SEE SECURITY
CYBER SECURITY COLLEGE

Cyber Warfare Defence & Attack
Seminar for Corporate & Policy Executives
(2 days)

A unique seminar to introduce Corporate & Policy Executives (non-IT) with the world of cyber warfare, including the fundamentals of cyber defence and attack, and awareness of the best practices of the field

This programme aims to provide an overview of the world of cybersecurity for corporate and policy executives (non-IT). It is specifically suitable for executive who do not need to have to a technical knowledge or skills in the field of cybersecurity, but rather interested in covering the essentials of the field by learning the strategic, tactical aspects of cybersecurity policies and programmes including the understanding of basic cybersecurity concepts and terminologies, policy framework and the fundamentals of cyber defence and offensive security.

Cyber Warfare Seminar for Corporate & Policy Executives

About See Security College

See Security College is a highly specialised and international cybersecurity college. One of seven colleges of its kind, our college offers training programmes aimed for absolute beginners to more advanced professionals. The college delivers its study programmes worldwide, through the See Security International brand as well as well-known governmental and special cybersecurity agencies.

See-Security CEO, Mr. Avi Weissman is one of the leaders of the Israeli Cyber industry and serves as an advisor and commentator to the Israeli government for the regulation of cyber professions. Further, Mr. Weissman was the co-founder of the Israeli Forum for Information Security (IFIS) together with Maj. Gen. (Res.) and former head of National Security Council, Yaakov Amidror. In addition to his role in leading the college, Avi is also a co-CEO of a cyber human resources company See-HR, and a cybersecurity consulting company, See Secure – Managed SIEM/SOC.

About the Seminar

This programme aims to provide a short overview of the world of cybersecurity:
In the first part, we shall describe the technologies, offensive & defensive techniques, and the risks and threats in a technical, yet adaptive manner, relevant to the managerial level.
In the second part, we will dive into the organisational and personal risks and threats that managers and policymakers must understand, and depict how an organisation can learn to optimise its preparedness for cyber attacks.
The course will introduce sophisticated methods and best practices to assess risks, ultimately enhancing the functioning of businesses.

Target Audience

This programme aims to provide an overview of the world of cybersecurity and its risks, for corporate and policy executives (non-IT).

Key Features	
Cost	2000 USD
Audience	Managerial level: Policy Executives
Orientation	Theoretical, and practical (based on real-life scenarios)
Objectives	The programme aims to provide an overview of the world of cyber warfare, including the fundamentals of cyber defence and cyber offensive strategies, tactics, and operational management
Entry requirements	None
Certifications	CWD&A Seminar for Corporate & Policy Executives
Academic hours	16 academic hours (2 days)
Course format	Online lectures

Learning Objective

The participant will:

- Be able to describe the landscape of cybersecurity defence and attack.
- Be familiar with the world of penetration testing (PT) and hacker groups.
- Be familiar with international cybersecurity incidents.
- Be familiar with the operational procedures when dealing with cybersecurity incidents.
- Practise scenario planning (as part of cyber war gaming) including implementing solutions for common cybersecurity threats and challenges

Requirements

None. A good command of the English language is expected.

Certification

A See-Security certificate.

Academic Staff

Our lecturers are highly experienced cybersecurity professionals, with demonstrated training capabilities and organisational and Business perspective. Among our staff, you can find leading CISOs, Offensive Security Experts, Malware Analysts, Forensics experts and more.

Curriculum

Cyber Warfare Overview (3 hours)

1. **Introduction to Cyber Warfare**
   - The birth of Cyber Attack & Cyber Security
   - National cyber security Vs. Organizational Cyber security
2. **Cyber Warfare main players**
   - Main Motivation behind Cyber Attacks
   - Hacker groups
   - National Agencies & Armies
   - Global Cyber Militia's
   - Cyber Crime Groups
   - Cyber Terror Groups
   - Hacktivists & Anarchists
   - Cyber Crime Markets & The Onion Router (TOR)
   - International Attacks History
3. **The everyday of a typical hacker**
   - How to make money'
   - The Statistical approach: detecting vulnerabilities using robots
   - Phishing
   - Taking over on information, stealing, and encrypting information
   - Collecting the money
   - Escaping tactics

Cyber Warfare Defence (2 hours)

4. **Cyber Defence Technologies & tactics**
   - Cyber Defence Principles
   - Tools & Technologies by layers (System, Networking, Mobile, Application, WEB, Cloud etc.)
   - Architecture Design of Cyber Security Tools
   - Partitioning & Implementation
   - Governance, Risk & Compliance
   - Achieving a Defined Security Posture through Business Integration
   - Cybersecurity Processes
   - Situational Awareness (Assessments and Evaluations)
   - Continuity of designing & Partitioning
5. **Industrial / Finance / Healthcare / Other Systems Security**
   - Emphasis in information security of sectors and industries
6. **The structure of Cyber Unites**
   - Personnel and their responsibilities
   - Schematic description of the everyday activities
   - Schematic description of the procedures, activities, and interplays in a real cybersecurity event

Cyber Warfare Offense and Threats (1 hours)

7. **Cyber Intelligence**
8. **Infrastructure Attack**
9. **Web Attack**
10. **Human Attack**

Cyber Incident Response (2 hours)

11. **SOC Roles**
12. **Investigation**
    - Digital Forensics
    - Malware Analysis
    - Cyber Threat Intelligence
13. **Cyber Security Team Response**

C-level & Directors (8 hours)

14. **Management Awareness**
15. **Ongoing monitoring**
16. **Cyber Risk Management**
17. **Management Response**
    - Authorities
    - Public Relations
    - Partners & Customers, Employees
    - Management Incident Response: Processes
18. **Simulation of Cyber Incident Response in organization**