להיות מיישם הגנת סייבר מוסמך לפי הרגולציה של מטה הסייבר, או שלא.

המסלול להכשרה ולהסמכת מיישמי הגנת סייבר

CSP: Cyber Security Practitioner

יועץ אקדמי: מר אבי ויסמן, מרצים ראשיים: אלעד בר-איתן, נדב נחמיאס

(תאריכים בעמוד הראשי של המכללה)

לתשומת הלב:

- הידע המועבר בתוכנית זו מהווה דרישת-סף גם עבור מקצוע טכנולוג הגנת סייבר (ארכיטקט), ועבור מקצוע מתודולוג הגנת סייבר, וזאת, על-בסיס ההחלטה לאסדרת מקצועות הסייבר של מטה הסייבר הלאומי!
- מכללת See Security הינה הנציגה הבלעדית והרשמית של ארגוני ההסמכה הבינלאומיים **CompTIA** ו- **(ISC)²**.

מבוא

תוכנית הלימודים "מיישמי הגנת סייבר", הינה תוכנית מקורית אשר נבנתה **על בסיס דרישות מטה הסייבר הלאומי** במסגרת האסדרה למקצועות הסייבר. המטה פרסם בינואר 2016 את מקצועות הליבה ותכולות הידע, ובהם: מיישם טכנולוגיות סייבר (Cyber Security Practitioner). התוכנית עוסקת בתחומים הטכניים הקשורים בהטמעה, תפעול, תחזוקה וניהול של מוצרים ופתרונות מעולם אבטחת המידע. המיישם מוגדר כאדם בעל ידע תיאורטי בסיסי ויכולת מעשית-יישומית (Hands on), האחראי על יישום הגנת הסייבר בארגון, בזווית הראייה הספציפית ובהיבטים הבאים: (1) התקנה, ניהול, תפעול ותחזוקה של מוצרי הגנת הסייבר. (2) יישום תהליכי אבטחה שגרתיים. זאת תוך הכרת והבנת הפעילות, הצרכים והמטרות הארגונית.

מאפייני תוכנית הלימודים	
קהל:	מנהלים / סביבתיים / **מקצוענים**
אוריינטציה:	מנהלית/ **טכנית** / יישום
שלב:	מתחילים / **מתקדמים**
רוחב:	ממוקד / רחב
עומק:	סוקר / **עמוק**
הסמכות:	See-CSP, Security+, SSCP, CCNA Security, CCSA
שעות:	180 שעות
מתכונת:	36 מפגשי ערב, כ- 4 חודשים
תרגול ביתי:	לא קיים / **קיים**

מטרת התוכנית

הכשרת אנשי מקצוע בתחומי היישום והאינטגרציה של מוצרים ופתרונות בעולם אבטחת המידע.

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 לא מתאים למתחילים.

דרישות קדם

בעלי ידע קודם ומעשי בתחום התקשוב (מערכות הפעלה ותקשורת מחשבים, אף רצוי ידע בסיסי מעולם כלי האבטחה המקובלים) ובעלי תואר (תואר ראשון או שני במדעי המחשב, הנדסת תוכנה\חומרה). **המסלול לא מתאים למתחילים.**

בעלי ידע מעשי בתחום תשתיות מחשב (מערכות הפעלה ותקשורת, וכן רצוי ידע בסיסי בכלי אבטחה בסיסיים), או בעלי הסמכת MCSA (או Linux), והסמכת CCNA, או בוגרי תואר ראשון או שני במדעי המחשב, הנדסת תוכנה\חומרה. המסלול לא מתאים למתחילים.

- נכונות לעבודה עצמית מונחית (כ- 250 שעות לימוד ביתי).
- ראיון אישי.

תובל 30, רמת-גן – 5252242, טל': 03-6122831, 03-5799555, 054-5222305, פקס: 03-6122593
www.see-security.com avi@see-security.com

הסמכה

התוכנית נבנתה לצרכי ידע מעשי. לעומדים בדרישות התוכנית, תוענק תעודה מטעם See-Security:

"מיישם הגנת סייבר - Cyber Security Practitioner"

מי שאינם עומדים בדרישות, זכאים לתעודת השתתפות, ולהשתתפות חוזרת / עבודות ומשימות) ללא תשלום.

