SEE SECURITY
CYBER SECURITY COLLEGE

CISO-CISSP Training Programme

A unique course to train Cybersecurity Architects (CSTP) and Methodologists (CSMP) for a full CISO certification

Including preparation for the (ISC)²-CISSP and associated certifications

This programme is designed for individuals with a solid background in IT and cybersecurity, who wish to take their knowledge and skills to the managerial level and master architectural (technologies) and methodological (governance and policies) aspects of cybersecurity towards a full Chief Information Security Officer (CISO) certification. Students can accredit their knowledge by taking the prestigious CISSP certification at the end of the course.

This well-designed programme was originally built for government and special agencies in Israel and is considered the 'gold-standard' training for senior cybersecurity 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 multidisciplinary professional.

Chief Information Security Officer Training Programme

CSTP: Cyber Security Technology Professional &
CSMP: Cyber Security Methodology Professional

A unique programme for IT professional and experienced cybersecurity personnel who wish to advance their skills to the managerial level as cyber Architects, Methodologists and CISOs

About See Security College

See Security College is a highly specialised and international cybersecurity college. 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 Events – Managed SIEM/SOC.

About the CISO Programme [CSTP & CSMP]

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

Key Features	
Cost	19,900 NIS (tax included)
Aaudience	Advanced
Orientation	Technical, theoretical and applicative knowledge
Objectives	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, networking and cybersecurity technologies OR BSc in Computer Science or Software Engineering
Certifications	CISSP, CISM, ISO27001, CRISC
Academic hours	Total of 288 online training sessions
Homework	Total of 320 homework assignments
Course format	Online lectures accompanied with 1-on-1 session with the lecturers

In 2004, See-Security has created the first CISO programme in the world. The programme is in accordance with the Israeli National Cyber Directorate regulations as well as the $(ISC)^2$ requirements for the CISSP certification. The programme allows students to take the ISACA-CISM, CSA-CCSK and PECB-ISO27001 exams and is continuously updated 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 in both the technological architecture and governance aspects which are embedded in a well-established and proven pedagogical methodology.

The curriculum is designed to train cyber defense experts who are able to advise, guide and make decisions on information security tasks, both in the technology-tactical and administrative-governmental aspects. These abilities will be acquired through mastery of the best practice strategies, tactics, techniques, and industry-related regulations, including risk management skills, law aspects, and knowledge in offensive and intelligence principles. Step by step, you will gain a full theoretical and practical mastery as an aspiring CISO.

This programme 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 $(ISC)^2$-CISSP. Naturally, our graduates can also take easier international certifications such as ISACA's CISM, CompTIA's Security + or $(ISC)^2$-SSCP.

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

This cybersecurity certification is an elite way to demonstrate your knowledge, advance your career and become a member of a community of cybersecurity leaders. It shows you have all it takes to design, engineer, implement and run an information security program.

The CISSP is an objective measure of excellence. It is the most globally recognized standard of achievement in the industry. And this cybersecurity certification was the first information security credential to meet the strict conditions of ISO/IEC Standard 17024.

At the end of our CISO programme you will get the official $(ISC)^2$ CISSP Bootcamp, to make sure you consolidate the knowledge you have learnt and to allow you to take the exam after graduation

About the ISACA-CISM Certification

ISACA's Certified Information Security Manager (CISM) certification indicates expertise in information security governance, program development and management, incident management and risk management. This certification is recommended for methodologist who do not wish to work as Cyber Architects.

Target Audience

This programme is designed for those who have theoretical and practical experience in system and networking, or those with a BSc (or equivalent) in Computer Science or Software Engineering who wish to gain education in cybersecurity architecture and methodologies en-route to a CISO certification.

Further, the programme is suitable for cybersecurity professionals who want to acquire the skills involved in the role of cyber defense architect and cybersecurity methodologist with a deep understanding of how to lead a cyber unit in organizations. Candidates can take the CISSP or CISM certifications with upgraded capabilities and knowledge to accredit their studies via international and highly known cybersecurity accreditation organizations [$(ISC)^2$ and ISACA].

