מתי
מכון התקנים הישראלי

See
see security technologies ltd
בית ספר לאבטחת מידע
וללוחמת מידע

# המסלול להכשרה ולהסמכת
# מהנדסי ומנהלי אבטחת מידע ארגוניים – CISO
## מחזור מס' 22

**יועץ אקדמי: מר אבי ויסמן ***

**תוכנית לימוד שנתית למנהלי תשתיות טכנולוגיות, למפתחים ולמנהלי מערכות מידע המעוניינים להתמחות בהנדסה, ארכיטקטורה ובניהול יחידות אבטחת מידע**

**פתיחת מסלול בתל-אביב: 3 בינואר 2012 בימי שלישי (ערב) ושישי (בוקר)**

### מבוא

להשאר לעד "מנהל רשת", משמעו, ללכת לאחור ולהאבק על התפקיד מול אלפי בני ה- 20 המציפים את הענף. פריחתו של ענף אבטחת המידע אינה דורשת הסבר. כמות הידע הנדרשת על-מנת להתמודד עם אתגרי ההתקפות ובעיות הסייבר תלויה בסוג התפקיד. קיימים שישה תפקידי רוחב שונים, ומספר גדול עוד יותר של תפקידי התמחות, כפי שיוסבר בהמשך.

בין ששת תפקידי הרוחב הקיימים במערך אבטחת המידע, נמנים: מינהלן, מיישם (טכנאי), מומחה, מומחה בעל התמחות, מנהל אבטחה ב- IT, מנהל אבטחה ארגוני (CISO), ומבקר אבטחה. בנוסף, קיימים "תפקידי עומק" שמשמעו – בעל התמחות ספציפית (Pen-Tester, App-Tester וכו').

התפקידים הזוטרים (מינהלן אבטחה ומיישם/טכנאי אבטחת מידע) מחייבים רכישת ידע בסיסי בהתקנה, הגדרה ותחזוקה של כלים בסיסיים (פיירוול, אנטי וירוס ודומיהם), ולצורך כך נדרש לימוד עצמי או קורסים בסיסיים כגון CCSA, CCNA, ISA ודומיהם (מסלול זה אינו מתאים לצורך זה).

אולם עיקר נטל האבטחה אינו מוטל על המיישמים, אלא על מתכנני מערך האבטחה ומעצביו (מהנדס/ מתכנן /ארכיטקט/ מומחה). כל ארגון נזקק לעמוד שידרה זה, והארגונים הקטנים מקבלים שרות זה באמצעות חברות היעוץ.

לכן, הדרישה ההולכת וגוברת למהנדסים-יועצים ולמנהלי אבטחת מידע משכילים ובעלי ידע רחב ומעמיק, מחייבת רקע רחב ועמוק במיוחד, במסגרת מתודולוגית סדורה אשר תאפשר השתלטות על המידע הרב, וזו מהות המסלול.

**השתלבות בתפקידי יעוץ, הנדסה וניהול אבטחת מידע**

מסלול CISO זה הינו המסלול הראשון בישראל, וקיים משנת 2004. התכנים והמשקלות לנושאי הלימוד נבנו ומעודכנים על-ידי קובעי הדרך – ה- CISO's של הארגונים הגדולים והמובילים את הענף. אין תקדים לחומרי הלימוד העשירים הנשענים על קונצנזוס מקצועי של הפורום הישראלי לאבטחת מידע. המסלול זוכה להערכה רבה של קברניטי המעסיקים במשק הישראלי.

**מדוע הפך מסלול CISO של See Security למותג? מדוע קיים פטור ממכרז? התשובות – במפגש המידע.**

### מטרת התכנית

קורס ניהול אבטחת מידע CISO עוסק רק בדרגות האסטרטגיות – **מומחה, מהנדס, ארכיטקט, מנהל ומבקר אבטחה**, ואינו עוסק בתפקידי טכנאות אבטחה (לא בהתקנות ובתחזוקה). המסלול יקנה לבוגר את היכולת להתמודד עם תפקיד ה- CISO ועם תפקיד ארכיטקט/מהנדס אבטחת מידע, יקנה יכולת לתכנן מערך אבטחת מידע, לבחור את הרכיבים הנכונים, ליישמו בטכניקה נבחרת, לעקוב ולנטר אירועי אבטחת מידע, לנתח ולהבין אירועי אבטחה, להגיב באופן מיידי והולם לאירועי האבטחה, ליזום "סדר" בפעילויות האבטחה הארגוניות, להתמודד עם הדרישות העסקיות, לקיים את החוקים, הרגולציות והתקנים הישראליים והבינלאומיים הנוגעים לנושא ולהציב עצמו כמועמד לתפקיד הבכיר של מנהל אבטחת המידע הארגוני.