בנוסף: הכנה למבחני הסמכה הבינלאומיים (ISC)² SSCP, CompTIA Security+, וכן CCNA Security:

ספרות

- ערכות שקפים.
- ספר SSCP מקורי
- ספר Security+ מקורי.

מטלות תוכנית הלימודים

- קיימת חובת נוכחות ב-80% מהמפגשים.
- כל מודול נלמד מחייב עמידה במבחן פנימי ו/או בעבודות בציון 70 לפחות (ראה תקנון קורס במכללה).
- בנושאים הטכניים - תרגול (Hands-on) בכיתה (מעבדת מחשבים).

מתכונת הלימודים

משך התכנית כ- 180 שעות, במתכונת של 36 מפגשי ערב (כ- 4 חודשים). הלימודים מתקיימים בקמפוס See Security ברמת-גן. המסלול נפתח פעמיים בשנה.

עלות הלימודים

סך 12,500 ₪ + 400 ₪ דמי רישום (כולל מע"מ)

תמצית תוכנית לימודים

A. Cyber & IT Introductions — 20 hours
1. General IT Introduction
2. Cyber Arena Introduction
3. Cyber Defense Techniques
4. Cyber Regulation

B. Tools &Technologies Methods — 40 hours
1. Endpoint Protection Controls
2. Network Security Controls
3. Application and Database Security Controls
4. Data Protection Controls
5. Mobile Security Considerations
6. Cyber Security Processes
7. Operational Technology Controls

C. Tools &Technologies LAB — 100 hours
1. Firewalls and Next Generation UTM's
2. Intrusion Prevention Systems (IPS)
3. Mail Security
4. Web Security
5. Endpoint Security

D. Cyber Certification Marathons — 20 hours
1. (ISC)² SSCP Certification
2. CompTIA Security+ Certification

TOTAL: 180 Hours

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

מסלול מיישמי הגנת סייבר נבנה תחת דרישות הרגולציה של מטה הסייבר הלאומי, ועל סמך היכרות המכללה עם עולם אבטחת המידע והסייבר בישראל ובעולם. התכנים נבנו בסיוע אנשי מקצוע מהמעולים בתחום הנושאים על גבם ניסיון ארוך טווח והיכרות טכנולוגית מגוונת בתחומי הלימוד.

הערות לתוכנית הלימודים

א. תוכנית הלימודים מחייבת בהכנת שיעורי בית להשגת יעדי הלימוד.
ב. משימות קריאה מהווים חובה לימודית.
ג. תכנים, נושאים ו/או יצרנים עשויים להשתנות במהלך הרצת התוכנית כתוצאה ממגבלות שיווקיות / אחרות.

הערות מינהל

- 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

תוכנית לימודים מלאה

Chapter A: Cyber & IT Introductions

מטרת המבואות: לספק סקירה המהווה חובה על-פי מטה הסייבר הלאומי.

1. General IT Introduction

סקירה אודות מונחים מקצועיים בעולם ה- IT הכללי לצורך "יישור קו מקצועי".

- Virtualization
- מחשוב ענן
- Hosting
- Big Data
- יישומי ERP, CRM, Billing

2. Cyber Arena Introduction

סקירה אודות מונחים מקצועיים, וסקירה על אירועים וכוחות בעולם.

- הגדרות וטרמינולוגיה (מונחים והמשגה).
- איומי סייבר.
- סוגי יריבים והמוטיבציות שלהם.
- משמעויות (כלכליות, מוניטין, משמעויות מעבר לרמת הארגון).
- גופים לאומיים העוסקים בתחום בישראל.

3. Cyber Defense Techniques

סקירה אודות טכניקות הגנה ואודות שיטות תקיפה ואיומים טיפוסיים.

- שיטות גיבוי ושחזור.
- בקרת גישה (שיטות)
- Hardware Security
- קריפטוגרפיה
- ניהול תהליכים
- הגנה בשכבות Defense in Depth
- השלכות/משמעויות (נזק לרכוש, נזק לגוף, פגיעה במוניטין, השלכות על צד ג').

