מומחה מתודולוגיות הגנת סייבר

למינהל ולממשל הגנת סייבר

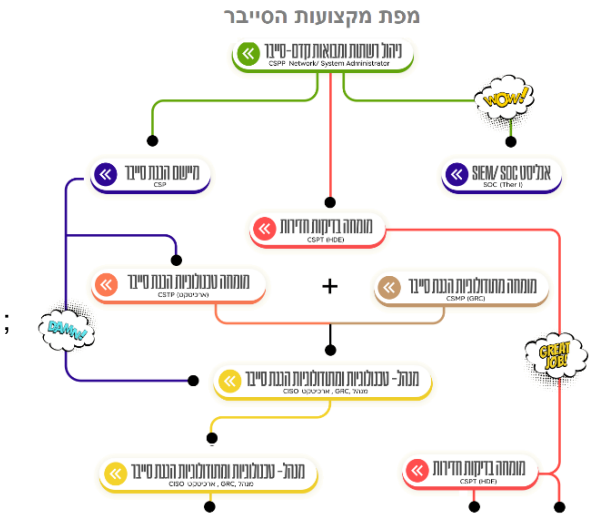
CSMP: CYBER SECURITY METHODOLOGY PROFESSIONAL

על-פי מערך הסייבר הלאומי

(אסדרת מקצועות הסייבר בישראל)

https://www.gov.il/he/Departments/israel_national_cyber_directorate

תכנית CSMP מבינה למקצוע מומחה מתודולוגיות הגנת סייבר במוגדר ע"י מערך הסייבר, לרבות הכנה למבחן לקבלת תעודה רשמית של מערך הסייבר הלאומי. עבור בעלי בסיס טכנולוגי חזק, כולל קורס זה גם הכנה להסמכה CISSP ונמוכות ממנה (כאופציה).



להיות מומחה מתודולוגיות הגנת סייבר.

מומחה מתודולוגיות: אחראי על גיבוש, אפיון ומימוש תפיסות, שיטות ומתודולוגיות, הטמעת אסדרה ותקינה ישראלית ובינלאומית והיבטי הגנת הפרטיות, ניהול סיכונים, ליווי תהליכים ארגוניים, זאת תוך הכרת והבנת הפעילות, הצרכים והמטרות הארגונית, הכל- לצורך הגנת הסייבר בארגון.

התקנים הבינלאומיים הפכו להיות הפקטור החשוב ביותר למנהל עסקים ולניהול סיכונים!

וְלֹא פָּחוֹת חָשׁוּב: נִלְמָד כְּפִי שֶׁרַק שִׂיא סֶקְיוּרִיטִי יוֹדַעַת לְלַמֵּד **נכון**, וְעִם **הַלֵּב**.

התוכנית להכשרת מומחי מתודולוגיה למינהל ולממשל הגנת סייבר:
CSMP: Cyber Security Methodology Professional

התוכנית נבנתה בהתאמה לרגולציה של מערך הסייבר הלאומי (אסדרת מקצועות הסייבר בישראל)

אודות המכללה

מכללת See Security הנה מכללה **בינלאומית** התמחותית למקצועות ניהול רשתות וסייבר, אחת מ- 7 מכללות מסוגה בעולם ומהמוערכות שבהן, ועוסקת בלעדית בתחום זה בכל זמנה, במתודולוגית הדרכה שנבנתה עבור גורמים ממלכתיים.

המכללה מייצאת את תכניות הלימודים לכל רחבי העולם, באמצעות המותג *See Security International*, ובאמצעות גופי סייבר ישראליים ידועי-שם העוסקים ביצוא בטחוני.

מנהל הקבוצה שבה משולבת המכללה, מר אבי ויסמן, הינו ממובילי ענף הסייבר, יועץ לממשלת ישראל בנושא "אסדרת מקצועות הגנת הסייבר" בישראל, פרשן בערוצי השידור בארץ ובחו"ל, מקימו של הפורום הלאומי לאבטחת מידע IFIS יחד עם האלוף במיל' וראש המל"ל לשעבר, יעקב עמידרור, מנכ"ל משותף בחברה להשמת כוח אדם בענף הסייבר - *SeeHR*, בחברה לייעוץ *See Consulting – Cyber*, בחברה לפתרונות Managed SEIM/SOC – *See Events*, ובמכללה הבינלאומית לסייבר *See Security College International*.