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 the 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 and networking.

b. Familiarity with cybersecurity solutions and products
c. Good command of the English language
d. Passing an admission interview

Or:

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

Pedagogical Requirements

a. Attendance in 80% of the sessions
b. Passing grade in each of the exams and assignments
c. Passing an admission interview

Certifications

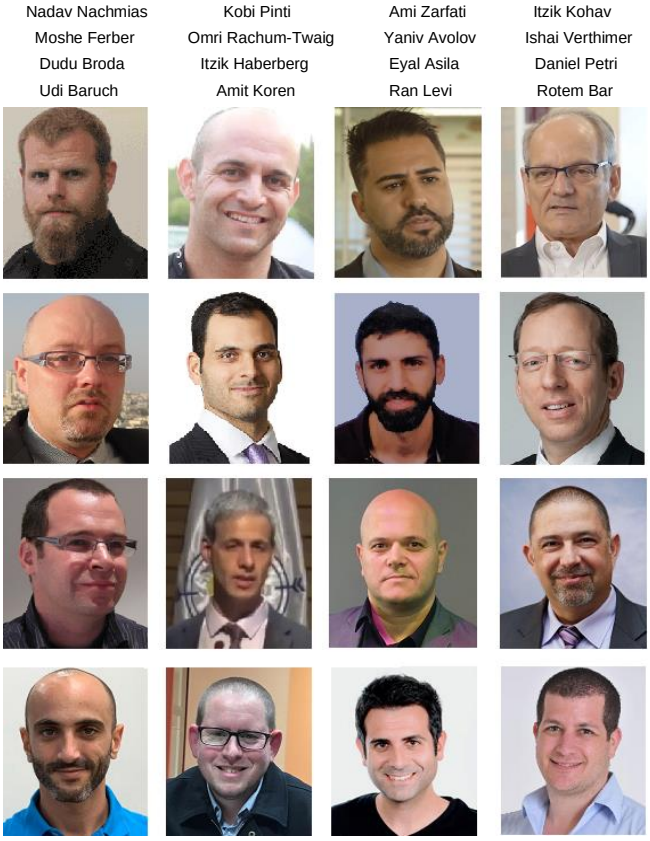
A See-Security certificate will be awarded to students who fulfil the pedagogical requirement:

CISO: Chief Information Security Officer

Students can also attempt the CISSP exam upon graduation. Those who wish to take easier certifications can also attempt the CISM, ISO27001 and SSCP certification.

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.



Remarks

a. Registration for external examinations is the responsibility of the student
b. The programme will open only if there are enough enrolled students
c. The registration fee is not refundable

Curriculum

Thinking Security

- **Track overview**: academic requirements, Security Concepts
- **The Art of War**: Information security and the Art of War, The technical landscape
- **Threats, Vulnerabilities**: Digital Threats, Vulnerabilities, The Human Factor, adversaries, end users
- **Attack and defense techniques**: attacks types, methodologies
- **Defense in Depth**: Defensive: Defense in Depth, trusted computing
- **InfoSec engineering & common criteria**: Information system security engineering, common criteria, summary

Cyber Technologies: Technologies, Tools, Techniques & Architecture

- **Cryptography**
- **Certification Authorities**: Installing Configuring & Maintaining Certification Authorities, Configuring, Deploying & Maintaining Certificates, Smart Card Certificates, EFS
- **Access Control**: What is Access control? Chapter 2: Identification and authentication (I&A), Authorization and AC Models, Centralized Access Control Methodologies
- **Perimeter Protection**: Enclave defined, The need for Perimeter Protection, Router security, Firewalls, VPN Technology, NAC
- **Detection & Response**: The Need for Detection Systems, IDS Systems Capabilities, Implementation & Management, Security Information & Event Management, Log Retention and Management, SIEM.
- **Anti-Malware**: Malware threats and Anti Malware tools
- **Application** & Code Security
- **DB** Security
- **Virtualization** Security
- **Cloud Security**
- **DLP**
- **Hardware Security**
- **Files Security & Whitening**: Hidden Content in files, Why Antivirus is insufficient, Metadata, Utilizing features to abuse
- **Social Networks Security**
- **Infosec Technologies Trends**
- **Information Technologies Architecture**: Security Architecture creation methodologies

