Building a Cyber Fusion Centre 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

A Cyber Fusion Center is a cutting-edge operational model that integrates traditional security functions like a Security Operations Center with Threat Intelligence, Incident Response (IR), Threat Hunting, Vulnerability Management, and sometimes Physical Security and Fraud teams. The goal is to move from siloed, reactive security to a unified, proactive, and intelligence-driven defense posture.

Building a Cyber Fusion Centre Training Course is designed to equip security leaders and practitioners with the strategic framework, technical skills, and collaborative methodologies needed to design, build, and operate a high-functioning Cyber Fusion Center. Participants will master the integration of people, processes, and technology to accelerate Mean Time to Detect and Mean Time to Respond, enabling a Collective Defense strategy that dramatically enhances organizational cyber resilience against Advanced Persistent Threats and Ransomware-as-a-Service attacks. Strong emphasis is placed on Security Orchestration, Automation, and Response, AI-Driven Defense, and adherence to global frameworks like MITRE ATT&CK and the NIST Cybersecurity Framework.

Programme Curriculum

Building a Cyber Fusion Centre Training Course

Introduction

A Cyber Fusion Center is a cutting-edge operational model that integrates traditional security functions like a Security Operations Center with Threat Intelligence, Incident Response (IR), Threat Hunting, Vulnerability Management, and sometimes Physical Security and Fraud teams. The goal is to move from siloed, reactive security to a unified, proactive, and intelligence-driven defense posture.

Building a Cyber Fusion Centre Training Course is designed to equip security leaders and practitioners with the strategic framework, technical skills, and collaborative methodologies needed to design, build, and operate a high-functioning Cyber Fusion Center. Participants will master the integration of people, processes, and

technology to accelerate Mean Time to Detect and Mean Time to Respond, enabling a Collective Defense strategy that dramatically enhances organizational cyber resilience against Advanced Persistent Threats and Ransomware-as-a-Service attacks. Strong emphasis is placed on Security Orchestration, Automation, and Response, AI-Driven Defense, and adherence to global frameworks like MITRE ATT&CK and the NIST Cybersecurity Framework.

Course Duration

5 days

Course Objectives

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

1. Define and justify the strategic value of a Cyber Fusion Center (CFC) over a traditional SOC.
2. Design a CFC operating model that effectively integrates Threat Intelligence and Incident Response workflows.
3. Implement effective cross-functional collaboration and communication strategies to break down organizational silos.
4. Master the use of Security Orchestration, Automation, and Response (SOAR) platforms to accelerate MTTD/MTTR.
5. Develop an intelligence-driven threat hunting program using the MITRE ATT&CK framework.
6. Integrate Vulnerability Management and Risk Assessment into the CFC's continuous defense lifecycle.
7. Establish governance, risk, and compliance (GRC) policies specific to CFC operations.
8. Define, measure, and report on key CFC metrics and Key Performance Indicators, including MTTD and MTTR.
9. Apply AI/ML and Behavioral Analytics for enhanced Threat Detection and anomaly identification.
10. Formulate an advanced, multi-stage Incident Response Plan for sophisticated attacks like RaaS.
11. Structure and manage a Purple Teaming exercise for continuous control validation and security maturity.
12. Select and implement a Cyber Threat Intelligence (CTI) platform and workflow for contextualizing threats.
13. Drive a cultural shift towards collective defense and proactive risk mitigation across the enterprise.

Target Audience

1. SOC Managers/Team Leads.
2. Chief Information Security Officers.
3. Threat Intelligence Analysts.
4. Incident Responders.
5. Security Architects.
6. IT/Security Program Managers.
7. Senior Security Analysts.
8. Risk and Compliance Officers.

Course Modules

1. The Strategic Shift: From SOC to Cyber Fusion Centre

- Defining the CFC Model.
- Justifying the Business Case for CFC.
- Organizational Design and Cross-Functional Teaming

- Governance and Leadership structure for a unified center.
- Mapping CFC capabilities to NIST Cybersecurity Framework.
- Case Study: Aligning Fraud and Cyber Teams for a $10M Reduction in Annual Losses.

2. Operationalizing Threat Intelligence (CTI)

- The Intelligence Cycle and its application in a CFC.
- Selecting and leveraging a Threat Intelligence Platform.
- Creating Actionable Intelligence from raw feeds
- Tactical, Operational, and Strategic CTI use cases.
- Integrating CTI directly into SOAR playbooks and SIEM correlation rules.
- Case Study: Using Custom CTI to Predict and Pre-empt an APT Group Targeting Industrial Control Systems.

3. Advanced Threat Detection & Threat Hunting

- Mastering the MITRE ATT&CK Framework for defense and hunting.
- Developing Behavioral Analytics and anomaly detection use cases.
- Designing an effective Threat Hunting program.
- Log Management and Security Information and Event Management optimization for Fusion.
- Leveraging Endpoint Detection and Response data for deep visibility.
- Case Study: A Threat Hunting Exercise Uncovers a Covert, Living-off-the-Land Attack Chain.

4. Security Orchestration, Automation, and Response (SOAR)

- SOAR platform selection, implementation, and integration best practices.
- Developing and stress-testing automated playbooks for common incidents.
- Workflow Design for cross-tool communication and data enrichment.
- Metrics for measuring the ROI of Automation.
- Governing automation to prevent cascading or erroneous actions.
- Case Study: Automating Phishing Triage and Vulnerability Patching to Cut IR Time by 65%.

5. Unified Incident Response (IR) and Forensics

- The integrated Fusion IR Process
- Advanced Containment Strategies in Cloud and hybrid environments.
- Digital Forensics and Incident Response techniques for evidence preservation.
- Communication protocols and reporting to executive leadership during a crisis.
- Post-incident analysis and feeding lessons back into CTI and Threat Hunting.
- Case Study: Coordinated Cyber/Legal/Comms Fusion Center Playbook Minimizes Downtime and Avoids Regulatory Penalties.

6. Vulnerability, Risk, and Attack Surface Management

- Continuous Vulnerability Assessment and Penetration Testing integration with CFC.
- Prioritizing vulnerabilities based on CTI context and potential exploitability.
- Implementing Continuous Threat Exposure Management principles.
- Managing the Expanded Attack Surface
- Designing and executing Purple Teaming exercises for control validation.
- Case Study: Simulating a Supply Chain Attack to Validate and Optimize Cloud WAF and EDR Controls.

7. People, Culture, and Training

- CFC Staffing Model.
- Strategies for analyst Retention, Well-being, and Burnout Prevention.
- Building a Collective Defense Culture of trust and information sharing.
- Developing a continuous, hands-on Training Program for the Fusion Team.
- Legal, ethical, and Privacy/Civil Liberties considerations in data fusion.
- Training Methodology: Interactive Workshops, Cyber Range Simulations, Scenario-Based Exercises, Live SOAR Playbook Development, Guest Speakers

8. The Future of Fusion: AI, Zero Trust, and Cloud

- The role of Generative AI and Machine Learning in security operations.
- Integrating the Zero Trust Architecture principles into the CFC model.
- Security challenges and fusion strategies for Cloud-Native and Multi-Cloud environments.
- Preparing for the impact of Quantum Computing on encryption.
- Creating a CFC Roadmap for long-term capability maturity.
- Case Study: Implementing AI-Driven Behavioral Analytics to Enforce Zero Trust Micro Segmentation Policy.

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 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