- סוגים/וקטורים לתקיפות (מרחוק/מתוך הארגון, חדירה פיזית למתחמי מחשב, Social Engineering).
- אופניי הפגיעות במערכות מידע (זמינות, אמינות, סודיות, חבותיות).
- בקרות Operational-People-Technology (ניהול סיכונים, אחריות ותפקידים, מדיניות-תקנים-נהלים, מיפוי נכסים וסיווגי מידע, תרבות ארגונית, ביקורות, מודעות)

4. Cyber Regulation

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

- אסדרה באמצעות: שוק, חוק, תרבות וארכיטקטורה.
- חקיקה ישראלית: חוק הפרטיות, חוק המחשבים, חוקי ייסוד.
- אסדרת מקצועות הסייבר
- תקינה בינלאומית (ISO, IEFT, NIST).
- הכרת ISO27000, NIST SP800
- הסדרה מוסדית: הוראה 357, הוראה 257, הנחיות ממוקדות מטעם משרדי ממשלה.
- הסדרות שוק כגון: PCI-DSS

Chapter B: Tools & Technologies Methods

1. Endpoint Protection Controls

מיקוד בטכנולוגיות ההגנה על מערכות קצה, ובפרט:

- מערכות הפעלה והקשחתם
  - הקשחת עמדות משתמשים
  - הקשחת שרתים
- מבוא למעבדה: Endpoint Security
  - מערכות Anti-Virus / Anti-Malware
  - הגנת מידע Full Disk Encryption
  - בקרת התקנים Device Control
  - הגנה מקומית מאנומליות – HIPS

2. Network Security Controls

מיקוד במערכות הגנה רשתיות (למשל לזיהוי אנומליות) ומערכות בקרת הגישה (Access Control) ברמת הרשת, ובפרט:

- הפרדת משאבים (Segmentation)
  - מבוא למעבדה: Firewall ו- IPS/IDS
  - בניית ארכיטקטורה נכונה (הפרדת סביבות, שימוש ב-VLAN)
- הגנת נקודות הגישה לרשת (Network Access Control)
- קישור רשתות מאובטח וגישה מרוחקת
  - הכרת עולם ה VPN ו- SSL-VPN
- מערך מלכודות מבוזר (Honey Pots / Honey Nets)

3. Application and Database Security Controls

מיקוד בבקרות טכנולוגיות שמטרתן התמודדות עם רמות גבוהות יותר מרובד הרשת ועמדות המשתמש. רמות אלו רלוונטיות להגנה על מאגרי מידע ולהגנה על האפליקציה, ובפרט:

- הגנת מאגרי מידע (Database Security)
- הגנת אפליקטיבית על אתרי אינטרנט (Web Application Firewall)

4. Data Protection Controls

מיקוד בבקרות טכנולוגיות הקשורות להגנה על מידע לכשעצמו (ללא תלות בפלטפורמת האגירה, השינוע או העיבוד שלו). פרק זה גם מתייחס לניטור וניתוח מידע (למשל במסגרת תעבורת רשת). בין היתר ידונו הנושאים הבאים:

- מערכות הלבנה והשחרה
- הכרת מניעת דלף מידע (Data Leakage Prevention)
- פתיחת הצפנה לניטור (SSL Termination)
- ניטור תעבורת מידע (Network Traffic Analysis)

5. Mobile Security Considerations

בעיות ואתגרים בעולם הציוד הנייד ודרכי יישום הגנות ובקרות:

- ניהול רכיבים ניידים - Mobile Device Management
- שיקולים של BYOD

6. Cyber Security Processes

מיקוד בבקרות הטכנולוגיות התומכות במרכיב התפעולי של הגנת הסייבר – תהליכים במערך תפעולי (מדיניות, תקנים ונהלים) ובמערך אנושי, ובקרות הטכנולוגיות הנדרשות ליישום התהליכים.

- מרכז ניהול אירועי סייבר (Security Operations Center)
  - מערך ניטור ובקרת אירועים (SIEM)
  - מערך ניהול אירועי סייבר (Incident Management)
- מבוא לניהול זהויות והרשאות (Identity and Access Management)
  - ניהול חשבונות פריבילגיים (Privileged Account)
- מבוא למערכי גיבוי והתאוששות עסקית (DR, BCP)

7. **Operational Technology (OT) Controls**

האתגרים בהגנת מערכות תשתית תעשייתיות (בקרי בניין, מעליות, מיזוג, מים), Industrial Control Systems ו- SCADA.

