Faysal Aziz

Cybersecurity - Threat hunting

3-day course outline for mastering the essentials

FA-0147 · 3-day

Cybersecurity

Introduction

Welcome to our 3-Day Intensive Course on Threat Hunting in Cybersecurity, a specially designed program aimed at equipping IT security professionals with the knowledge and skills to proactively search for and neutralize cyber threats within their organizations.

In the digital age, reactive security measures are no longer sufficient to protect against the sophisticated and constantly evolving cyber threats. This course emphasizes the importance of a proactive approach to cybersecurity, where threat hunting plays a crucial role. By identifying and mitigating threats before they can exploit vulnerabilities, organizations can significantly enhance their security posture.

This course is ideal for security analysts, system administrators, and any IT professionals interested in taking an active role in improving their organization's cybersecurity defenses.

Learning outcomes

Upon completing this course, participants will be able to:

- Understand the principles and importance of proactive threat hunting.
- Identify the common tools and techniques used in threat hunting.
- Analyze network traffic and logs to detect potential threats.
- Develop and implement effective threat hunting strategies.
- Use various cybersecurity frameworks to guide threat hunting activities.
- Collaborate and communicate findings within a cybersecurity team effectively.

Prerequisites

- Basic understanding of cybersecurity concepts and terminologies.
- Familiarity with network architecture and security controls.
- Experience with using basic security tools and analyzing logs.
- Ability to read and understand system and network logs.

Training outline

1. Introduction to Threat Hunting

Defining Threat Hunting

1. Difference between threat hunting and traditional security measures
2. The importance of threat hunting in modern cybersecurity

The Cyber Kill Chain and MITRE ATT&CK Framework

1. Understanding attacker tactics, techniques, and procedures (TTPs)
2. How to use frameworks to guide threat hunting activities

2. Threat Hunting Tools and Technologies

Security Information and Event Management (SIEM) Systems

1. Basics of SIEM
2. How SIEM aids in threat hunting

Endpoint Detection and Response (EDR) Tools

1. Role of EDR in identifying threats

Open Source Tools and Resources

1. Utilizing open-source tools for threat hunting (e.g., Wireshark, ELK Stack)

3. Developing a Threat Hunting Hypothesis

Creating Effective Hypotheses

1. Based on known threats
2. Based on emerging trends

Identifying Indicators of Compromise (IoCs)

1. Tools and techniques for IoC discovery

4. Threat Hunting Techniques

Network Traffic Analysis

1. Identifying anomalies in network traffic
2. Tools and techniques for network analysis

Log Analysis and Aggregation

1. Analyzing system, application, and security logs
2. Leveraging log aggregation tools for efficient analysis

Memory and Forensic Analysis

1. Basics of memory analysis
2. Tools for forensic investigation

5. Strategies for Effective Threat Hunting

1. Proactive vs. Reactive Hunting Strategies

Building and Organizing a Threat Hunting Team

1. Roles and responsibilities within a threat hunting team

Integration with Incident Response

1. Transitioning from threat hunting to incident response

6. Communication and Reporting

Documenting Threat Hunting Activities

1. Importance of documentation
2. Tools and formats for effective documentation

Communicating Findings

1. Preparing and delivering reports
2. Communicating with different stakeholders

7. Case Studies and Practical Exercises

Real-World Threat Hunting Scenarios

1. Analyzing and responding to simulated threat scenarios

Hands-on Threat Hunting Exercises

1. Utilizing tools and techniques covered in the course

Collaborative Threat Hunting Simulation

1. Working in teams to identify and neutralize simulated threats

This intensive 3-day course combines theoretical knowledge with practical exercises, including real-world case studies and hands-on simulations, to provide participants with a comprehensive understanding of threat hunting in cybersecurity.

By the end of the course, participants will be equipped with the skills and confidence to proactively hunt for threats and contribute to the cybersecurity resilience of their organizations.

© 2026 Faysal Aziz · Kuala Lumpur