על המרצים נמנים מובילי הענף, בהם: מנהלי אבטחת מידע ידועי שם, ומומחים מקצועיים המובילים בתחומם.

ISO IEC NIST isc² ISACA Gartner

* יו"ר הפורום הישראלי לאבטחת מידע IFIS ומנכ"ל ביה"ס חברת אבטחת המידע See Security

4 Maale' Hshachar St. Ramat-Gan 52383, Israel. Tel: +(972)-3-6122831, Fax: +(972)-3-6122593
http://www.see-security.com avi@see-security.com

מתי
מכון התקנים הישראלי

See
see security technologies ltd
בית ספר לאבטחת מידע
וללוחמת מידע

## קהל היעד

קורס מנהלי אבטחת מידע CISO ומהנדסי אבטחת מידע מיועד לבעלי ידע מעשי בתחום התשתיות (מערכות הפעלה ותקשורת, ורצוי ידע בסיסי בכלי אבטחה בסיסיים) וכן בוגרי תואר ראשון או שני במדעי המחשב, הנדסת תוכנה\חומרה, המעוניינים לרכוש התמחות מקצועית וידע מעמיק וכן כלים ניהוליים בעולם אבטחת מערכות מידע ארגוניות (טכני וניהולי), לשם התמחות גבוהה בעולם אבטחת מידע וקבלת אחריות ניהולית ומקצועית בתחום הסיכונים העסקיים, ומעוניינים לגשת למבחני ההסמכה של CISSP או CISM או CEH.

המסלול איננו מתאים למתחילים.

## תנאי הקבלה

- רקע קודם בניהול רשתות Windows או Linux או באבטחת מידע או בפיתוח תכנה. נדרשת הכרת Windows, Linux, TCP/IP, Web ושירותים כגון: HTTP, SMTP, TELNET, FTP, DNS,.
- נכונות לעבודה עצמית מונחית רבת היקף (כ- 400 שעות לימוד ביתי).
- ראיון אישי.

להיות פשוט "מנהל רשת" זה כבר לא מספיק. להיות מיישם / טכנאי Cisco או CheckPoint היה נכון בתחילת דרכנו. בעידן של התקפות הסייבר, צריך ללמוד. ממש ללמוד, כי אין ברירה.

מסלול CISO מבוסס על מטריצת ששת מקצועות האבטחה ו- 5 עולמות הידע, ומוגש לתקינה והסמכה במכון התקנים.

## מתכונת הלימודים

משך התכנית כ- 280 שעות, במתכונת של 70 מפגשים הפרושים על-פני כ- 35 שבועות. הלימודים מתקיימים בקמפוס See Security ברמת-גן. המסלול נפתח כ- 3 פעמים בשנה.

## מטלות הקורס

- כל מודול נלמד מחייב עמידה במבחן פנימי בציון 75 לפחות. קיים מועד נוסף לנכשלים/נעדרים.
- חובת עמידה בעבודות בית המקנות ציון, ובעבודה מקיפה.
- בנושאים הטכניים - תרגול (Hands-on) בכיתה (מעבדת מחשבים).

## עלות התכנית

סך 18,000 ₪ + 400 ₪ דמי רישום.

## זכאות לתעודה

- קיימת חובת נוכחות ב-80% מהמפגשים, ועמידה במבחנים/עבודות, בציון 70.
- לעומדים בדרישות התכנית תוענק תעודת הסמכה מטעם See Security ומכון התקנים: **"מנהל אבטחת מידע ארגוני בכיר – CISO"**
- התוכנית נבנתה לצרכי **ידע מעשי**, ומשמשת כהכנה מלאה למבחני **CISSP**.

