CSP: Cyber Security Practitioner Training Programme

A unique course to train cyber security practitioners (CSP)

Including preparation for CompTIA-Security+ and associated certifications

This programme is designed for individuals with a solid background in IT and fundamentals in cybesecurity, who wish to take their knowledge and skills to the practical, hands-on level and master the implementation of cybersecurity technologies in organizations.

This well-designed programme was originally built for the Israeli government and is the 'gold-standard' training for cybersecurity practitioners personnel in the Israeli market. Let us share our experience and pedagogical approach to give you the skills, best practices, and knowledge to become a cybersecurity professional and lead your organization as a multidisciplinary expert.

CSP: Cyber Security Practitioner Training Programme

A unique programme for IT professional who wish to take their knowledge and skills to the practical, hands-on level and master the implementation of cybersecurity technologies in organizations.

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 programs 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 Events – Managed SIEM/SOC.

About the CSP Programme

The programme has been designed to accommodate the contents and skills taught in various CSP programmes offered by different cybersecurity educational institutes around the world.

The programme is in accordance with the Israeli National Cyber Directorate regulations as well as the CompTIA requirements for the Security+ certification. The programme also allows students to take the $(ISC)^2$-SSCP exams and is continuously updating to follow the new regulations and best-practices of the field.

The growing demand for well-educated and knowledgeable cyber defense experts requires a broad and in-depth background both in technological solutions and methodologies aspects which are embedded in a well-established hands-on rich programme

Key Features	
Cost	TBD
Aaudience	Advanced: IT professionals
Orientation	Ttechnical, theoretical and applicative knowledge, hands-on rich
Oobjectives	To train cybersecurity consultants, architects and methodologists who can take the CISSP certification and serve in key roles in the cybersecurity industry.
Entry requirements	Practical knowledge in OS (Microsoft and Linux), networking and preferably foundations in Python
Certifications	CompTIA-Security+ or $(ISC)^2$-SSCP
Academic hours	Total of 306 online training sessions, Including lectures, discussions, hands-on labs
Homework	Total of 320 homework assignments
Course format	**Online lectures** accompanied with 1-on-1 session with the course lecturers

The CSP curriculum is designed to train cyber defense experts who are able to implement, guide and make decisions on information security defense tasks, in technological aspects These abilities will be acquired through mastery of the best practice strategies, techniques, and industry-based regulations in these areas, including risk

management skills. These will be learnt and practice through **comprehensive hands-on labs** and accompanying theoretical and practical lectures. Step by step, you that will allow you will gain a full theoretical and practical mastery as an aspiring CSP.

This program is in accordance with the requirements of the Israeli National Cyber Directorate (INCD) and includes preparation for the world's top international certification in Cyber Defense - the $(ISC)^2$-SSCP and CompTIA-Security+.

About the CompTIA-Security+ Certification

CompTIA Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on trouble-shooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents – not just identify them.

Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation, because it provides confidence and trust in the outputs of an accredited program. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

About the $(ISC)^2$-SSCP Certification

The Systems Security Certified Practitioner (SSCP) is the ideal certification for those with proven technical skills and practical, hands-on security knowledge in operational IT roles. It provides confirmation of a practitioner's ability to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability. The broad spectrum of topics included in the SSCP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following 7 domains: • Access Controls • Security Operations and Administration • Risk Identification, Monitoring, and Analysis • Incident Response and Recovery • Cryptography • Network and Communications Security • Systems and Application Security.

Target Audience

This program is designed for those who have theoretical and practical experience in system and networking, preferably with some experience in programming (python).

Requirements

You will not be tested on these requirements for enrolment. However, we emphasize that without background knowledge, it will be difficult to keep up with materials covered throughout the course and even more challenging to pass the exams and assignments. The following are required:

a. Practical knowledge and experience in IT systems (Linux and Microsoft) and networking.
b. Familiarity with cybersecurity solutions and products
c. Good command of the English language
d. Preferably: basic knowledge in python

Or:

e. BSc (or equivalent) in Computer Science or Software Engineering
f. Good command of the English language

