Advanced Cybersecurity Threat Hunting for Critical Infrastructure Training Course

Ref: #CYB8882

Course Introduction / Overview:

This comprehensive training course is designed to provide cybersecurity professionals with the advanced skills and methodologies required for proactive threat hunting within critical infrastructure environments. Critical infrastructure, including energy, water, and transportation systems, is a prime target for sophisticated cyber threats from nation-states and criminal organizations. This program goes beyond a reactive security posture and focuses on the techniques used to actively search for and identify malicious activity that has bypassed traditional defenses. Participants will learn how to analyze network traffic, use threat intelligence, and hunt for indicators of compromise (IOCs) in an operational technology (OT) environment. We will cover key topics like malware analysis, anomaly detection, and the use of specialized tools for hunting within industrial control systems (ICS). Drawing from the academic research of renowned authors like Richard Bejtlich and his work in his book "The Practice of Network Security Monitoring," this program provides a strategic and practical framework for finding and neutralizing threats before they can cause catastrophic damage. His work emphasizes the importance of human intuition and continuous monitoring, which are core principles of effective threat hunting. This course at BIG BEN Training Center will empower you to become a skilled threat hunter who can protect the nation’s most vital assets.

Target Audience / This training course is suitable for:

- Threat hunters.
- Cybersecurity analysts.
- Security operations center (SOC) staff.
- Industrial control systems (ICS) security professionals.
- Network security engineers.
- Digital forensics investigators.
- Critical infrastructure operators.

Target Sectors and Industries:

- Energy and utilities.
- Manufacturing.
- Telecommunications.
- Transportation and logistics.
- Public services.
- Government agencies and equivalents.
- Defense and military.

Target Organizations Departments:

- Security Operations Center (SOC).
- Cybersecurity.
- Operational Technology (OT).
- Information Security.
- Incident Response.
- Threat Intelligence.
- IT Audit.

Course Offerings:

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

- Conduct proactive threat hunting in an OT environment.
- Analyze network traffic for malicious activity.
- Use threat intelligence to guide hunting efforts.
- Identify advanced persistent threats (APTs).
- Correlate data from multiple sources to find hidden threats.
- Develop a custom threat hunting plan.
- Communicate hunting findings to stakeholders.

Course Methodology:

This training course at BIG BEN Training Center uses a hands-on, lab-intensive methodology that simulates the unique challenges of threat hunting within critical infrastructure. The program includes a series of virtual labs and scenarios where participants will analyze network packet captures and log data from an emulated industrial network. You will learn to use specialized tools for network monitoring, log analysis, and malware investigation. The course emphasizes a structured, analytical approach. It teaches you to form and test hypotheses about malicious activity. The instructor will provide expert guidance and feedback throughout the labs, ensuring that you develop the critical thinking and problem-solving skills required for high-staking roles. This approach ensures the knowledge and skills gained are directly applicable to safeguarding critical infrastructure from sophisticated threats.

Course Agenda (Course Units):

Unit One: The Threat Hunting Mindset

- Introduction to proactive threat hunting.
- The difference between threat hunting and incident response.
- Developing a hypothesis-driven approach.
- Threat intelligence for critical infrastructure.
- The MITRE ATT&CK framework.
- The anatomy of a cyberattack.
- Case study: a nation-state attack.

Unit Two: Hunting on the Network

- Analyzing network traffic.
- Identifying command-and-control (C2) traffic.
- Using network security monitoring tools.
- Hunting for lateral movement.
- Detecting network anomalies.
- Packet analysis for malicious payloads.
- Practical lab: a network packet analysis exercise.

Unit Three: Hunting on the Endpoint

- Endpoint data collection.
- Hunting for malicious process behavior.
- Analyzing memory dumps.
- Using endpoint detection and response (EDR).
- Hunting for living off the land (LotL) attacks.
- PowerShell and scripting attacks.
- Practical lab: an endpoint data analysis.

Unit Four: Hunting in OT Environments

- The unique challenges of OT threat hunting.
- Hunting for threats in SCADA and ICS networks.
- Protocol analysis for industrial protocols.
- Securing and monitoring legacy systems.
- The Purdue Model for network segmentation.
- Incident response in an OT environment.
- Case study: an industrial control system attack.

Unit Five: The Threat Hunting Program

- Building a threat hunting program.
- The role of automation.
- Communicating findings to leadership.
- Reporting and documentation.
- Metrics and key performance indicators.
- Final project: a comprehensive threat hunting plan.
- Continuous improvement.
- Frequently Asked Questions:

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:

Threat hunting, by its nature, requires an in-depth understanding of both offensive and defensive techniques. How can an organization ensure its threat hunters maintain an ethical mindset while constantly thinking and acting like a malicious actor?

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

This course stands out by providing a unique and vital focus on advanced threat hunting techniques specifically for critical infrastructure. Unlike many general cybersecurity courses, this program addresses the distinct challenges of securing operational technology (OT) and industrial control systems (ICS). The curriculum is built around a proactive, hands-on approach. It teaches you to actively search for hidden threats that have bypassed traditional defenses. The emphasis on network analysis, digital forensics, and OT-specific hunting methodologies distinguishes this course from others. It is for professionals who are ready to move from a reactive defense to a proactive, human-led approach that protects the nation's most vital systems from sophisticated attacks.