Proactive Security Intelligence and Threat Analysis Training Course



23 - 27 Nov 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #SM4124_132476

Course Introduction / Overview:

In today's complex and rapidly evolving threat landscape, a reactive security posture is no longer sufficient. Organizations must adopt a proactive approach, anticipating threats before they materialize. This course provides a comprehensive framework for developing a robust security intelligence and threat analysis capability. It moves beyond simple data collection to instill a deep understanding of the complete threat intelligence lifecycle, from planning and direction to collection, analysis, and dissemination. Drawing upon foundational principles articulated by experts like Richards J. Heuer Jr. in his seminal work, "Psychology of Intelligence Analysis," this program emphasizes the critical role of structured analytic techniques in overcoming cognitive biases and improving analytical rigor. Participants will learn to transform raw information from diverse sources, including open-source intelligence (OSINT) and human intelligence (HUMINT), into actionable insights that inform strategic decision-making and enhance organizational resilience. BIG BEN Training Center has designed this course to equip professionals with the analytical tradecraft and critical thinking skills necessary to identify, assess, and neutralize emerging threats effectively, ensuring their organizations can operate with confidence in an uncertain world.

Target Audience / This training course is suitable for:

- Security Analysts and Investigators.
- Threat Intelligence Professionals.
- Corporate Security Managers.
- Risk Management Specialists.
- Law Enforcement and Intelligence Agency Personnel.
- Cybersecurity Consultants.
- IT Security and Network Administrators.
- Business Continuity and Crisis Management Planners.
- Compliance and Audit Professionals.

Target Sectors and Industries:

- Financial Services and Banking.
- Information Technology and Telecommunications.
- Critical Infrastructure (Energy, Utilities, Transportation).
- Healthcare and Pharmaceuticals.
- Government, Defense, and Public Safety Agencies.
- Retail and E-commerce.
- Consulting and Professional Services.
- Manufacturing and Industrial Control Systems.

Target Organizations Departments:

- Security Operations Center (SOC).
- Corporate and Physical Security.
- Cybersecurity and Information Security.
- Risk Management and Compliance.
- Business Intelligence and Strategy.
- Fraud Prevention and Investigation.
- IT Operations and Network Management.
- Legal and Internal Audit.
- Business Continuity and Disaster Recovery.

Course Offerings:

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

- Master the complete threat intelligence lifecycle from planning to dissemination.
- Apply advanced open-source intelligence (OSINT) collection techniques effectively.
- Develop comprehensive profiles of threat actors, including their motives, capabilities, and tactics.
- Utilize structured analytic techniques to reduce cognitive bias and improve analytical accuracy.
- Conduct in-depth threat and vulnerability assessments for their organization.
- Analyze complex data sets to identify patterns, anomalies, and indicators of compromise.
- Create clear, concise, and actionable intelligence reports for executive leadership.
- Integrate threat intelligence into existing security operations and incident response protocols.
- Understand the legal and ethical considerations governing intelligence gathering activities.
- Evaluate and select appropriate tools and platforms for threat intelligence management.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, immersive, and practical, ensuring that participants can immediately apply their newly acquired skills in their professional roles. We believe that adult learning is most effective when it combines theoretical knowledge with hands-on application. Therefore, this course moves beyond traditional lectures to incorporate a dynamic blend of teaching techniques. A significant portion of the training is dedicated to real-world case studies and simulation exercises, where participants will work in teams to analyze complex threat scenarios, gather intelligence, and develop response strategies. These collaborative activities foster critical thinking, problem-solving, and teamwork. The course includes interactive group discussions, expert-led Q&A sessions, and practical workshops on specific analytical techniques. Our experienced instructors provide continuous feedback and guidance, creating a supportive learning environment where participants can explore challenging concepts with confidence. The emphasis is on learning by doing, transforming theoretical understanding into demonstrable, real-world competence in security intelligence and threat analysis.

Course Agenda (Course Units):

Unit One: Foundations of Security Intelligence

- Introduction to the Intelligence Discipline.
- The Complete Threat Intelligence Lifecycle.
- Differentiating Strategic, Operational, and Tactical Intelligence.
- Requirement Analysis and Intelligence Collection Planning.
- Legal Frameworks and Ethical Considerations in Intelligence Gathering.
- Understanding the Modern Threat Landscape.
- Key Concepts in Risk and Vulnerability Assessment.

Unit Two: Advanced Intelligence Collection Techniques

- Mastering Open-Source Intelligence (OSINT) Methodologies.
- Introduction to Human Intelligence (HUMINT) and Source Vetting.
- Leveraging Social Media Intelligence (SOCMINT).
- Exploring the Deep and Dark Web for Threat Data.
- Technical Intelligence Collection (TECHINT) and Signal Intelligence (SIGINT) Overview.
- Evaluating the Reliability and Credibility of Sources.
- Practical Exercises in Advanced Search and Data Extraction.

Unit Three: Core Principles of Threat Analysis

- The Art and Science of Intelligence Analysis.
- Structured Analytic Techniques (SATs) for Rigorous Analysis.
- Identifying and Mitigating Cognitive Biases in Analysis.
- Analysis of Competing Hypotheses (ACH).
- Threat Modeling and Kill Chain Analysis.
- Indicator of Compromise (IoC) and Indicator of Attack (IoA) Analysis.
- Connecting Disparate Data Points to Form a Coherent Picture.

Unit Four: Threat Actor Profiling and Campaign Analysis

- Understanding Threat Actor Motivations and Objectives.
- Profiling Techniques for Nation-State, Cybercriminal, and Hacktivist Groups.
- Analyzing Tactics, Techniques, and Procedures (TTPs).
- Introduction to the MITRE ATT&CK Framework.
- Attribution and its Challenges in the Digital Age.
- Tracking and Analyzing Malicious Campaigns.
- Predictive Analysis and Threat Forecasting.

Unit Five: Intelligence Reporting, Dissemination, and Integration

- Crafting Actionable Intelligence Reports.
- Writing for Different Audiences (Technical, Managerial, Executive).
- Effective Briefing and Presentation Techniques.
- Dissemination Strategies and Need-to-Know Principles.
- Integrating Threat Intelligence into Security Operations (SecOps).
- Measuring the Effectiveness of an Intelligence Program (Metrics and KPIs).
- Final Simulation: From Raw Data to Executive Briefing.

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:

In an era of AI-driven disinformation, how can intelligence analysts maintain the integrity and reliability of their sources and analysis?

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

This course distinguishes itself by focusing intensely on the cognitive and strategic aspects of intelligence analysis, rather than merely on the technical tools of data collection. While many programs teach which buttons to press, we teach the critical thinking and structured methodologies required to interpret the data correctly. We delve deeply into the principles outlined by authorities like Richards J. Heuer Jr., dedicating significant time to structured analytic techniques designed to overcome the inherent cognitive biases that can lead to catastrophic intelligence failures. The curriculum is built around a series of progressively complex, reality-based simulations that compel participants to move beyond theory and apply their skills under pressure. This practical, hands-on approach ensures that learning is not just absorbed but internalized. Furthermore, the course places a strong emphasis on communication, training analysts to translate their complex findings into clear, concise, and actionable intelligence that can be used by senior leaders to make critical business and security decisions. It bridges the crucial gap between raw data and strategic foresight, empowering professionals to become true intelligence advisors to their organizations.