Behavioral Analytics for Insider Threat Mitigation Training Course



14 - 18 Dec 2026

Cape town

4600 € (Per Person)

Ref: #CYB8141_272268

Course Introduction / Overview:

The escalating risk of insider threats, whether malicious or unintentional, poses a significant challenge to modern organizations, often bypassing traditional perimeter security measures. This course provides a comprehensive framework for understanding, detecting, and mitigating these internal risks through the powerful application of behavioral analytics. Moving beyond conventional security protocols, this program delves into the psychological and technical indicators of insider threats, equipping participants with the skills to establish a proactive defense posture. As discussed by security expert Dr. Eric Cole in his works, the focus must shift from merely building walls to understanding the activities within them. This training course from BIG BEN Training Center is designed to bridge the gap between security technology and human behavior, drawing on principles outlined in publications like "Insider Threat Program: A Guide to Development and Operation". Participants will learn to leverage User Behavior Analytics (UBA), analyze data from various sources to create user baselines, and identify anomalies that signal potential threats. The curriculum integrates strategic program development with hands-on analytical techniques, ensuring that attendees can build and manage an effective insider threat program from the ground up, thereby safeguarding critical assets and maintaining organizational integrity in an evolving threat landscape.

Target Audience / This training course is suitable for:

- Cybersecurity Analysts and Specialists.
- IT Security Managers and Directors.
- Security Operations Center (SOC) Personnel.
- Threat Intelligence Analysts.
- Human Resources and Legal Professionals.
- Compliance and Risk Management Officers.
- Digital Forensic Investigators.
- System and Network Administrators.
- Internal Audit Staff.
- Information Security Officers (ISO).

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceutical.
- Government, Defense, and Intelligence Agencies.
- Technology and Telecommunications.
- Energy and Critical Infrastructure.
- Consulting and Professional Services.
- Retail and E-commerce.
- Education and Research Institutions.

Target Organizations Departments:

- Information Security and Cybersecurity.
- Information Technology (IT) Operations.
- Human Resources (HR).
- Legal and Compliance.
- Internal Audit and Risk Management.
- Physical Security.
- Executive Management.
- Fraud Prevention and Investigation.

Course Offerings:

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

- Develop a comprehensive insider threat program framework tailored to their organization.
- Identify the key psychological and behavioral indicators of potential insider threats.
- Utilize User Behavior Analytics (UBA) to establish normal user baselines.
- Detect anomalous activities and deviations from established behavioral patterns.
- Integrate data from SIEM, DLP, and other security tools for holistic analysis.
- Conduct preliminary investigations into suspected insider threat incidents.
- Formulate effective mitigation strategies and incident response plans.
- Understand the legal, ethical, and privacy considerations of employee monitoring.
- Enhance security awareness programs to proactively reduce insider risk.
- Report on insider threat metrics and program effectiveness to senior leadership.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring participants can apply learned concepts directly to their professional roles. This course moves beyond theoretical lectures by integrating real-world case studies of notable insider threat incidents, allowing for in-depth analysis of attack vectors, detection failures, and successful mitigation tactics. A significant portion of the training is dedicated to hands-on simulated exercises where participants will work with sample data sets to practice establishing user baselines and identifying suspicious anomalies using behavioral analytics principles. Collaborative group discussions and workshops are central to the learning experience, encouraging participants to share insights, debate ethical considerations, and develop comprehensive insider threat program policies. Our expert instructors facilitate these sessions, providing personalized feedback and guiding participants through complex scenarios. The methodology emphasizes a blended learning approach, combining expert instruction with peer-to-peer learning and practical application to build not just knowledge, but tangible skills in insider threat management. This ensures a robust and engaging educational experience that fosters critical thinking and problem-solving abilities.

Course Agenda (Course Units):

Unit One: Foundations of Insider Threat Management

- Defining the Insider Threat Landscape.
- Types of Insider Threats: Malicious, Unintentional, and Collusive.
- Psychological Motivations and Behavioral Precursors.
- The Critical Role of Organizational Culture in Threat Mitigation.
- Legal, Privacy, and Ethical Frameworks for Monitoring.
- Key Components of a Formal Insider Threat Program.
- Case Studies of High-Profile Insider Incidents.

Unit Two: Principles of Behavioral Analytics

- Introduction to User and Entity Behavior Analytics (UEBA).
- Establishing a Baseline of Normal User Activity.
- Key Data Sources for Behavioral Analysis (Logs, Network, Endpoint).
- Techniques for Anomaly Detection and Pattern Recognition.
- Differentiating Between Benign Anomalies and Genuine Threats.
- The Role of Machine Learning and AI in Behavioral Analytics.
- Integrating Behavioral Analytics with Existing Security Infrastructure.

Unit Three: Technical Detection and Investigation Tools

- Leveraging SIEM for Insider Threat Correlation.
- Implementing Data Loss Prevention (DLP) Policies Effectively.
- Utilizing Privileged Access Management (PAM) for High-Risk Users.
- Endpoint Detection and Response (EDR) for User Activity Monitoring.
- Introduction to Digital Forensics for Insider Investigations.
- Analyzing Network Traffic for Suspicious Data Exfiltration.
- Building a Technical Insider Threat Detection Playbook.

Unit Four: Developing and Implementing an Insider Threat Program

- Gaining Executive Buy-In and Establishing Governance.
- Defining Roles and Responsibilities for the Insider Threat Team.
- Creating Policies and Procedures for Monitoring and Reporting.
- Designing and Delivering Effective Security Awareness Training.
- Developing a Communications Plan for the Program Rollout.
- Integrating the Insider Threat Program with HR and Legal Departments.
- Metrics and Key Performance Indicators (KPIs) for Program Success.

Unit Five: Advanced Mitigation and Incident Response

- The Insider Threat Incident Response Lifecycle.
- Techniques for Evidence Collection and Preservation.
- Strategies for Containing and Eradicating Insider Threats.
- Conducting Effective and Fair Employee Interviews.
- Post-Incident Recovery and System Hardening.
- Advanced Threat Hunting for Proactive Detection.
- Capstone Exercise: Responding to a Simulated Insider Threat Scenario.

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 an organization balance robust employee monitoring for insider threat detection with the preservation of employee privacy and trust?

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

This course distinguishes itself by focusing on the critical intersection of human psychology, organizational policy, and technical analytics, rather than concentrating solely on security tools. While many programs teach how to operate specific software, this training course emphasizes the development of a strategic, proactive insider threat program rooted in a deep understanding of behavioral indicators. We prioritize the 'why' behind insider actions, enabling participants to build predictive models and create a security culture that acts as a primary line of defense. The curriculum is built around a series of real-world case studies and a capstone simulation, forcing participants to move beyond theory and apply their knowledge to complex, ambiguous scenarios that mirror actual corporate challenges. Furthermore, the course dedicates significant time to the legal, ethical, and privacy dimensions of employee monitoring, a crucial aspect often overlooked in purely technical training. This holistic approach ensures that graduates are not just tool operators, but are prepared to be strategic leaders who can design, implement, and manage a comprehensive, effective, and legally compliant insider threat mitigation program that protects the organization while respecting its employees.