INSTITUTE OF
advanced
cyber defence

Cyber Defence Simu-Labs - experience hands-on cyber security events

The Simu-Lab Suite is the product of extensive military and industry experience, which offers practical training in a virtual machine environment.
Our suite of labs brings much-needed practical work experience directly to learners.

Brought to you by The Institute of Advanced Cyber Defence

The Institute of Advanced Cyber Defence aims to advance both the quantity and quality of knowledge and skills in the domain of cyber intelligence and security. Our mission is to bridge the global skills gap and address the dearth of cyber defence competencies.

An often touted statistic from IBM is the fact that 95% of cyber attacks occur on account of human error. It is, however, less clear what organisations should do to prevent these. At the Institute we believe that cyber resilience - the ability to successfully and continuously withstand cyber attacks - is best served by advanced cyber defence training, covering a broad spectrum of cyber intelligence and security topics.

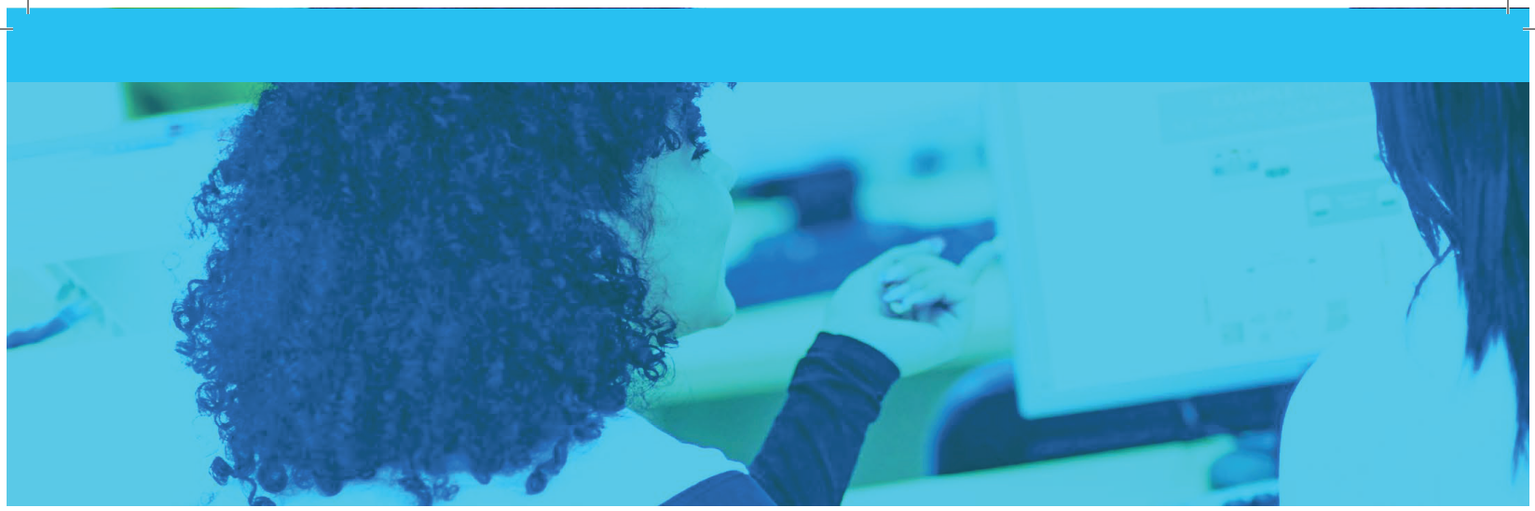
Awareness training with superficial tips and tricks is no longer enough. To maximise their security posture, all employees need to have a thorough understanding of threat actors and their motives and methods, as well as hackers' tactics, techniques and procedures. This is how best to secure a fighting chance at preventing sophisticated, yet very prevalent cyber attacks aimed at gaining access to corporate networks via staff.

