

## Contents

Company Overview .....	3
Our Mission .....	3
Company History .....	5
Products and Services .....	5
Industry Participation.....	7
The Mapping Process.....	7
The Development Effort .....	8
The Market Goals .....	9
Current Available Courses.....	9
Current Markets .....	12
Marketing Method .....	13
See's Courses Series Advantages .....	14
Education emphases.....	15
Prerequisites and Acceptance Tests .....	17
CEP - Continuity Education Program.....	17
See Security Lecturers and Trainers .....	19
Graduations and Certifications – Not Complete.....	20
Competitors.....	21

### **Attached to this Document:**

- Appendix A – Sub-Professions definitions
- Appendix B – How to learn, how to teach IT Security
- Appendix C – See Security Lecturers CV's
- Appendix D – See Security Courses Catalogue
- Appendix E – Franchises Basic Info document

## ***Company Overview***

### **Our Mission**

1. Provide strategic and real world IT Security Education solutions.
2. Provide “top-notch” technical IT Security consulting services to medium and large organizations.
3. Execute vulnerabilities research for the public benefit.

**See-Security Technologies Ltd.** was founded in 2002 by highly skilled academic personnel and professional information systems researchers and attackers.

See Security is an IT security education organization totally committed to the delivery of breakthrough information-security (IS) technology solutions that address security education needs of various professions involved in this technology area. We take a holistic view of information security, delivering continuing education programs that meet today's needs, adapt to future requirements and are continuously improving the programs day by day.

See Security's business scope is based on its deep technical knowledge in the "offensive security" field including strategies, methodologies and techniques, and have built a family of asset prone services which are designed for the client's best interest.

We understand that organizations - be it a corporation or government agency - faces unprecedented security challenges as they extend the boundaries of their network for critical transactions, collaboration and information sharing.

While this increased interconnectivity brings efficiencies and expansion of markets, it also demands assessment, protection and auditing of the security of the IT assets and business processes. Our response to this security challenge is to provide organizations with unmatched security education and services, from our world-class security talent.

See Security caters to a wide range of International and local clientele. Amongst our clients are major industry leaders and governmental agencies.

See Security has been proven to be a unified IT security service provider with unparalleled capabilities, innovative skills and proven expertise – able to cope with the rapidly changing business challenges and technologies of its diversified clients.

See's main objectives are:

1. Founding an international Security Education Organization (SEO) and establishing a new edge of Security Education based on Continuing Education Program (CEP).
2. To be European Security Consulting Group.
3. To be partner of international non-profit security organizations for new security standards.

See prides itself as being:

- A well-known security education organization in France, Italy, England and South Africa, and “Trusted Partner” of ISC2 non-profit foundation.
- The main security consultant for large scale of organizations in Israel such as, government institutions,

commercial banks, leading High-tech companies, insurance and industrial organizations.

### **Company History**

Incorporated in 2002 as a department in another company by three founders and employees with extensive backgrounds in information security, See Security has become an international IT Security Education Organization (SEO) with headquarters in Israel. The company is privately funded and has received International recognition by the ISC2 (International Information Systems Security Certification Consortium). During its history, See Security became an independent company, collaborated with leading firms and organizations such as ISC2 to provide its expertise in the industry.

Till December 2003 See Security was developing its educational programs. On January 2004 the company made its first marketing efforts.

### **Products and Services**

All of See Security's products and services are cost-effective, highly related to the current industry needs and based on the knowledge of a group of high skilled professionals in IT security, warfare and Pedagogies.

See Security deals in mainly 2 fields:

- 1) IT Security Education.
- 2) Technical Consulting Services

The company does not deliver any products or proprietary services and does not deliver any kind of implementation due to its independent status as a consultant.



## Industry Participation

Due to See Security's heavy investment in security expertise, its leaders regularly present at industry conferences and write for numerous technical publications. See is a partner of the ISC<sup>2</sup> and the Technion University (Israel institute of Technology), for developing the next generation of IT Security Education.

See Security is heavily involved in consulting and education for large Israeli companies in the finance, industry, commerce, hi-tech sectors and governmental agencies.

