CSTP. CYBER SECURITY TECHNOLOGY PROFESSIONAL

התכנית להכשרה ולהסמכת מומחי טכנולוגיות הגנת סייבר

פתיחה: ראה עמוד הבית באתר המכללה

תכנית לימוד חצי-שנתית המיועדת למנהלי תשתיות, למפתחים ולמנהלי מערכות מידע המעוניינים להתמחות בהנדסה, ארכיטקטורה ובניהול יחידות סייבר, לתפקידי יעוץ טכנולוגי להגנת סייבר (ארכיטקט הגנת סייבר)

מבוא

מכללת See Security יצרה את תכנית הלימודים CISO הראשונה בעולם בשנים 2004-2005, והחלק הראשון מבין השניים שבה, הוא המסלול להכשרת מומחים לטכנולוגיות הגנת סייבר CSTP. התכנית עוקבת בקפידה אחר הוראות מטה הסייבר מחד, ומאידך - אחר צרכי משרד הביטחון, דרישות הארגונים הבינלאומיים (ISC)^2, ו- ISACA, ומתעדכנת ללא הרף, בליווי חומרי הלימוד העדכניים ביותר על-מנת לעמוד בדרישות הרגולציה בישראל ולצלוח את המבחנים להסמכות הבינלאומיות הנדירות.

הדרישה ההולכת וגוברת לארכיטקטים-יועצים ולמנהלי הגנת סייבר משכילים ובעלי ידע, מחייבת רקע רחב ועמוק במיוחד, במסגרת מתודולוגית סדורה אשר תאפשר השתלטות על המידע הרב, וזו מהות המסלול. מטה הסייבר הלאומי פרסם בינואר 2015 רשימה רשמית למקצועות ליבה, ובהם: מיישם הגנת סייבר (CSP: Cyber Security Practitioner), **מומחה טכנולוגיות הגנת סייבר (CSTP: Cyber Security Technology Professional)**, מומחה מתודולוגיות הגנת סייבר (CSMP: Cyber Security Methodology Professional), מומחה בדיקות חדירות (Hacker/Penetration Tester), ומומחה חקירות (Forensics). תפקיד מנהל הגנת הסייבר נובע ממקצועות CSTP ו- CSMP. גם משרד הגנה של ארה"ב (DoD) פרסם ב- 2004 הוראה מס' 8570.1 בנושא: "הדרכת סייבר, הסמכה וניהול כוח אדם". ההוראה מחייבת כי כל בעל מקצוע טכני או מינהלי בסייבר יוכשר ויוסמך בהתאם לתקן ברור, על-מנת לאפשר הגנה יעילה על מידע, מערכות מידע ותשתיות מידע של DoD, והגדיר קבוצות של מקצועות, ורמות בכירות שונות. [הוראה 8570.1].

מאפייני תכנית הלימודים	
קהל:	מנהלים / סביבתיים / **מקצוענים**
אוריינטציה:	**מנהלית**/ **טכנית-הנדסית**
שלב:	מתחילים / **מתקדמים**
רוחב:	ממוקד / **רחב**
עומק:	סוקר / **עמוק**
הסמכות:	**CSTP, CompTIA Security+, (ISC)^2-SSCP,** and partial: **CISSP**
שעות כיתה ותרגול:	**180 שעות כיתה ו-220 שעות משימות חובה. סה"כ 400 שעות.**
מתכונת:	**45 מפגשי ערב, כ- 6 חודשים**

מטרת התכנית

תכנית הלימודים היוקרתית CSTP נועדה להכשיר מומחי הגנת סייבר המסוגלים לייעץ, להנחות ולקבל החלטות במשימות הגנת המידע, בתחום הטכנולוגי-טקטי, ללא התחום המינהלי-מימשלי. היכולת תירכש מתוך היכרות עמוקה עם האסטרטגיות, הטקטיקות, הטכניקות, והוראות העבודה הנהוגות (Best Practice) בתחומים אלו, לרבות הכרת תורת התקיפה והמודיעין. יכולת זו תוקנה לתלמיד בתכנית הלימודים באמצעות הרצאות, התנסויות ותרגול רב.

