INFOSECTRAIN

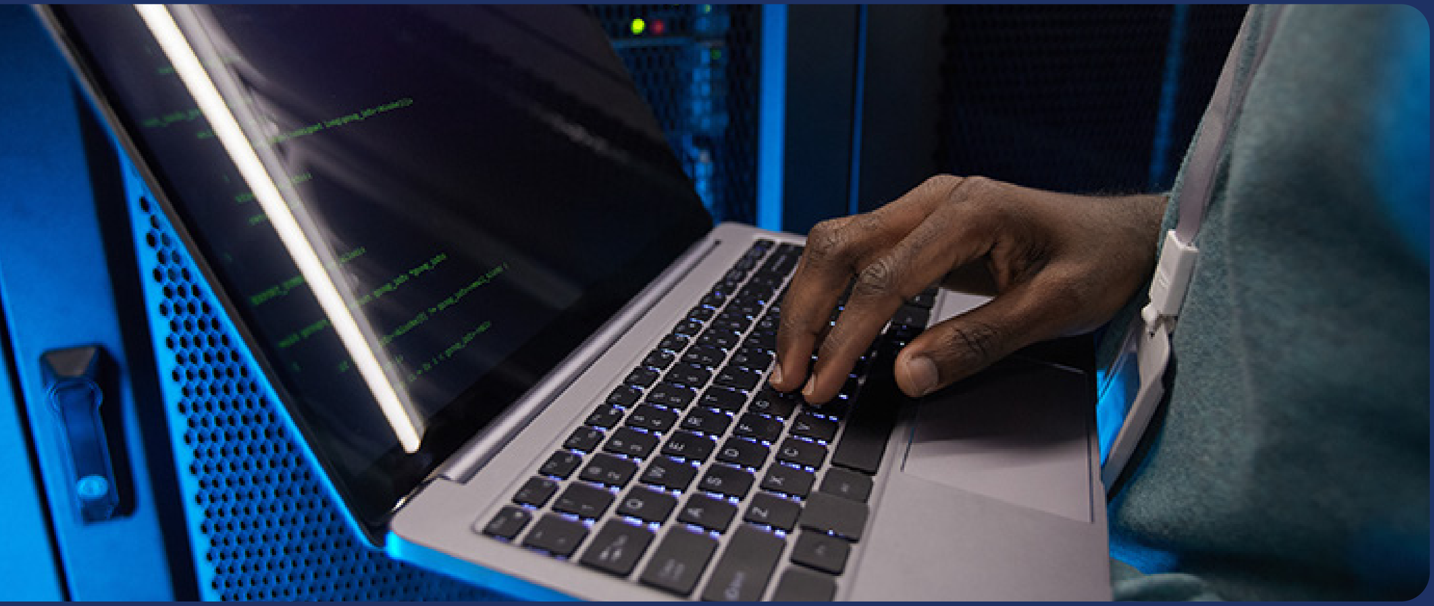
Threat Hunting Professional

TRAINING COURSE

Learn from Industry Experts
32 hrs of instructor-led training

www.infosectrain.com

sales@infosectrain.com



Course description

Threat hunting and Incidence response techniques have been enhanced over years. Organizations are using advanced techniques to identify the threats with skilled threat hunters before any damage or loss takes place. Our Threat Hunting Professional Online Training Course empowers your skills and helps to understand the threats and their objectives.

InfosecTrain has curated Threat Hunting Professional online training course that gives you the skills to proactively hunt for threats and become a stealthier penetration tester. Our expert trainers will teach you the principles and process of threat hunting and the step-by-step instructions are provided to hunt for threats in the network.

Target Audience

- Software Engineers
- IT Managers
- Cyber Security Analysts
- Network Security Engineers
- Red Team Members / Penetration Testers
- Incident Response Team Members

Pre-requisites

- Experience of network monitoring and pentesting tools and methodology
- Fundamental command-line skills in Linux and Windows
- Understanding of basic information security concepts
- Working understanding of networking devices and protocols such as switches, routing, security devices, common network protocols, etc.

Threat Hunting Course Objectives

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

- Define the Threat Hunting and its objectives to the organization
- Implement the Threat mission to identify, and automate the hunting process
- Understand the use cases for the hunting program
- Develop the hunt missions for threat hunting
- Grab the endpoints and network for hunting

Why Infosec Train?