אודות מערך הסייבר הלאומי: רגולציה רשמית למקצועות הסייבר בישראל

המערך אשר פועל במשרד ראש הממשלה כיחידה עצמאית, החליט להפעיל אסדרה (רגולציה) מחייבת בנושא הגדרתם של המקצועות השונים בעולם הסייבר, ומפעיל המלצות ברורות בנוגע לתכני הידע לכל מקצוע, וזאת, על מנת להפסיק את הכאוס הקיים בלימודים במוסדות מסחריים.

אודות תכנית CSMP להכשרת מומחה מתודולוגיות הגנה

מכללת See Security יצרה את תכנית הלימודים CISO הראשונה בעולם בשנים 2004-2005. התכנית עוקבת בקפידה אחר הוראות מערך הסייבר הלאומי מחד, ומאידך - אחר צרכי משרד הביטחון, דרישות הארגונים הבינלאומיים (ISC)[2], ISACA, CSA ו- ISO 27001, ומתעדכנת ללא הרף, בליווי חומרי הלימוד העדכניים ביותר על-מנת לצלוח את המבחנים להסמכות הבינלאומיות.

מאפייני תוכנית הלימודים	
עלות:	**קורס CSMP ללא CISSP: 7,100 ₪ + 400 ₪ דמי רישום (כולל מע"מ).** **קורס CSMP כולל מרתון CISSP: 13,600 ₪ + 400 ₪ דמי רישום**
קהל:	מנהלים / סביבתיים / **מקצוענים**
אוריינטציה:	מנהלית/ **טכנית / יישום**
מטרה:	הכשרת יועצי אבטחת מידע איכותיים, עתירי ידע לתפקידי יעוץ טכני, מינהלי ומימשלי באבטחת מידע, לצד הקניית בסיס איכותי למבחן CISSP הבינלאומי.
שלב:	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.
רוחב:	ממוקד / **רחב**
עומק:	סוקר / **עמוק**
הסמכות:	**CISSP, CISM, מומחה טכנולוגיות הגנת סייבר-ארכיטקט (מערך הסייבר), מומחה מתודולוגיות הגנת סייבר (מערך הסייבר),**
שעות:	**88 שעות**
פתיחה:	ראה בעמוד הראשי של המכללה
מתכונת:	הלימודים בקמפוס המכללה ברמת גן, מתקיימים פעמיים בשבוע בימי בערב: 17:30 עד 21:00 (4 שעות אקדמיות למפגש), במשך כ-3 חודשים
תרגול בית:	**בהיקף 100 שעות**

מערך 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). 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.

מטרת התכנית

תכנית הלימודים היוקרתית CSMP נועדה להכשיר מומחי הגנת סייבר המסוגלים לייעץ, להנחות ולקבל החלטות במשימות הגנת המידע, התחום המנהלי - ממשלי, ללא התחום הטכנולוגי-טקטי. היכולת תירכש מתוך היכרות עמוקה עם התקנים הבינלאומיים, הלאומיים, המגזריים והעסקיים, הכרת שיטות לקביעת מדיניות ארגונית, נהלים, והוראות העבודה הנהוגות (Best Practice) בתחומים אלו, לרבות טכניקות ניהול. יכולת זו תוקנה לתלמיד בתכנית הלימודים באמצעות הרצאות, התנסויות ותרגול רב.

לצד הידע המקצועי, פועלת התכנית להקניית הסמכת ISO 27001 Lead Auditor, ולחלק בהסמכת CISSP.

סגנון לימודי

מינהלי, תיאורטי ומשימות המאפיינות את עולם המתודולוגיות: תקנים, רגולציות, ניהול סיכונים וניהול סייבר.

עלות

קורס CSMP ללא CISSP בעלות של 7,100 ₪ + 400 ₪ דמי רישום (כולל מע"מ)*[1].

