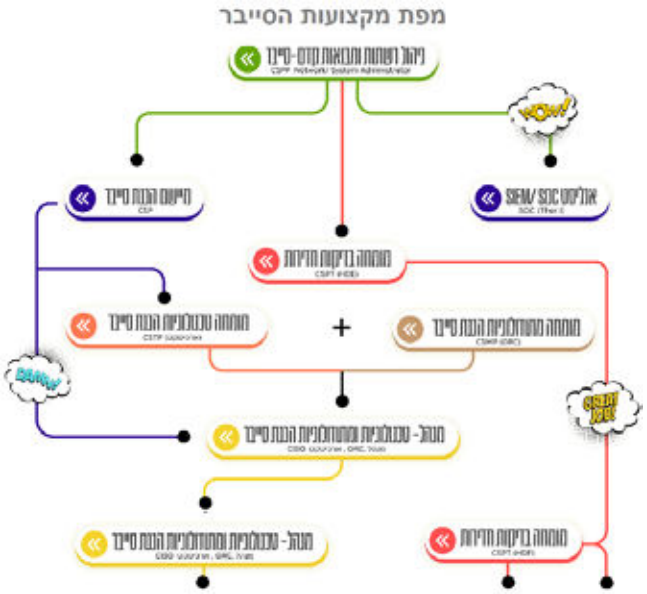
התכנית ללימודי מקצוע
מנהל טכנולוגיות הגנת סייבר

תכנית זו מיועדת לבעלי רקע נרחב בתשתיות

מנהל טכנולוגיות הגנת סייבר (CSP)

התוכנית נועדה להכשיר אנשי hands-on בעלי רקע טכנולוגי יישומי עשיר לניהול משימות הגנת סייבר בארגונים. התוכנית מאופיינת במעבדות מתקדמות, אשר מלוות את הנושאים התיאורטיים. הנושאים זוקקו והתואמו לדרישות מעסיקים בישראל.

מאושר על ידי משרד הכלכלה לפיקדון חיילים משוחררים ולתוכנית השוברים



להיות מנהל טכנולוגיות הגנת סייבר.

מנהל טכנולוגיות הגנת סייבר אחראי על תכנון מענה טכנולוגי, תוך שילוב טכנולוגיות ושיטות אבטחה, התאמת מוצרי הגנה ושילובם וליווי אירועי אבטחה מתוך הבנת הפעילות, הצרכים והמטרות הארגונית, הכל- לצורך הגנת הסייבר בארגון.

וְלֹא פָּחוֹת חָשׁוּב: נִלְמָד בְּפִי שָׁרַק שִׁיא סֶקְיוּרִיטִי יוֹדַעַת לָלַמֵּד: **נִבוֹן**, וְעִם **הַלֵּב**.

התכנית ללימודי מקצוע מנהל טכנולוגיות הגנת סייבר (CSP)

התוכנית נבנתה בהתאם לאסדרת מקצועות הסייבר בישראל ועבור הסמכה הבינלאומית **Security+**

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 Secure*, ובמכללה הבינלאומית לסייבר *See Security College International*.

אודות תכנית הלימודים

התוכנית נועדה להכשיר אנשי hands-on בעלי רקע טכנולוגי יישומי עשיר לניהול משימות הגנת סייבר בארגונים. התוכנית מאופיינת במעבדות מתקדמות, אשר מלוות את הנושאים התיאורטיים. הנושאים זוקקו והתואמו לדרישות מעסיקים בישראל.

הדרישה ההולכת וגוברת למומחי הגנת סייבר משכילים ובעלי ידע, מחייבת רקע רחב ועמוק במיוחד, במסגרת מתודולוגית סדורה אשר תאפשר השתלטות על המידע הרב, וזו מהות המסלול.

מערך הסייבר 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). תכנית זו הינה שילוב CSTP ו- CSMP – כמפורט ונכלל בתכנית זו.

מאפייני תוכנית הלימודים	
עלות:	15,500 שח + 400 שח דמי הרשמה
קהל:	מנהלים / סביבתיים / מקצוענים
אוריינטציה:	מנהלית/ טכנית / יישום
מטרה:	הכשרת אנשי Hands-on של טכנולוגיות אבטחת מידע איכותיים, עתירי ידע.
שלב:	בעלי ידע מעשי בתחום התשתיות (מערכות הפעלה ותקשורת).
רוחב:	ממוקד / רחב
עומק:	סוקר / עמוק
הסמכות:	CompTIA Security+ or: (ISC)^2 SSCP
שעות:	155 שעות
פתיחה:	ראה בעמוד הראשי של המכללה
מתכונת:	הלימודים בקמפוס המכללה ברמת גן, מתקיימים פעמיים בשבוע בימי בערב: 17:30 עד 21:30 (5 שעות אקדמיות למפגש), במשך כ-5 חודשים
תרגול בית:	בהיקף כ-200 שעות

סגנון לימוד

טכני, Hands-on, ותיאורטי.