Certified & Experienced Instructor

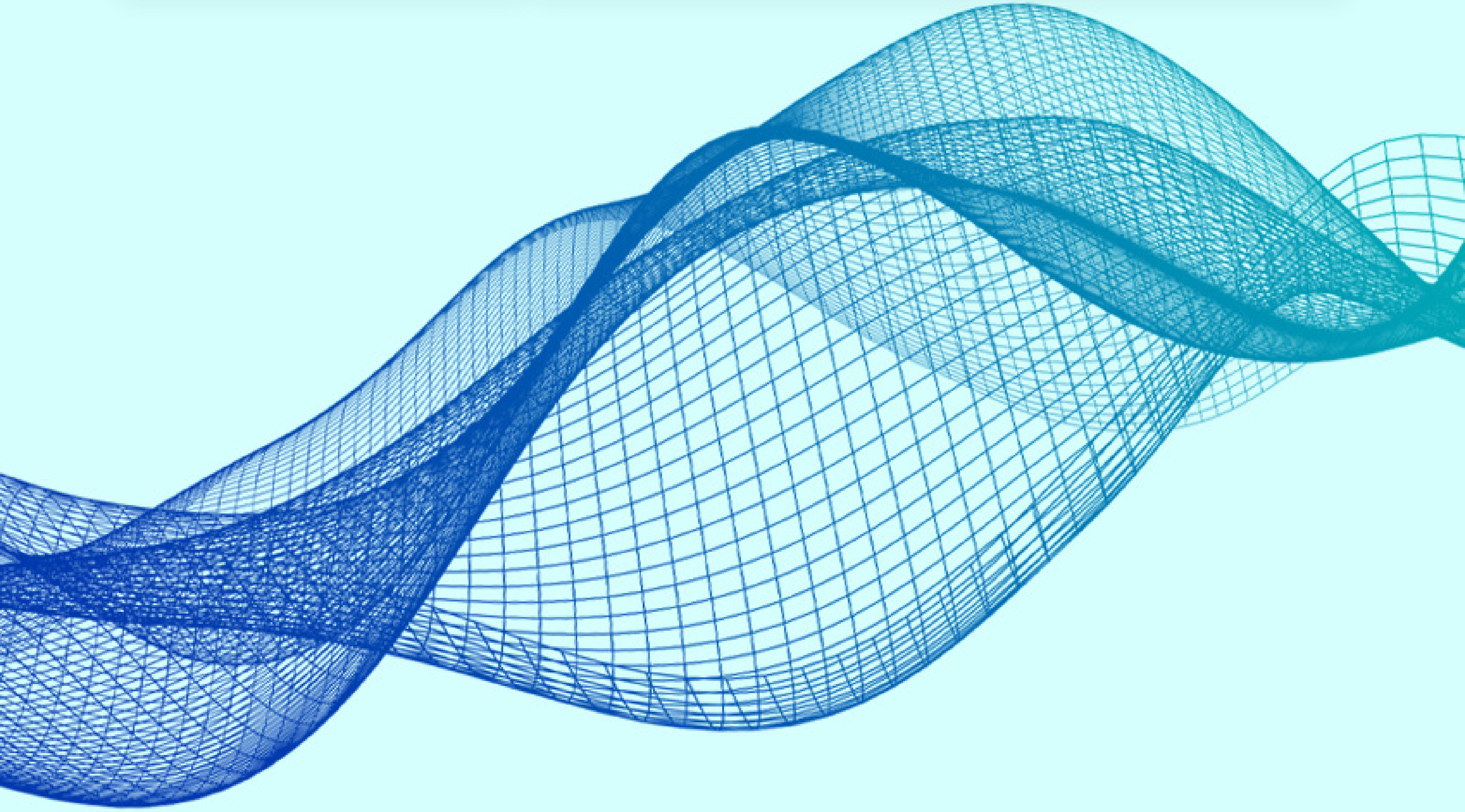
Flexible Schedule

Access to the recorded sessions

Post Training Support

Tailor Made Training

4 hrs/day in Weekend/ Weekday



Tools Covered in the Training

VOLATILITY

MITRE
ATT&CK™

Redline

Course Content

1. Threat Hunting Terminology

- What is Threat, its Types
- Incident Response & Threat Hunting Relationship
- Incident Response Plan, Policies & Practices
- Rapid Response and Breach Assessment
  - Earliest Detection
  - Communication and Notification
  - Containment & Eradication
  - Stop to Subsequent Attacks
- APT : Advanced Persistent Threat
- Tactics, Techniques, and Procedure
- Pyramid of Pain
- Hash values , Ip address , Domain names , Network /Host artifacts , tools , TTP’s.
- Cyber Kill Chain
- Diamond Model Analysis

2. Threat Hunting Hypothesis

- MITRE ATT&CK Framework
- Pre and Post Compromise Detection with Mitre ATT&CK
- Data Collection
- Hunting Hypothesis and Methodology

  A. Pick a Tactic and Technique

  B. find procedure(s)

  C. perform a attack simulation

  D. Identify evidence to collect

  E. Set scope.

3. Network Traffic Hunting

- ARP Traffic
- ICMP traffic
- TCP and UDP Analysis
- HTTP and HTTPS traffic suspects
- Detecting SQL Injection,Command injection From Network Traffic
- Network Hunting and Forensics
- Wireshark, Network Miner

4. Web Hunting

- Introduction
- Web Shell Process
- Types of Web Shells
- Hunt , Analyse for Web Shells
- File Upload Detection
- RFI LFI Detection
- XSS Detection
- Analyzing Web Server Logs

5. Endpoint Hunting

- Introduction
- Windows Processes
  - smss.exe
  - Winlogon.exe
  - Wininit.exe
  - Services.exe
  - Lsass.exe
  - Svchost.exe
  - Taskhost.exe
  - explorer.exe
- Endpoint Baselines
- Threat Hunting with PowerShell
- Registry Analysis

6. Malware Hunting

- Malware Overview
- Redline:
  - Collector
  - Usage
  - File Analysis
  - Detection Code Injection
- Memory Forensics Analysis for Threat Hunting
  - Understanding Common Windows Services and Processes
  - Identify Rogue Processes
  - Analyze Process DLLs
  - Review Network Artifacts
  - Check for Signs of a Rootkit
  - Acquire Suspicious Processes
  - Memory analysis using Volatility
  - Steganography, ADS ,Overwriting Metadata - Anti Forensics Detection
  - Corporate Case Study
  - Case Study : Ransomware as a Service

7. Hunting with ELK

- Introduction to the Elastic Stack
- Introducing Logstash
- Elasticsearch - The heart of the stack
- Beats and Agents
- Viewing Elasticsearch data with Kibana
- Leveraging the Elastic Stack for Collection and Analysis
- Operationalizing Threat Hunting
- Using Kibana to Pivot Through Data to Find Adversaries

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com