

ICCP International Center for Cyber Professions

A unique collaboration between TESI and the
Cyber Company of ELTA Systems



Proposed plan

A variety of integrated and groundbreaking learning programs that offer, in a unique collaboration, professional training and practical training in an advanced simulator for cyber professions.

Incorporate cyber subjects into your studies to attain a sought-after a career that combines technological challenges, creative thinking and innovative developments in one of the most popular industries in the high-tech and technology worlds today.



For further information:

Uriel Nachum ✉ uriel@limudey-hutz.co.il ☎ 972-54-7800731

📍 Meir Weissgel Road 2, Science Park, Rehovot, Israel



www.israel-cyber.com
www.limudey-hutz.co.il

The cyber professions - in demand the world over



'We are outnumbered' - cybersecurity pros face a huge staffing shortage as attacks surge during the pandemic

(CNBC | 5.9.20)



The cybersecurity industry was facing a talent shortage prior to Covid-19. As companies shifted to remote work, some cyber professionals were re-assigned to other tasks, including IT support. Nearly half a million workers are needed in cybersecurity roles around the country.



76% of Cybersecurity Leaders Face Skills Shortage

(Security | 6.5.20)



"The latest findings of the Stott and May Cyber Security in Focus research reveal that leaders are still struggling with the skills gap and access to talent. Most respondents (76 percent) believe there is a shortage of cybersecurity skills in their company, which represents an improvement on 2019 (88 percent), however, the problem still seems more potent for mid-market and large enterprise businesses. Organizations are still struggling to source cybersecurity talent (97 percent) with no material improvement around time-to-hire from 2019".



In recent years, the accelerated technological development combined with the COVID-19 crisis has created fertile ground for various network attacks that can occur at any given moment against individuals, civil and governmental bodies, companies and organizations. The cyber divisions have become vital and critical in every company and organization that need them as part of permanent protection systems maintaining the security of information and users. These units have become the spearhead of those companies, and they are courting and looking for workers in a field where there is a shortage of over 4m workers (!). These many demands have created a situation in which advanced degrees in engineering, computers

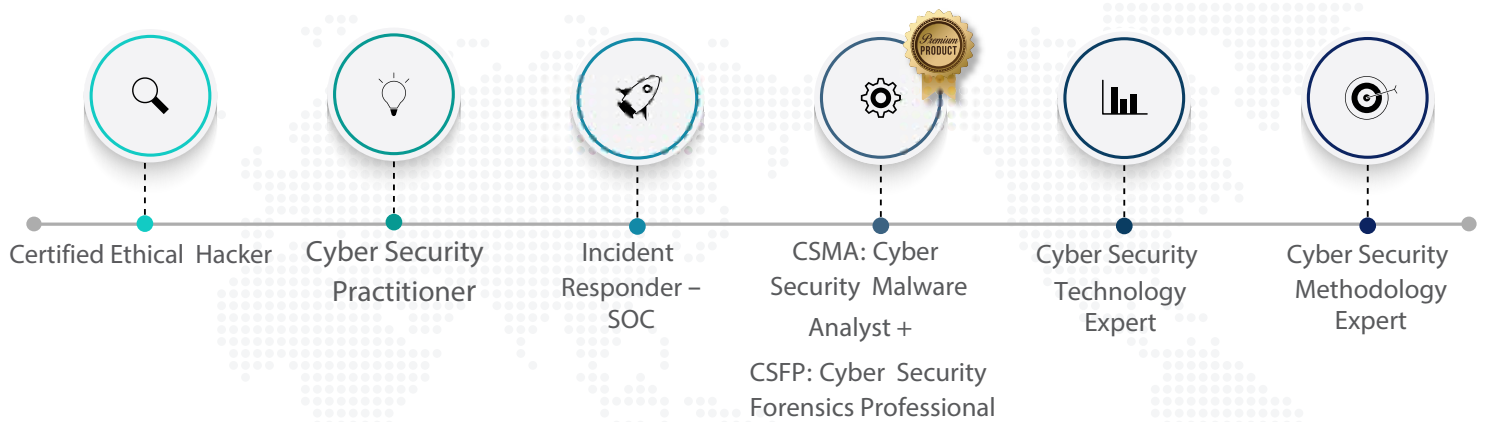
or technology are no longer needed and recruitment is quick and almost immediate for graduates of various professional courses, even without experience in the field. Respectively, the salaries in these professions reach tens of thousands of shekels for beginners, who are constantly courted for different jobs and benefit from desirable conditions. These employees are much needed to maintain the various databases - which are always - and more than ever, facing threats such as exposure and hacking that can cause damages of billions of shekels and even cause the collapse of companies, technologies, networks and organizations.