מעבדות תרגול בינלאומיות

תכנית זו הינה עתירת תרגול מעשי במעבדות בינלאומיות מתקדמות המיועדות גם **לתרגול מבית התלמיד**.

עלות

סך 15,500 שח + 400 שח דמי רישום (כולל מע"מ).

קהל יעד

למעוניינים להתמחות כמיישמי הגנת סייבר, או להמשיך למקצועות מוסמך טכנולוגיות הגנת סייבר, ונדרשים להכשרת מיישמי הגנת סייבר כדרישת סף לקראת ההכשרה במקצועות אלו בהמשך לימודיהם. [ראה בסוף המסמך: מפת התפתחות מקצועית בענף הסייבר].

דרישות סף

- ידע וניסיון בתחום התשתיות (סיסטם ותקשורת).
- אנגלית ברמה טובה.
- ראיון אישי לבחינת ההתאמה לתכנית.

מתכונת הלימודים

משך התכנית 155 שעות כיתה, ו-200 שעות משימות (סך הכל 355 שעות), פעמיים בשבוע בערב בשעות 17:30 עד 21:30 במשך כ-5 חודשים, 5 שעות אקדמיות למפגש. הלימודים מתקיימים בקמפוס See Security ברמת-גן (צמוד לתחנת רכבת מרכז).

חובות אקדמיות

קיימת חובת נוכחות ב-80% מהמפגשים. קבלת תעודת המכללה מותנית בעמידה במבחני מעבר, בציון 70 לפחות (מבחן חוזר ללא תשלום). בנושאים הטכניים - תרגול (Hands-on) בכיתה ובבית.

זכאות לתעודה והסמכות בינלאומיות

לעומדים בדרישות התכנית תוענק תעודת הסמכה יוקרתית מטעם המכללה:

"CSP: Cyber Security Practitioner"

בנוסף להסמכות הבינלאומיות כמפורט (Security+ או SSCP) לתלמידים אשר ניגשים עצמאית לאחר השלמת חוק לימודיהם במכללה.

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

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.

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.

מה אנחנו מצפים מבוגר התכנית?

1. בתקופת הלימודים תשקיע את כל הזמן כדי לקיים את הנחיות המרצה, אינך הראשון ולא תהיה האחרון שימצא עצמו מיישם הגנת סייבר בלב התעשייה.
2. בסיום לימודיך היעזר בהנהלת המוסד לבניית טופס קורות חיים ההולם את מאמצייך.
3. הסתפק בתחילת דרכך במשרה רלבנטית מכל סוג שהוא כדי לצבור ניסיון (נסה לעשות זאת כבר בתקופת הלימודים).
4. בדוק עם היועץ האקדמי את איכות עמידתך בריאיון אישי לקראת ראיונות העבודה האמיתיים, במקרים מסויימים אפילו תלמיד מצטיין זקוק לתיקונים (פשוטים יחסית) שמשביחים מאוד את יכולתו למצוא משרה איכותית.
5. צא לדרכך, אל תשכח להמשיך ללמוד, דאג תמיד להיות מבחינת ידע רמה אחת יותר מהאחרים, כי ככל שתגביה כך יהיו לך פחות מתחרים, שכר גבוה יותר, וסיפוק רב יותר.

תוכנית לימודים לדוגמה בעמודים הבאים:

- **המכללה מביאה לידיעת הנרשמים והסטודנטים, כי ייתכנו שינויים במערך התכנית, במועדי הלימוד והבחינות או בכל נושא אחר. הודעה על שינוי תימסר למשתתפים.**

מה אני עושה לאחר סיום הלימודים? הצעד הבא

בסיום הקורס תוכל לבחור מהו הצעד הבא שלך:

1. **להתחיל לעבוד כמיישם סייבר.**
2. **להמשיך בצעד הבא - תכנית הלימודים CSTP – ארכיטקט הגנת סייבר.**

3. **להמשיך בצעד הבא - תכנית הלימודים CSPT – מומחה בדיקות חדירות** (האקר, מבוסס על תכנית הלימודים הבינלאומית Hacking Defined Experts).

