Certificate of Competence in Zero Trust Training Course

Professional Development Training Course Outline

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

Course Introduction

The outdated perimeter-based security model has proven fatally insufficient against modern threats like Ransomware Attacks, Supply Chain Exploits, and advanced AI-Powered Phishing. The future of enterprise security is the Zero Trust Architecture (ZTA), operating on the principle of "Never Trust, Always Verify." This paradigm shift is not merely a technology upgrade, but a foundational change in organizational security philosophy, demanding a new cohort of skilled Cybersecurity Professionals. Certificate of Competence in Zero Trust Training Course provides the non-negotiable competency required to design, plan, and deploy a robust ZTA, drastically reducing the Attack Surface and mitigating the risk of Lateral Movement even during an internal breach. Our certification is aligned with industry-leading frameworks like NIST 800-207 and the CISA Zero Trust Maturity Model, ensuring practical, vendor-agnostic knowledge for immediate application.

This CCZT course offers a comprehensive, practical curriculum focused on the core pillars of Zero Trust: Identity Verification, Micro-Segmentation, Least Privilege Access, and Continuous Monitoring. Security leaders are actively seeking certified expertise to drive the Digital Transformation securely, especially in complex Hybrid Cloud and Multi-Cloud Environments. By mastering Zero Trust Network Access (ZTNA) and the practical implementation of Adaptive Authentication, graduates will possess a verified, in-demand skill set essential for career acceleration. The course methodology emphasizes real-world Case Studies and Hands-on Labs to transition theoretical knowledge into proven Implementation Skills, empowering attendees to lead their organizations toward a state of true Cyber-Resilience against evolving threats.

Programme Curriculum

Certificate of Competence in Zero Trust Training Course

Introduction

The outdated perimeter-based security model has proven fatally insufficient against modern threats like Ransomware Attacks, Supply Chain Exploits, and advanced AI-Powered Phishing. The future of enterprise security is the Zero Trust Architecture (ZTA), operating on the principle of "Never Trust, Always Verify." This paradigm shift is not merely a technology upgrade, but a foundational change in organizational security philosophy, demanding a new cohort of skilled Cybersecurity Professionals. Certificate of Competence in Zero Trust Training Course provides the non-negotiable competency required to design, plan, and deploy a robust ZTA, drastically reducing the Attack Surface and mitigating the risk of Lateral Movement even during an internal breach. Our certification is aligned with industry-leading frameworks like NIST 800-207 and the CISA Zero Trust Maturity Model, ensuring practical, vendor-agnostic knowledge for immediate application.

This CCZT course offers a comprehensive, practical curriculum focused on the core pillars of Zero Trust: Identity Verification, Micro-Segmentation, Least Privilege Access, and Continuous Monitoring. Security leaders are actively seeking certified expertise to drive the Digital Transformation securely, especially in complex Hybrid Cloud and Multi-Cloud Environments. By mastering Zero Trust Network Access (ZTNA) and the practical implementation of Adaptive Authentication, graduates will possess a verified, in-demand skill set essential for career acceleration. The course methodology emphasizes real-world Case Studies and Hands-on Labs to transition theoretical knowledge into proven Implementation Skills, empowering attendees to lead their organizations toward a state of true Cyber-Resilience against evolving threats.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Define and articulate the core principles of Zero Trust Architecture (ZTA) and the "Never Trust, Always Verify" philosophy.
2. Analyze the failures of traditional Perimeter Security and justify the business case for ZTA adoption to C-Suite Leadership.
3. Implement robust Multi-Factor Authentication (MFA) and Adaptive Authentication for all users and services.
4. Design and enforce Least Privilege Access (LPA) policies based on user, device, and resource context.
5. Apply Micro-Segmentation techniques to limit Lateral Movement and protect the Protect Surface.
6. Evaluate and secure modern Cloud Environments (Hybrid and Multi-Cloud) using ZTA principles.
7. Map organizational assets and data flows to define the Protect Surface and Attack Surface.
8. Integrate Continuous Monitoring and Behavioral Analytics for real-time threat detection and anomaly flagging.
9. Develop a phased Zero Trust Strategy and Implementation Plan aligned with the NIST 800-207 framework.
10. Assess the security posture of an organization's endpoints and devices to enforce Device Health verification.
11. Govern and ensure Compliance by mapping ZTA controls to regulatory frameworks like GDPR, HIPAA, and ISO 27001.
12. Master the concepts of Zero Trust Network Access (ZTNA) as an alternative to outdated VPN technology.
13. Adapt and apply ZT principles to address emerging threats like Account Takeover (ATO) and sophisticated Social Engineering attacks.

