Training Course on Behavioral Analytics for Insider Threat Hunting

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's interconnected digital landscape, organizations face an escalating and insidious threat: insider attacks. These threats, originating from within an organization by current or former employees, contractors, or business partners, leverage legitimate access to compromise sensitive data, systems, and intellectual property. Traditional perimeter-based security measures often prove insufficient against these sophisticated and often subtle attacks. **Behavioral Analytics** emerges as a critical and highly effective countermeasure, offering a proactive approach to **Insider Threat Hunting** by identifying anomalous user behaviors that deviate from established baselines. This course provides comprehensive knowledge and practical skills to detect, investigate, and mitigate these complex internal risks, safeguarding organizational assets and maintaining business continuity in an increasingly volatile cybersecurity environment.

Training Course on Behavioral Analytics for Insider Threat Hunting is designed to empower cybersecurity professionals with the advanced techniques of **User and Entity Behavior Analytics (UEBA)**. Participants will delve into the nuances of **data exfiltration detection**, **privilege escalation monitoring**, and **anomaly detection**, utilizing cutting-edge tools and methodologies. By focusing on **proactive threat identification** and **risk mitigation strategies**, this course addresses the urgent need for skilled professionals capable of defending against the evolving landscape of internal cyber threats, ensuring robust **organizational resilience** and **data security**.

Programme Curriculum

Training Course on Behavioral Analytics for Insider Threat Hunting

Introduction

In today's interconnected digital landscape, organizations face an escalating and insidious threat: insider attacks. These threats, originating from within an organization by current or former

employees, contractors, or business partners, leverage legitimate access to compromise sensitive data, systems, and intellectual property. Traditional perimeter-based security measures often prove insufficient against these sophisticated and often subtle attacks. **Behavioral Analytics** emerges as a critical and highly effective countermeasure, offering a proactive approach to **Insider Threat Hunting** by identifying anomalous user behaviors that deviate from established baselines. This course provides comprehensive knowledge and practical skills to detect, investigate, and mitigate these complex internal risks, safeguarding organizational assets and maintaining business continuity in an increasingly volatile cybersecurity environment.

Training Course on Behavioral Analytics for Insider Threat Hunting is designed to empower cybersecurity professionals with the advanced techniques of **User and Entity Behavior Analytics (UEBA)**. Participants will delve into the nuances of **data exfiltration detection**, **privilege escalation monitoring**, and **anomaly detection**, utilizing cutting-edge tools and methodologies. By focusing on **proactive threat identification** and **risk mitigation strategies**, this course addresses the urgent need for skilled professionals capable of defending against the evolving landscape of internal cyber threats, ensuring robust **organizational resilience** and **data security**.

Course Duration

5 days

Course Objectives

1. **Master User and Entity Behavior Analytics (UEBA)** principles and their application in **Insider Threat Detection**.
2. Develop robust **behavioral baselines** and identify significant deviations indicative of malicious or negligent insider activity.
3. Implement advanced **data exfiltration prevention** techniques through behavioral pattern analysis.
4. Proactively identify and investigate **privilege escalation** attempts and suspicious access patterns.
5. Leverage **Machine Learning (ML)** and **Artificial Intelligence (AI)** for enhanced **anomaly detection** in user behavior.
6. Understand and apply **threat intelligence** to enrich behavioral analytics for more accurate threat hunting.
7. Develop **incident response playbooks** tailored to behavioral analytics alerts and insider threat scenarios.
8. Analyze **network traffic anomalies** and **endpoint activities** to pinpoint hidden insider threats.
9. Comprehend the legal and ethical considerations of **user monitoring** and data privacy in behavioral analytics.
10. Utilize **Security Information and Event Management (SIEM)** systems in conjunction with UEBA for comprehensive threat visibility.
11. Design and implement effective **insider risk management programs** within organizational frameworks.
12. Conduct thorough **forensic investigations** of insider incidents using behavioral data.
13. Stay abreast of emerging **insider threat vectors** and adapt behavioral analytics strategies accordingly.

Organizational Benefits

- Significantly reduce the Mean Time To Detect (MTTD) insider threats, preventing data breaches and intellectual property theft before they escalate.
- Safeguard sensitive information and critical assets from unauthorized access and misuse by internal actors.
- Minimize the financial impact of insider incidents, including regulatory fines, remediation costs, and reputational damage.
- Strengthen adherence to data protection regulations and internal security policies.
- Streamline threat hunting processes and reduce false positives by focusing on truly anomalous behaviors.
- Build a more resilient and adaptive security framework capable of defending against evolving insider threats.
- Foster a culture of security awareness and accountability among employees.
- Efficiently allocate security resources by prioritizing high-risk insider activities.