The International Center for Cyber Professions of the External Studies Institute and the Cyber Company of ELTA Systems

Due to the situation created by the reality of various threats combined with the high demands in the cyber domain, the TESI and the Cyber Company of ELTA jointly lead the International Center for Cyber Professions the combined with the Cyber Simulator. The center offers a variety of formations in high demand, and will provide its graduates with integrated training of the most advanced in the world, and a sought-after professional certificate.

The variety of frontal and online trainings combined with the simulator, as part of the practical practice of the course, will allow students to study, specialize, gain practical experience, and will provide graduates with advanced professional certificates and a variety of employment options tailored to their interests.

The courses



2021 Breakthrough Learning

Combined with TAME Range simulator training in Elta Systems' cyber skills center.

Learning in all courses and trainings is integrated and contains theoretical and practical studies, practice and training in this advanced simulator, which offers a variety of realistic defense and attack scenarios.

These simulator trainings are also used by Government and civil companies as well as private organizations (such as financial institutions, medical centers, insurance companies, etc.) and are adapted to complex scenarios in accordance with existing threats to those organizations.

Training with these various scenarios, in the scope of all the courses, will strengthen the learners' practical understanding and abilities to manage and operate defense systems, and reduce the exposure to various attacks. At the same time, they will benefit the graduates with practical experience as close to the field as possible, creating for them a significant advantage in securing a job in their field of expertise.

TESI is the largest college in Israel for vocational training and includes the largest online school in Israel where the best academic lecturers and senior professionals in the country teach.

Tens of thousands graduates have already studied and experienced the 100+ trainings and study tracks of TESI, which also operates a career development incubator for the employment service, with over 80% success in quality placements!

TESI has branches all over the country. It leads the entire set of courses and trainings of all civil servants in Israel on behalf of the Accountant General, the State Commissioner and the Ministry of Finance, as well as leading the largest school in Israel for career and business innovation.

TESI offers international training, courses under the full supervision of the Ministry of Economy, the Ministry of Education, recognized continuing education programs, the Institute of Tax Consultants and more. All this is in order to provide its graduates with the most comprehensive certification for achieving a competitive advantage in the employment market.



A unique cooperation for a sought-after certification

IAI ELTA ELTA Systems Ltd. is one of the four divisions of the Israel Aerospace Industry, is one of the leading division of the Defense Industry in Israel. It is also a world leader in the military sector. Elta actually develops advanced technological solutions for military and civilian protections in various fields, for governments, public and private customers. Its developments include solutions for intelligence, security, fire control, ground systems, cyber and more

The Cyber Division is a center of excellence of the Israel Aerospace Industry and is designed to address the challenges faced by countries, defense systems, infrastructure and more through unique solutions for cyber protections - protection and monitoring, forecasting, identification, intelligence and accessibility.

IAI, through the Cyber Division, leads the Cyber Companies Association (ic3), which offers various cyber security solutions and is supported by the Ministry of Labor, the Ministry of Foreign Affairs, the Ministry of Defense, the National Cyber Council and the Israeli Export Institute.



TAME™ Range is an advanced cyber skills center, offering advanced and innovative solutions for comprehensive cyber learning management.

This simulator offers a training environment for realistic cyber wars, and is designed to improve the resilience of various organizations, using the latest and most updated discovered threats. This simulator offers personal and team training platforms, attack and defense scenarios, and includes training, research and simulation of cyber scenarios with various components such as IT topology, OT and IoT environments, and more.



Still hesitating to embark on a new program of studies?



5 good reasons to study cyber professions:

1. One of the most sought after and coveted fields in the high-tech world today. Among the only professions that had intensified demand for workers due to the COVID-19 crisis.
2. Quick integration into the employment world - employers will court you!
3. (Very) high salaries from the very beginning of your initial career in the field
4. A fascinating and challenging field for career development in Israel and abroad
6. Considered one of the hottest fields and one of the professions of the future - 2021. You can continue training for more certifications in a field that will ever reinvent itself.