- Introduction to SCADA
- Security and SCADA
- Control Center Security
- Field Devices Security
- Standards and Processes

Chapter C:Tools & Technologies hands on Lab

1. **Firewalls and Next Generation UTM's**

מטרת הפרק להזכיר לתלמידים את עולם ה-Firewalls ולעבות אותו בטכנולוגיות הנוספות שכיום הספקים המובילים בשוק מוסיפים לרכיב ה-Firewall. הפרק סוקר את הצורה הנכונה בה יש להגדיר ולהטמיע רכיבי Firewall תוך הצגת השיקולים הסביבתיים והארגוניים (ארכיטקטורת רשת נכונה, ניתוב נכון, מנגנוני הגנה על מערכות ה-Firewall וכו'). הפרק כולל התנסות מעשית (Hands On) במוצרים המובילים היום בשוק כגון: Checkpoint ו-Palo Alto.

- **Basics of Firewalls:** Layer 2 and Layer 3 architecture; Routing; Anti-Spoofing, etc.
- **Policy Enforcement:** Introduction to Objects and Subjects; Firewalls Rulebase; Advanced Firewall Policy; Monitoring and Logging.
- **Advance Topics:** Advanced Security Configurations (such as IPS, Anti-Virus/Anti-Malware, URL and Content Filtering, etc.;

2. **Intrusion Prevention Systems (IPS)**

פרק מרכזי נוסף בתוכנית הלימודים אשר חושף את התלמידים לטכנולוגיות האבטחה העקיפות המעבות את מערך אבטחת המידע הארגוני. מטרתו להציג לתלמידים את המשמעויות שבהטמעת מערכת לזיהוי ומניעת אנומליות וחדירות לרשת. הפרק כולל התנסות מעשית (Hands On) במוצרים המובילים היום בשוק.

- **Basics of IPS:** Layer 2 and Layer 3 architecture; Network Connections (inline); Multi-Sensor Architecture and Central Management of IPS Devices.
- **Policy Enforcement:** Introducing IPS Policies Terminology and Best Practices (Analysis of Events; Alterting/Preventing by Signature/Protocol/Learning analysis); Advanced IPS Configuration; Vendors Best Practices; IDS Configurations.
- **Advance Topics:** Security Configuration According to: Geographic Parameters, Contextual Awareness and Vendors Recommendations; Advanced Security Features: Sandboxing, File Filtering, Anti-Malware.

3. **Mail Security**

מלבד מערכות ההגנה הרישתיות המוזכרות בקורס זה, התלמידים ייחשפו גם למערכות הגנה נוספות בערוצי תקשורת נוספים כמו ערוץ הדוא"ל. מדובר במערכות ה-Mail Relay שמטרתן סינון וזיכוי תעבורת דוא"ל לכיוון הארגון (לרוב מרשת האינטרנט, וכמובן במעבר בין רשתות ממתחמי אבטחה שונים). הפרק כולל התנסות מעשית (Hands On) במוצרים המובילים היום בשוק כגון: Symantec.

- **Basics of Mail Security:** Basic Architecture (Internal, External); Network Connections; Routing; Configuring Email Connections.
- **Policy Enforcement:** Email Filtering Policies; Anti-Spam, Anti-Virus and Content/File Filtering; Understanding Logging and Monitoring.
- **Advance Topics:** Configuring Advanced Mail Security Policies: DLP, File Filtering, Content Filtering.

4. **Web Security**

הפעלת מערכות הגנה מול רשת האינטרנט, ומניעת כניסה של קוד עוין, חסימת גישה לאתרים, והתנסות מעשית (Hands On) במוצרים המובילים בענף כגון: Websense.

- **Basics of Web Security:** Introduction to Web Site Filtering (Content Filtering, URL Filtering, Contextual Filtering, Threat Categorization).
- **Policy Enforcement:** Enforcing Web Security Policies; Correlation between Systems.

5. **Endpoint Security**

הטמעה והגדרה של מוצרי ההגנה על עמדות הקצה ברשת הארגונית. בעוד הפרקים האחרים בקורס עוסקים בהגנת שכבות הרשת השונות, פרק זה עוסק בנושאי ההגנה של המחשבים, השרתים, מערכות ההפעלה ותחנות הקצה. הפרק כולל התנסות מעשית (Hands On) במוצרים המובילים בענף כגון: McAfee Suits.