## ה ע ר ו ת :

- פתיחת כל תכנית מותנית במספר הנרשמים.
- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי ביה"ס.
- דמי ההרשמה ומבחנים חיצוניים כלשהם אינם כלולים בשכר הלימוד.
- בית הספר מביא לידיעת הנרשמים והתלמידים כי ייתכנו שינויים במערך התכנית, במועדי הלימודים והבחינות או בכל נושא אחר. הודעה על כל שינוי תימסר למשתתפים.

**לכל מידע נוסף או לתיאום ראיון אישי או פגישת יעוץ:**

**מידע מינהלי:** אלוירה אליסייב, 03-6122831, 052-8787889, elvira@see-security.com

**יועץ אקדמי:** אבי ויסמן: 054-5222305, avi@see-security.com

מתי
מכון התקנים הישראלי

See
see security technologies ltd
בית ספר לאבטחת מידע
וללוחמת מידע

# מתודולוגיה: מקצועות אבטחת מידע ותחומי אבטחת מידע

המסלול נבנה על-בסיס פדגוגי ודידקטי ואוריינטציה פרקטית בפיקוח אקדמי, במדרג של בעלי תארים (רמות שונות), והכרה בארגונים בעלי אתיקה דומה (ISC2, ISACA, GIAC, ISSA, SII). תשומת לב ניכרת ניתנת לדגשים הנהוגים בישראל (הפורום הישראלי לאבטחת מידע IFIS).

המתודולוגיה המתוארת מתבססת על רשימת כל המקצועות התעסוקתיים המקובלים בתעשיית אבטחת המידע ולוחמת המידע, ומולם – כל תחומי הידע הקיימים בעולם זה.

מהמטריצה נגזר הידע הנדרש לכל מקצוע, ומכאן - נגזרים מסלולי הלימוד והקורסים, היקפיהם ומיקודם. מטריצה זו של הפורום הישראלי לאבטחת מידע מהווה עמוד שידרה למתודולוגיית הלימודים של See Security.

**מקצועות והתמחויות בעולם אבטחת המידע** (מודגשים המקצועות הנפוצים יותר)

1. מינהלן אבטחת מידע - **ISAD** - Information Security Administrator
2. מיישם מערכות אבטחת מידע - **ISSI** - Information Systems Security Integrator
3. מהנדס אבטחת מידע - **ISSE** - Information Security Systems Engineer
4. מנהל אבטחת מידע יח' המחשב - **ISSO** - Information Systems Security Officer
5. מנהל אבטחת מידע ארגוני - **CISO** - Chief Information Security Officer
6. מבקר אבטחת מידע - **ISA** – Information Security Auditor

**התמחויות** (מומחה תחומי באבטחת מידע - Information Security Expert – ISE)

A מומחה ניטור אירועי אבטחה - Information Security Incident Expert - ISIE
B מומחה בדיקות חדירות - Testing Information Security Penetration Expert - ISPTE
C מומחה חקירות למערכות מידע - Forensics Information Systems Expert - ISFE
D מומחה אבטחה פיזית למערכות מידע - Physical Security Information Systems Expert - ISSPE
E מומחה אבטחת יישומים ופיתוח - Security Application Development Expert - ADSE
F מנהל פרוייקט למערכות אבטחת מידע - Information Security Systems Project Manager - ISSPM

**עולמות ידע (תחומים) בעולם אבטחת המידע**

העולמות השונים המהווים יחד "אבטחת מידע" או "הגנת מידע", מפורטים להלן. לכל אחד מהעולמות, ניתן להתייחס מאחת מהדיסציפלינות הבאות:

א. זוית הראייה של מיישם (הפן הטכני של התקנה ותחזוקה).
ב. זוית הראייה של מהנדס/ארכיטקט (פן התכנון המרחבי).
ג. זוית הראייה של מנהל אבטחת המידע הארגוני (משימות, נהלים ותהליכים).