5 additional excellent reasons why to cyber with us:



1. Practical training combined with an advanced simulator for training in the field - accumulation of practical experience during the training, performed jointly with the training center of the cyber division of ELTA, Israel largest and leading company in security developments and a world leader in its field.
2. TESI offers a variety of trainings in which you can integrate according to your areas of interest - and also continue to specialize in additional trainings in the domain.
3. Cooperation of the largest college in Israel and the leading company in Israel and the world in the defense sector - a coveted diploma that will open for you a lot of employment doors and more!
4. An expert team of lecturers and trainers who will accompany you throughout the entire training and professional formation, as well as an administrative support team for any topic that arises before and during the training.
5. Fascinating studies, advanced programs integrating theoretical and practical learning, exercises, test cases, simulations and more...

1/ Cyber and information security course combined with the Cyber Simulator of ELTA Systems.

General background

In this training, the students will study a variety of fields to specialize in different domains of the cyber industry and easily integrate into sought-after employment positions. This course is a comprehensive and professional track, which includes specialization in the world of hacking, SIEM-SOC, and a combination of attack and protection for all the infrastructure and platforms that currently exist worldwide. The course is taught in combination with hands-on experience with the advanced simulator from ELTA Systems cyber division .

A preliminary preparatory course is performed at the beginning of the program, to bring all the participants to a common level, and during which the introductory and basic contents of the course will be studied. The preparatory course will take place in about 4 sessions, after which the advanced program start .

The course will teach the most relevant content to the cyber industry world, divided into professional modules such as Cyber infrastructure, Linux, Cisco, Mobile security, Penetration testing, Python programming, Cyber attack and defense in addition to Information Security Monitoring Center - SIEM-SOC and more .

In addition to the theoretical learning during the sessions, the students will gain hand-on experience in the TAME™ Range, an advanced simulator from ELTA Systems cyber division, which offers a training environment for most realistic cyber wars, and is designed to improve the resilience of various organizations using the latest and updated threats. This simulator offers personal and team training platforms, attack and defense scenarios, an includes training, research and simulation of various cyber scenario .

Course duration

Theoretical and practical learning hours (350h) - Includes training in the cyber simulator in collaboration with the cyber division of ELTA Systems

Diploma of Completion and Certification | a student who successfully meets the course requirements will be awarded the Graduate of the Cyber and Information Security course - a diploma from TESI and the division of ELTA System.

Our study program covers what the students need to proceed to LINUX, CCNA, CEH and PYTHON exams. However, it is the students responsibility to make sure they register and meet the terms for each of these exams

Web application

Basic website construction module
Operating system for servers
CSS
HTML
Javascript
DOM

Windows Server 2016

Microsoft operating system for servers
Introduction to the Domain environment
Introduction and installation of Server 2016
Establishment of a Domain and Active Directory management
Management of domain services - DNS, DHCP
File sharing and permissions
Policy creation using GPO
Introduction to corporate network structure

Linux

The Linux operating system
Linux Distros & Kali Linux
Introduction to Offensive Linux
Basic Commands
Networking
File system structure
Users & Groups
Password & shadow file
Permissions and ownership
Package management
Common services SSH / TELNET / FTP
Task schedulers
Process management
Final Lab

Cisco

This module provides knowledge and basic tools for technicians / network administrators and is critical to succeed in cyber positions. In addition, it is a preparation for the CCENT certification exam, a professional certification for the management and operation of communication equipment from CISCO, the global company, which gives information technicians and information security personnel the ability to troubleshoot network equipment more effectively, a better understanding and the ability to establish efficient protection system using network equipment. This certificate is an essential step in obtaining additional certifications in the world of CISCO's information security and networks such as Security CCNA and CCNP.

In-depth knowledge of the basics of the network and the rules of computer communication (TCP/IP & OSI).

Knowledge of the various components of the network and their role in the corporate network. Knowledge of and operation of the IOS operating system. In-depth knowledge of V4 & V6 (IP) protocols

Knowledge of the concept of routing with an emphasis on static routing.

Establishment and management of virtual networks (VLANS).

Specializing in defining the various protocols and technologies, including initial settings and troubleshooting for network equipment, with an emphasis on routers and switches, basic and advanced security settings, and filtering information packages, setting up and managing a small-medium enterprise network.



