Digital Safety Systems Training Course

Professional Development Training Course Outline

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

Course Introduction

The Digital Safety Systems Training is a comprehensive, future-focused program designed to equip professionals with advanced competencies in cybersecurity resilience, industrial digital safety, critical infrastructure protection, AI-driven threat detection, and secure digital transformation. As organizations rapidly adopt cloud computing, IoT ecosystems, OT/IT convergence, and smart automation systems, the need for robust digital safety architecture, real-time threat monitoring, and risk governance frameworks has become essential. Digital Safety Systems Training Course provides hands-on and strategic insights into building secure digital environments aligned with global standards such as NIST Cybersecurity Framework, ISO 27001, Zero Trust Architecture, and SOC operations best practices.

Participants will gain practical expertise in designing, implementing, and managing next-generation digital safety systems, including SIEM platforms, intrusion detection systems (IDS/IPS), endpoint protection, incident response workflows, and AI-powered cybersecurity analytics. The program blends theory with real-world simulations to prepare learners for modern threats such as ransomware, phishing campaigns, insider threats, and advanced persistent threats (APT). By the end of the course, learners will be capable of leading digital safety initiatives that ensure organizational continuity, regulatory compliance, and cyber resilience in an increasingly interconnected digital world.

Programme Curriculum

Digital Safety Systems Training Course

Introduction

The Digital Safety Systems Training is a comprehensive, future-focused program designed to equip professionals with advanced competencies in cybersecurity resilience, industrial digital safety, critical infrastructure protection, AI-driven threat detection, and secure digital transformation. As organizations rapidly adopt cloud computing, IoT ecosystems, OT/IT convergence, and smart automation systems, the need for

robust digital safety architecture, real-time threat monitoring, and risk governance frameworks has become essential. Digital Safety Systems Training Course provides hands-on and strategic insights into building secure digital environments aligned with global standards such as NIST Cybersecurity Framework, ISO 27001, Zero Trust Architecture, and SOC operations best practices.

Participants will gain practical expertise in designing, implementing, and managing next-generation digital safety systems, including SIEM platforms, intrusion detection systems (IDS/IPS), endpoint protection, incident response workflows, and AI-powered cybersecurity analytics. The program blends theory with real-world simulations to prepare learners for modern threats such as ransomware, phishing campaigns, insider threats, and advanced persistent threats (APT). By the end of the course, learners will be capable of leading digital safety initiatives that ensure organizational continuity, regulatory compliance, and cyber resilience in an increasingly interconnected digital world.

Course Duration

5 Days

Course Objectives

1. Master Zero Trust Security Architecture (ZTNA) implementation
2. Develop expertise in SOC (Security Operations Center) operations
3. Analyze and mitigate Advanced Persistent Threats (APT attacks)
4. Implement SIEM (Security Information and Event Management) solutions
5. Strengthen cloud security and hybrid infrastructure protection
6. Apply ISO 27001 compliance and governance frameworks
7. Design incident response and digital forensics workflows
8. Integrate AI-powered cybersecurity threat intelligence systems
9. Secure IoT and OT/IT converged environments
10. Conduct penetration testing and vulnerability assessments
11. Manage endpoint detection and response (EDR/XDR) systems
12. Build resilience against ransomware and phishing attacks
13. Establish risk management and cyber resilience strategies

Target Audience

- Cybersecurity Analysts and Engineers
- IT Infrastructure and Network Administrators
- SOC Analysts and Incident Responders
- Cloud Security Architects
- Risk and Compliance Officers
- Government and Critical Infrastructure Personnel
- Software Developers working in secure environments
- Students and graduates in IT, Computer Science, or Cybersecurity

Course Modules

Module 1: Foundations of Digital Safety Systems

- Cybersecurity fundamentals and threat landscape
- Digital safety vs traditional security models
- Security layers and defense-in-depth strategy

- Introduction to cyber risk management
- Security policies and governance frameworks
- **Case Study:** Data breach analysis in a multinational enterprise

Module 2: SOC Operations and Monitoring

- SOC architecture and workflows
- Real-time threat monitoring systems
- Log management and SIEM integration
- Alert triaging and escalation processes
- Threat hunting methodologies
- **Case Study:** SOC response to ransomware outbreak

Module 3: Network Security & Zero Trust Architecture

- Zero Trust implementation principles
- Network segmentation and micro-segmentation
- Firewall and IDS/IPS configurations
- VPN and secure remote access systems
- Identity and access management (IAM)
- **Case Study:** Preventing lateral movement in enterprise networks

Module 4: Cloud Security & DevSecOps

- Cloud security models (IaaS, PaaS, SaaS)
- Shared responsibility model
- DevSecOps pipeline integration
- Container and Kubernetes security
- Cloud access security brokers (CASB)
- **Case Study:** Cloud misconfiguration leading to data exposure

Module 5: Incident Response & Digital Forensics

- Incident response lifecycle
- Evidence collection and preservation
- Malware analysis techniques
- Forensic imaging and reporting
- Legal and compliance considerations
- **Case Study:** Investigating insider data theft

Module 6: AI & Threat Intelligence Systems

- AI in cybersecurity automation
- Threat intelligence platforms (TIPs)
- Behavioral analytics and anomaly detection
- Machine learning for intrusion detection
- Predictive cybersecurity models
- **Case Study:** AI detection of APT attack patterns

Module 7: OT/IoT & Critical Infrastructure Security

- Industrial control systems (ICS/SCADA) security

- IoT device vulnerability management
- Smart city and critical infrastructure protection
- Protocol security (MQTT, Modbus, etc.)
- Physical-cyber convergence risks
- **Case Study:** Cyberattack on smart grid infrastructure

Module 8: Governance, Risk & Compliance (GRC)

- ISO 27001 implementation roadmap
- Cybersecurity risk assessment frameworks
- Regulatory compliance (GDPR, POPIA concepts)
- Audit and reporting structures
- Business continuity and disaster recovery
- **Case Study:** Compliance failure in financial institution

Training Methodology

- 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
28 Sep 2026	02 Oct 2026	Online	$1,000
28 Sep 2026	02 Oct 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$0
28 Sep 2026	02 Oct 2026	Physical	$0
28 Sep 2026	02 Oct 2026	Physical	$0
28 Sep 2026	02 Oct 2026	Physical	$0
28 Sep 2026	02 Oct 2026	Physical	$0
28 Sep 2026	02 Oct 2026	Physical	$0

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

Register Online Now

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