1. עולם אבטחת תשתיות מיחשוב (מערכת הפעלה, תקשורת, אלחוטית, ניידים, קוד ואפליקציה, Web)
2. עולם הכלים והטכנולוגיות (FW, IDS, IPS, PKI, VPN, Anti's, Spofer, Scanner, Biometrics…)
3. עולם התקיפה והלוחמה הקיבנטית (Hacking & Cyber Warfare)
4. עולם מימשל אבטחת המידע (Governance: Laws, Regulations, Standards & Business needs)
5. עולם הניהול והאו"ש של יחידת אבטחת מידע (משימות, תהליכים, תיאור התפקיד)

* עולם האבטחה הפיזית – לא נכלל במתודולוגיה, אך נושק לעולם אבטחת המידע ואף חופף לו בהיבטים אחדים, בהגנה ובהתקפה.

4 Maale' Hshachar St. Ramat-Gan 52383, Israel. Tel: +(972)-3-6122831, Fax: +(972)-3-6122593
http://www.see-security.com avi@see-security.com

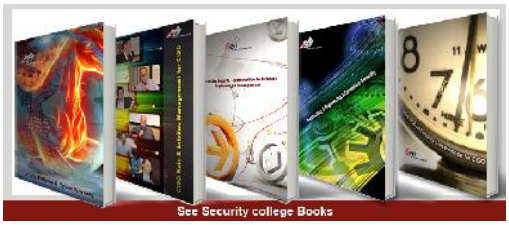
מתי
מכון התקנים הישראלי

See
see security technologies ltd
בית ספר לאבטחת מידע
וללוחמת מידע

# תכנית הלימודים

| קורסים במסלול: | שעות |
|---|---|
| 1. סדנת סקירה – **Thinking Security** – מקורות הצורך לאבטחת מידע, מושגי יסוד באבטחת מידע, האיומים ואסטרטגיות התשובה עליהם, מקצועות האבטחה, התמחויות והסמכות. | 20 |
| 2. קורס **Linux Fundamentals** - קורס Basics Linux נכלל בתוכנית. | 20 |
| 3. קורס **Hacking Techniques** - כבעולם השחמט, אין די בהכרת תפקודם של הכלים השונים. עלינו ללמוד "לשחק". הקורס מכשיר להכרת עולם הטכניקות והכלים כאחד למשימות Penetration Testing. הקורס פורט לפרוטות את האיומים הקלאסיים לנכסי המידע הנגרמים ע"י גורם אנושי זדוני. | 56 |
| 4. קורס **Architecting & Engineering Information Security** - כבעולם השחמט, יש להבין אלו כלי עזר עומדים לרשותנו, מהי מהותם וכיצד להפעילם במלחמתנו בתוקף. לימוד המהויות של כל כלי, השימושים העיקריים בהם, ושילובם במערך אבטחה יעיל. הכלים והטכניקה משלימים זה את זה כחלק מהמענה הטכנולוגי לאיומים. | 88 |
| 5. מעבדת **Windows Hardening** – תכנון ההגנה על רשתות המידע באמצעות ההגנה על רכיבי הרשת התשתיתיים, שרתים ותחנות קצה באמצעות הקשחת מערכות ההפעלה שלהם? | 20 |
| 6. סדנת **Secured development** - כיצד יש לעצב, לחייב ולפקח על מפתחי תכנה? כמחצית חורי האבטחה אינם נוגעים לתשתיות מערכת ההפעלה והתקשורת, אלא לקוד הפיתוח ולאופן יישום האפליקציה הארגונית. | 4 |
| 7. קורס **Security Governance** - תחום הארגון והשיטות של עולם אבטחת המידע, ע"פ הפרקטיקה היום-יומית: האבטחה ISC2-CISSP, ISACA-CISM, תקני ISO 27000, SOX, DoD, PCI, ועל-בסיס החקיקה בישראל והרגולציות הענפיות. | 32 |
| 8. קורס **CISO Roles & Functions** - מה עושה מנהל אבטחת המידע מדי יום? מהי רשימת משימותיו ומהו סדר הפעולות הנכון? כיצד הופך התוצר של כל פעולה לחומר גלם של הפעולה הבאה?התורה הבלתי כתובה של תפקודי ה-CISO. | 32 |
| 9. מרתון הכנה למבחן CISSP. | 8 |
| 10. עבודות: **RFP & Security Architecture Design A + B** .<br>11. עבודה: **הכנת תוכנית עבודה שנתית למחלקת אבטחת המידע**.<br>12. מבחנים נושאיים / קורסיאליים. | |

