About the Course

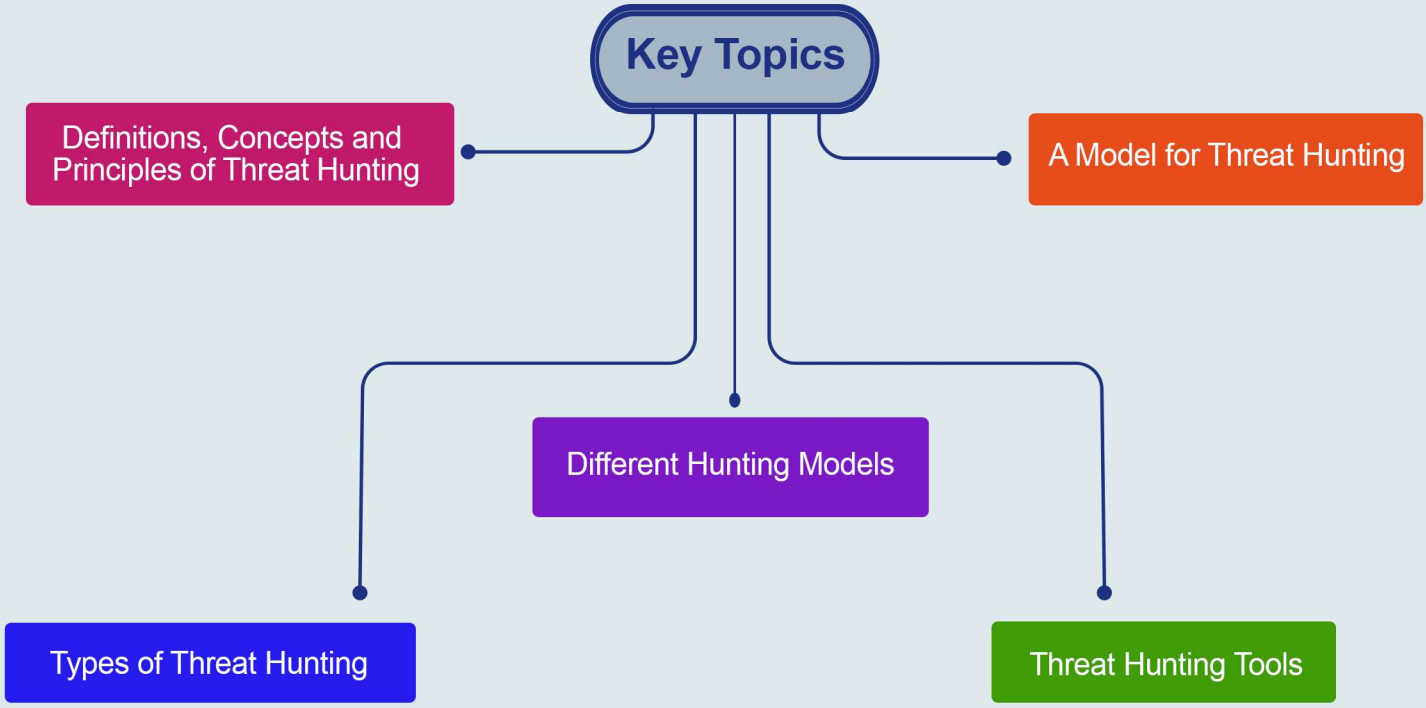
Cybersecurity leaders are engaged in a difficult arms race against the threat actors who seek to attack their organizations. The root of the problem is that cybercrime pays well for the criminals. Threat hunting provides a second level of defense, intended to address gaps in the overall cybersecurity architecture by finding and disrupting attackers that have evaded the organization's automated defenses. The course is to introduce an effective framework and methodology to threat hunting that enables SecOps teams to plan and conduct hunts that maximize the opportunity to successfully find and disrupt attacks in progress.

Learning Objectives

1. Define Cyber Threat Hunting and articulate its value to an organization
2. Create or enhance an existing hunting program
3. Leverage provided use cases for your Hunting Program
4. Build hunt missions for threat hunting in your organization
5. Leverage both endpoint and network data for successful hunting
6. Implement a hunting mission to hunt, find, and automate the hunting process

Terminus System

Key Topics



Pre Requisites

- Log Management Course
- Ethical Hacking & Penetration Testing Concepts Course

What You Will Receive

Course Presentation File

Complementary Files

Threat Hunting eBook

Who Should Attend

Network security professionals and incident responders who will be using security and logging products to assist with their network and endpoint hunting responsibilities. This course is also for:

- Threat & Vulnerability Analyst

Syllabus

Introduction to Hunting

- What is threat hunting?
- Why conduct a threat hunt?
- Hunting Process
- Defining Hunt Missions
- Creating Hunt Program
- The difference between threat hunting and threat intelligence

Types of Threat Hunting

- Structured hunting
- Unstructured hunting
- Based on status

Different Hunting Models

- Intel-based hunting
- Hypothesis hunting
- Conventional hunting

Threat Hunting Tools

- Managed Diagnosis and Response
- SIEM
- Security Analytics

A Model for Threat Hunting

- Diamond model
- Target
- Territory
- Equip

Syllabus

- Planning
- Performance
- Feedback

Initial Access

- Drive-By Compromise
- External Remote Services
- Spear phishing Attachment
- Spear phishing Link

Execution

- Command Line Interface

Persistence

- BITS Jobs
- External Remote Services
- Port Knocking
- Install Root Certificate

Credential Access

- Brute Force
- Forced Authentication
- Network Sniffing

Discovery

- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Remote System Discovery

Syllabus

Lateral Movement

- Remote Desktop Protocol
- Remote Services
- Windows Admin Shares

Collection

- Archived Control Data
- Automated Collection
- Data From Network Shared Drive

Command & Control

- Commonly Used Ports
- Non-Standard Ports
- Encrypted Channel
- Fallback Channels, Multi-stage Channels
- Ingress Tool transfer
- Non-Application Layer Protocol
- Proxy
- Web Service

Exfiltration

- Automated Exfiltration
- Data Transfer Size Limit

Endpoint Hunting

- Operating System Technology Review
- Malware Hiding Techniques
- Uncovering Internal Reconnaissance

Syllabus

o Uncovering Lateral Movement
o Data Acquisition Techniques

Network Hunting

o Network Technology Review
o Tunneling Techniques
o Suspicious HTTP Traffic
o Data Acquisition Techniques

Hands-on Training

- Lab 1: Hunting Tools
- Lab 2: Endpoint Hunting
- Lab 3: Network Hunting