Implementing the Zero Trust Extended Ecosystem 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 modern enterprise landscape is defined by digital transformation and the dissolution of the traditional network perimeter, rendering legacy security models ineffective against sophisticated, AI-powered cyber threats. The Zero Trust Extended Ecosystem (ZTX) is the mandatory, future-proof security framework designed to meet this challenge. It operates on the core principle of "never trust, always verify," demanding continuous authentication and authorization for every user, device, application, and data access request, regardless of location. This paradigm shift secures the distributed enterprise, encompassing hybrid cloud environments, remote workforces, and the burgeoning IoT/OT landscape, effectively mitigating risks like lateral movement and insider threats. This course provides the strategic roadmap and practical, hands-on skills required for security professionals and leaders to architect, implement, and govern a comprehensive, NIST SP 800-207 compliant ZTX across their entire digital estate.

Implementing the Zero Trust Extended Ecosystem Training Course focuses not just on theoretical concepts but on the real-world implementation of the seven Zero Trust pillars: Identity, Devices, Data, Applications, Network/Workload, Automation & Orchestration, and Analytics & Visibility. We will dive deep into micro-segmentation, Just-In-Time (JIT)/Just-Enough-Access (JEA) principles, and advanced policy enforcement. The curriculum integrates leading vendor solutions and utilizes live, hands-on labs to ensure mastery of the technical components necessary for deployment. Graduates will be equipped to drive significant cyber risk reduction, enhance regulatory compliance, and establish a data-centric security posture that is resilient against the most advanced persistent threats, transforming their organizations' security from reactive to proactive and adaptive.

Programme Curriculum

Implementing the Zero Trust Extended Ecosystem Training Course

Introduction

The modern enterprise landscape is defined by digital transformation and the dissolution of the traditional network perimeter, rendering legacy security models ineffective against sophisticated, AI-powered cyber threats. The Zero Trust Extended Ecosystem (ZTX) is the mandatory, future-proof security framework designed to meet this challenge. It operates on the core principle of "never trust, always verify," demanding continuous authentication and authorization for every user, device, application, and data access request, regardless of location. This paradigm shift secures the distributed enterprise, encompassing hybrid cloud environments, remote workforces, and the burgeoning IoT/OT landscape, effectively mitigating risks like lateral movement and insider threats. This course provides the strategic roadmap and practical, hands-on skills required for security professionals and leaders to architect, implement, and govern a comprehensive, NIST SP 800-207 compliant ZTX across their entire digital estate.

Implementing the Zero Trust Extended Ecosystem Training Course focuses not just on theoretical concepts but on the real-world implementation of the seven Zero Trust pillars: Identity, Devices, Data, Applications, Network/Workload, Automation & Orchestration, and Analytics & Visibility. We will dive deep into micro-segmentation, Just-In-Time (JIT)/Just-Enough-Access (JEA) principles, and advanced policy enforcement. The curriculum integrates leading vendor solutions and utilizes live, hands-on labs to ensure mastery of the technical components necessary for deployment. Graduates will be equipped to drive significant cyber risk reduction, enhance regulatory compliance, and establish a data-centric security posture that is resilient against the most advanced persistent threats, transforming their organizations' security from reactive to proactive and adaptive.

Course Duration

5 days

Course Objectives

1. Strategically design a comprehensive Zero Trust Architecture (ZTA) and Extended Ecosystem (ZTX) aligned with business transformation goals.
2. Master the NIST SP 800-207 framework and CISA Zero Trust Maturity Model for practical implementation and gap analysis.
3. Implement robust Identity Governance and Multi-Factor Authentication (MFA) across all user and non-user identities
4. Develop and enforce dynamic, risk-based adaptive access policies for users and devices leveraging Continuous Verification.
5. Architect and deploy micro-segmentation and Zero Trust Network Access (ZTNA) solutions to eliminate network-based implicit trust.
6. Secure the cloud and hybrid environment by applying ZTX principles to IaaS, PaaS, and SaaS workloads.
7. Classify and protect sensitive data using data-centric security controls, including encryption and Data Loss Prevention
8. Integrate Security Orchestration, Automation, and Response with ZTX for automated policy enforcement and threat detection.
9. Evaluate and select appropriate ZTX vendor platforms and technologies
10. Measure and report on Zero Trust maturity and its impact on key cyber risk metrics.
11. Apply least privilege principles using Just-in-Time (JIT) and Just-Enough-Access (JEA) for privileged accounts.

12. Plan and execute a phased ZTX migration strategy while managing organizational change and legacy systems.
13. Utilize telemetry and analytics for continuous monitoring, anomaly detection, and enhancing the Policy Decision Point (PDP).

Target Audience

1. Security Architects & Engineers.
2. Chief Information Security Officers & Security Directors.
3. Cloud Security Professionals
4. Network Engineers & Architects.
5. Identity and Access Management Specialists.
6. IT Risk & Compliance Managers.
7. System Administrators & Operations Teams.
8. Technical Program Managers.

Course Modules

Module 1: Zero Trust Foundations and Strategic Planning

- Foundational Concepts.
- Zero Trust Pillars
- Frameworks and Models.
- Strategic Alignment.
- Case Study: Google BeyondCorp.

Module 2: Identity, Device, and Access Control (IDAC)

- Identity as the New Perimeter.
- Device Posture Assessment.
- Adaptive Policy Engine
- Enforcing Least Privilege Access for human and machine identities.
- Case Study: Financial Services Firm.

Module 3: Network and Micro-segmentation

- De-perimeterization.
- Micro-segmentation Design.
- Zero Trust Network Access.
- Software Defined Perimeter.
- Case Study: Healthcare Provider.

Module 4: Securing Data and Applications/Workloads

- Data-Centric Security.
- Application Workload Protection.
- Secure DevSecOps Pipelines.
- Policy Enforcement Points.
- Case Study: SaaS Company.

Module 5: Cloud and Multi-Cloud ZT Implementation

- Hybrid Cloud Security
- Cloud Identity Management.
- Cloud Workload Protection Platforms.
- Infrastructure as Code and ZT.
- Case Study: Global Retailer

Module 6: Automation, Orchestration, and Analytics

- Telemetry and Visibility
- Policy Decision Point (PDP) Logic.
- SOAR Integration.
- User and Entity Behavior Analytics.
- Case Study: E-Commerce Platform.

Module 7: Implementation Strategy and Change Management

- ZTX Roadmap Development
- Organizational Change Management.
- Stakeholder Buy-in.
- Vendor Selection and Integration.
- Case Study: Government Agency.

Module 8: Governance, Risk, and Continuous Improvement

- Risk Mitigation.
- Regulatory Compliance.
- ZTX Testing and Validation.
- Maturity Progression.
- Case Study: Industrial Control Systems Security.

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