Please feel free to contact us at [info@see-security.com](mailto:info@see-security.com).

## The Mapping Process

In 2002, See decided to invest its own resources and knowledge in developing the Information Security Education Program.

The IT Security arena is multi-dimensional, multi-layered, and multi-discipline and spread out over multiple issues, sub issues, technologies and more. See decided to "take the bull by the horns" *define* security.

See performed a heavy process of mapping or defining the IT Security field, and divided it into 2 main arenas: (1) The Technical arena. (2) The management arena (e.g. Policies, procedures, etc.).

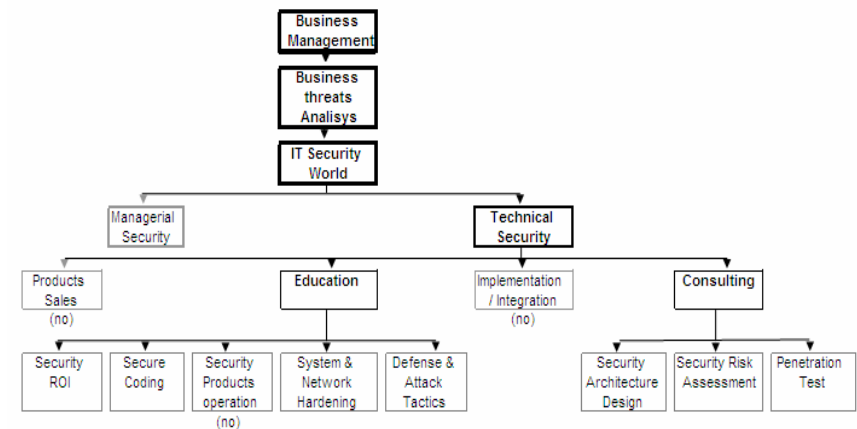
Since See is a technically orientated company, the defining process was done according to the companies professionals experience in real world security and it was decided to *define* security from an angle different from the norm, this angle was

offence or hacking – hence the companies flagship course series name: *Hacking Defined*.

## The Development Effort

The development commenced in November 2002, under a holistic point of view and based on the results of a market analysis and the mapping process. The effort to design an appropriate methodology with the right point of view to respond the market needs still continues.

### See Security Activities in IT SECURITY

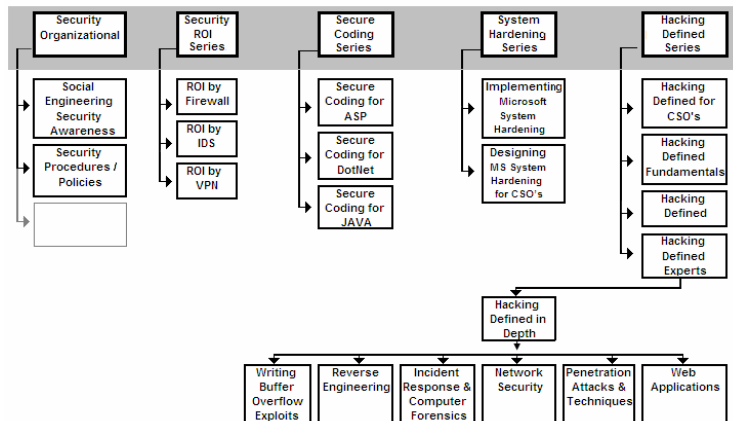


## The Market Goals

The lessons outline implement or meet some areas:

- End users.
- IT professionals.
- Software and hardware developers.
- System and Communication experts.
- Technical security professionals.
- Organizational, business and management people involved in IT Security.

