Training Course on Advanced Identity and Access Management Forensics

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's complex digital landscape, robust **Identity and Access Management (IAM)** is the cornerstone of cybersecurity. Organizations face relentless sophisticated threats, where compromised identities are frequently the initial vector for major breaches. This advanced training course delves into the critical discipline of **IAM Forensics**, equipping cybersecurity professionals with the specialized knowledge and hands-on skills required to investigate, analyze, and respond to identity-related security incidents. From detecting anomalous access patterns to unraveling sophisticated privilege escalation attacks, participants will gain expertise in preserving digital evidence, conducting in-depth forensic analysis of IAM systems, and implementing proactive measures to fortify identity infrastructure against future compromise.

Training Course on Advanced Identity and Access Management Forensics moves beyond foundational IAM concepts, focusing specifically on the investigative and remedial aspects crucial for **incident response** and **threat hunting**. We will explore cutting-edge techniques for dissecting authentication logs, authorization policies, and identity lifecycle events to reconstruct attack timelines and identify threat actors. With a strong emphasis on **cloud IAM security**, **zero-trust architectures**, and the emerging role of **AI in forensics**, this course prepares participants to tackle the most pressing challenges in modern identity security. Mastering IAM forensics is no longer a niche skill but a fundamental requirement for any organization committed to safeguarding its digital assets and maintaining **regulatory compliance**.

Programme Curriculum

Training Course on Advanced Identity and Access Management Forensics

Introduction

In today's complex digital landscape, robust **Identity and Access Management (IAM)** is the cornerstone of cybersecurity. Organizations face relentless sophisticated threats, where compromised identities are frequently the initial vector for major breaches. This advanced training course delves into the critical discipline of **IAM Forensics**, equipping cybersecurity professionals with the specialized knowledge and hands-on skills required to investigate, analyze, and respond to identity-related security incidents. From detecting anomalous access patterns to unraveling sophisticated privilege escalation attacks, participants will gain expertise in preserving digital evidence, conducting in-depth forensic analysis of IAM systems, and implementing proactive measures to fortify identity infrastructure against future compromise.

Training Course on Advanced Identity and Access Management Forensics moves beyond foundational IAM concepts, focusing specifically on the investigative and remedial aspects crucial for **incident response** and **threat hunting**. We will explore cutting-edge techniques for dissecting authentication logs, authorization policies, and identity lifecycle events to reconstruct attack timelines and identify threat actors. With a strong emphasis on **cloud IAM security**, **zero-trust architectures**, and the emerging role of **AI in forensics**, this course prepares participants to tackle the most pressing challenges in modern identity security. Mastering IAM forensics is no longer a niche skill but a fundamental requirement for any organization committed to safeguarding its digital assets and maintaining **regulatory compliance**.

Course Duration

10 days

Course Objectives

1. Develop expertise in structured forensic investigation techniques tailored for complex Identity and Access Management incidents.
2. Gain proficiency in dissecting security breaches and anomalous activities within leading cloud provider IAM services (e.g., AWS IAM, Azure AD, GCP IAM).
3. Understand and forensically analyze deviations from Zero Trust principles, including micro-segmentation bypasses and continuous verification failures.
4. Conduct in-depth investigations into compromised privileged accounts, session hijacking, and lateral movement stemming from PAM vulnerabilities.
5. Explore and apply artificial intelligence and machine learning tools for anomaly detection, behavioral analytics, and accelerated incident triage in IAM environments.
6. Identify and forensically analyze attacks exploiting vulnerabilities in identity federation (e.g., SAML, OAuth, OIDC) and Single Sign-On (SSO) implementations.
7. Understand the forensic implications and investigative techniques for decentralized identity systems leveraging blockchain technology.
8. Specialize in forensic analysis of on-premises Active Directory and cloud-based Azure Active Directory environments for identity-related breaches.
9. Master the extraction, normalization, and correlation of extensive IAM logs from various sources within Security Information and Event Management (SIEM) platforms for forensic purposes.
10. Design and execute proactive threat hunting strategies to identify dormant threats and sophisticated attacks targeting identity infrastructure.
11. Identify common IAM misconfigurations and vulnerabilities that contribute to security incidents and learn to recommend remediation.
12. Understand the legal and compliance implications (e.g., GDPR, HIPAA, PCI DSS) for identity-related investigations and evidence handling.