Course Modules

Module 1: Foundational Zero Trust Concepts and Strategy

- Evolution from Perimeter to Zero Trust Architecture, defining the Protect Surface.
- The 'Never Trust, Always Verify' mantra, ZTA Pillars
- Mapping ZTA to business goals, regulatory Compliance.
- Deep dive into NIST SP 800-207 and the CISA Maturity Model stages.
- Case Study: Analyzing a large financial institution's strategic shift from a VPN-centric model to a comprehensive, multi-year ZT roadmap.

Module 2: Identity as the New Perimeter

- Implementing mandatory Multi-Factor Authentication and risk-based Adaptive Authentication.
- Designing and enforcing Least Privilege Access and Just-In-Time access for all roles.
- Managing user and service accounts, lifecycle, and privileged access management.
- Integrating Device Health checks and security posture into the access decision-making process.
- Case Study: Reviewing an organization's defense against an Account Takeover attack, focusing on how contextual access policies blocked the threat.

Module 3: Micro-Segmentation and Network Security

- Perimeter Elimination.
- Segmentation Strategy.
- Practical steps for implementing host-based and network-based Micro-Segmentation techniques.
- Zero Trust Network Access.
- Case Study: Simulating a ransomware breach scenario to demonstrate how effective micro-segmentation contains the infection to a single segment, minimizing impact.

Module 4: Securing Data and Applications in ZTA

- Data-Centric Security.
- Implementing encryption in transit and at rest, and Data Loss Prevention under ZT.
- Securing application workloads and APIs with identity-driven access controls.
- Implementing strong identity for non-human entities like microservices and serverless functions.
- Case Study: Designing a ZT data protection plan for an e-commerce platform that processes PII and credit card data across multiple application tiers.

Module 5: Cloud and Hybrid Environment Security

- Applying Zero Trust to Hybrid Cloud and Multi-Cloud Environments.
- Securing infrastructure and platform services with native cloud identity and access policies.
- Implementing secure, governed access to third-party SaaS Applications
- Cloud Configuration.
- Case Study: A company's successful migration of its legacy on-premise application to a Zero Trust-enabled AWS/Azure hybrid environment without service disruption.

Module 6: Continuous Monitoring and Threat Response

- Establishing comprehensive logging and security data collection across all ZT components.
- Using User and Entity Behavior Analytics to detect anomalies and insider threats.

- Integrating with Security Information and Event Management and Security Orchestration, Automation, and Response.
- Developing playbooks and automated responses tailored for a ZT environment.
- Case Study: Analyzing a real-time threat detection scenario where anomalous user behavior was flagged and remediated automatically by the ZT policy engine.

Module 7: ZT Implementation Planning and Transition

- Assessing the current security state, identifying quick wins, and long-term ZT objectives.
- Strategies for integrating or transitioning Legacy Systems that do not natively support ZT principles.
- Developing a practical, incremental, and risk-managed Zero Trust Implementation Plan.
- Overcoming user resistance, training employees, and gaining executive sponsorship.
- Case Study: Documenting the challenges and solutions in a mid-sized enterprise's one-year phased rollout, prioritizing data segmentation over a full infrastructure overhaul.

Module 8: ZT Governance, Risk, and Emerging Trends

- Designing and maintaining dynamic, centralized ZT policies using the Policy Engine and Policy Administrator.
- Establishing ongoing governance, auditing mechanisms, and key performance indicators for ZT success.
- Exploring the role of AI/Machine Learning in ZT and securing IoT/OT environments.
- Review of leading ZT vendors, tools, and the role of vendor-agnostic certification.
- Case Study: Examining an organization's compliance audit where ZT controls were successfully validated against multiple international regulatory standards, demonstrating Cyber-Resilience.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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
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