## Current Available Courses



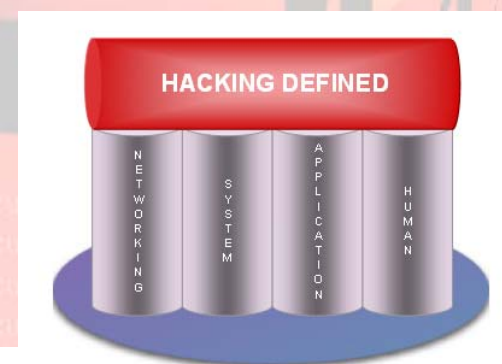
Course Description	Length	Course Code	Target Audience
<b>Hacking Defined Series</b>			
<b>Hacking Defined for CSO's</b>	24 hrs (3 Days)	HD-3- CSO	CSO's
<b>Hacking Defined Fundamentals</b>	40 hrs (5 Days)	HDF-5- EWL	Infrastructure, system & Networks experts w/ no security experience and knowledge
<b>Hacking Defined – Attack Basics</b>	40 hrs (5 Days)	HD-5- IWL	Infrastructure, system & Networks experts w/ security fundamental knowledge
	40 hrs (evening)	HD-5- IWL- night	
<b>Hacking Defined Expert</b>	100 hrs (12 Days)	HD-8- AWM	System, Networks & Security experts or: HD-5-NWL Graduate
	100 hrs (evening)	HD-8- AWM- night	
<b>Hacking Defined in Depth Workshops</b>			
<b>Web Applications</b>	24 hrs (3 Days)	WA-3- AMH	Security experts, Programmers, web application designers
<b>Penetration Attacks &amp; Techniques</b>	24 hrs (3 Days)	PEN-3- ANH	System, Networks & Security experts or: HD-5-NWL Graduate
<b>Network Security</b>	24 hrs (3 Days)	NS-3- IMM	Infrastructure engineers & Security experts or HD-5-NWL Graduate
<b>Incident Response &amp; Computer Forensics</b>	24 hrs (3 Days)	IR-3- ANM	System, Networks & Security experts or: HD-5-NWL Graduate

Reverse Engineering	24 hrs (3 Days)	RE-3- ANH	Security experts, programmers
Writing Buffer overflow exploits	24 hrs (3 Days)	BO-3- ANH	System, Networks & Security experts or: HD-5-EWL Degreed
<b>System Hardening Series</b>			
<b>Designing Microsoft System Hardening for CIO</b>	24 hrs (3 Days)	DMS-3- IWL	CIO's and CSO's of organizations using Microsoft products
<b>Implementing Microsoft System Hardening</b>	40 hrs (5 Days)	IMS-5- AWM	Microsoft System Administrators
<b>Implementing Unix System Hardening</b>	40 hrs (5 Days)	HDU-5- IMM	Unix System Administrators
<b>Secure Coding Series</b>			
Secure Coding for ASP	32 hrs (4 Days)	SC- 4ASP- AMH	Security experts, Programmers, web application designers
Secure Coding for .Net	32 hrs (4 Days)	SC-4.Net -AMH	Security experts, Programmers, web application designers
Secure Coding for JAVA	32 hrs (4 Days)	SC- 4JAVA- AMH	Security experts, Programmers, web application designers
<b>ROI (Return On Investment)</b>			
Open Source IDS solutions	24 hrs (3 Days)	ROI-3- IDS	System, Networks & Security experts or HD-5-NWL Graduate
Open Source Honeypot Solutions	8 hrs (1 Days)	ROI-1- HNY	System, Networks & Security experts or ROI-3-IDS Graduate
Open Source Firewall Solutions	24 hrs (3 Days)	ROI-3- FW	System, Networks & Security experts or HD-5-NWL Graduate

Open Source VPN solutions	8 hrs (1 Day)	ROI-1- VPN	System, Networks & Security experts or ROI-3-FW Graduate
<b>Organizational</b>			
Social Engineering-Security Awareness	8 hrs (1 Day)	SE-1- WM	Executive to entry level employees
Security Procedures / Policies	40 hrs (evening)	SP-5- WM- evening	CSO's & Security Managers

### Current Markets

See Security targeted Europe countries for the market in 2004. In Israel, See appointed “John Bryce Training” as its representative, and so – local famous organizations in France, Italy, Great Britain and South Africa. In these countries See trains professionals with its experience, knowledge, labs and in-house developed documentation.



### Marketing Method

See markets its courses via local educational centers in each country or city. See will commence marketing efforts in the United States not before January, 2005. The basics for the partnership are as detailed:

#### Supplied by See Security



- o Documentation sets, 600 to 2,500 pages, depending of the course nature, and a CD where applicable



- o Unique wood case for the documentation.



