Proactive Threat Hunting and Cyber Intelligence Analysis Training Course



14 - 18 Dec 2026

Cairo

3700 € (Per Person)

Ref: #CYB2032_272205

Course Introduction / Overview:

This course provides a comprehensive immersion into the proactive world of cybersecurity, shifting the focus from reactive incident response to proactive threat hunting and intelligence analysis. In today's evolving threat landscape, waiting for an alert is no longer a viable strategy. This program is designed to equip cybersecurity professionals with the mindset, methodologies, and skills to actively seek out hidden adversaries within their networks before significant damage occurs. Drawing on principles articulated by experts like Robert M. Lee, a pioneer in the field, we explore how to build and execute intelligence-driven hunt missions. The curriculum delves deep into the threat intelligence lifecycle, teaching participants not just how to consume intelligence, but how to produce and operationalize it. Concepts from foundational texts such as "Intelligence-Driven Incident Response" are integrated to provide a structured approach to analysis. At BIG BEN Training Center, we empower participants to move beyond tool-centric security, fostering the critical thinking and analytical tradecraft necessary to deconstruct complex attacks and understand adversary tactics, techniques, and procedures (TTPs). This course is the definitive guide for transforming your security operations into a formidable, proactive defense function.

Target Audience / This training course is suitable for:

- Cybersecurity Analysts.
- Security Operations Center (SOC) Analysts and Engineers.
- Threat Intelligence Analysts.
- Incident Responders and Digital Forensics Investigators.
- Security Architects and System Administrators.
- IT Security Managers and Team Leads.
- Penetration Testers and Ethical Hackers seeking to understand defensive strategies.

Target Sectors and Industries:

- Financial Services and Banking.
- Technology and Telecommunications.
- Healthcare and Life Sciences.
- Energy, Oil, and Gas.
- Government, Public Sector, and Defense Agencies.
- Critical Infrastructure and Utilities.
- Retail and E-commerce.
- Consulting and Managed Security Service Providers.

Target Organizations Departments:

- Security Operations Center (SOC).
- Cyber Threat Intelligence (CTI) Unit.
- Incident Response (IR) Team.
- Digital Forensics and Investigations.
- Information Security and Cybersecurity Department.
- Risk Management and Compliance.
- IT Infrastructure and Network Security.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop and test proactive threat hunting hypotheses based on intelligence.
- Master the complete cyber threat intelligence lifecycle from planning to dissemination.
- Apply frameworks like the MITRE ATT&CK and the Cyber Kill Chain for analysis.
- Analyze network traffic and endpoint data to uncover hidden adversary activities.
- Conduct effective open-source intelligence (OSINT) investigations.
- Profile threat actors and map their tactics, techniques, and procedures (TTPs).
- Create actionable intelligence reports for both technical and executive audiences.
- Integrate threat intelligence into security operations for a proactive defense posture.
- Utilize structured analytic techniques to reduce cognitive bias in investigations.

Course Methodology:

The training methodology at BIG BEN Training Center is designed for maximum knowledge retention and practical application. This course adopts an immersive, hands-on approach that goes far beyond traditional lectures. Participants will engage in a series of intensive lab exercises that simulate real-world threat scenarios, allowing them to apply learned techniques in a controlled environment. We utilize a blend of interactive sessions, expert-led demonstrations, and collaborative group workshops to foster a dynamic learning atmosphere. A significant portion of the course is dedicated to the analysis of complex case studies derived from actual cyber incidents, enabling participants to deconstruct sophisticated attacks and understand the attacker's mindset. Team-based activities encourage peer-to-peer learning and problem-solving, mirroring the collaborative nature of modern security teams. Continuous feedback and guided practice are central to our philosophy, ensuring that participants not only grasp the theoretical concepts but also build the confidence and competence to apply these advanced skills directly in their professional roles upon completion of the course.

Course Agenda (Course Units):

Unit One: Foundations of Proactive Cyber Defense

- Introduction to Threat Hunting and Threat Intelligence.
- Contrasting Reactive Security with Proactive Hunting.
- The Threat Hunting Loop and Maturity Model.
- Understanding the Cyber Threat Intelligence (CTI) Lifecycle.
- Exploring Key Frameworks: Cyber Kill Chain and MITRE ATT&CK.
- Developing a Hunter's Mindset and Analytical Tradecraft.
- Legal and Ethical Considerations in Threat Hunting and Intelligence Gathering.

Unit Two: Data Sources and Collection for Threat Hunting

- Identifying and Prioritizing Critical Data Sources.
- Leveraging SIEM for Proactive Threat Hunting.
- Endpoint Detection and Response (EDR) Data Analysis.
- Advanced Network Traffic and Protocol Analysis.
- Analyzing Host-Based Artifacts (Registry, File System, Memory).
- Working with Log Data from Firewalls, Proxies, and DNS.
- Introduction to Threat Intelligence Platforms (TIPs).

Unit Three: Threat Hunting Methodologies and Techniques

- Hypothesis-Driven Hunting: From Idea to Execution.
- Hunting for Indicators of Compromise (IOCs) vs. Indicators of Attack (IOAs).
- Techniques for Hunting on the Endpoint: Processes, Persistence, and Lateral Movement.
- Techniques for Hunting on the Network: Beacons, Tunneling, and Data Exfiltration.
- Using Threat Intelligence to Drive Hunt Missions.
- Introduction to Scripting for Hunters (PowerShell and Python).
- Documenting and Managing the Hunt Process.

Unit Four: Mastering Cyber Threat Intelligence Analysis

- Intelligence Collection Techniques: OSINT, HUMINT, and Technical Sources.
- Investigating the Dark Web and Underground Forums.
- Threat Actor Profiling and Attribution Challenges.
- Introduction to Malware Analysis for Intelligence Gathering.
- Structured Analytic Techniques (SATs) for Cybersecurity.
- Analyzing and Validating Third-Party Intelligence Feeds.
- Understanding the Geopolitical Context of Cyber Threats.

Unit Five: Operationalizing Intelligence and Advanced Topics

- Creating and Disseminating Actionable Intelligence Reports.
- Briefing Different Audiences: Technical Teams vs. Executive Leadership.
- Integrating Threat Hunting and Intelligence into Incident Response.
- Automating Intelligence Processing and Hunting Tasks.
- Measuring the Effectiveness and ROI of a Hunt Program.
- Advanced Adversary TTPs and Evasion Techniques.
- Final Capstone Exercise: End-to-End Hunt and Intelligence Simulation.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

How can organizations effectively measure the return on investment (ROI) of a proactive threat hunting program, moving beyond simple metrics like 'threats found' to demonstrate true risk reduction?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by holistically integrating the disciplines of threat hunting and cyber intelligence analysis into a single, cohesive methodology. Unlike programs that teach these as separate functions, our curriculum is built on the principle that the most effective hunting is intelligence-driven, and the most valuable intelligence is that which is actionable for hunters. We move beyond a mere survey of tools and techniques to cultivate a deep analytical tradecraft, teaching participants *how* to think, not just *what* to do. The emphasis is on developing a proactive mindset and mastering structured analytic techniques to overcome cognitive biases and improve the quality of analysis. Participants will not just learn to follow a checklist; they will learn to formulate creative hypotheses, pivot between disparate data points, and construct a comprehensive narrative of adversary activity. The course's focus on real-world case studies and a capstone simulation ensures that the skills learned are not just theoretical but are immediately applicable, empowering professionals to transform their organization's defense posture from reactive to predictive and resilient.