CyberHunt

ADVANCED THREAT HUNTING SERVICES

Advanced Threat Hunting Services

Proactive detection of hidden and sophisticated threats using expert-led investigations.

Find attackers before they find you.

- Proactive Hunting
- Behavior Detection
- Deep Analysis
- Expert Analysts

Request a Call Back

5000+	95%	100+	24/7
Students Trained	Success Rate	Hiring Partners	Support

CyberHunt

Program Highlights

- 40-Hour Instructor-Led Training
- EC-Council Authorized Partner
- Practical Training on Latest Tools
- Telegram Group for Exam Support
- Learn from CEI Certified Trainers
- 98% Exam Pass Rate
- Post Training Support till Exam
- Access to Recorded Sessions
- Career Guidance & Mentorship

https://cyberhuntit.com/

CyberHunt

ABOUT COURSE

Advanced Threat Hunting Expert Program

Advanced Threat Hunting is a proactive, human-led cybersecurity practice focused on uncovering sophisticated attackers who bypass traditional security defenses. Unlike automated tools that rely only on alerts, threat hunters actively investigate endpoints, logs, and network behavior to detect hidden malicious activity before major damage occurs.

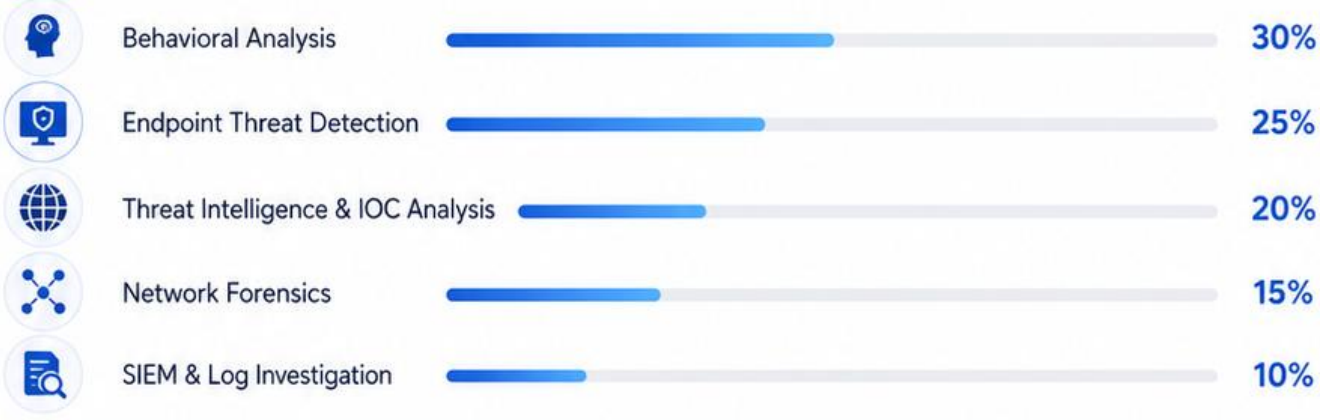
This program prepares cybersecurity professionals to identify advanced persistent threats (APTs), detect lateral movement, analyze attacker behavior, and respond to stealthy intrusions across enterprise environments. Students will work with real-world attack scenarios, behavioral analytics, SIEM investigations, and endpoint threat analysis.

With a curriculum spanning threat intelligence, log analysis, endpoint detection, network forensics, adversary simulation, and proactive defense strategies, this is one of the most comprehensive Advanced Threat Hunting programs designed for modern security operations teams.

WHAT YOU GET

- **Deep environment analysis**
- **Threat actor behavior detection**
- **Risk exposure reporting**
- **Identification of hidden vulnerabilities**

Threat Hunting Coverage



CyberHunt

Target Audience

- Security Analysts
- Ethical Hackers
- System Administrators
- Network Administrators
- Network and Security Engineers
- Cyber Security Managers
- Information Security Auditors
- Security Professionals

Pre-Requisites

- Basic understanding of network essentials and core concepts, including server and network components.

CyberHunt

Module-Wise Syllabus
Advanced Threat Hunting

Proactive. Persistent. Precision.

A hands-on program to hunt hidden threats before they strike.

01 Hypothesis Generation

Threat hunting doesn't start with random searching. We begin by formulating a strong hypothesis based on the latest threat intelligence, industry trends, and the specific architecture of your organization.

We ask questions like: "If an Advanced Persistent Threat (APT) targeted our Active Directory today, how would they maintain persistence without triggering alarms?" This guides our entire investigation.

- Threat Intel Integration
- Industry Profiling
- Strategic Planning
- Vulnerability Modeling

02 Deep Environment Analysis

Once the hypothesis is set, we collect and parse massive amounts of telemetry from your endpoints, network traffic, cloud infrastructure, and identity management systems.

Our analysts dive deep into your environment, looking far beyond standard alerts. We hunt for hidden webshells, unauthorized scheduled tasks, and dormant lateral movement trails.

- Telemetry Collection
- Endpoint Deep-Dive
- Network Flow Analysis
- Log Parsing

03 Threat Actor Behavior Detection

Attackers change their tools constantly, but their fundamental behaviors remain similar. We utilize the MITRE ATT&CK framework to search for specific Tactics, Techniques, and Procedures (TTPs).

Instead of just looking for known bad IP addresses, we look for anomalous behaviors—such as PowerShell executing encoded commands, unexpected administrative credential usage, or suspicious registry modifications.

- MITRE ATT&CK Mapping
- TTP Identification
- Behavioral Analytics
- Living-off-the-Land Detection

04 Anomaly Investigation & Validation

When an anomaly is discovered, our analysts manually investigate it to filter out false positives from legitimate business operations.

If an actual threat or compromise is validated, we immediately isolate the threat and pivot into Incident Response mode, working with your team to contain the attacker before data is lost.

- False Positive Filtering
- Manual Triage
- Rapid Containment
- Incident Validation

05 Risk Exposure Reporting

The hunt concludes with a comprehensive Risk Exposure Report. Whether an active attacker is found or not, you gain immense value by identifying previously unknown security gaps.

We provide actionable recommendations to improve your security posture, such as closing open ports, tightening IAM policies, or writing new SIEM detection rules to catch similar activity automatically in the future.

- Gap Identification
- Executive Summaries
- New Detection Rules
- Posture Hardening

Outcome: Detect What Others Miss. Stop Breaches Before They Happen.

CyberHunt

TRAINING ENQUIRIES

Have questions or need more information about our training programs? We're here to help!

For Training
+91 99599 06195
+91 93156 97737

Email
trainings@cyberhuntit.com

Website
www.cyberhuntit.com

Empowering Your Future
Industry-relevant training designed to upskill and empower you.

Follow us on