اتحاد شركات الاستثمار
UNION OF INVESTMENT COMPANIES

مركز دراسات الاستثمار
ISC
INVESTMENT STUDIES CENTER

CYBER SECURITY AND INCIDENT MANAGEMENT

(Sunday - Tuesday) 16th – 18th February 2025 (3 days)
09:00AM - 03:00PM
In-person @ UIC premises
Arabic/material in English

FEES FOR UIC MEMBERS	FEES FOR NON-MEMBERS
KWD 250	KWD 300

Roland Abi Najem

Introduction:

This training program is to provide participants with a solid understanding of cybersecurity principles and incident management processes. It aims to equip learners with the knowledge to identify and respond to security incidents, while emphasizing the importance of prevention and proactive defense. Participants will gain practical skills in detecting threats, managing security breaches, and developing incident response plans, along with learning how to improve cybersecurity resilience through continuous monitoring and post-incident analysis.

Target Audience:

- Executive Leadership
- Risk and Security Management
- IT and Operations Management
- Investment Professionals
- Compliance and Legal Management

اتحاد شركات الاستثمار
UNION OF INVESTMENT COMPANIES

مركز دراسات الاستثمار
ISC
INVESTMENT STUDIES CENTER

CYBER SECURITY AND INCIDENT MANAGEMENT

Outcome:

1. **Understand key cybersecurity concepts** and the threat landscape, including common cyber threats and attack methods.
2. **Identify security incidents** and apply detection methods using tools such as SIEM, firewalls, and intrusion detection systems (IDS).
3. **Implement an effective incident management process**, from detection through to recovery and post-incident analysis.
4. **Create and improve incident response plans**, incorporating best practices and lessons learned from previous incidents.
5. **Apply cybersecurity best practices** to prevent and mitigate future incidents, ensuring a proactive and resilient approach to security.
6. **Communicate effectively** during a security incident, including escalation, reporting, and managing internal and external stakeholders.

Outline:

Day1: Introduction to Cybersecurity and Threat Landscape

- **Session 1: Cybersecurity Overview**
  - Definition of Cybersecurity
  - Key Concepts: Confidentiality, Integrity, Availability (CIA Triad)
  - Types of Cybersecurity: Network Security, Information Security, Application Security, and Operational Security

- **Session 2: Cyber Threat Landscape**
  - Common Cyber Threats: Malware, Phishing, Ransomware, Social Engineering, Insider Threats
  - Attack Vectors: Email, Web, Network, and Physical
  - Real-world Examples: Notable Cyber Attacks (e.g., WannaCry, SolarWinds)

- **Session 3: Risk Management in Cybersecurity**
  - Identifying Cyber Risks and Vulnerabilities
  - Risk Assessment and Risk Mitigation Strategies
  - Introduction to Security Frameworks: NIST, ISO 27001, CIS Controls

Day 2: Incident Management Process

- **Session 1: Incident Detection and Identification**
  - Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs)
  - Tools for Incident Detection: SIEM, IDS/IPS, Antivirus, Firewalls
  - How to Identify and Categorize Security Incidents

- **Session 2: Incident Response Process**

CYBER SECURITY AND INCIDENT MANAGEMENT

- Phases of Incident Response: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned
- Roles and Responsibilities in Incident Response
- Incident Response Frameworks and Plans
- Hands-on Exercise: Simulated Incident Response (e.g., phishing attack simulation)

- **Session 3: Communicating During an Incident**
  - Internal and External Communication: Incident Reporting, Escalation, and Stakeholder Engagement
  - Legal and Regulatory Considerations (GDPR, HIPAA, etc.)
  - Post-Incident Communication: Lessons Learned and Reporting

Day 3: Post-Incident Analysis, Prevention, and Best Practices

- **Session 1: Post-Incident Analysis and Recovery**
  - Conducting a Post-Mortem Review: Root Cause Analysis
  - Continuous Monitoring and Improvement
  - Incident Documentation and Reporting

- **Session 2: Building and Improving an Incident Response Plan**
  - Components of an Effective Incident Response Plan (IRP)
  - Integrating Lessons Learned into IRP and Policies
  - Developing a Cybersecurity Culture: Training, Awareness, and Drills

- **Session 3: Preventive Measures and Cybersecurity Best Practices**
  - Strengthening Defenses: Network Segmentation, Patching, MFA, Encryption
  - Monitoring and Threat Intelligence: Keeping Systems Updated
  - Best Practices for Preventing Future Incidents

Hands-on Exercise: Developing a Cybersecurity Best Practices Checklist

اتحاد شركات الاستثمار
UNION OF INVESTMENT COMPANIES

مركز دراسات الاستثمار
ISC
INVESTMENT STUDIES CENTER

CYBER SECURITY AND INCIDENT MANAGEMENT

Expert's Profile: Roland Abi Najem

Roland Abi Najem Founder and CEO of Revotips – Expert Tech Consultants and Solutions. He was the IT & Cyber Security Consultant at the Ministry of Information – Kuwait and the Personal Consultant for the Minister of Information From 2014 till 2016.

Certified Trainer & Content Developer by ISTD (International Society For Trainers & Developers)

He holds a Master's in Business Administration (MBA), Focus on M.I.S Management Information Systems.

Technical Consultant and Information Security Expert with the Mohammed Al Jassim Group for Lawyer and Legal Consultation and specialized in Cyber Crimes.

Roland is the Chairman at several seminars and conferences in the region and also Keynote speaker & Panelist.