לצד הידע המקצועי, פועלת התכנית להקניית הסמכות בינלאומיות מבוקשות: (א) הסמכת (ISC)^2-SSCP, הסמכת CompTIA Security+, ולחלק הארי בהסמכת CISSP.

קורס ניהול הגנת סייבר CSTP עוסק בדרגות האסטרטגיות ומשלב את הידע והדיסציפלינות הנדרשות למומחה ולארכיטקט. המסלול יקנה לבוגר את היכולת להתמודד עם תפקיד ארכיטקט הגנת סייבר, יקנה יכולת לתכנן מערך הגנת סייבר, לבחור את הרכיבים הנכונים, ליישמו בטכניקה נבחרת, לעקוב ולנטר אירועים, לנתח ולהבין אירועים, להגיב באופן מיידי והולם לאירועים, וליזום "סדר" בפעילויות הגנת הסייבר הארגוניות. יעדי התכנית: התמחות גבוהה בעולם הסייבר וקבלת אחריות מקצועית בתחום הסיכונים העסקיים, ותשתית הולמת למבחני ההסמכה אלו.

CSTP. CYBER SECURITY TECHNOLOGY PROFESSIONAL

קהל יעד

בעלי ידע מעשי בתחום התשתיות (מערכות הפעלה ותקשורת, ורצוי ידע בסיסי בכלי אבטחה בסיסיים) וכן בוגרי תואר ראשון או שני במדעי המחשב, הנדסת תוכנה\חומרה. המסלול איננו מתאים למתחילים.

תעודה

התכנית נבנתה לצרכי ידע מעשי, ומשמשת כהכנה למבחני **Security+**, **(ISC)²-SSCP**, מבחן **CCSK** וחלקית גם למבחני **CISSP**. לעומדים בדרישות התכנית, תוענק תעודה מטעם See-Security:

"מומחה טכנולוגיות הגנת סייבר (ארכיטקט)"

Cyber Security Technology Professional

מי שאינם עומדים בדרישות יהיו זכאים לתעודת השתתפות, ולהשלמת מחויבויותיהם (השתתפות חוזרת / עבודות ומשימות) ללא תשלום.

2005 – 2016:
עשור של הובלה לאומית

ב- 2004 התקבלה בקשה של גוף ממלכתי, לעצב, לתכנן וליישם מערך הכשרה ייחודי ליועצי ארכיטקטורת סייבר, המשולבת בתכנית ליועצי מינהל וממשל סייבר.

התכנית קרמה עור וגידים בסיועם של מובילים בעולם אבטחת המידע והסייבר במגזר העסקי והממלכתי, ומחזור מס' 1' הושק ב- 2005.
במקביל וללא כל קשר, הוגדרו מקצועות הסייבר ותכניהם, בתחילה על-ידי הפורום הישראלי לאבטחת מידע IFIS בראשותם של האלוף (מיל') וראש המועצה לביטחון לאומי (לשעבר) יעקב עמידרור ושל אבי ויסמן, ובהנחייתו המקצועית של איתי ינובסקי, ובהמשך, על ידי מטה הסייבר הלאומי, בינואר 2015.

המטרה: מקצוע
(ולא "קורס")

בוגרי מסלול CSTP מצוידים בידע מעמיק מאוד בתחומי הארכיטקטורה, והאיומים בניהול הגנת סייבר.

ידע זה חיובי לתפקיד היועץ (ברמות הגבוהות). מהיותו ברבות השנים סטנדרט דה-פקטו בתעשייה הישראלית, אין כיום בישראל חברת יעוץ בינונית או גדולה ללא בוגרים של מסלול זה. מתוך 200 הארגונים הגדולים בישראל, משובצים בוגרי המסלול בכ- 170 מהם.

הכרה

תכנית CSTE הינה החלק הארי מהתכנית המקורית שעוצבה ונבנתה עבור משהב"ט ב- 2004, על-בסיס ההחלטות הרשמיות של המטה הקיברנטי הלאומי מינואר 2015, ומוערכת מאוד בישראל בקרב המעסיקים והמומחים. מומלץ גם להשלים ידע להסמכת CISSP הבכירה מסוגה בעולם, הנפוצה בקרב השכבה הבכירה, ומוכרת באופן רישמי במסגרת הוראה 8570.1 של משרד ההגנה האמריקאי DoD לקטגוריה הבכירה ביותר IAT level III וגם IAM level III.