- **Basics of Endpoint Security:** Introduction to endpoint security mechanisms and their significance; How endpoint security works (signature, pattern and behavior analysis); Introducing HIPS, HFW, Device Control and Application Control.
- **Policy Enforcement:** Proper Implementation of Endpoint Security Suit (Policy Configuration; Enforcing Organizational Requirements; Preventing Policy Bypass); Simulating Detection and Prevention of Exploits and Malware.
- **Other Topics:** Architectural Recommendations; HOST URL Filtering; Correlation with SIEM (Syslog, Traps); Multi-Sensor Implementation

Chapter C:International Cyber Certifications Marathons

(ISC)^2 SSCP Certification Preparation

הסמכת SSCP של (ISC)2, ארגון ההסמכות הידוע ביותר בעולם הסייבר, מהווה הוכחה לכישורים טכניים מוכחים וידע מעשי (hands on) בתפקידי IT מבצעיים. ההסמכה מהווה אישור ליכולת של המוסמך ליישם, לפקח ולנהל תשתית IT בהתאם למדיניות אבטחת המידע והנהלים המבטיחים סודיות נתונים, שלמות וזמינות, ונחשבת למובילה בתעשייה. ההסמכה עוסקת בנושאים כגון הצפנה ובקרת גישה, כמו גם בהיבטי סייבר הנוגעים לניהול בארגון: התאוששות מאסון וניהול סיכונים. עד היום הוסמכו אלפי מומחים ברחבי העולם, לרבות עובדי ה- United States Department of Defense. נושאי בחינה כוללים: אימות, בדיקות Cyber, גילוי פריצה, מניעת פריצה, תגובה לאירועי סייבר והתאוששות, אמצעים נגד תקיפות, קריפטוגרפיה, אמצעים נגד קוד זדוני, ועוד.

1. Testing-Taking Tips & Study Techniques
   - Preparation for the SSCP Exam
   - Submitting Required Paperwork
   - Resources and Study Aids
   - Passing the Exam the First Time
2. Security Operations and Administration
   - Change Control/Configuration Management
   - Dual Control, Separation of Duties, Rotation of Duties
   - Vulnerability Assessment and Pen-Testing
3. Access Controls
   - AAA
   - Authentication Methods (Types 1, 2, & 3)
   - Authorization - DAC, RBAC, MAC
   - Accounting - Logging, Monitoring, Auditing
   - Central/Decentralized and Hybrid Management
   - Single Sign-On - Kerberos, Radius, Diameter, TACACS
   - Vulnerabilities - Emanations, Impersonation, Rouge Infrastructure, Social Engineering
4. Cryptography
   - Intro/History
   - Symmetric
   - Asymmetric
   - Hashing
   - Cryptosystems - SSL, S/MIME, PGP
   - PKI
   - Cryptanalysis
5. Malicious Code and Malware
   - Layering, Data Hiding, and Abstraction
   - Database Security
   - AI
   - OOD
   - Mobil Code
   - Malware Architecture Problems - Covert Channels + TOC/TOU, Object Reuse
   - Network Vulnerabilities
6. Networks and Telecommunications
   - OSI/DoD TCP/IP Models
   - TCP/UDP/ICMP/IP
   - Ethernet
   - Devices - Routers/Switches/Hubs
   - WAN Technologies - X.25/Frame Relay/PPP/ISDN/DSL/Cable
   - Voice - PBX/Cell Phones/VOIP
   - IPSec
   - Firewalls
   - Wireless
7. Risk, Response, and Recovery
   - CIA
   - Roles and Responsibilities - RACI
   - Asset Management
   - Taxonomy - Information Classification
   - Risk Management
   - Policies, Procedures, Standards, Guidelines, Baselines.
   - Knowledge Transfer - Awareness, Training, Education
   - BIA Policy
   - BIA Roles and Teams
   - Data Backups, Vaulting, Journaling, Shadowing
   - Alternate Sites
   - Emergency Response
   - Required notifications
   - BIA Tests
8. Analysis and Monitoring
   - Ethics - Due Care/Due diligence
   - Intellectual Property
   - Incident Response
   - Forensics
   - Evidence
   - Laws - HIPAA, GLB, SOX
9. Review and Q&A Session

CompTIA Security+ Certification Preparation

הסמכת Security+ עוסקת בנושאים כגון הצפנה ובקרת גישה, כמו גם בהיבטי סייבר הנוגעים לניהול בארגון: התאוששות מאסון וניהול סיכונים. עד היום הוסמכו למעלה מ-45,000 מומחים ברחבי העולם, לרבות עובדי ה- United States Department of Defense. נושאי בחינה כוללים: אבטחת רשת, תאימות ואבטחה מבצעית, איומים ונקודתי תורפה, יישום, נתונים ואבטחת שרתים, הצפנה, בקרת גישה וניהול זהויות.