13. Participate in hands-on labs and simulations to practically apply forensic techniques in response to realistic identity-centric cyberattack scenarios.

Target Audience

1. Security Analysts and Engineers.
2. Incident Response Team Members.
3. Digital Forensics and e-Discovery Specialists
4. IAM Architects and Administrators.
5. Threat Hunters.
6. Security Operations Center (SOC) Analysts
7. IT Auditors and Compliance Officers.
8. Cybersecurity Consultants

Course Outline

Module 1: Foundations of Advanced IAM Forensics

- In-depth Review of IAM Principles and Architecture.
- Legal and Ethical Considerations in Digital Forensics
- Forensic Readiness Planning for IAM Systems
- Methodologies for IAM Incident Response.
- Introduction to Specialized IAM Forensic Tooling
- **Case Study:** Analyzing a compromised multi-factor authentication (MFA) system due to phishing, focusing on log analysis and initial containment.

Module 2: Cloud IAM Security Forensics (AWS & Azure)

- Forensic Artifacts in AWS IAM.
- Azure AD Identity Forensics.
- Identifying Overly Permissive Cloud IAM Policies.
- Cloud Identity Governance and Administration (IGA) in Forensics
- Investigating Cloud API Compromises.
- **Case Study:** A cloud environment breach originating from a compromised IAM role with excessive permissions in AWS, leading to data exfiltration.

Module 3: Zero Trust Architecture (ZTA) Forensics

- Forensically Analyzing Micro-segmentation Bypass.
- Continuous Verification and Adaptive Access Logs
- Investigating Device Trust and Posture Assessment Failures.
- User and Entity Behavior Analytics (UEBA) for ZTA Forensics.
- Forensic Implications of Just-in-Time (JIT) and Just-Enough-Access (JEA)
- **Case Study:** An insider threat attempting to escalate privileges in a Zero Trust network, with forensics focusing on policy violations and access attempts from unauthorized locations.

Module 4: Privileged Access Management (PAM) Forensics

- Investigating PAM System Breaches.
- Detecting Privileged Account Compromise.
- Analyzing Lateral Movement and Privilege Escalation
- Forensics of Credential Theft Attacks.
- Break-Glass Account Forensics.

- **Case Study:** A ransomware attack initiated through a compromised privileged account, with forensics focusing on the PAM system's logs and session recordings.

Module 5: Advanced Authentication & Authorization Forensics

- Multi-Factor Authentication (MFA) Bypass Forensics.
- SSO and Identity Federation Forensic Analysis.
- Detecting Session Hijacking and Token Theft.
- Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) Forensics.
- Passwordless Authentication Forensics
- **Case Study:** A breach involving the abuse of an SSO token obtained through a social engineering attack, leading to unauthorized access to multiple enterprise applications.

Module 6: Identity Lifecycle Forensics

- Forensics of Account Provisioning and Deprovisioning Anomalies.
- Analyzing User Onboarding/Offboarding Incidents.
- Role and Entitlement Review Forensics
- Investigating Ghost Accounts and Dormant Accounts
- Synchronization Service Forensics
- **Case Study:** An ex-employee retaining access to sensitive systems due to improper deprovisioning processes, leading to data theft.

Module 7: Digital Evidence Collection and Preservation in IAM Forensics

- Strategies for Live Response and Data Acquisition.
- Forensic Imaging and Data Integrity.
- Cloud-Specific Evidence Collection Challenges.
- Handling Encrypted Identity Data
- Maintaining Chain of Custody for IAM Evidence.
- **Case Study:** Responding to a suspected insider threat within an IAM team, focusing on proper collection and preservation of logs and configuration files.