להלן הגדרות מטה הסייבר הלאומי למקצוע מומחה טכנולוגיות הגנת סייבר:

מהות המקצוע

אדם בעל רקע אקדמי, העמקה מקצועית וידע תיאורטי מקיף, האחראי על ההיבטים:

1. תכנון מענה טכנולוגי להגנת סייבר בארגון, תוך שילוב טכנולוגיות ושיטות אבטחה.
2. התאמת מוצרי הגנה ושילובם בתשתיות המחשוב לרבות מערכי אחסון ושיטות גיבוי.
3. ליווי הטיפול באירועי אבטחה בהיבט הטכנולוגי.

זאת תוך הכרת והבנת הפעילות, הצרכים והמטרות הארגונית.

ידע מקצועי נדרש

1. ידע ברמת "מבואות" בעולם הסייבר:
   א. מונחים.
   ב. איומים.
   ג. סוגי יריבים והמוטיבציות שלהם.
   ד. סוגי תקיפות (תקיפת מחשב מרחוק/מתוך הארגון, חדירה פיזית למתחמי מחשב, Social Engineering).
   ו. משמעויות (כלכליות, מוניטין, משמעויות מעבר לרמת הארגון).
   ז. דרכי התמודדות ארגוניות (מינוי בעלי תפקידים, הגדרת מדיניות ונהלים, הגדרת נכסי מידע ומערכות חיוניות, ניהול סיכונים, אבטחה פיזית, המרכיב האנושי ומהימנות עובדים, מודעות, הטמעה בתרבות הארגונית, דיווחים ובקרות).

ז'בוטינסקי 1, בית הדר-די מול קומה 1', רמת-גן – 5252242, טל': 03-6122831, 03-5799555, 054-5222305, פקס: 03-6122593
www.see-security.com avi@see-security.com

CSTP. CYBER SECURITY TECHNOLOGY PROFESSIONAL

ה. סוגי פגיעות במערכות/במידע (היבטי זמינות, אמינות, סודיות). ח. גופים לאומיים העוסקים בתחום בישראל.

2. מבוא לרגולציה ישראלית

ידע בסיסי בחוקים, החלטות ממשלה, תקינה ואסדרה בנושאי הגנת סייבר, אבטחת מידע ופרטיות הנהוגים בישראל.

3. דרישות טכנולוגיות בסייבר

הכרות ברמת "מבואות" עם מוצרים ושיטות אבטחה מקובלות, כולל הטכנולוגיה, אופן היישום, קונפיגורציה, עדכוני תוכנה וחומרה, דרכי התחזוקה ודרכי הניהול.

4. שליטה בתהליכי האבטחה השגרתיים בארגון:

הכרות ברמת "מבואות" עם מונחים, ניהול חשבונות והרשאות, סיסמאות, גישת משתמשים, ניהול גיבויים, עדכונים.

5. תכנון מענה טכנולוגי להגנת סייבר בארגון:
   א. טופולוגיה / ארכיטקטורה תשתיתית מאובטחת.
   ב. תכנון מערכים אפליקטיביים ומערכי WEB מאובטחים.
6. מוצרי הגנה:
   א. הכרת מגוון מוצרי הגנה וחלוקתם למשפחות.
   ב. השוואה בין מוצרים בהתאם לצרכי הארגון.
   ג. השפעת הטמעת המוצרים על הארגון ועל מערכי המיחשוב שלו.
7. תקינה טכנולוגית:

לרבות הכרת Protection Profiles ורמות הסמכה (EAL) של Common Criteria.

8. אחסון:

מערכות אחסון ושיטות גיבוי ושחזור של מידע.

9. קריפטוגרפיה:

א. שיטות קריפטוגרפיות נפוצות (אלגוריתמים סימטריים וא-סימטריים).
ב. PKI.
ג. CA (Certificate Authority).
ד. Challenge Response.
ה. Digital Signatures.
ו. Hash function.
ז. סטגנוגרפיה.