Pedagogical Requirements

a. Attendance in 80% of the sessions

b. A passing grade in each of the exams and assignments

Certifications

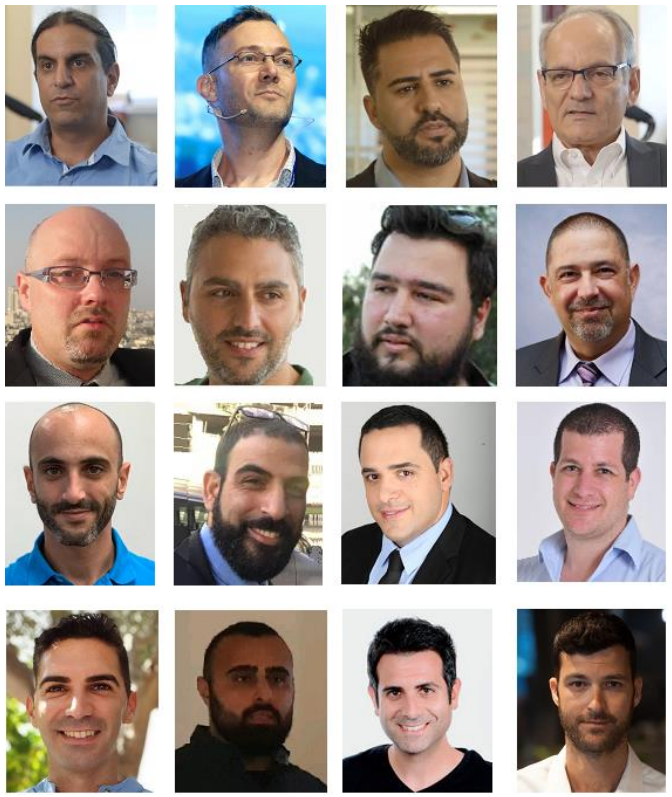
See-Security certificate will be awarded to a student who fulfils the pedagogical requirement.

CSP: Cyber Security Practitioner

Students can also attempt the CompTIA-Security+ or the (ISC)^2-SSCP exam upon graduation.

Academic Staff

Such a multi-disciplinary programme requires uncompromising and dedicated experts. The lecturers include industry cybersecurity leaders, renowned CISOs, and leading professional experts in their respective field.



SSCP®

Curriculum

Introduction to Cybersecurity

- Ontology of information security and cyber: terms, threats, relationships between the various terms, NIST concept, quality assurance concept, and other ontologies. The term dependability.
- Types of offenders and motivation for attack.
- Types of attacks including remote attacks, insider's threats, physical intrusion into computer complexes.
- Social Engineering, Integrated Assault, Malware Sites.
- Types of vulnerabilities in systems / data, including aspects of availability, reliability, integrity and confidentiality.
- Implications and meanings of cyberattacks - financial, reputation, implications beyond the level of the organization.
- Organizational coping methods - appointing officials, defining policies and procedures, defining information assets and vital systems, risk management, physical security.
- The human component and employee reliability - awareness, assimilation in the organizational culture, reports and controls
- Information security policies and procedures.
- Information security in the project management, assimilation of aspects of information security in the software development lifecycle, including the stages of distribution to create and manage changes.

Physical Security

- Guidelines of the law regarding the security of the computer environment.
- What to protect
- Security and monitoring measures to prevent unauthorized access by.
- Measures to deal with various extreme events such as power outages, earthquakes, war and other natural disasters

Securing the Network

- Security and protection products for LAN / WAN, Wireless and Bluetooth.
- Remote access to organizational resources and protection of these access routes.
- Handling access via computers / mobile devices such as smartphones, iPad.
- Setting up a VLAN.
- Aspects of information security / networks / organization when connecting the organization's network to the Internet,
- Network security technologies and products
- Construction of DMZ
- Description of the applicative protocols, HTML5, HTML3, WebRTC, applications and security aspects
- Web Filtering and WAF (web application firewall).

Cryptography and Authentication

- Symmetric and asymmetric encryption - DES DES3, RSA
- Authentication of users
- protocols that support encryption and authentication such as: IPSEC, SSL, HTTPS, SSH.

Severs and OS Hardening

- Implementation of information security within the framework of the following operating system services: Unix, Win, Android, VM.
- Basics of User Identification and Verification Processes, Kerberos. Object and Subject permissions, files
- Operating system logs that support information security.
- Principles of the hardening process.
- Basic operations of the various operating systems Unix, Win, VM.
- Server hardness test.
- Products support hardening.
- Anomalies detection

Aspects of information security in databases

- Database Basics: SQL, Relational DB, MongoDB, Architecture.
- Aspects of information security in the above systems
- Operating system support for maintaining the database, support for the database software on security issues.
- Referential integrity
- Storage systems and the information security in them.