Incident Response

- **SOC & Incident Response**: SOC Operation, Incident response methodology
- **Detection & Response-Lab**: Implementing a SIEM Project
- **Computer Forensic & Intellectual Rights**: Computer Crime investigation, forensics & guarding, Intellectual property.

Hacking Defined Advanced

- HD Introduction
- Hacking Methodologies
- Reconnaissance
- Internal Network Attacks
- External Network Attacks and Exploitation Intro
- PT reports + Hacking Defined - Exam
- Mobile Hacking

Cyber Methodology / GRC: InfoSec Governance, Risk & Compliance

- **Legal & Regulatory**: The Applicable Legislation, The privacy Act, Information reservoirs Registration & Protection, The Regulation, 357, 257, SOX & iSOX, BASEL II, HIPPA, 361, 367
- **Program Management**: The InfoSec Program from Three Points of View, Security Architecture Defined, Policies, Standards, Procedures, Baselines & Guidelines, InfoSec as a Process, Process Quality Management
- **Governance, Strategic plan**: Corporate Governance Defined, InfoSec Governance,
- **ISO 27001 Lead Auditor Preparation** Corporate, IT & InfoSec Governance Relationship, Corporate strategy defined, Infosec Positioning, Infosec Strategy, InfoSec Strategic Planning. Statement of Applicability
- **Controls & Control Objectives**: ISO 27001 -ISMS, InfoSec Control Objectives
- **Control Environment**: Controls, Designing a Control Environment, Cobit, COSO
- **Privacy in the Digital Age**
- **Program Audit & Maintenance**: Internal Audit Defined, IT General Audit, Infosec Audit, Program Improvement, Vulnerability Assessment, Pen tests

CISO Function & Role

- **The Evolving CISO Role**
- **Risk Assessment**: Risk Management Fundamentals, Risk Assessment, Qualitative and Quantitative Assessment, The Hybrid approach, Asset Management, MSAT, Identifying Asset Vulnerability, Formalizing Risk Statement, Risk Register, Prioritizing Risk, Stating Solutions
- **InfoSec Processes**: InfoSec Process & Process Catalogue, Process & Program maturity
- **InfoSec Project**: Project Management Defined, Creating an InfoSec Project, Business Case - Business Case

- **Capital Planning & Investment Control:** Capital Planning & Budget Decision, Corrective Action Impact and Priority, System Based Project Scoping, Enterprise Project Scoping, Choosing Your Battle, Project Investment Control,
- **Corporate InfoSec Policy**: The Need for a Corporate InfoSec Policy, Policy Governance & Authority, Scope, Responsibility & Accountability, The Policy Chapters
- **The IAM Process**: Role Definition, Workflow, User Provisioning / De-provisioning, Audit & monitor
- **BCM - Business Continuity Management**: BCM Planning, COOP, CCP, ORP, ITCP, CIP, BRP, DRP, DRP Project
- **Relationship & Communication**: Implementing a Security & Awareness Program - Creating & Implementing a Security Marketing Plan
- **Measuring Security**: Security measurements & Metrics Implementing metrics in security processes (KPI, KRI).
- **Putting it all Together:** The New CISO 1st Year Timeline, from Security Strategy to Governance to Security Program & Projects

Official (ISC)²-CISSP Bootcamp Preparation

- TEST Marathon