10. אתיקה מקצועית.

עד כאן: הגדרות מטה הסייבר הלאומי

תנאי קבלה

- רקע קודם בניהול רשתות Windows או Linux או בסייבר או בפיתוח תכנה. נדרשת הכרת Windows, Linux, TCP/IP, Web.
- נכונות לעבודה עצמית מונחית רבת היקף (כ- 320 שעות לימוד ביתי).
- ראיון אישי.

מטלות תכנית הלימודים

- קיימת חובת נוכחות ב-80% מהמפגשים.
- כל מודול נלמד מחייב עמידה במבחן פנימי ו/או בעבודות בציון 70 לפחות. קיים מועד נוסף לנכשלים/נעדרים.
- בנושאים הטכניים - תרגול (Hands-on) בכיתה (מעבדת מחשבים).

CSTP. CYBER SECURITY TECHNOLOGY PROFESSIONAL

מתכונת הלימודים

משך התכנית כ- 180 שעות, במתכונת של 44 מפגשי ערב (כ-6 חודשים), וכן כ- 230 שעות משימות אישיות. הלימודים מתקיימים בקמפוס See Security ברמת-גן. המסלול נפתח כ- 3 פעמים בשנה.

עלות הלימודים

סך 15,400 ₪ + 400 ₪ דמי רישום (כולל מע"מ)

המרצים בתכנית

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

הערות

- 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.
- ייתכנו שינויים במערך התכנית, במועדי הלימודים והבחינות או בכל נושא אחר. הודעה על כל שינוי תימסר למשתתפים.

מידע נוסף

- **מידע מינהלי:** אלוירה אליסייב, 03-6122831, 052-8787889, elvira@see-security.com.
- **יועץ אקדמי:** אבי ויסמן, 054-5222305, avi@see-security.com

מתודולוגיה

המסלול נבנה על-בסיס פדגוגי ודידקטי ואוריינטציה פרקטית, בראייה של בעלי מקצוע שונים ורמות בכירות שונות. הדגשים נשענים על הנחיות מטה הסייבר הישראלי, הפורום הישראלי לאבטחת מידע IFIS, המלצות ה- DoD (US Department of Defense), והכרה בארגונים בעלי אתיקה דומה (ISC2, ISACA, GIAC, ISSA, SII). המתודולוגיה המתוארת מתבססת על רשימת כל המקצועות התעסוקתיים המקובלים בתעשיית אבטחת המידע ולוחמת המידע, ומולם – כל תחומי הידע הקיימים

CSTP. CYBER SECURITY TECHNOLOGY PROFESSIONAL

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 ליבה בעולם הסייבר

מקצוע	ר"ת	Profession	התייחסות DoD	הסמכות נפוצות	הסמכות יצרנים
מיישם מערכות סייבר	**CSP**	Cyber Security Practitioner	IAT level-I & II	Security+, (ISC)² SSCP	CCNA, CCNE, CCSA, CCSE etc.
מומחה טכנולוגיות – ארכיטקט סייבר	**CSTP**	Cyber Security Technology Professional	IAT level-II & III	Security+, (ISC)² SSCP (ISC)² CISSP	CISO, ISSA
מומחה מתודולוגיות סייבר	**CSMP**	Cyber Security Methodology Professional	IAM level I & II & III	Security+, (ISC)² CISSP, CISM	CISO, GRCM
מנהל סייבר ארגוני	**CISO**	Chief Information Security Officer	IAT level-III & IAM level III	(ISC)² CISSP, CISM, CASP	CISO
מומחה מבדקי חדירה	**CSPTE**	Cyber Security Penetration Testing Expert	IAT level-III	CEH	HDE for CEH

תכנית הלימודים

16 שעות

Thinking Security

פרק הכניסה לעולם האמיתי של אבטחת המידע דן במקורות הצורך לסייבר, מושגי יסוד בסייבר, האיומים ואסטרטגיות המענה הנהוגות בעולם עליהם, במקצועות האבטחה, בהתמחויות והסמכות, ובסקירת הנושאים הנלמדים בתכנית כולה, על-מנת לקבל תמונה כוללת של האתגר.