- o Certificates recognized by ISC2 for CISSP and SSCP CPE's.



- o Hands-On training sophisticated lab environments, includes tens of "virtual systems and organizations"



- o Experienced Security professional's famous lecturers and trainers.

#### Supplied by partner



- o Marketing agenda based on Call centers, Brochures, emailing etc.



- o Class facilities, networks, WS's and servers as defined by See.



- o Experienced Security professional certified trainers (after one year).

### See's Courses Series Advantages

The main advantages are as detailed:

1. The only **SEO** (IT Security Education Organization) worldwide to practically map the IT Security knowledge arena, followed by training programs based on this mapping process.
2. The only **SEO** to build and represent an Education Continuity Program (**ECP**) for the participants, for various levels, various professions, to enable vertical or horizontal personal development.
3. The only **SEO** based on Academic concepts for educational programs, to determine the course duration by factors such as: Skill Level, Coverage Range, and Detail of Coverage.

<b>Course Description</b>	Course title		
<b>Duration</b>	Course length in days		
<b>Skill Level</b>	[A]dvanced,	[I]ntermediate	[N]ovice
<b>Coverage Range</b>	[W]ide,	[M]edium,	[N]arrow
<b>Detail of Coverage</b>	[H]igh,	[M]edium,	[L]ow

E.g. *HD-8-AWM*

4. The only **SEO** to be recognized by the ISC<sup>2</sup> for 64 CPE's for CISSP and SSCP graduation (The highest worldwide).
5. One of the only **SEO** to combine at least 40% of Hands-On-Training activities within its courses, based on a large amount of attacking and defending exercises, designed

and built by the best professionals over a long period of time.

6. One of the only SEO that combine and base the studies either on attacking and defending knowledge, for better understanding of the IT security needs.
7. The only **SEO** to base and use one clear and proved methodology, with determined rules for study contents, syllabi, documentation structure, and even phonetic and marketing rules.
8. The only **SEO** to use heavily pedagogies professionals, taking in consideration factors such as duration, scope, timing, time-of-the-day, sequences, human perception and didactic methods.
9. Vast treatment to the participant feedback booklet and improvement program based on those feedbacks.

#### *Education emphases*

1. **Clear Methodology** - describes and define basic rules of lesson outlines for all the courses, syllabus format, and even marketing or fonts for the above.
2. **Pedagogical response** – adoption of pedagogical rules by security professionals, including limits, estimations and pedagogic success goals. The main pedagogic goal we choose: “Satisfaction level of the participant”. The training base on various of pedagogical and technological instruments and tools, by recorded exercises, frontal teaching, live demonstrations, one-on-one exercises and “catch the flag” games.

3. **Duration Model** – for each course series we defined a formula takes in consideration the (1) sub-subjects quantity, the (2) depth of each sub-subjects, the (3) beginning level, and finally – (4) the goal of each course. Those parameters were defined to enable separate solutions for different participant needs.
4. **The Hacker insight** – IT Security studies couldn’t be reached without the depth understanding of the attackers thinking figures. Rules (if exists), and operations. The “hacker way” demonstrate clearly hoe each small, naive, pointed mistake may cause enormous opportunity for the hackers. That’s why the participant will learn how attackers use this mistakes and how to block them.
5. **Hand’s on Experience** – IT Security studies can’t reach the high level goals by frontal teaching only. at least 40% of each course based on Lab training with trainers next to the participants.
6. **“Know-How” instead of “Know the Product”** – one of the basics most important rules is to teach the participant to think one layer on top of product understanding. This method enables the participant to contend with several of tools produced by different producers, by understanding the way it wad designed.
7. **Intensively studies** – The lecturers measurement process base on one goal: The best marks they can reach of the participants at the last course day. Potential participant failure will be considered as their own failure, so they should take it in consideration during all the course period.

## 8. Basic Lecture Structure – each subject based on:

- a. Real World Scenario
- b. Overview
- c. Objectives
- d. Thinking Security
- e. Theoretical Explanation
- f. Practical Explanation
- g. Challenges / Lab exercise
- h. Review
- i. Countermeasures and Defenses

### *Prerequisites and Acceptance Tests*

See Security use interview as the best way to help the participant to choose its best orientation and course level. The lecturer may avoid during the interview of participant entrance to specific course, but their mission is to help him by his own decision to choose the right decision.