Module 8: Advanced Log Analysis and SIEM Correlation for IAM

- Deep Dive into IAM-Related Log Sources
- Automated Log Parsing and Normalization
- Correlation of Disparate Identity Logs
- Building Custom SIEM Dashboards and Alerts for IAM Threats
- Using UEBA and SOAR in IAM Forensics.
- **Case Study:** Reconstructing a complex attack path involving multiple compromised accounts by correlating logs from Active Directory, Okta, and a cloud application.

Module 9: AI and Machine Learning in IAM Forensics

- Fundamentals of AI/ML for Anomaly Detection.
- Applying Machine Learning to User Behavioral Analytics.
- AI-Driven Threat Intelligence for IAM
- Challenges and Limitations of AI in Forensics.
- Future Trends: Explainable AI (XAI) in IAM Forensics
- **Case Study:** Using a UEBA solution to identify a compromised account based on unusual login times and access to previously untouched resources.

Module 10: Advanced Active Directory and Azure AD Forensics

- Deep Dive into Active Directory Attack Paths.
- Analyzing Active Directory Logs for Compromise
- Forensic Tools for Active Directory.
- Azure AD Identity Protection and Risky Sign-ins Forensics
- Investigating Azure AD Application and Service Principal Compromises.
- **Case Study:** A multi-stage attack involving an initial compromise of an Active Directory user, leading to a Golden Ticket attack and subsequent access to cloud resources via Azure AD.

Module 11: Blockchain Identity and Decentralized Identity Forensics

- Understanding Blockchain Fundamentals for Identity.
- Forensic Considerations for Self-Sovereign Identity.
- Analyzing On-Chain Identity Transactions.
- Challenges of Pseudonymity and Privacy in Blockchain Forensics
- Future of Blockchain in Digital Identity Forensics
- **Case Study:** Investigating a fraudulent identity claim on a decentralized identity network, tracing the origin of the identity and any associated transactions.

Module 12: Forensics of Identity-Related Compliance Violations

- Data Privacy Regulations and IAM Forensics.
- PCI DSS and SOX Compliance in IAM Security Incidents
- Auditing and Reporting on IAM Forensic Findings.
- Remediation and Post-Incident Review for Compliance
- Preparation for External Audits of IAM Controls.
- **Case Study:** A data breach involving personally identifiable information (PII) due to an IAM misconfiguration, with a focus on preparing forensic reports for regulatory submission.

Module 13: Advanced IAM Threat Hunting Techniques

- Developing Proactive Hunting Queries for IAM Data
- Identifying Anomalous Identity Behavior Patterns
- Hunting for Persistence Mechanisms in IAM Systems.
- Using MITRE ATT&CK for Identity-Focused Threat Hunting
- Building Custom Detection Rules for Emerging IAM Threats
- **Case Study:** A proactive threat hunt uncovers a dormant phishing campaign targeting privileged users, using behavioral analytics and advanced log correlation.

Module 14: Practical Labs & Incident Simulation

- Hands-on Incident Scenarios.
- Evidence Collection and Analysis Workshop.
- Report Writing and Presentation
- Tabletop Exercises.
- Post-Mortem Analysis and Lessons Learned
- **Case Study:** Full-scale simulation of a multi-stage attack involving Active Directory compromise, lateral movement, and cloud account takeover, requiring integrated forensic analysis.

Module 15: Emerging Trends & Future of IAM Forensics

- Quantum-Resistant Cryptography and its Impact on IAM
- Identity of Things (IDoT) Forensics
- DevSecOps and IAM Forensics.
- Graph Databases for Identity Analytics.
- The Evolving Threat Landscape for Identities.
- **Case Study:** Discussing the forensic challenges posed by a hypothetical supply chain attack where a trusted identity provider is compromised.

Training Methodology

- Instructor-Led Lectur

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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