Global Horizon
TRAINING CENTER

Training Course:
Advanced Cybersecurity Operations, Threat Intelligence & Regulatory Compliance in Financial Services

13 - 17 December 2026

In-House

Training Course:
Advanced Cybersecurity Operations, Threat Intelligence & Regulatory Compliance in Financial Services

Training Course code: SC236589 From: 13 - 17 December 2026 Venue: In-House - Training Course Fees: Euro

Introduction

The Advanced Cybersecurity Operations, Threat Intelligence & Regulatory Compliance in Financial Services training program is designed by Global Horizon Training Center to strengthen the cybersecurity capabilities of information security and technology professionals working within regulated financial environments.

This program focuses on advanced cybersecurity operations, proactive threat detection, incident response, secure cloud architecture, zero-trust security principles, vulnerability management, and regulatory compliance requirements applicable to financial institutions in the Kingdom of Saudi Arabia.

The training addresses key regulatory frameworks, including the SAMA Cybersecurity Framework CSF, SAMA Information Technology Governance Framework ITGF, NCA Essential Cybersecurity Controls ECC, NCA Cloud Cybersecurity Controls CCC, and cybersecurity requirements within the SAMA Open Banking Framework, enabling participants to enhance organizational cyber resilience and align security practices with regulatory expectations.

Objectives

By the end of this training program, participants will be able to:

- Understand the evolving cybersecurity threat landscape affecting financial institutions.
- Apply advanced threat hunting methodologies and security monitoring approaches.
- Enhance cybersecurity incident response capabilities across the incident lifecycle.
- Understand secure cloud architecture principles within regulated environments.
- Apply zero-trust architecture concepts to improve security posture.
- Understand penetration testing concepts and vulnerability management practices.
- Perform cybersecurity gap assessments against SAMA CSF requirements.
- Improve cyber threat intelligence capabilities and response strategies.
- Strengthen alignment between cybersecurity operations and regulatory compliance requirements.

Course Methodology

The program will be delivered through:

- Instructor-led presentations and expert discussions.

- Analysis of cybersecurity scenarios and financial sector incidents.
- Review of regulatory frameworks and industry practices.
- Interactive discussions on cybersecurity challenges.
- Examination of emerging cyber threats affecting financial institutions.

Organizational Impact

Upon completion of this program, organizations will benefit from:

- Enhanced cybersecurity readiness and operational resilience.
- Improved ability to detect and respond to cyber threats.
- Stronger compliance alignment with SAMA and NCA cybersecurity requirements.
- Better understanding of cloud security risks and mitigation strategies.
- Improved security governance and risk management practices.
- Increased capability to protect critical digital infrastructure.

Target Audience

This program is designed for:

- Information Security Professionals.
- Cybersecurity Analysts.
- IT Operations Teams.
- Cloud Engineering Professionals.
- Risk Technology Specialists.
- Digital Infrastructure Teams.
- Security Operations Center SOC Personnel.
- Technology Risk Management Professionals.

Outlines

Day 1:

Cybersecurity Landscape, Regulatory Frameworks & Security Governance

Cybersecurity in Financial Services

- Evolution of cyber threats targeting financial institutions.
- Cybersecurity challenges in digital banking environments.
- GCC financial services cyber threat landscape.
- Common attack techniques targeting banking infrastructure.

Regulatory Cybersecurity Frameworks in KSA

- Overview of SAMA Cybersecurity Framework CSF.
- Mandatory cybersecurity compliance requirements.
- SAMA Information Technology Governance Framework ITGF.
- NCA Essential Cybersecurity Controls ECC.
- NCA Cloud Cybersecurity Controls CCC.
- Cybersecurity considerations within SAMA Open Banking Framework.

Cybersecurity Governance and Risk Management

- Cybersecurity governance structures.
- Security policies and control frameworks.
- Cyber risk identification and management.
- Regulatory compliance mapping approaches.

