INFOSECTRAIN

Threat Hunting Professional

TRAINING COURSE

40 hours of Instructor-led training

www.infosectrain.com | sales@infosectrain.com

Course description

Threat hunting techniques have 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 a 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.

This course is a Preliminary course for most of the Professional Threat Hunting Certifications(eCTHPv2,CCTHP,Threat Hunter training course - Group-IB)

Course Objectives:

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

- Define 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

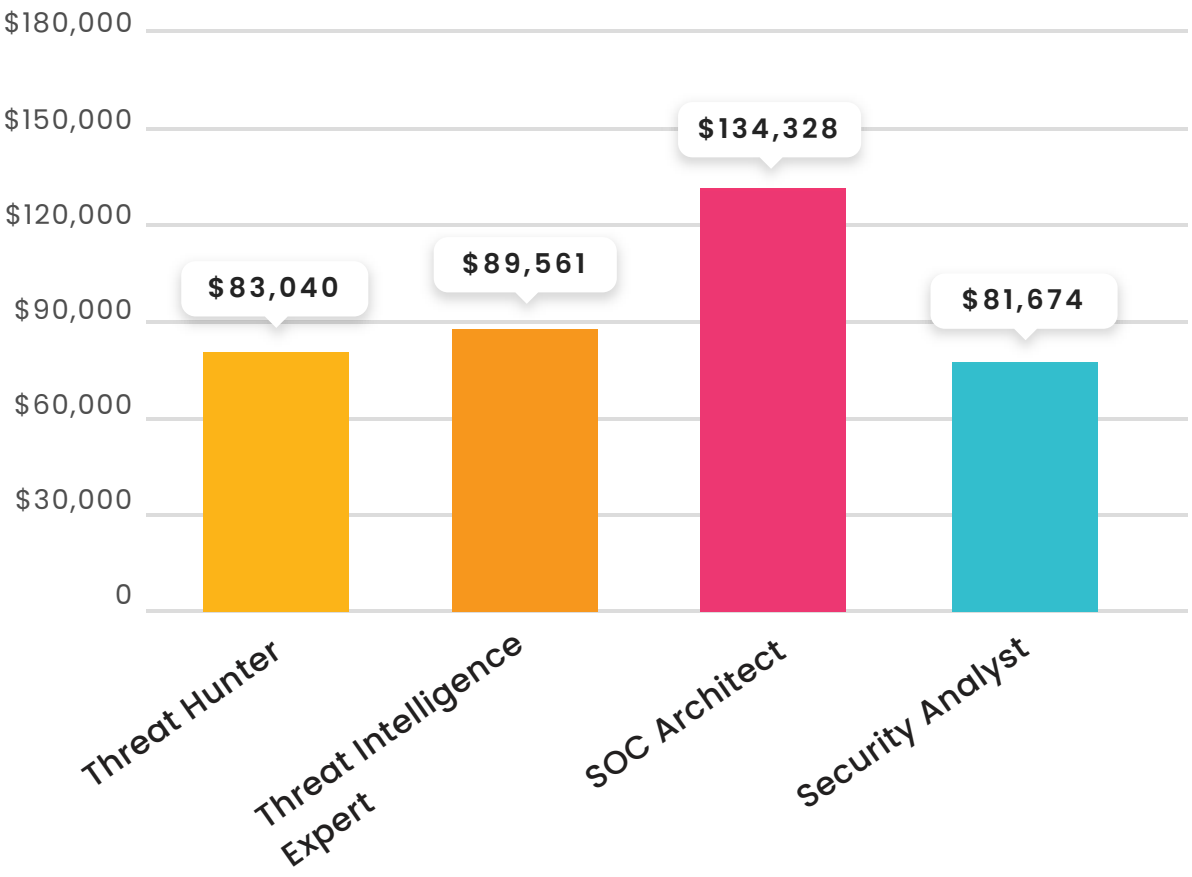
Target Audience:

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

Prerequisites

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

Course Benefits



Hiring companies

Microsoft IBM wipro zoom Deloitte.

Source: Glassdoor

Course Content

INFOSECTRAIN

1. Introduction to Threat Hunting

> What is Threat Hunting?
> What is Threat Intelligence?
> 5 Whys of Threat Hunting
> Introduction to Endpoint Threat Hunting
> Introduction to Network Threat Hunting

2. Threat Hunting Basics

> Log Analysis(Perimeter devices, Endpoints, Security Solutions)
> Basics of Malware Analysis
> Types of Threat Hunting(Intel Driven, Hypothesis Driven, Request Driven, Hybrid Hunting)
> Digital Forensics and Incident Response
> Detection of LOLBins & GTFOBins
> Hunting based on OSI Layers
> Brief Introduction to Windows Logging and Internals
> Brief Introduction of TH Frameworks

MITRE ATT&CK **Diamond Model** **Cyber Kill Chain**

> Basics of Log Forensics
> OSINT for Threat Hunting
> YARA Rules

3. Network Threat Hunting

> Networking Primer from a Security standpoint
> Network-Based Attacks and in-depth analysis
> Port based attacks and hunting
> Netmon for Threat Hunting
> Packet Analysis & Tools

Live Network Captures

Port Mirroring

Network Tap

MAC Floods

ARP Poisoning

Netmon

Wireshark

> Suspicious Traffic Hunting: ARP,ICMP,TCP,DHCP,DNS,HTTP/HTTPS, Unknown Traffic Hunting, Hunting WebShells
> Network Forensics:
> Protocol Anomalies 101
> Network Threat analysis : SSH, DNS, ICMP Tunneling analysis
> Command and Control detection
> Injection attacks detection.
> Case Study

4. Endpoint Threat Hunting

> Introduction to Endpoint Threats
> Event IDs and Logging
> Primer on Windows Processes and threats
> In-depth understanding of Event IDs and Threat Hunting based on them.
> LOLBins and GTFOBins
> Sysmon for Threat Hunting
> Primer on Malware Analysis
> Hunting Macros, Mimikatz, and Remote Threads using Sysmon & ELK stack
> Hunting with Powershell
> Persistence Hunting
> Case Study

5. MITRE ATT&CK based Threat Hunting and Detection

> Detailed Introduction to ATT&CK Framework
> Matrices/Platforms
> Tactics, Techniques, and Sub-Techniques
> Data Sources and Detections
> Groups and Software
> Ransom Case Study and Hands-on Analysis-2 hours
> ATT&CK Based Hunting with ELK-Lab-3 Hours
> Introduction to D3FEND Framework
> Defense mechanisms
> Mapping Defense mechanisms with Attack vectors
> Implementing Defense Mechanisms-Lab-2 Hours

Tools to be learnt

> SIEM/ELK Stack for Threat Hunting
> Python for Threat Hunting
> MITRE ATT&CK framework

Lab

> Labs at end of Every Module
> Final Lab/Capture the Flag Event with 50+ Threat Hunting Challenges(Ranging from Basic to Advanced)

Bonus Content

> Interview Prep
> Lab VM gives away
> Custom-built list/repository of openly available resources
> Custom-built MindMaps of Frameworks and Major concepts discussed in the course ex: MITRE ATT& CK and D3F3ND

System Requirements

> 4-bit Intel i5/i7 2.0+ GHz processor or equivalent

> 8GB of RAM

> Ability to run at least (1) virtual machine using Virtual Box, or an equivalent virtualization software

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

> Local administrator privileges