1MALAYSIA GRIP PROGRAMME

# CYBERSEC FIRST RESPONDER

Fully funded by:

- HRDF MALAYSIA -

# THREAT DETECTION & RESPONSE

5+2 days

## The Importance of People

There's no lack of resources available to secure a network. From HW/SW solutions to third-party services, the marketplace is full of options. Yet, for all of the talk of technology-based solutions, the threat of cyber-attack continues to grow. When securing an information system, we can't forget about the "wetware". For too long, people have played a supporting role in the fight against cyber crime, under-utilized in the defense of our information systems.

## 95% of Data Breaches Are Due to Human Error

With so many attacks due to human error, the need for a better training solution is apparent. Are your employees helping or hurting your cybersecurity efforts? What role is your IT team playing in securing the organization? The resources are there, but a more holistic approach to educating our security teams is needed.

## Prevent, Detect, Respond & Evolve

A varied and sophisticated threat requires a varied approach. Traditional training programs have focused on specific aspects of securing a network, failing to equip security professionals to act before, during and after and attack. Organizations today need a training solution that prepares professionals to act throughout the attack spectrum.

Brought to you by:

KNOWledge group of companies

Logical Operations™

## LESSON OBJECTIVES

- Assessing Information Security Risk
- Creating an Information Assurance Lifecycle Process
- Analyzing Threats to Computing and Network Environments
- Designing Secure Computing and Network Environments
- Operating Secure Computing and Network Environments
- Assessing the Security Posture Within a Risk Management Framework
- Collecting Cybersecurity Intelligence Information
- Analyzing Cybersecurity Intelligence Information
- Responding to Cybersecurity Incidents
- Investigating Cybersecurity Incidents
- Auditing Secure Computing and Network Environments

## LIMIT BREACHES, SAVE MONEY

- Helps organizations effectively secure and protect computer networks through education.
- Saves money by allowing organizations to utilize their networking staff to help defend information systems (vs. hiring external candidates or third-party providers).
- Limits the incident of costly cyberattacks, reducing customer churn as a result of data loss.
- Allows organizations to strengthen their cyber defenses without the need for additional investment in infrastructure.

Knowledge Group of Companies | Phone: +603 2170 1588 | Fax: +603 2166 5451 | Email: survinder@knowledgegroupco.com

## MODULE 1: Assessing Information Security Risk

- Identify the Importance of Risk Management
- Assess Risk
- Mitigate Risk
- Integrate Documentation into Risk Management

## MODULE 2: Creating an Information Assurance Lifecycle Process

- Evaluate Information Assurance Lifecycle Models
- Align Information Security Operations to the Information Assurance Lifecycle
- Align Information Assurance and Compliance Regulations

## MODULE 3: Analyzing Threats to Computing and Network Environments

- Identify Threat Analysis Models
- Assess the Impact of Reconnaissance Incidents
- Assess the Impact of Systems Hacking Attacks
- Assess the Impact of Malware
- Assess the Impact of Hijacking and Impersonation Attacks
- Assess the Impact of Denial of Service Incidents
- Assess the Impact of Threats to Mobile Infrastructure
- Assess the Impact of Threats to Cloud Infrastructures

## MODULE 4: Designing Secure Computing and Network Environments

- Information Security Architecture Design Principles
- Design Access Control Mechanisms
- Design Cryptographic Security Controls
- Design Application Security
- Design Computing Systems Security
- Design Network Security

## MODULE 5: Operating Secure Computing and Network Environments

- Implement Change Management in Security Operations
- Implement Monitoring in Security Operations
- Test and Evaluate Information Assurance Architectures

## MODULE 6: Assessing the Security Posture Within a Risk Management Framework

- Deploy a Vulnerability Assessment and Management Platform
- Conduct Vulnerability Assessments
- Conduct Penetration Tests on Network Assets

## MODULE 7: Collecting Cybersecurity Intelligence Information

- Deploy a Security Intelligence Collection and Analysis Platform
- Collect Data from Security Intelligence Sources
- Establish Baselines and Make Sense of Collected Data

## MODULE 8: Analyzing Cybersecurity Intelligence Information

- Analyze Security Intelligence to Address Incidents
- Incorporate Security Intelligence and Event Management

## MODULE 9: Responding to Cybersecurity Incidents

- Deploy an Incident Handling and Response Architecture
- Perform Real-Time Incident Handling Tasks
- Prepare for Forensic Investigation

## MODULE 10: Investigating Cybersecurity Incidents

- Create a Forensics Investigation Plan
- Securely Collect Electronic Evidence
- Identify the Who, Why, and How of an Incident
- Follow Up on the Results of an Investigation

## MODULE 11: Auditing Secure Computing and Network Environments

- Deploy a Systems and Processes Auditing Architecture
- Maintain a Deployable Audit Toolkit
- Perform Audits Geared Toward the Information Assurance Lifecycle

PRE-EXAMINATION - To prepare the participants for the written examination that is required for the certification

EXAMINATION - Examinees who pass the CFR Exam earn the CFR designation and become Certified Cyber Security First Responder Professionals