Information Technology Institute

Cyber Security

People Develop Countries… We Develop P.E.O.P.L.E.

Program Admission Arrangements

Who May Apply?

Graduates of:

- **Computer Engineering,**
- **Communications Engineering**
- **Computer Science**

Prerequisites

These topics will be discussed with you in the interviews (Resources applicants can visit or study before interview)

- **Introduction to computer networks**
  https://maharatech.gov.eg/course/view.php?id=37
- **Introduction to cybersecurity**
- **https://maharatech.gov.eg/mod/page/view.php?id=14058**
- **Vmware Foundation**
  https://maharatech.gov.eg/course/index.php?categoryid=228
- **ITI values that could be found here:** https://iti.gov.eg/about-us

Selection Process

- **Phase 1: IQ and Problem-Solving exam | English exam**
- **Phase 2: Technical Exam**
  Computer-based technical exam in the field of your interest
- **Phase 3: Technical Interview**
  Those applicants would be discussing with the interviewing panel their pre-work -"Before You Apply"- in a one-to-one interview
- **Phase 4: Interpersonal Skills Interview**
  Those how pass phase 3 will be promoted to this interview

Delivery Approach

- 75% face to face Learning| 25 % Online
- Common Hardware
- Common Software

Student deliverables

- Each student must deliver an international certficates based on his track.

Cyber Security

Graduates Job Profiles

- **Penetration Testers**

Can be considered ethical hackers, as they try to break into computers and networks in order to find potential security breaches. Penetration Testers duties include running tests, writing reports about their findings, designing new tests, and running security audits.

- **Cyber Incident Responder**

His main responsibility is to respond to security disruptions, threats, and incidents. He/she works on investigating and analyzing different logs, traffics and devices using a suite of forensic tools and analysis techniques. Incident responder works also to identify the damage, put remediation and containment plan and advice with recommendations to improve existing controls.

Industry/Academy Stakeholders

- **Kaspersky**
- **Palo Alto**
- **ELearnSecurity**
- **Eccouncil**
- **Cisco**

Targeted Outcome

- Security companies, such as; Zinad, Fixed Solution, Inovasys , CyShield, Security Meter
- Communication Mobile companies, such as; WE, Vodafone, _VOIS, Etisalat Misr, Orange
- Fintech Services Providers, such as; Fawry, Aman, Bee, PayMob, MaxAB
- Banks, such as; National Bank of Egypt, Bank Misr, Alex Bank

Certifications

- ELearnSecurity eWPT
- ELearnSecurity eMAPT
- ELearnSecurity EciR

eWPT Certification
eLearn Security Web application Penetration Tester

eMAPT Certification
eLearn Security Mobile Application Penetration Tester

ElearnSecurity Certified Incident Responder (ECIR)

Cyber Security

1506 Hours

Program Content Structure

Fundamental courses

Database Fundamentals
Introduction to Programming ©
Operating Systems Fundamentals
Cisco Internetworking
Cisco Network Associate
Microsoft Windows Active Directory
Microsoft Windows Infrastructure
Red Hat System Administration I
Red Hat System Administration II
Client-Side Technologies Fundamentals
Bash Shell Script
Introduction to Generative AI and prompt engineering

Soft Skills Courses

Communication Essentials for Professionals
High Impact Presentations
Job Seeking Skills
Professional Demeanor (Workshop)

Core Courses

Ethical Hacking and Security Assessment
Metasploit Essentials
Firewalls Technologies
Incident Handling
Introduction to Python Programming
Web Penetration Testing
Active Directory pentesting (Windows Security)
Introduction to bug hunting
Freelancing Basics
Malware Analysis and Reverse Engineering
Computer and Network Forensics
ITIL Foundation
Mobile Penetration Testing
Risk Assessment and Compliance
Introduction to PHP Programming
Operational Technology (OT) Security
Cyber Threat Hunting and threat intelligence