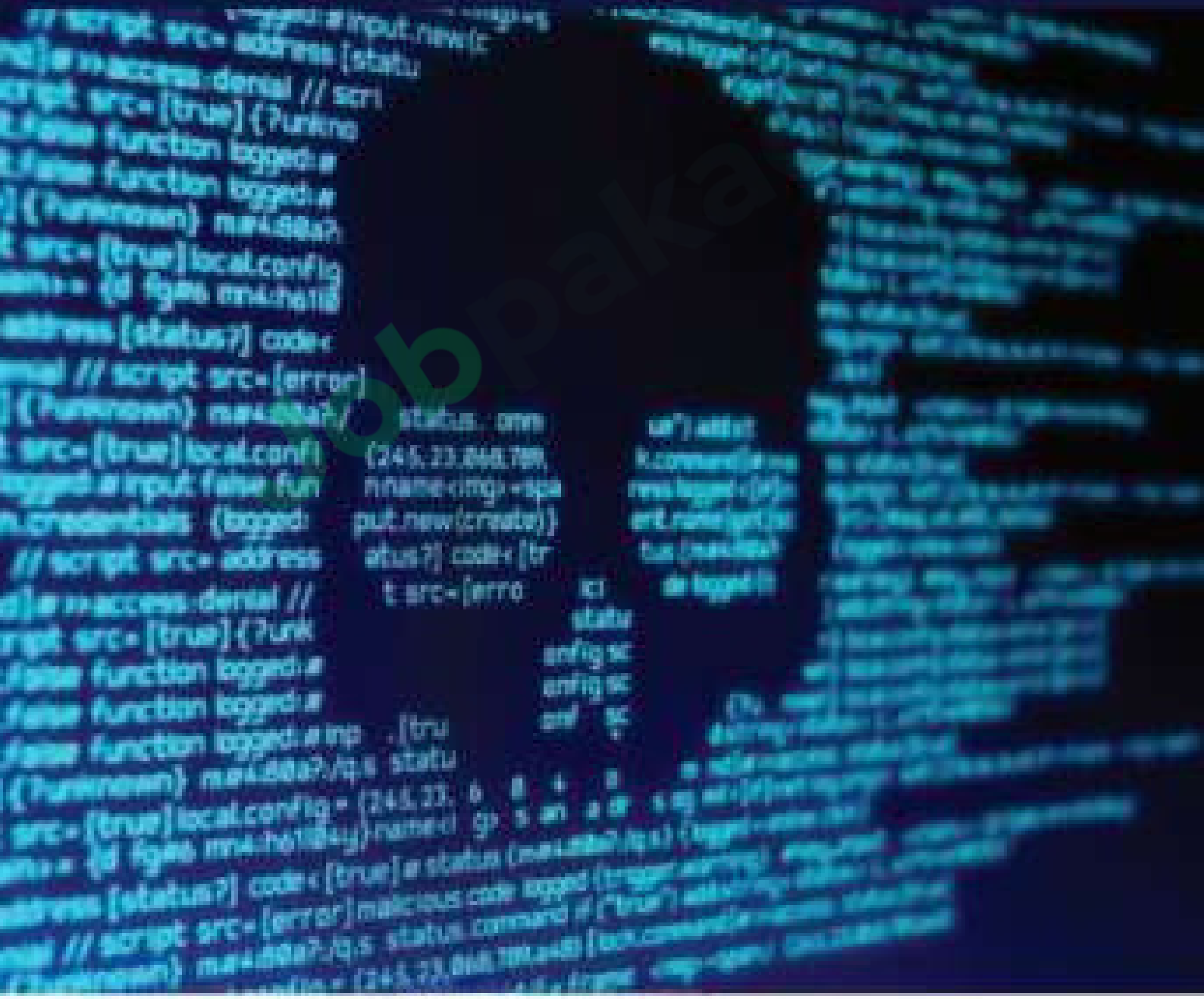
Jobpakado

Cyber Threat Hunting



Jobpakado

Table of Contents

About the Program

Creating a course on threat hunting involves a structured approach to teach the necessary skills, tools, and methodologies needed to detect and respond to cyber threats proactively. The course should ideally cater to both beginners and experienced cybersecurity professionals, with modules that are comprehensive and progressively build in complexity.

Jobpakado

CYBER THREAT HUNTING

1.Introduction to Threat Hunting

Objective: Explore various hunting techniques and methodologies.

- Definition and scope of threat hunting.
- Differences between threat hunting and automated detection.
- Key roles and responsibilities in a threat hunting team.
- Overview of the threat landscape.

2.Cyber Threat Intelligence

Objective: Learn how to use intelligence to drive hunting activities.

- Understanding threat intelligence sources.
- Intelligence sharing platforms and how to use them.
- Applying intelligence to generate hypotheses for hunting.
- Integrating threat intelligence in the hunting workflow

3.Security Tools and Technology

Objective: Gain knowledge of the tools used in threat hunting.

- Overview of Security Information and Event Management (SIEM) systems.
- Endpoint Detection and Response (EDR) systems and their usage.
- Network monitoring tools and techniques.
- Using forensic tools in threat hunting.

4.Developing Hunting Hypotheses

Objective: Learn how to develop effective hypotheses based on risk and intelligence

- Understanding hypothesis-led hunting.
- Creating effective and actionable hypotheses.
- Examples of common hypotheses in real-world scenarios.

5.Data Collection and Analysis

Objective: Understand how to gather and analyze data effectively

- Key data types for threat hunting.
- Techniques for data collection and management.
- Data analysis methods and tools.
- Practical exercises on data analysis.

6.Hunting Techniques and Methodologies

Objective: Explore various hunting techniques and methodologies.

- Behavioral analytics and heuristics.
- Pattern detection and anomaly hunting.
- Using AI and machine learning in threat hunting.
- Case studies on successful hunts.

7.Practical Labs and Exercises

Objective: Apply learned concepts in practical settings.

- **Simulated attack scenarios.**
- **Hands-on labs using real tools and data.**
- **Group projects and individual assessments.**

8.Assessment and Certification

Objective: Evaluate the skills and knowledge gained.

- **Written exams.**
- **Practical tests.**
- **Certification process and criteria.**

Each module should include both theoretical and practical components to ensure that learners not only understand the concepts but are also capable of applying them in real-world scenarios. This structured approach helps build a strong foundation in threat hunting and prepares learners for advanced responsibilities in cybersecurity.