Training Course on Investigating Zero-Trust Architecture Incidents

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 an era of escalating cyber threats and evolving network paradigms, the Zero-Trust Architecture (ZTA) framework has emerged as a vital model for modern enterprise security. Unlike traditional perimeter-based models, Zero Trust operates on the principle of "never trust, always verify," requiring strict identity verification and continuous monitoring. As organizations migrate to hybrid and cloud-native environments, understanding how to investigate security incidents within a Zero-Trust framework has become critical. Training Course on Investigating Zero-Trust Architecture Incidents is designed to equip cybersecurity professionals, IT administrators, and incident response teams with cutting-edge tools, methodologies, and investigative techniques tailored specifically for Zero-Trust ecosystems.

This course focuses on real-time breach analysis, behavioral anomaly detection, micro-segmentation enforcement breaches, access control failures, and compromised identity incidents across cloud, on-premise, and hybrid environments. With hands-on labs, simulated incident scenarios, and advanced detection frameworks such as MITRE ATT&CK, participants will master incident triage, digital forensics, lateral movement tracking, and policy-based response mechanisms. Participants will emerge with advanced proficiency in investigating Zero-Trust incidents, enabling proactive threat mitigation, compliance assurance, and security resilience in high-stakes IT infrastructures.

Programme Curriculum

Training Course on Investigating Zero-Trust Architecture Incidents

Introduction

In an era of escalating cyber threats and evolving network paradigms, the Zero-Trust Architecture (ZTA) framework has emerged as a vital model for modern enterprise security. Unlike traditional perimeter-based models, Zero Trust operates on the principle of "never trust, always verify," requiring strict identity verification and continuous monitoring. As organizations migrate to hybrid and cloud-native environments, understanding how to investigate security incidents within a Zero-Trust framework has become critical. Training Course on Investigating Zero-Trust Architecture Incidents is

designed to equip cybersecurity professionals, IT administrators, and incident response teams with cutting-edge tools, methodologies, and investigative techniques tailored specifically for Zero-Trust ecosystems.

This course focuses on real-time breach analysis, behavioral anomaly detection, micro-segmentation enforcement breaches, access control failures, and compromised identity incidents across cloud, on-premise, and hybrid environments. With hands-on labs, simulated incident scenarios, and advanced detection frameworks such as MITRE ATT&CK, participants will master incident triage, digital forensics, lateral movement tracking, and policy-based response mechanisms. Participants will emerge with advanced proficiency in investigating Zero-Trust incidents, enabling proactive threat mitigation, compliance assurance, and security resilience in high-stakes IT infrastructures.

Course Objectives

1. Understand the core principles of Zero-Trust Architecture (ZTA) in enterprise security.
2. Conduct digital forensics in micro-segmented and software-defined perimeters.
3. Apply behavioral analytics and machine learning for threat detection.
4. Detect and mitigate identity-based attacks using real-time access logs.
5. Implement incident response playbooks aligned with Zero Trust.
6. Leverage SIEM/SOAR tools for Zero-Trust incident detection and response.
7. Analyze policy violations in least-privilege access controls.
8. Investigate and remediate east-west lateral movement within networks.
9. Use zero-trust policy enforcement data for root-cause analysis.
10. Integrate cloud forensics techniques in ZTA investigations.
11. Conduct threat hunting using Zero-Trust telemetry data.
12. Utilize MITRE ATT&CK and NIST frameworks in ZTA breach investigations.
13. Document and report Zero-Trust incidents for regulatory compliance and audits.

Target Audiences

1. Cybersecurity Analysts
2. Incident Response Teams
3. Network Security Engineers
4. Cloud Security Architects
5. Government Cyber Forensics Units
6. IT Auditors and Compliance Officers
7. CISOs and Security Managers
8. Penetration Testers and Red Team Operators

Course Duration: 10 days

Course Modules

Module 1: Foundations of Zero-Trust Architecture

- Introduction to Zero-Trust principles
- Micro-segmentation and trust zones
- Policy engines and enforcement points
- Role of identity and access control
- ZTA vs traditional security models
- **Case Study**: Transitioning a legacy enterprise to Zero Trust

Module 2: Threat Landscape in ZTA Environments

- Modern cyber threats targeting ZTA
- Attack vectors and vulnerabilities
- Identity-based threats

- Zero Trust attack surface
- Detection techniques overview
- **Case Study**: Stopping an insider attack using ZTA logs

Module 3: Forensic Data Collection in ZTA

- Identifying forensic artifacts in Zero Trust
- Leveraging telemetry and log aggregation
- Endpoint Detection and Response (EDR) tools
- Data retention and compliance
- Legal and chain-of-custody considerations
- **Case Study**: Using telemetry to trace unauthorized access

Module 4: Identity and Access Incident Analysis

- Investigating login anomalies and credential abuse
- Multi-factor authentication failures
- Identity federation and SSO risks
- Log correlation from IdP and endpoints
- Remediation and access revocation
- **Case Study**: Investigating a stolen credential attack

Module 5: Lateral Movement and Containment

- East-west traffic analysis
- Micro-segmentation breach forensics
- Policy-based containment strategies
- Detecting command-and-control channels
- Network flow visualizations
- **Case Study**: Halting malware spread in Zero Trust networks

Module 6: SIEM and SOAR Integration in ZTA

- Using SIEMs to monitor Zero Trust activity
- Automating response with SOAR platforms
- Alert triaging and enrichment
- Workflow orchestration
- Incident lifecycle management
- **Case Study**: Automating privilege escalation alerts

Module 7: Investigative Playbooks and Compliance

- Creating Zero-Trust-specific IR playbooks
- Compliance considerations (HIPAA, GDPR, NIST)
- Evidence documentation
- Collaboration across security teams
- Reporting to regulatory bodies
- **Case Study**: Regulatory audit after a ZTA breach

Module 8: Cloud and Hybrid Zero-Trust Forensics

- Investigating across multi-cloud and on-prem setups
- Cloud-native forensics tools (Azure, AWS, GCP)
- SASE and edge environments
- Hybrid policy enforcement issues
- Cross-domain identity challenges

- **Case Study**: Cross-cloud identity compromise investigation

Training Methodology

- Interactive lectures with real-world case studies
- Virtual labs with sandboxed ZTA environments
- Group exercises simulating incident response
- Role-based investigative scenarios
- Gamified challenges for threat detection
- Final capstone project analyzing a Zero-Trust breach

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org 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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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