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

בוגרי ובוגרות מכללת שיא סקיוריטי?

קבלו מיועצי הלימודים הצעה מיוחדת.

לתשומת ליבך!

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

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.

תוכנית קורס - מנהלי טכנולוגיות הגנת סייבר (CSP)

מס'	נושא ראשי	שם השיעור	נושאי השיעור
1	Introduction to Cybersecurity	פתיחת הקורס והיכרות, סקירת הנושאים הנלמדים בקורס, הצגת עולם ב-Cyber Security ו-CASE STUDIES	השיעור הראשון בקורס, נועד לייצר אוריינטציה והכוונה לתלמידים לקראת המשך הקורס: * היכרות עם מנהל הקורס * היכרות עם אדמיניסטרציית הקורס (מערכת LMS, ערוצי קשר עם המכללה, עדכניות לו"ז) * הצגת הדרישות/חובות במהלך הקורס.
2		יסודות בעולם הסייבר ואבטחת המידע [שיעור כפול]	* מונחים ומושגי יסוד * בקרת גישה (Access Control) לרבות בעולם הפיזי, ברשתות, במערכות הפעלה. עיקר המיקוד יעשה סביב שני צירים משיקים – (1) הזדהות, אימות והרשאות (כהקדמה לעולם ה-2) (IAM); הגבלת גישה בתקשורת. * עקרונות אבטחת מידע (הצורך בידיעה, עקרון ההרשאה המינימלית, זיכוי משאבים משותפים)
3		יסודות בעולם הסייבר ואבטחת המידע [שיעור כפול]	* נושאים בקריפטוגרפיה - בדגש תעודות דיגיטליות ומערכי PKI
4		מבוא להתמודדות עם איומי סייבר [שיעור כפול]	היכרות עם השיטות והכלים הקיימים להתמודדות קטגוריות עם איומי סייבר. * מתודולוגיית MITRE ATT@CK MATRIX (כולל Workshop) * עולם ה-Anti-Malware – מושגים (סוגי Malware), שיטות להתמודדות (Signature, Heuristics, Protocol Deviations, Behavioral / Contextual)
5		מבוא להתמודדות עם איומי סייבר [שיעור כפול]	* עולם ה-Firewall – סקירה מהירה של האבולוציה מ-Packet Filter ל-Stateful Inspection והדגשת הפערים בין הגנה (או פעילות) בשכבות OSI השונות (הצגת עולם ה-Network Firewall vs. Application Firewall) * עולם ה-IDPS – התייחסות גם ל- Intrusion Detection וגם ל- Intrusion Prevention. * ההבדל בין Host-IDPS (ו Host-FW) לבין Network-IDPS (ו Network-FW).
6	Cybersecurity and the Business	היכרות עם עולם הכספים.	האיומים והחולשות במישור הארגוני , לרבות הכרת המשמעויות של "תהליכים", "מדיניות", "תקנים" - כיצד מתנהל סייבר בארגון

לא לומד? אל תתפלא.

college@see-security.com | www.see-security.com | טלפון: 03-6122831 | ז'בוטינסקי 1 רמת-גן – בנין דימול

תוכנית קורס - מנהלי טכנולוגיות הגנת סייבר (CSP)