Cyber Infrastructure

Threats in the digital world
Introduction to Information Security and Cyber
Traffic analysis and scans
Performing internal network scans
Traffic analysis using Wireshark
PCAP file investigation
OSINT
Performing external network scans
System scan, service scan, application scan
Open network information gathering
Dictionary / Password attacks
Brutal force attack against services
Cracking encrypted files
Wi-Fi
Knowledge of the wireless internet world
Introduction to cryptography
Security standards and encryptions in Wi-Fi networks
Known weaknesses and their exploitation
Social engineering
Introduction to SE
SEToolKit
HiddenEYE
Establishing landing pages for Phishing
Network Anonymity
Dark Net & Deep Web
Proxy & VPN
Proxychains
MITM
Introduction to "Middleman"
Various technics for performing MITM
Interception of encrypted traffic
HTTPS downgrade
Metasploit and known CVE
Metasploit & Exploit- DB & Shodan
CVE & BugBounties
Searching for and finding known weaknesses
Creating malware and weakness exploitation
Creating a CNC control server
Bind / Reverse Shell

SIEM-SOC

Information Security Monitoring Center SOC
Using the SIEM system for real time identification and response to attacks
SOC lifecycle
Security measures
SIEM implementation and configuration
Log analysis and attack detection
Filtering the right way
Using SIEM for incidents response

Cross Platform Elevation of Privileges

Sophisticated escalation methods that allow you to become an admin in all operating systems, even when there is no user in that system.
Privilege Escalation Techniques
Local & Remote Privilege escalation
Credential Dumping & Pass the Hash
Privilege Escalation Using Common exploits
Local & Remote Privilege escalation in Linux
Privilege Escalation Using Automated Tasks
Permission misconfiguration & Post Exploitation
Techniques in Windows & Linux





Mobile Security

The Android and iOS operating systems, how they are built, their weaknesses and how to exploit them.

Reprogramming existing applications to allow them to perform new operations and bypass existing logics, and how to capture application traffic, plant bugs and exploit vulnerabilities. How to create a malicious app and plant it in the target phone for taking over the device.

Android

- Introduction to Android
- Android Security Architecture
- Android Permissions
- Reversing Android Applications
- Analyzing Android Traffic
- Analyzing Android Malwares
- Introduction to Drozer
- SSL Pinning and ways to bypass it
- Lab configuration for application

iOS

- Introduction to iOS Security
- Setting up Hacking tosh environment
- Jailbreaking iOS
- Exploiting iOS Applications
- Dynamic runtime analysis

Advanced Infrastructure Attacks

Infrastructure, data collection about the customer, bypassing protection systems, performing escalations in the authorization system and network traffic and more. Lateral Movement Methodology & Internal Cyber attack cycle

Enumerating an Organization and Exploiting Services & Ports

SMB Relay & Responder

PowerShell as a Weapon

Kerberoasting & Pass the Ticket

Get the Domain Admins

Veil-Framework & Obfuscation techniques

Office Exploitation

Python Programming

Development and writing in the most evolving language in the world, used daily by thousands of information security people.

Python introduction

Data types

Conditions & Loops

Code Handling

Functions

Sockets

Using Python for Hacking

Final project

Web Application Penetration Testing

The most powerful attacks on the Internet, which allow an attacker to take over the site itself and even the host computer.

Web Technologies

OWASP Top 10

Burp Suite / ZAP

XSS

CSRF

SQL/NOSQL Injection

LFI\RFI

XML Injections

Exploiting Upload Mechanism and Path Traversal

Bypassing Authentication

Clickjacking

Web Shells

Report Writing



Introduction to Malware Analysis & Reverse Engineering

Static and dynamic investigation, Trojans and their investigation, various methods for backward programming and code modification by attackers.

Static Malware Analysis

Dynamic Malware Analysis

Assembly Registers

Debugging Using OllyDbg & Immunity Dbg

Debugging Using Ida

Anti-Debugging

Packing & Unpacking

Manual Packing & Assembly Editing

Understand the CODE

Software & Hardware Breakpoints

Anti-Virus Evasion

Reversing Challenges

Memory Corruption Attacks

Final Lab

Integrated Practical training in the TAME™ Range cyber simulator

TAME™ Range simulator training in the cyber skills division of ELTA Systems.

Throughout the course, the learning is integrated and includes training in an advanced simulator in parallel with the theoretical studies, offering a variety of defense scenarios and realistic attacks

The training in the various scenarios will include scenarios adapted to the study topics in the various modules and will strengthen the students' practical understanding and their abilities to manage and operate defense systems, and reduce the success chances of various attacks. At the same time, they will provide the graduates with practical experience as close to the real world as possible, which will create for them a significant advantage for securing a job in Cyber

Study only
with the best



, The company reserves the right to change the structure of the trainings, including topics duration, lecturers and more