קורס CSMP כולל CISSP - מרתון רשמי של (ISC)[2] בעלות של 13,600 ₪ + 400 ₪ דמי רישום

*[1] המחיר למסלול CISO המלא – 19,500 ו- 400 שח דמי רישום.

קהל יעד

הקורס מיועד לבעלי רקע בתחום התשתיות, או לבעלי רקע בפיתוח, בעלי רקע ארגוני.. [ראה בסוף המסמך: מפת התפתחות מקצועית בענף הסייבר].

דרישות סף

- רקע ארגוני.
- רצוי רקע באבטחת מידע / IT.
- אנגלית ברמה טובה.
- ראיון אישי לבחינת ההתאמה לתכנית.

או:

- תואר אקדמי*
- ראיון אישי לבחינת ההתאמה לתכנית.

* לצורך פטור נדרשת החלטת ועדת חריגים בראשות המנהל האקדמי של התכנית.

מתכונת הלימודים

משך התכנית (לא כולל CISSP) כ- 84 שעות כיתה ו- 200 שעות משימות, במתכונת של 26 מפגשים, פעמיים בשבוע בערב בשעות 17:30 עד 21:00 במשך כ- 4 חודשים, 4 שעות אקדמיות למפגש. הלימודים מתקיימים בקמפוס See Security ברמת-גן (צמוד לתחנת רכבת מרכז). המסלול נפתח כ- 3 פעמים בשנה.

למידע נוסף / פגישת יעוץ:

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

יועץ אקדמי: אבי ויסמן, 03-6122831, 054-5222305, avi@see-security.com

חובות אקדמיות

- 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.

זכאות לתעודה והסמכות בינלאומיות

לעומדים בדרישות, תוענק תעודה מטעם See-Security:

"מומחה מתודולוגיות הגנת סייבר - CSMP".

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

בבוונת מערך הסייבר למסד בעתיד גם מבחן מטעמה להסמכה ייחודית בישראל, על-בסיס תכנים אלו.

לתשומת ליבך!

תהליך הייעוץ והסינון של היועץ האקדמי משמעותי לבחינת סיכוייך להצליח במסלול זה ו/או במסלולים אחרים, ובעתידך התעסוקתי בכלל.

כיצד נבנה המוניטין של המכללה?

מנקודת המבט של הנהלת המכללה, תלמיד מצליח אך ורק אם הצליח להשתלב אצל מעסיק בתפקיד רלוונטי. לכן הגדרת תכני הקורס נבנתה בהתאם לדרישת המעסיקים.

המעסיק דורש ומצפה כי בוגר של מכללה ייעודית לסייבר כמו See Security יגיע בוגר יותר, עשיר יותר ובעל ידע רב תחומי, ויחזיק ברשותו גם הסמכה בינלאומית מוכרת באופן רשמי.

"המתחרה" של המועמד איננו המעסיק. להיפך: הוא מבקש את הטוב ביותר לעצמו. כאשר הוא מבקש לקלוט מועמד של מכללה מקצועית-ייעודית, הוא מצפה לפחות שיהיה בעל ידע רב יותר ממועמד המגיע מחברות אחרות המשווקות קורסים.

מה אנחנו מצפים מבוגר התכנית?

אנו ממליצים כי תבקש פגישת יעוץ עם אבי ויסמן, בין אם הנך משדרג מעמדך מעולם ה-IT, ובין אם הנך מבקש ליזום הסבה מקצועית.

סגל המרצים

תכנית לימודים כל-כך מולטי-דיסציפלינארית ובכירה, מחייבת שימוש נרחב ובלתי מתפשר במומחים יעודיים, איש לתחומו. על המרצים נמנים מובילי הענף, בהם: מנהלי סייבר ידועי שם, ומומחים מקצועיים המובילים בתחומם. כמדינה הנוטלת על עצמה להוביל את הגנת הסייבר בעולם, רואה עצמה המכללה מחויבת לדרישות גבוהות ולסטנדרט גבוה מאוד של מרצים.