ספרות:




**הערות לתוכנית הלימודים:**

א. תוכנית הלימודים מחייבת בהכנת שיעורי בית להשגת יעדי הלימוד.
ב. נושא DB Hardening – לא כלול בתוכנית הלימודים.
ג. נושא System Hardening – לא כלול בתוכנית הלימודים.
ד. נושא טכנאות אבטחת מידע (התקנות ותחזוקה) לא כלול בתוכנית הלימודים (ראה תוכנית מתחילים)

4 Maale' Hshachar St. Ramat-Gan 52383, Israel. Tel: +(972)-3-6122831, Fax: +(972)-3-6122593
http://www.see-security.com avi@see-security.com

מתי
מכון התקנים הישראלי

See
see security technologies ltd
בית ספר לאבטחת מידע
וללוחמת מידע

# סילבוס מקוצר

## Track Overview

**Track overview**: academic requirements, Security Concepts

## Thinking Security

**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

## Linux Basics

**Understanding Linux**: History, Distributions, Kernel, File System, Shell, Live CD, VM
**Shell**: Prompt, Basic Commands, GUI
**File Systems & Networking**: Environmental Variable, Process Environment
**Shell Redirection**: Pipes, Bash Scripting
Overview & Test

## Hacking Defined

HD Introduction
**HD ToolKit**: Linux, Back Track, Development Environment, Disassembly, Hacking Today Presentations
**Low Technology Reconnaissance**: Social Engineering, Attack tree (Lio), Passive Reconnaissance
**Web base Reconnaissance**: Google, Who-Is, DNS
**Google Hacking & API**: Advanced Key-Words, Boolean Search, Google API
**Info Gathering Tools**: Maltego, Win-Finger-Print, SAM Spade
**Finger Printing**: SMTP, SNMP, DNS, Net-Bios, RPC, LDAP, HTTP, SSH, Banner Grabbing
**NetCat**: Port Scanning, Banner Grabbing, File Transfer, Bind Shell, Reverse Shell
**Port Scanners**: SL, Nmap, Super-Scan, Unicorn Scan
**Traffic Interception & Analyze**: Wire-Shark, TCP-Dump, Com-View,
**Traffic Manipulation**: Man-In The-Middle, DNS Spoofing, SSL Spoofing, Skype Spoofing
**Buffer Overflow**: Scenarios, Frameworks: Meta-Sploite
**Vulnerability Scanners & Client Side Attack**: Accunetix, Nessus, Shadow, W3F, Web & Host Scan
**SQL Injection & Wireless Hacking**: Attack Overview, SQL Ninja Priamos
**House-Keeping**: Trojan Horses, Root-Kit, Packer
Final Challenge Test

## Architecting & Engineering Information Security

**Cryptography**: Introduction to cryptography, Classic cryptography to Modern Cryptography, Basics of Modern Cryptography, Symmetric Key Algorithms, Block Ciphers Modes of Operation, Stream ciphers, Key Management, Public Key Cryptography, Message Integrity and Authentication Controls, Public Key Infrastructure:: 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, IDPS Systems Capabilities, Implementation & Management
Security Information & Event Management, Log Retention and Management, SEIM.
**Detection & Response-Lab**: Implementing a SIEM Project
**Anti-Malware**: Malware threats and Anti Malware tools
**Wireless Security**: Wireless Technologies, Vulnerabilities and Countermeasures
**VOIP**: Telephone Systems Security & VOIP, Mobile Phones & PDA (Smart Phones)
**DRP**: Disaster Recovery Technologies & planning Technologies Summery

## Windows Server 2008 Security

**Designing Security for a Windows Server 2008 Environment.** Determine Risks**.**
**Threats and Countermeasures:** Security Settings in Windows server 2008 and Windows 7.
**Determine Needs:** Enterprise Client (EC) vs. Specialized Security – Limited Functionality (SSLF)
**Security Baselines:** Security Compliance Manager
Hardening Windows Server 2008 Server Roles

מתי
מכון התקנים הישראלי

See
see security technologies ltd
בית ספר לאבטחת מידע
וללוחמת מידע

## The CISO Role

**The Evolving CISO Role**

**Legal & Regulatory**: The Applicable Legislation, The privacy Act, Information reservoirs Registration & Protection, The Regulation, 357, 257, SOX & iSOX, BASEL II, HIPPA