Target Audience

1. Security Analysts & Engineers.
2. Threat Hunters.
3. Incident Responders.
4. Security Operations Center (SOC) Personnel.
5. Forensic Investigators.
6. IT Auditors & Compliance Officers.
7. Risk Management Professionals.
8. Cybersecurity Consultants

Course Outline

Module 1: Foundations of Insider Threat and Behavioral Analytics

- Understanding the evolving landscape of insider threats: malicious, negligent, and compromised.
- Defining key concepts: User Behavior Analytics (UBA) and User and Entity Behavior Analytics
- The psychological and motivational factors driving insider threats.
- Distinction between traditional security measures and behavioral analytics in insider threat detection.
- Legal and ethical considerations of monitoring employee behavior.
- **Case Study:** The Edward Snowden Leaks – Analyzing how behavioral anomalies could have signaled the massive data exfiltration by a privileged insider.

Module 2: Data Sources and Collection for Behavioral Analytics

- Identifying critical data sources: logs, network traffic, endpoint activity, application usage, HR data.
- Techniques for centralized data aggregation and normalization
- Data quality and its impact on behavioral analytics accuracy.
- Privacy-preserving data collection methods and anonymization.
- Integrating diverse data sets for a holistic view of user behavior.
- **Case Study:** Financial Institution Fraud – How correlating transaction logs, login times, and access patterns identified an employee systematically siphoning funds.

Module 3: Establishing Behavioral Baselines and Anomaly Detection

- Methodologies for establishing normal user and entity behavior baselines.
- Statistical analysis and machine learning algorithms for anomaly detection.
- Types of anomalies: rare events, deviations from peer groups, time-based anomalies.
- Tuning behavioral models to reduce false positives and false negatives.
- Visualizing behavioral data for intuitive threat hunting.
- **Case Study:** Intellectual Property Theft by a Departing Employee – Illustrating how unusual access to R&D files and data transfer attempts outside normal working hours flagged a potential IP theft.

Module 4: Advanced Behavioral Analytics Techniques

- Leveraging supervised and unsupervised machine learning for behavioral analysis.
- Techniques for detecting privilege escalation and lateral movement.
- Analyzing communication patterns and data exfiltration channels
- Detecting unusual access to sensitive data and critical systems.
- Introduction to advanced analytics platforms and tools for UEBA.
- **Case Study:** Critical Infrastructure Sabotage – How a sudden change in an engineer's access patterns and unusual commands on SCADA systems led to the discovery of a planned sabotage attempt.

Module 5: Insider Threat Hunting Methodologies

- Developing a hypothesis-driven approach to insider threat hunting.
- Proactive searching for indicators of compromise (IoCs) and indicators of attack (IoAs) within behavioral data.
- Using threat intelligence feeds to contextualize behavioral anomalies.
- Integrating behavioral analytics with SIEM and EDR (Endpoint Detection and Response) solutions.
- Building effective threat hunting teams and workflows.
- **Case Study:** Supply Chain Compromise – How a series of seemingly innocuous, low-risk behaviors across multiple employees, when correlated, revealed a sophisticated supply chain attack orchestrated by an insider.

Module 6: Incident Response and Remediation for Insider Threats

- Establishing a robust insider threat incident response plan.
- Triage and prioritization of behavioral alerts.
- Containment strategies for ongoing insider incidents.
- Forensic data collection and preservation from behavioral analytics platforms.
- Post-incident analysis, reporting, and lessons learned.
- **Case Study:** Healthcare Data Breach – Demonstrating the rapid response and mitigation efforts initiated after behavioral analytics detected an employee accessing and downloading an unusual volume of patient records.

Module 7: Building and Managing an Insider Threat Program

- Key components of a comprehensive insider threat program (ITP).
- Roles and responsibilities within an ITP (HR, Legal, Security, IT).
- Policy development and enforcement for insider risk management.
- Training and awareness programs for employees on insider threat prevention.
- Continuous evaluation and improvement of the ITP.

- **Case Study:** Government Agency Insider Threat Program – A successful example of how a multi-disciplinary approach, with behavioral analytics at its core, significantly reduced insider risk within a sensitive environment.

Module 8: Future Trends and Emerging Technologies

- The impact of AI and Generative AI on insider threat detection and new attack vectors.
- Leveraging behavioral biometrics for enhanced authentication and anomaly detection.
- The role of Zero Trust architectures in mitigating insider risks.
- Cloud security challenges and behavioral analytics in cloud environments.
- Emerging threats and adaptive defense strategies for the future.
- **Case Study:** Nation-State Espionage – Exploring how advanced persistent threats (APTs) are leveraging insider access and how cutting-edge behavioral analytics is evolving to detect these sophisticated, long-term compromises.

Training Methodology

This training course employs a blended learning approach designed for maximum engagement and practical skill development:

- **Interactive Lectures:** Core concepts will be delivered through engaging presentations and discussions.
- **Hands-on Labs:** Participants will gain practical experience using simulated environments and industry-standard behavioral analytics tools.
- **Real-world Case Studies:** In-depth analysis of actual insider threat incidents to illustrate concepts and best practices.
- **Group Exercises & Discussions:** Collaborative problem-solving and sharing of insights among participants.
- **Expert Demonstrations:** Live demonstrations of behavioral analytics platforms and techniques.
- **Q&A Sessions:** Dedicated time for participants to ask questions and receive personalized guidance.
- **Capstone Project/Simulation:** A culminating exercise where participants apply learned skills to a realistic insider threat hunting scenario.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com