Day 2:

Threat Hunting, SIEM Operations & Cyber Threat Intelligence

Technical Threat Hunting Methodologies

- Principles of proactive threat hunting.
- Threat hunting lifecycle.
- Identifying indicators of compromise IoCs.
- Behavioral analysis and anomaly detection.

- Advanced attacker techniques and tactics.

SIEM Integration and Security Monitoring

- Role of SIEM platforms in cybersecurity operations.
- Log collection and analysis.
- Security event correlation.
- Alert prioritization and investigation.
- Improving SOC monitoring capabilities.

Cyber Threat Intelligence

- Cyber threat intelligence lifecycle.
- Intelligence sources and analysis techniques.
- Understanding threat actors targeting financial services.
- GCC cybersecurity threat trends.
- Using intelligence to improve security decisions.

Day 3:

Cyber Incident Response & Security Operations

Cyber Incident Response Framework

- Incident detection and classification.
- Incident response lifecycle.
- Preparation and response planning.
- Containment strategies.
- Threat eradication approaches.
- Recovery and post-incident activities.

Incident Investigation and Management

- Incident analysis techniques.

- Root cause identification.
- Digital evidence considerations.
- Incident documentation and reporting.
- Lessons learned and security improvement actions.

Security Operations Enhancement

- SOC operational models.
- Incident escalation procedures.
- Coordination between security teams and business units.
- Improving response efficiency.

Day 4:

Secure Cloud Architecture, Zero Trust & Vulnerability Management

Secure Cloud Architecture in Regulated Environments

- Cloud security challenges in financial institutions.
- Secure cloud design principles.
- Identity and access management in cloud environments.
- Data protection and encryption considerations.
- Cloud security controls aligned with KSA requirements.

Zero Trust Architecture Principles

- Zero Trust security model fundamentals.
- Identity-centric security approach.
- Continuous verification concepts.
- Network segmentation and access controls.
- Implementing Zero Trust within enterprise environments.

Vulnerability Assessment and Penetration Testing Concepts

- Vulnerability management lifecycle.
- Security assessment methodologies.
- Penetration testing concepts.
- Common vulnerabilities affecting financial systems.
- Risk prioritization and remediation strategies.

Day 5:

SAMA CSF Gap Analysis, Compliance Mapping & Future Cyber Challenges

SAMA CSF Gap Analysis

- Understanding cybersecurity maturity assessment.
- Identifying control gaps.
- Mapping security practices against SAMA CSF requirements.
- Prioritizing cybersecurity improvement initiatives.

Cybersecurity Compliance and Assurance

- Regulatory compliance challenges.
- Security control effectiveness evaluation.
- Documentation and evidence requirements.
- Continuous cybersecurity improvement.

Future Cybersecurity Trends

- Emerging cyber threats in GCC financial services.
- Artificial intelligence and cybersecurity.
- Advanced persistent threats APTs.
- Future evolution of financial sector cyber risks.
- Building sustainable cyber resilience.

Registration form on the Training Course: Advanced Cybersecurity Operations, Threat Intelligence & Regulatory Compliance in Financial Services

Training Course code: SC236589 From: 13 - 17 December 2026 Venue: In-House - Training Course Fees: Euro

Complete & Mail or fax to Global Horizon Training Center (GHTC) at the address given below

Delegate Information

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Company Information

Company Name: .....
Address: .....
City / Country: .....

Person Responsible for Training and Development

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Payment Method

☐ Please find enclosed a cheque made payable to Global Horizon

☐ Please invoice me

☐ Please invoice my company

Easy Ways To Register

Telephone:	Fax your completed registration	E-mail to us :	Complete & return the booking form with cheque to:Global Horizon
+201095004484 to provisionally reserve your place.	form to: +20233379764	info@gh4t.com or training@gh4t.com	3 Oudai street, Aldouki, Giza, Giza Governorate, Egypt.