BCP/DRP

- Theory of DRP and BCP, methodology for backup and recovery - full, partial backup, use of blogs as backup.
- Environmentally dependent methods - split computer sites, different operating systems.
- Operating system services for backup and recovery.
- Complementary external products
- Organizational aspects of disaster recovery
- Information security aspects of backup and recovery.

Malware and Anomaly Detection

- Theory of DRP and BCP, methodology for backup and recovery - full, partial backup, use of blogs as backup.
- Environmentally dependent methods - split computer sites, different operating systems.
- Operating system services for backup and recovery.
- Complementary external products
- Organizational aspects of disaster recovery
- Information security aspects of backup and recovery.

Access Control

- User identification and authentication theory, a brief review of the existing mechanisms in the operating system for user identification and authentication.
- The concept of Multifactor authentication
- Additional software / hardware for user identification and authentication such as: Tokens, Smart cards, and Biometric devices
- Processes of linking the hardware component to a specific user
- Definition and use of Identity management systems, including organizations for identifying and verifying users and their permissions in the various systems
- Interface with DNS for user management.
- Event alert.
- Recognizing access of permitted mobile devices (BYOD access),
- Application management and access to them - MAM (Mobile application management) products
- Actions to prevent the connection of unauthorized equipment such as a laptop to the organization's network.

DLP

- Definition of the concept, routs of data leakage, identifying data leakage, means and existing methods for preventing / reducing the phenomenon, for identification and detection.
- Law aspects of DLP
- Protection / prevention / reduction of information leaks in databases, storage systems.
- Protection / prevention / reduction of information leaks in mobile devices such as smartphones, laptops.
- Detachable memory devices - disk-on-key.
- Products and technologies for prevention / detection / identification - such as content filtering products

Management and registration of information security events (Audit)

- SOC (security operation center) products
- SIEM products (security information event management),
- Network access control (NAC) products
- Sensors - installation and configuration. Process definition of product rules, false alerts versus true alerts, tracking, updating, maintenance.
- Integrating these products into the organization, reporting routes.
- Dealing with the warning information received from an external or internal source to the organization

Aspects of information security in network and hardening equipment

- Principles of the hardening process.
- Hardening depends on network equipment (for example a CISCO router versus a router from another manufacturer)
- Software update, firmware, networking equipment.
- Equipment hardening test.
- Products support hardening.
- Synchronization with security products to report anomalies.

Cloud computing, hosting services, virtualization

- Familiarity, the different types of cloud computing. Receiving reports from the various logs and understanding them. Aspects of law. Identifying anomalies, products that support guest and host security.
- Familiarity, the different types of hospitality services. Receiving reports from the various logs and understanding them. Aspects of law. Identify

anomalies, products that support guest and host security.
- Understanding the need for the VM environment, its types, and security aspects

Application Security

- Identifying the risks facing software / application system.
- Determining information security requirements for the software system / application.
- The various activities, in terms of information security, that must be performed at every stage of the software / application development life cycle.

Risk Managements and ISO

- ISO27001 standards, and risk survey standards.
- Methodologies for conducting risk surveys
- The various stages of a risk survey.
- The objectives of risk surveys
- Types - Integrated quality quantitative.
- Subject of the surveys - applications, infrastructure, for security systems, integration of surveys.

Penetration Testing – Infrastructures and Applications

- Methodologies for performing PT.
- The various components of PT
- Identifying potential weaknesses in systems.
- Familiarity with accepted software tools in the field.
- Processes of reporting the findings.

Ethics

- Ethical consideration in cybersecurity
- International law regulations in the field

Incident Response

- Knowledge of types of attacks such as: DoS / DDoS, Spear Phishing, etc.
- Understanding the process of carrying out the attack
- Understanding the damage caused by the attack.
- Measures that may assist the organization in identifying the existence of an assault.
- Familiarity with the subject of false, false positive and false negative alerts.
- How to handle detected attacks
- Activation of inhibitory mechanisms and testing their effectiveness,
- Damage inspection, realization of forensic processes
- Recovery processes,
- Drawing conclusions at the various organizational levels.
- Expanding the organizational knowledge base
- Reporting to law enforcement of cybersecurity incidents