עובד משרד הבטחון / צה"ל / משרד ראש הממשלה / מערך הסייבר / מערך הסייבר / בוגר מכללת שיא סקיוריטי

בדוק עם הנהלת המכללה דרכי ההרשמה ומחירי משהב"ט/ראה"מ לגבי המסלול.

הערות

- ההרשמה לכל מבחן חיצוני, הנה בתשלום ותבוצע באחריות הסטודנט בלבד.
- פתיחת כל תכנית מותנית במספר הנרשמים.
- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי המכללה.
- המכללה מביאה לידיעת הנרשמים והסטודנטים כי ייתכנו שינויים במערך התכנית, במועדי הלימוד והבחינות או בכל נושא אחר. הודעה על שינוי תימסר למשתתפים.

CSMP: CYBER SECURITY METHODOLOGY PROFESSIONAL

המכללה ללימודי מקצועות הסייבר

The Regulation for Cyber Security Professions

Cyber Security Professions

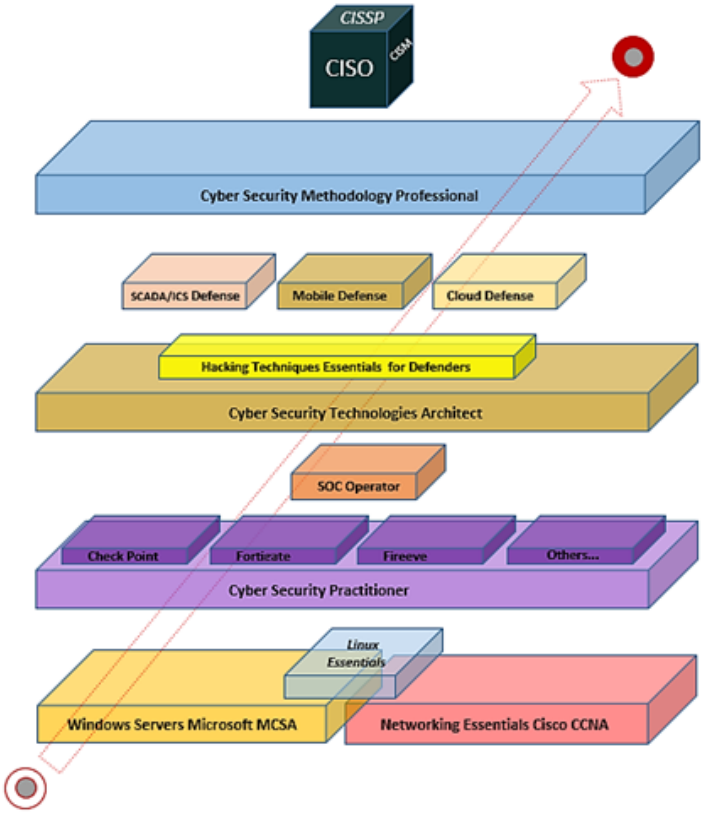
ה- CISO (Chief Information Security Officer), הוא מנהל הגנת הסייבר בארגון, בתפקידו משלבאת הידע של ארכיטקט\טורת הגנת סייבר, מתודולוגיות הגנת סייבר, והבנה ארגונית כללית (כלכלה / תעשיה, ניהול,

CSMP (Cyber Security - מתודולוגיות הגנת סייבר (Methodology Professional, יוצק לתבנית ההגנה הטכנולוגית חוקים, כללים, הוראות עבודה, על מנת לקיים בו בזמן את חוקי התברה, המדינה, ולמנוע את ההגנה. המומחה יהיה בעל רקע אקדמי, האחראי על: (א) גיבוש, אסיון ומימוש תפיסות, שיטות ומתודולוגיות להגנת הסייבר בארגון, (ב) הטמעת היבטי אסדרה ותקינה ישראלית ובינלאומית והיבטי הגנת הפרטיות, (ג) ניהול סיכונים, (ד) ליווי תהליכים ארגוניים בסייבר (ליווי הקמת מערכות, פרויקטים, שרשרת האספקה, המשכיות עסקית.), זאת תוך הכרת והבנת הפעילות, הצרכים והמטרות הארגונית.