1. Network Theory
   - Networking Overview
   - Network Standards and the OSI Model
   - Network Types
   - Identify Network Configurations
   - Data Transmission Methods
2. Security Fundamentals
   - The Information Security Cycle
   - Information Security Controls
   - Authentication Methods
   - Cryptography Fundamentals
   - Security Policy Fundamentals
3. Security Threats and Vulnerabilities
   - Social Engineering
   - Physical Threats and Vulnerabilities
   - Network-Based Threats
   - Wireless Threats and Vulnerabilities
   - Software-Based Threats
4. Network Security
   - Network Devices and Technologies
   - Network Design Elements and Components
   - Implement Networking Protocols
   - Apply Network Security Administration Principles
   - Secure Wireless Traffic
5. Managing Application, Data, and Host Security
   - Establish Device/Host Security
   - Application Security
   - Data Security
   - Mobile Security
6. Access Control, Authentication, and Account Management
   - Access Control and Authentication Services
   - Implement Account Management Security Controls
7. Managing Certificates
   - Install a CA Hierarchy
   - Enroll Certificates
   - Secure Network Traffic by Using Certificates
   - Renew Certificates
   - Revoke Certificates
   - Back Up and Restore Certificates and Private Keys
8. Compliance and Operational Security
   - Physical Security
   - Legal Compliance
   - Security Awareness and Training
9. Risk Management
   - Risk Analysis
   - Implement Vulnerability Assessment Tools and Techniques
   - Scan for Vulnerabilities
   - Mitigation and Deterrent Techniques
10. Managing Security Incidents
    - Respond to Security Incidents
    - Recover from a Security Incident
11. Business Continuity and Disaster Recovery Planning
    - Business Continuity
    - Plan for Disaster Recovery
    - Execute DRPs and Procedures
    - Appendix A: CompTIA® Security+® (Exam SY0-401) Objectives Mapping

CCNA Security

מיקוד בעולם ה-Firewalls ולעבות אותו בטכנולוגיות הנוספות שהספקים המובילים מוסיפים לרכיב ה-Firewall. הפרק סוקר את הצורה הנכונה בה יש להגדיר ולהטמיע רכיבי Firewall תוך הצגת השיקולים הסביבתיים והארגוניים (ארכיטקטורת רשת נכונה, ניתוב נכון, מנגנוני הגנה על מערכות ה-Firewall וכו'). הפרק כולל התנסות מעשית (Hands On) במוצרים המובילים.

1. Modern Network Security Threats
   - Fundamental Principles of a Secure Network
   - Worms, Viruses and Trojan Horses
   - Attack Methodologies
2. Securing Network Devices
   - Securing Device Access and Files
   - Privilege Levels and Role-Based CL
   - Monitoring Devices
   - Using Automated Features
3. Authentication, Authorization and Accounting
6. Securing the Local Area Networks
   - Endpoint Security Considerations
   - Layer 2 Security Considerations
   - Wireless, VoIP and SAN Security Considerations
   - Configuring Switch Security
   - SPAN and RSPAN
7. Cryptography
   - Cryptographic Services
   - Hashes and Digital Signatures and authentication
   - Symmetric and Asymmetric Encryption

- Purpose of AAA
- Configuring Local AAA
- Configure Server-Based AAA

4. Implementing Firewall Technologies

- Access Control Lists
- Firewall Technologies
- Context-Based Access Control
- Zone-Based Policy Firewall

5. Implementing Intrusion Prevention

- IPS Technologies
- Implementing IPS

8. Implementing Virtual Private Networks

- VPNs
- IPSec VPN Components and Operation
- Implementing Site-to-Site IPSec VPNs
- Implementing a Remote Access VPN
- Implementing SSL VPNs

9. Managing a Secure Network

- Secure Network Lifecycle
- Self-Defending Network
- Building a Comprehensive Security Policy

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

נא לרשום אותי לתוכנית הלימודים ברמת גן

מיישמי הגנת סייבר CSP: Cyber Security Practitioner

<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:_____.