HUMAN FIREWALL

Cyber Security Workshop

By Mindsights Consulting

2-Day Cyber Security workshop
on
Cyber Threat Detection and Response Skills for Non-Cybersecurity Employees

TRAINING COURSE DETAILED SUMMARY

Course Title	Cyber Threat Detection & Response Skills for Non-Cybersecurity Employees
Type of Course	Cyber Security Awareness presented in non-technical format
Type of Training	Practical Classroom Activities Coaching Personal Development Online Assessment for Engagement and Readiness
Skill Focus Area	Cyber Security Skills
Duration (Days)	Two (2) days
Level of Certification	Certification for Completion (under TTT HRDF)
Certification Body	NA
Course Overview	Practically every client that we have come across have been hacked. Some have lost information and had to delay an IPO. Some have lost large sums of money from invoice fraud. Others, a loss of trust by vendors and clients. The Asian region accounts for 70% of the global cybersecurity specialist shortage. No wonder it has 80% of global hacking incidence! It takes 10 years or more to train cybersecurity specialists. They will be out of reach of SMEs in foreseeable future. Furthermore, a typical Malaysian SME receives between 5,000 to 100,000 hacking alerts (mostly automated attacks) per day. No more than a handful of these alerts are investigated due to the sheer volume of the attacks. Whether it is the Prime Minister of Singapore's health records being hacked (twice in 6 months!), or a local SME, the fact is we are losing out to the hackers. Post MCO, work-from-home (WFH) is now a norm for businesses. Hackers know the weakest link of a company lies in its employees. They are proven to be easily phished, baited and hooked. Certain personalities and behaviours are more prone to being baited and hackers know and exploit these.
PREREQUISITES	Participants are required to be currently employed by the company intending to upgrade the Cyber Security infrastructure.

Course Objective

This course has 2 unique key deliveries:

1. Getting each employee to know their own personality and behavior vulnerability to being hacked and how to be alert.

2. The program introduces a practical solution for companies to detect and be aware of the response required when faced with incidents of compromise. This includes awareness of being socially engineered either internally or externally, types of email compromised, crypto jacking, ransomware, OSINT, weapons of hacking and persuasion techniques used by hackers.

Using a proprietary Cyber Intelligence Threat Hunting platform - Vigilante Platform*, it is now possible to train non-IT employees in SMEs to recognize threats and elevate response on behalf of the organization as part of their daily work.

Embedding cyber self-awareness and democratization of cyber intelligence is the key benefit of this course hence keeping SME employees safe online at a fraction of the cost of normal cybersecurity fees.

*we have exclusive licence to use for this course

Learning Outcomes

By applying the lessons of the program, managers and officers of companies will gain clarity and focus on what it takes to equip themselves against Cyber Threats. It will enable them to understand the following:

- Understand the different types of Cyber Threats
  - Understand the levels of Cyber Threats.
  - Understand the common types of threats currently in being used by hackers.
  - Understanding the Hacking Process.
  - Types of Hacking tools.

- Impact
  - Teen Hack | Script Kiddies, Cyber Criminal Gangs, Hacktivists and Govt Nation-State Hacking | Advanced Persistent Threats (APT).
  - Impact on Businesses and Organization security | Primary, Secondary and Second Tier Impact.
  - Brand credibility, Financial Implications, Insurance costs, Public Impact, etc.

- Risk Mitigation
  - Cyber Health checks and Hygiene
  - The Para Cyber Specialists role
  - Using Cyber Threat Hunting platform

Course Content

This introduction to "Cyber Threat Detection & Response Skills for Non-cybersecurity Employees" is designed to help SME companies to gain clarity of direction on how to equip themselves against the mounting cyber threats in the world. This is covered in three main topics:

- The gaps available in your organization that hackers will exploit
  - Understanding how hackers will exploit your vulnerabilities based on your behavior.
  - How social engineering gives way to exploiting your organisations weakness.
  - How to close those gaps.

- Understanding the Hacking World
  - Types of hackers and motivations.
  - The common areas of organizational hacks and impact.
  - Understanding the ins and outs of the Dark Web, Cloud Computing and Office 365.
  - Best Practices.

- The Champion Cyber Security Team
  - How to be empowered in the face of Cyber Threats.
  - How to upskill teams for Cyber Threats and Future Threats.
  - Horizon: Platform for Threat Hunting and Cyber Assurance

Learning Activities

- Cognitive and Motivational Assessment
- Personality Analyzer
- The Evolution of the Surface Net and The Dark Net Game
- Lecture
- Role Play
- Video lectures
- Practical Exercise Case Studies
- Learning Activities Video Presentation
- Self- Evaluation Training
- Application of Cyber Threat Hunting Platform
- Online Class and Check-ins

Target Group

- HRDF registered/ Non HRDF registered SME Employers.
- SME Employers from HRDF registered and SME Employers from Non HRDF registered SME companies.
- The participants are managers and officers whose motivation, resilience and agility have direct impact on company's business performance.

WHAT DIFFERENTIATES US

Learning Rationale

It can be a scary time for businesses and consumers who are worried about cyber threats. The threats certainly exist, and they're getting increasingly potent and frequent. The attackers are varied, with many worrisome imbalances between attackers and their targets.

However, there are solutions for these problems. But it entails awareness and upskilling of employees especially those in charge of the security of their business data.

Even if a company is targeted by a powerful nation-state, it is still possible to protect critical digital assets. It takes planning and commitment of resources, but a good security operations team or a proactive individual can stay on top of most of the most serious cyber threats.

The uniqueness of our program is based 2 main key deliverables:

1. **Getting to know the employee's personality and behavioral vulnerability to being hacked and identifying ways to be alert**

Our scientific approach, tools and platform make the execution of leadership objectives, consistent and extendable to all levels of management with quantifiable measures of thinking, motivation, and behaviour.

Candidate performance is measured scientifically pre- and post-program participation with our proprietary Momentum-Assessor tool, to assess the following cognition and motivation areas each for Work and Life dimensions:

- Cognitive Structure (CS) – Measures the employee's ability to make sense of the situations and challenges faced at work/life.
- Energy (E) – Measures the total emotions (both negative and positive) an employee feels about his/her work/life.
- Emotional Balance (EB) – Gives the net direction of an employee's emotions (negative, neutral, positive) about work/life.
- Problem Solving Approach (PS) - Indicates how confident an employee's approach to problems and challenges are at work/life.
- Performance (P) – This is an employee's inner view of his/her own job performance and life management at present.

The Assessor measures 5 cognitive and motivational metrics with 5 levels each which are critical to performing at work. Basically, it gives employers the answer to what drives Performance:

Performance Behaviours = Cognitive Structure x Motivation

2. **Introduction of a Practical Solution for companies using a proprietary Cyber Intelligence Threat Hunting Platform (Horizon)**

The Horizon Platform is an exclusive license granted to our company, making it possible now to train non-IT employees to recognise threats and elevate response on behalf of the organization as part of their daily work.

This embeds cyber self-awareness and democratisation of cyber intelligence as the key benefit of this course, Hence, keeping SME employees safe online at a cost fraction of normal cybersecurity fees.