In some cases, the interviewer will help the potential participant to complete some technical pre-requisites before registration. Each interview may take 10 to 30 minutes. These interviews are absolutely non-disclosures.

### *CEP - Continuity Education Program*

The CEP basically designate for IT Security profession holders, both in technical or non technical areas.

**For technical professionals**, See had design the preliminary first-step 40 hours “Hacking Defined Fundamental” courses. The pre-requisites for this course are: System managers with basic of 1 year experience in system management, familiar

with UNIX and Windows systems, networks and TCP/IP protocol. No previous IT Security knowledge needed.

Participants needs better technical ground before starting this course will get our lecturers guiding to the right pre-requisite knowledge and resources to reach it.

In this course, the technical oriented participant will get security and attacking products families’ survey, general understanding of attacking and defense methods, and it’s meaning for the organizational infrastructures.

The second step course is HD-5-NWL 40 hours “Hacking Defined” course. This Novice skill level, wide cover range and low detail of coverage course will allow the participant to rich wide understanding of research and penetration attacks and techniques, security mechanisms and finally - house keeping methods.

The third step course was designed for advanced skill level participants. This 100 hours HD-8-AWM “Hacking Defined Experts” course is wide coverage range and medium detail of coverage, brings the participant with very high, rare and uncommon knowledge about security methods, techniques, by self experience through massive Lab exercises.

Participants completed this path, are absolutely high skilled It Security professionals, and are ready for wide set of very narrow expertise specific courses.

**For IT Security non-technical professionals**, See had design path that includes the same preliminary first-step 40 hours “Hacking Defined Fundamental” courses, but it’s defined as no pre requisite for the next steps.

See positions the next step course by 40 hours “IT Security Policy and procedures” course, and by 24 hours HD-3-CSO “Hacking Defined for CSO’s”. This allows CSO’s and non technical audiences to be exposed to special review of the technical security world, for better understanding of their responsibility field.

### *See Security Lecturers and Trainers*



**Alon Swartz** is the technical director of See Security where he leads the consulting and education sections of the company. Alon is an expert in large scale penetration testing, Risk Analysis, OS internals, application security, networking and developing attack code. Alon has been active in the Information Security/Warfare arena since 1996. Alon served in an InfoSec section in the Israeli Military.



**Liraz Siri** is an expert in Unix, networking, penetration testing, multi-layered security development, cryptographic systems development and rapid software prototyping. Liraz has been researching computer security since 1994 and is best known for the “Internet Auditing Project”. Liraz served in an InfoSec section in the Israeli Military.



**Itay Yanovski** is an expert in security management, risk analysis, penetration testing, application security and networking. Itay has been in the technology and information security arena since 1983 and has been a guest lecturer in various security conferences. Itay served in an InfoSec section in the Israeli Military.



**Mati Aharoni** is an expert in several OS’s, penetration testing, networking, social engineering and group dynamics. Mati has been in the technology and information security arena since 1992 and has trained courses in the fields of Microsoft, Linux, Unix, Cisco, HP and Security.



**Gadi Rapaport** is an expert in Microsoft OS’s, networking, .Net services and networking, and has been the lecturer for various Microsoft courses, for operating systems, services, security and more.

***Graduations and Certifications – Not Complete***

## ***Competitors***

### **Israel**

To our knowledge, there are no other IT Security Education organizations based on large and continuing education programs. Some companies do exist who offer some general Security courses, for different sub issues.

### **Overseas**

SANS and FoundStone are the famous organizations amongst See's competitors.

See "See Security's Courses Series Advantages" section in this document.

### ***Appendix A – Sub-Professions definitions***

See attached

### ***Appendix B – How to learn, how to teach IT Security***

See attached

### ***Appendix C – See Security Lecturers CV's***

See attached

### ***Appendix D – See Security Courses Catalogue***

See attached

### ***Appendix E – Franchises Basic Info document***

See attached