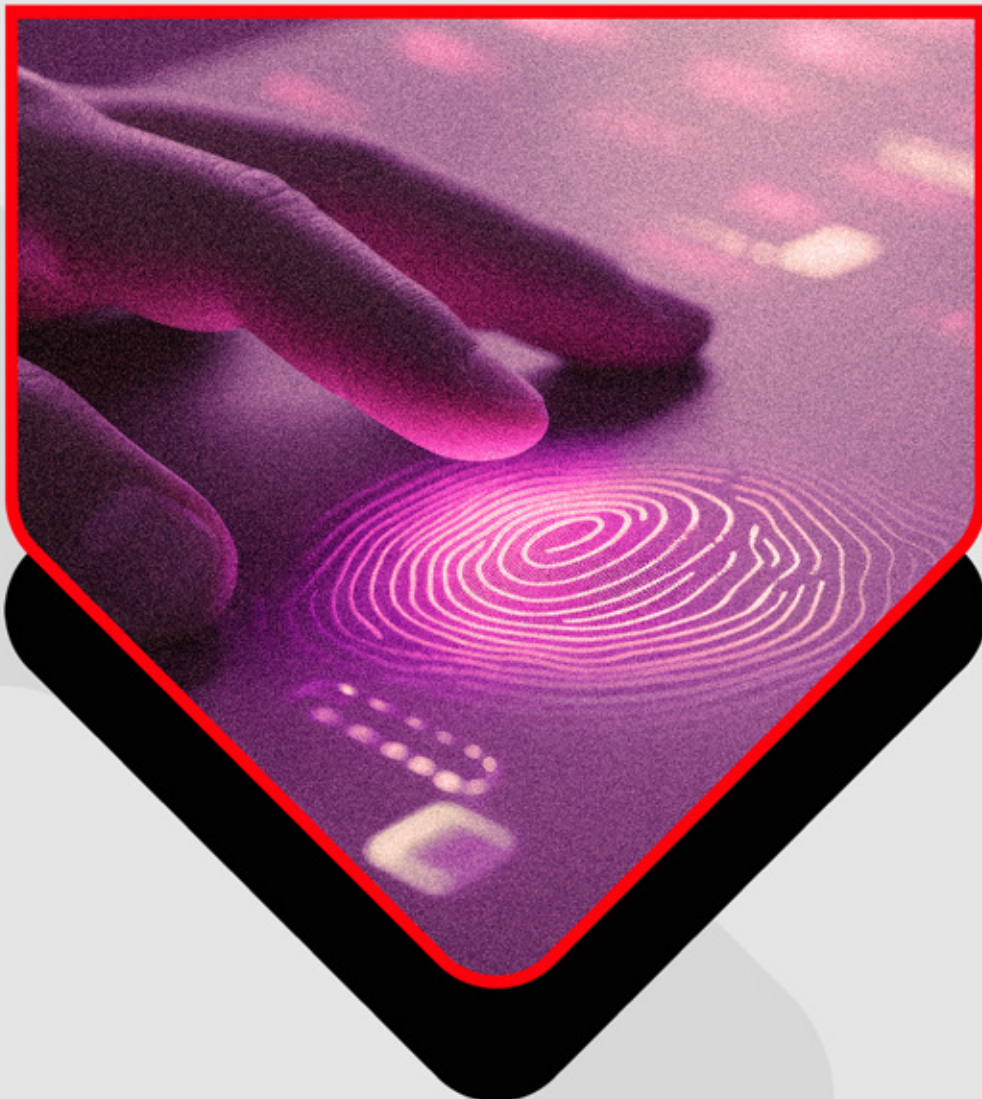


Advanced Threat Hunting

Digital Forensics & Incident Response (DFIR) Training



Course Highlights



40 hours
Instructor-led Training



Learn from
Industry Experts



Highly Interactive and
Dynamic Sessions



Hands-on Labs



Learn with
Real-World Scenarios



Access to
Recorded Sessions



Extended Post
Training Support



Career Guidance and
Mentorship



About Course

This comprehensive course is designed to equip cybersecurity professionals with advanced skills in cyber threat hunting, DFIR (Digital Forensics and Incident Response) tactics. Participants will gain hands-on experience in detecting, analyzing, and mitigating cyber threats using the latest tools and techniques. Through practical labs and real-world scenarios, learners will develop the expertise needed to effectively protect and defend their organizations from sophisticated cyber attacks.