7	Network Security	אבטחת רשתות תקשוב (אבטחת הרשת ואבטחת הרכיבים)	אבטחת רשתות תקשוב (והגנה על מערכות תקשורת) - Network Security. מיקוד במצופה ממיישם הגנת סייבר ככל שמדובר במערכות להגנת הרשת (והגנת רכיבי הרשת). * כניסה לעולם ההקשחות.
8		הקשחת מערכות הגנה רישתיות (הגנה על המערכות עצמן)	הקשחת מערכות הגנה רשתיות (הגנה על המערכות עצמן). תרגול מעשי של הגדרות הקשחה ברכיבים מכוננים (למשל Firewall, מתג או נתב) והצגת המשמעות של הקשחה לא מתאימה או לקויה. בין היתר, תרגול נושאים כגון: * ניהול מבוסס Out of Band – מתן גישת ניהול למקורות מסוימים (Access Control List) * ניהול משתמשים (מקומי / מרכזי) – והמשמעויות של שימוש במשתמש קבוצתי ידוע לכולם * כיבוי שירותים שאינם נדרשים – והמשמעויות של השארת שירותים נגישים (למשל SNMP)
9		Checkpoint Firewall - תרגול הגדרות תצורה לרכיבי רשת תוך ניסוי וטעיה בתרחישים	תרגול בכיתה (ובמקביל גם לפחות פי 2 שעות לתרגול בית) של הגדרת תצורה עבור Checkpoint Firewall (בהתאם לגרסאות. כרגע R81). הכרת המוצר וכיולו לתצורה הבסיסית ביותר המאפשרת עבודה ברשת ומכאן להתחיל ולתרגל שינויים ב-Policy תוך שינויי Wireshark ובאמצעות ניסוי וטעיה.
10		תרגול	הגדרות תצורה לרכיבי רשת תוך ניסוי וטעיה בתרחישים
11		Fortigate Firewall - תרגול הגדרות תצורה לרכיבי רשת תוך ניסוי וטעיה בתרחישים	תרגול בכיתה (ובמקביל גם לפחות פי 2 שעות לתרגול בית) של הגדרת תצורה עבור Fortigate Firewall (בהתאם לגרסאות. כרגע 7.0.1). הכרת המוצר וכיולו לתצורה הבסיסית ביותר המאפשרת עבודה ברשת ומכאן להתחיל ולתרגל שינויים ב-Policy תוך שינויי Wireshark ובאמצעות ניסוי וטעיה.
12	System Security	אבטחת עמדות ומערכות הפעלה	System Security בסביבות Microsoft. מותאם לידע הנדרש בהסמכת Security+.
13		תרגול הקשחות מערכות הפעלה ושרתים (בדגש ACTIVE DIRECTORY ו-GPO) - חלק 1	התמודדות עם הגדרות הקשחה שונות ברמת Active Directory ו-GPO.
14		תרגול הקשחות מערכות הפעלה ושרתים (בדגש ACTIVE DIRECTORY ו-GPO) - חלק 2	התמודדות עם הגדרות הקשחה שונות ברמת Active Directory ו-GPO.
15		תרגול כלים טכנולוגיים (EDR/ANTI-VIRUS) התקנות ותפעול	התמודדות עם פריסה, התקנה והגדרה של רכיבי Endpoint Security.
16		SYSTEM SECURITY	תרגול הרחבה
17	Practical Everday IT and Cybersecurity Skills	עולם ה- Regular Expression	תרגול מעשי
18		Powershell	הכרות עם עולם ה-Scripting
19		Powershell	תרגול פרקטי בעולמות Windows (ניהול / בקרה)

לא לומד? אל תתפלא.

college@see-security.com | www.see-security.com | טלפון: 03-6122831 | ז'בוטינסקי 1 רמת-גן – בנין דימול

תוכנית קורס - מנהלי טכנולוגיות הגנת סייבר (CSP)

20	Cybersecurity Incident Management Infrastructure - On Premise	עולם אירועי הסייבר ואבטחת המידע (מושגים והגדרות, כלים וטכנולוגיות), הצגת עולם ה-SOC	SOC והטכנולוגיות המופעלות בו (SIEM). הגדרה, תפעול ותחזוקה של מערכות SIEM
21		הכרות עם יומני מערכות (Event Logs),	עולם ה-Syslog, עיבוד נתוני יומן (Parsing)
22		הכרות עם מערכות SIEM	הבנת עולם ההתרעות, חוקי יסוד, חוקי קורלציה, חיפוש מידע
23		תרגול	מערכות SIEM SPLUNK - חלק 1
24		תרגול	מערכות SIEM SPLUNK - חלק 2
25	Cybersecurity Incident Management Infrastructure - On Cloud	הכרה של סביבות ענן וסביבות היברדיות	
26		תרגול	מערכת SIEM, יומני מערכות ושילובן בענן - 1
27		תרגול	מערכת SIEM, יומני מערכות ושילובן בענן - 2
28		תרגול	מערכת SIEM, יומני מערכות ושילובן בענן - 3
29	Cybersecurity Incident Handling and Response	מבוא לתגובה לאירועי סייבר	חיפוש ממוקד במערכות SIEM ובניית מודעות מצבית
30		תרגול	פעולות סינון/מיון התרעות - כהקדמה לעולם אירועי סייבר
31		תרגול	חקירת אירועי סייבר, תרגול פעולות סינון/מיון והתרעות

סה"כ: 155 שעות אקדמיות*

* ייתכנו שינויים בתוכנית השיעורים ובנושאי הלימוד

לא לומד? אל תתפלא.

college@see-security.com | www.see-security.com | טלפון: 03-6122831 | ז'בוטינסקי 1 רמת-גן – בנין דימול