**Risk Assessment**: Risk Management Fundamentals, Risk Assessment, Qualitative and Quantitative Assessment, The Hybrid Approach, Asset Management, MSAT, Identifying Asset Vulnerability, Formalizing Risk Statement, Prioritizing Risk, Stating Solutions

**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

**InfoSec Processes**: InfoSec Process & Process Catalogue, Process & Program maturity

**Governance, Strategic plan**: Corporate Governance Defined, InfoSec Governance, 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

**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

**SOC & Incident Response**: SOC Operation, Incident response methodology

**BCM - Business Continuity Management**: BCM Planning, COOP, CCP, ORP, ITCP, CIP, BRP, DRP, DRP Project

**Program Audit & Maintenance**: Internal Audit Defined, IT General Audit, Infosec Audit, Program Improvement, Pen tests

**Relationship & Communication**: Implementing a Security & Awareness Program - Creating & Implementing a Security Marketing Plan

**Putting it all Together:** The New CISO 1st Year Timeline, from Security Projects to Security Program

## CISSP

- Reporting Models, Computer ethics
- Physical (Environmental) Security
- Operation Security
- TEST Marathon

## סגל הוראה:

See Security Academic Staff

4 Maale' Hshachar St. Ramat-Gan 52383, Israel. Tel: +(972)-3-6122831, Fax: +(972)-3-6122593
http://www.see-security.com avi@see-security.com

מתי
מכון התקנים הישראלי

See
see security technologies ltd
בית ספר לאבטחת מידע
וללוחמת מידע

לכבוד
בית הספר לאבטחת מידע וללוחמת מידע
שיא סקיוריטי טכנולוג'יז בע"מ
רמת-גן – פקס: 03-6122593

**נא לרשום אותי לתוכנית הלימודים ברמת גן**

# מנהלי ומהנדסי אבטחת מידע - CISO

**פרטים אישיים:**

שם משפחה _____ שם פרטי _____ ת.ז._____ שנת לידה _____

כתובת פרטית _____.

טל' בבית:_____ טל' נייד_____פקס_____ .

כתובת E –mail _____.

**מקום עבודה:**

שם החברה_____טל' _____ תפקיד_____.

**לתשלום (נא סמן בחירתך):**

☐ 400 ₪ - דמי רישום (חובה בכל מקרה) ☐ _____ ₪ - מקדמה (בגובה 10% משכר הלימוד)

☐ שכר לימוד בסך _____₪

☐ מצ"ב שיק מס' _____ע"ס _____ ₪ (ניתן לשלם עד ____תשלומים בהמחאות דחויות)

**(את ההמחאות יש לרשום לפקודת שיא סקיוריטי בע"מ)**

☐ מצ"ב מכתב התחייבות המעסיק, אם הינך ממומן על ידו. (1) יודפס ע"ג נייר לוגו (2) בציון מספר ח.פ של החברה, (3) לתשלום שוטף + 30 ממועד הפתיחה לכל היותר)

☐ נא לחייב כרטיס אשראי ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ בתוקף עד ☐☐☐☐

☐ בתשלום אחד

☐ ב- _____ תשלומים (עד 18 תשלומים בקרדיט).

☐ ב- _____תשלומים ללא ריבית.

שם בעל הכרטיס _____ ת.ז. בעל הכרטיס _____תא' לידה של בעל הכרטיס _____.

כתובת בעל הכרטיס, המעודכנת בחברת האשראי _____.

טלפון בעל הכרטיס, המעודכן בחב' כרטיסי האשראי _____ .

שם בנק+סניף הבנק בו מנוהל חשבון כרטיס האשראי _____ .

- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי המכון וSee Security.
- דמי ההרשמה אינם כלולים בשכר הלימוד.
- יש לוודא כי התשלומים יסתיימו עד למועד סיום הקורס.

תאריך: _____ חתימה:_____.

4 Maale' Hshachar St. Ramat-Gan 52383, Israel. Tel: +(972)-3-6122831, Fax: +(972)-3-6122593
http://www.see-security.com avi@see-security.com