As it is a skill based training, this course focuses deeply into digital forensics, providing a thorough understanding of the techniques and methodologies used to uncover, preserve, and analyze digital evidence. Participants will learn how to conduct comprehensive memory forensics to uncover hidden artifacts and understand the state of a system at the time of an incident. The course also covers disk forensics, teaching participants how to find evidence on file systems, and registry forensics, which involves examining the Windows registry to uncover artifacts related to system and user activity.



Target Audience



Malware Analysts



Digital Forensic
Investigators



Cyber Security
Analysts



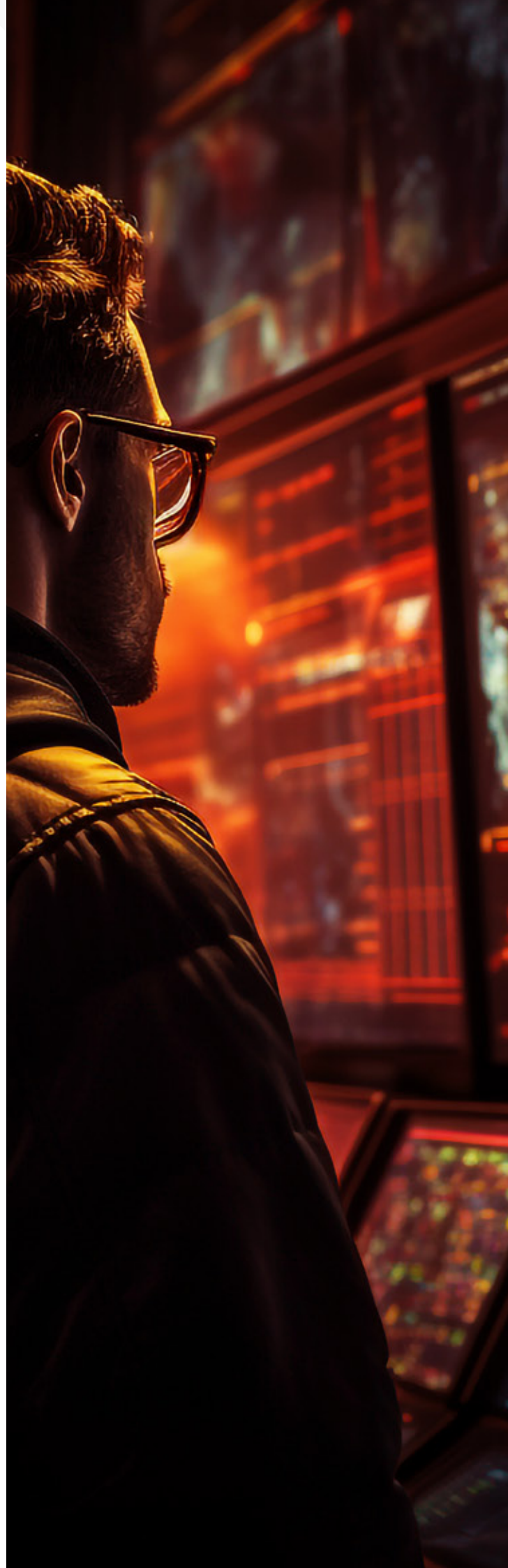
Network Security
Engineers



Red Team
Members/Penetration Testers



Incident Response
Team Members



Pre-Requisites

- ✔ Familiarity of Window and Linux at log level
- ✔ Comprehensive understanding of Information Security and its terms
- ✔ Basics of Networking
- ✔ Experience in Cyber Security is highly recommended

Course Objectives

At the end of the course, you will be able to:

- ✔ Understand the fundamentals of threat hunting and DFIR.
- ✔ Develop and implement detection engineering approaches.
- ✔ Utilize MITRE frameworks (ATT&CK, Engage, D3FEND) for threat analysis and response.
- ✔ Set up and configure a detection lab for simulating and identifying cyber threats.
- ✔ Perform static and dynamic malware analysis.
- ✔ Reverse engineer malware samples to uncover malicious behavior.
- ✔ Conduct threat hunting using event log, ETW, and kernel callbacks.
- ✔ Apply forensic investigation techniques to analyze memory, disk, and registry artifacts.
- ✔ Execute memory forensics and analyze results using specialized frameworks.
- ✔ Implement and manage disk and registry forensic processes.