מומחים בעלי התמחות בנגזרת טכנולוגית, מתבססים על לימודי ארכיטקטורה, ומאפשרים ידע מעמיק בנגזרת המקצועית בה הם מתמחים. בדרך-כלל, המקצועיות משלבת ידע דואלי - בארכיטקטורה הטכנולוגית של התחום הספציפי (ענף הניידים / התעשייה וכו'), לצד הידע של ארכיטקטורת הגנת סייבר.

הארכיטקט ("מומחה טכנולוגיות הגנת סייבר") CSTP (Cyber Security - Technology Professional), הוא "הראש" שמאחורי ההגנה על המידע. הוא-הוא שיעמוד מול התוקף, יתכנן את המערכת, ינחה את המיישמים בעבודתם, יעצב את שיטת העבודה, יעקוב אחר האירועים לצורך איתור התקפה, ויגיב את התגובה וההתמודדות עם התקפה. הארכיטקט אחראי לתכנן ולבניית ההגנה על מערכות ההפעלה, רשת התקשורת, הקוד והיישומים כנגד האקרים. את תפקידו יבצע באמצעות הנחיות למיישם אבטחת המידע. יימצא בארגונים כלליים בינוניים וגדולים ובחברות יעוץ ושירות בתחום אבטחת המידע. בחברות קטנות יבוצע התפקיד על-ידי מנהל הרשתות, מנהל הסיסטם או מנהל התקשורת.

מיישם הגנת סייבר (Cyber Security Practitioner) אחראי על הפעלת כלי אבטחת המידע בארגון. התפקיד דומה לתפקיד מנהל רשת, אך הטכנולוגיות שתחת אחריותו, הינן רבות ומתקדמות, ועוסקות בהגנה על המידע, על התקשורת, על אמצעי האחסון ועל המחשבים. בניגוד לסביבת הרשת שבה נמצות בעיקר מערכות Microsoft-ו Linux, בסביבת הגנת סייבר של ארגון טיפוסי, קיימים יצרנים רבים וכלי הגנה מגוונים מאוד. בישראל ובעולם קשה מאוד למצוא מומחים מסוג זה, קשה מאוד להכשירם, ולכן - השכר גבוה מאוד לאחר תקופה קצרה יחסית.



תכנית לימודים:

Cyber Methodology / GRC: InfoSec Governance, Risk & Compliance

עולם אבטחת המידע מקיים יחסי גומלין הדוקים עם תחום הממשל, ניהול הסיכונים והתאימות התאגידית, מזין ומוזן ממנו. מדובר בדיסציפלינה בעלת 3 משמעויות: ניהול הסיכון הארגוני כתוצאה מאירוע סייבר, עמידת הארגון בדרישות ההנהלה, החוק והרגולציה בהיבטים רלבנטיים (למשל: חוק הגנת הפרטיות, תקנה 7809, 627). ייסקרו 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.

- **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**

- **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

CISSP Preparation

סדנה משלימה להכנה מבחני CISSP של (ISC)2, בנוסף לתכנית הלימודים כולה הממוקדת סביב נושאי המבחן הבינלאומי.

- TEST Marathon

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

CISO Function & Roll

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.

- **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,

<u>הצהרת תלמיד בלימודי CISO</u>

הריני מאשר בזאת כי קיבלתי דף מידע זה, הבנתי את תכנו והסכמתי לתנאים המפורטים בו.

שם הנרשם: _____ תאריך: _____ חתימה _____

We invented a methodology
for cyber education,
because nobody else did it.

לכבוד
המכללה לאבטחת מידע וללוחמת מידע
שיא סקיוריטי טכנולוגי'ז בע"מ
רמת-גן – פקס: 03-6122593

נא לרשום אותי לתוכנית הלימודים ברמת גן

קורסמומחה מתודולוגיות הגנת סייבר - CSMP

<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 המכון וSee Security.
- דמי ההרשמה אינם כלולים בשכר הלימוד.
- יש לוודא כי התשלומים יסתיימו עד למועד סיום הקורס.

תאריך: _____ חתימה: _____.

שיא א. סקיוריטי טכנולוגי' בע"מ	ח.פ: 513431403	ספק משהב"ט: 83/168200