- **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

108 שעות

Cyber Technologies: Tools, Technologies, Techniques & Architecture

כבעולם השחמט, יש להבין אלו כלי עזר עומדים לרשותנו, מהי מהותם, איזה פונקציות הם ממלאים וכיצד להפעילם במשולב עם כלים אחרים וטכניקה נכונה, לימוד המהויות של כל כלי, השימושים העיקריים בהם, ושילובם במערך אבטחה יעיל. הכלים והטכניקה משלימים זה את זה כחלק מהמענה הטכנולוגי לאיומים, בשכבת מערכות ההפעלה, התקשורת, היישומים, הסביבות המיוחדות כמו ענן וניידים, ותחנות הקצה.

- **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 Capabilities, Implementation & Management, Security Information & Event Management, Log Retention and Management, SEIM.
- **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

ז'בוטינסקי 1, בית הדר-די מול קומה 1', רמת-גן – 5252242, טל': 03-6122831, 03-5799555, 054-5222305, פקס: 03-6122593
www.see-security.com avi@see-security.com

CSTP. CYBER SECURITY TECHNOLOGY PROFESSIONAL

- (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
- Infosec Technologies Trends
- **Information Technologies Architecture**: Security Architecture creation methodologies
- Technologies **Summary**

Independent Project: InfoSec Architecture for xyz Organization

הסטודנטים מתבקשים לכתוב פרויקט המסכם את הידע הנרכש בפרק הטכנולוגיות והארכיטקטורה, על-בסיס המתודולוגיות שנלמדו, בדגש על התמודדות עם אתגרים מהעולם האמיתי. התהליך הפרויקטלי מבוצע באינטראקציה קבועה עם סגל המכללה (סיוע ותמיכה).

24 שעות

Incident Response

הסטודנטים מתבקשים לכתוב פרויקט המסכם את הידע הנרכש CISO Function, לרבות משמעויות הנובעות מפרק ממשל סייבר וניהול תהליכי סייבר, ובהתבסס על הידע שנרכש בפרק הטכנולוגיות והארכיטקטורה.

- **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

יום אימון Incident Response במתקן האימונים של CyberGym וחברת חשמל בחפציבה (חדרה), הכולל תרגול אמת של תגובה לאירועי Cyber המוזרמים על-ידי מדריכי המתקן.

Hacking Defined Advanced

כבעולם השחמט, אין די בהכרת תפקודם של הכלים השונים. עלינו ללמוד "לשחק". לא תתקיים הבנה של דרכי ההגנה ללא הכרה של דרכי התוקף. הקורס מכשיר להכרת עולם הטכניקות והכלים כאחד למשימות Penetration Testing. הקורס פורט לפרוטות את האיומים הקלאסיים לנכסי המידע הנגרמים ע"י גורם אנושי זדוני. עולם התקיפה והמודיעין נלמד על-מנת להכיר את האיומים, הפגיעויות, הטכניקות, הטקטיקות והטכנולוגיות המשמשות את התוקף.

32 שעות

- **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
- 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**

ז'בוטינסקי 1, בית הדר-די מול קומה 1', רמת-גן – 5252242, טל': 03-6122831, 03-5799555, 054-5222305, פקס: 03-6122593
www.see-security.com avi@see-security.com

לכבוד
המכללה לסייבר
שיא סקיוריטי טכנולוג'יז בע"מ
רמת-גן – פקס: 03-6122593

נא לרשום אותי לתכנית הלימודים ברמת גן

מומחה טכנולוגיות הגנת סייבר - CSTP

<u>פרטים אישיים:</u>

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

כתובת פרטית _____.

טל' בבית:_____ טל' נייד_____פקס_____ .

כתובת E –mail _____.

<u>מקום עבודה:</u>

שם החברה_____טל' _____ תפקיד_____.

<u>לתשלום (נא סמן בחירתך):</u>

☐ 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 See Security.
- דמי ההרשמה אינם כלולים בשכר הלימוד.
- יש לוודא כי התשלומים יסתיימו עד למועד סיום הקורס.

תאריך: _____ חתימה:_____.