Course Content

1. Introduction to Threat Hunting and DFIR

- ✓ Overview of threat hunting and its importance
- ✓ Fundamentals of Digital forensics and Incident response
- ✓ Key concepts and terminology
- ✓ Windows logging and internal
- ✓ Important windows components

2. Detection Engineering Approaches and Scenarios

- ✓ Techniques for effective detection engineering
- ✓ Real-world scenarios and case studies
- ✓ Developing detection strategies

3. MITRE Frameworks (e.g., ATT&CK, Engage, D3FEND)

- ✓ Understanding and utilizing MITRE ATT&CK
- ✓ Introduction to MITRE Engage and D3FEND
- ✓ Applying frameworks to threat hunting and DFIR

4. MITRE ATT&CK based threat hunting and detection

- ✓ Deep dive into MITRE ATT&CK and detections based on it
- ✓ ATT&CK based hunting
- ✓ Tactics, Techniques, Procedures, Groups, Software, Detections, Mitigations

5. Detection Lab Setup (for Simulating and Detecting Attacks)

- ✓ Setting up a detection lab environment
- ✓ Tools and configurations for simulating attacks
- ✓ Detecting and analyzing simulated attacks

6. Malware Analysis (Static and Dynamic Analysis)

- ✓ Techniques for static malware analysis
- ✓ Dynamic analysis methods
- ✓ Tools and resources for malware analysis
- ✓ Sigma and Yara rules

7. Reverse Engineering a Malware Sample

- ✓ Introduction to reverse engineering
- ✓ Tools and techniques for reversing malware
- ✓ Practical exercises in malware reverse engineering

8. Hunting on Event Logs, ETW, and Kernel Callbacks

- ✓ Utilizing event logs for threat hunting
- ✓ Understanding and using ETW
- ✓ Kernel callback analysis

9. Call stack based Threat Hunting

- ✓ Analyzing suspicious function call stack trace
- ✓ Creating detection rules
- ✓ Live practical scenarios

10. Threat Hunting Scenarios

- ✓ Identifying and analyzing suspicious threads
- ✓ Practical threat hunting scenarios
- ✓ Techniques and tools for threat hunting

11. Forensic Investigation Techniques

- ✓ Core forensic investigation methods
- ✓ Evidence collection and preservation
- ✓ Analyzing forensic data

13. Analysis Using Memory Forensics Frameworks

- ✓ Overview of memory forensics frameworks
- ✓ Practical application of frameworks
- ✓ Case studies and real-world examples

14. Disk and Registry forensics

- ✓ Fundamentals of disk forensics
- ✓ Techniques for registry analysis
- ✓ Tools and practical exercises for disk and registry forensics

15. Ransomware Investigation scenario

- ✓ Combination of threat hunting, and forensic investigation technique
- ✓ Live demonstration and hands-on exercise
- ✓ Real world ransomware sample attack investigation

Tools to be learnt



SIEM platforms (such as Elastic)



Malware analysis tools (e.g., IDA Pro, x64dbg, windbg)



Forensics tools (e.g., Volatility, Eric Zimmerman tools)



ETW and event log analysis tools

Lab



Simulating and detecting cyber attack



Conducting malware analysis and reverse engineering



Ransomware Investigation



Practical threat hunting scenarios

Bonus Content



Interview preparation and guidance



Lab VM and malware samples for analysis



Custom-built list/repository of openly available resources



Custom-built mind-maps of different frameworks and major concepts discussed in the course (for example: MITRE ATT&CK)



Cheat sheets for important topics (for example: x64 assembly instructions, windbg commands, malware sample sources)

System Requirements



64-bit Intel i5/i7 2.0+ GHz processor or equivalent



At least 8GB of RAM and 50GB of free disk space



Ability to run at least 2 VMs (using Virtual Box, Vmware etc.)



Windows 10 or later, macOS 10 or later, or Linux



Internet access for downloading tools and resources



www.infosectrain.com | sales@infosectrain.com