It is baffling that organisations spend countless man-hours per annum on productivity software training, which barely improves workers' profitability contribution, whereas cyber defence training is often ignored, even though one individual's security lapse can have a devastating and lasting impact on the entire operation.

The Institute of Advanced Cyber Defence offers our training in partnership with Cybint Cyber Solutions.
Cybint was founded as a collaboration between military-trained cyber security and intelligence experts, industry professionals and well-seasoned educators.

The Cybint training solution is currently used by businesses, higher-education institutions and government agencies worldwide. The aim of the partnership is to enhance awareness, expand education and bolster the capacity of those involved to prevent, investigate and respond to cyber threats and cyber crime.

Cybint
Cyber Solutions



Methodology

IACD prides itself on an Accelerated Learning Model, designed to cater to learners with different levels of cyber security knowledge and experience. Programmes are:

- learner centred, with much of the content being self-paced
- skills-focused, creating a constructive learning environment
- authentic, drawing on realistic scenarios to allow you to gain hands-on experience
- assessed regularly throughout the course, ensuring you are aware of progress
- evergreen, with material being updated constantly to keep apace of change in the industry.

Certification

The Institute of Advanced Cyber Defence ensures that our education solutions are the latest and most relevant. The certification of our training is based on the NICE Cyber Security Workforce Framework of the National Initiative for Cyber security Careers and Studies (NICCS), which is the premier resource for cyber security training in the United States.

Delegates who complete the lab suite are awarded a CSA (Cyber Security Analyst) Certificate aligned with the Cyber Defence Analyst position in the NICE Framework.

Cyber Defence Simu-Lab Course Outline

How will I benefit?

Delegates will be empowered with:

- practical knowledge related to cyber security
- hands-on experience in solving basic cyber security incidents
- knowledge of appropriate questions to ask regarding cyber incidents you may encounter on a daily basis, and how to find the answers – specifically, how to: investigate cyber-related events within an organisation's IT systems, network and digital interactions to troubleshoot malfunctions and identify cyber attacks
- the ability to review and evaluate incoming cyber security information to determine its relevance and usefulness to identify and resolve the cyber security problem
- skills to choose the optimal solution for both non-fraudulent incidents and cyber threats
- knowledge on how best to liaise with employees, admin and authorities regarding cyber events within company policies and legalities
- the hands-on experience to reflect upon cyber events and how they were dealt with to offer constructive feedback and lessons learned.

Who should attend?

This course is suitable for all IT and allied staff who would like to acquire practical knowledge relating to resolving basic cyber security incidents.

Investment

R18,000 ex vat per person

Group rate: R15,000 ex vat for groups of 5 plus delegates from one corporate.

Course Schedule

Simulabs are scheduled for two hours at a time, and take place on a weekly basis.

Enquire with IACD to find out when the next Simulab series is taking place.

All sessions will be held at the Institute of Advanced Cyber Defence, 10 Lower Rd, Sandton

Curriculum Overview

THE FOLLOWING LAB SCENARIOS WILL BE COVERED OVER THE DURATION OF THE COURSE:

- **Scenario 1:** Getting to know Virtual Machines and Operating Systems: Windows and Linux
- **Scenario 2:** Data Tampering: SIEM, SQL, and IT Infrastructure
- **Scenario 3:** Holes in the Wall: Investigating System Logs, Permissions and Computer Hardware
- **Scenario 4:** Suspicious Network Traffic: Network Layer, Anti-Virus, and Malwares
- **Scenario 5:** Port Scanning: Transport Layer, Ports, and Firewall
- **Scenario 6:** Command and Control: Perimeter Defence and Phishing
- **Scenario 7:** Advanced Persistent Threat: DHCP, WMI, and Registry
- **Scenario 8:** Elevated Permissions: SIEM, DMZ, and VPN
- **Scenario 9:** Crashing the Cloud: DDoS, Cloud Computing, and Web Sever
- **Scenario 10:** Proactive Defence: Vulnerability Assessment and Patch Management

For more information, please contact training@iacd.io

INSTITUTE OF advanced cyber defence