התכנית ללימודי מקצוע

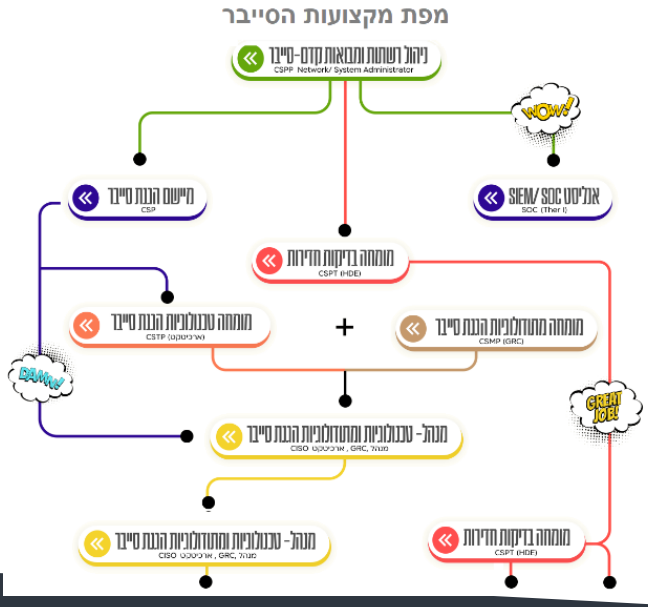
מנהל טכנולוגיות הגנת סייבר

תכנית ע"ו מיועדת לבעלי רקע רחב בתשתיות מיחשוב

מנהל טכנולוגיות הגנת סייבר ומיישם הגנה (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 משרד העבודה לפקדונות ולשוברים לחיילים משוחררים



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 כְּפִי שֶׁרַק שִׂיא סֶקְיוּריטִי יוֹדַעַת לְלַמֵּד **נכון**, וְעִם **הַלֵּב**.

התכנית ללימודי מקצוע מנהל טכנולוגיות הגנת סייבר ומיישם הגנה (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, עוסקת 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 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:	14,600 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:	220 שעות
פתיחה:	ראה בעמוד הראשי של המכללה
מתכונת:	הלימודים בקמפוס המכללה ברמת גן, מתקיימים פעמיים בשבוע בימי בערב: 17:30 עד 21:00 (5 שעות אקדמיות למפגש), במשך כ-6חודשים
תרגול בית:	בהיקף 320 שעות

סגנון לימודי

טכני, Hands-on, ותיאורטי.

מעבדות תרגול בינלאומיות

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

עלות

סך 14,600 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.
- ראיון אישי לבחינת ההתאמה לתכנית.

מתכונת הלימודים

משך התכנית כ- 220 שעות כיתה, מהם כ-110 במתכונת לימוד מרוחק מקוון ו- 320 שעות משימות (סך הכל 540 שעות), פעמיים בשבוע בערב בשעות 17:30 עד 21:30 במשך כ- 8 חודשים, 5 שעות אקדמיות למפגש. הלימודים מתקיימים בקמפוס See Security ברמת-גן (צמוד לתחנת רכבת מרכז). המסלול נפתח כ- 3 פעמים בשנה.

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.

תכנית לימודים (מקוצר, ראה תכנית מלאה בדפים הבאים)

	נושא	שעות עיוני
1.	מבוא לאבטחת מידע והגנת הסייבר	15
2.	איומים, נוזקות והתקפות	10
3.	מבוא לטכנולוגיות הגנת רשת	10
4.	Vulnerability Scanning	10
5.	הצפנה ואימות	20
6.	אבטחה במערכות הפעלה והקשחת שרתים	25
7.	אבטחת תקשורת, אבטחת גישה לציוד תקשורת, בידול והפרדת רשתות תקשורת	90
8.	אבטחת ענן, שירותי אירוח, וירטואליזציה	10
9.	SCADA	5
10.	דלף מידע	10
11.	ניהול ורישום אירועי אבטחת מידע, טיפול באירועי אבטחת מידע	10
12.	בחינה מעשית – Hands On	5
	סך הכל:	**220**

סך הכל: 220 שעות לימוד.

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.

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

תכנית לימודים:

מבוא לאבטחת מידע והגנת הסייבר

הנושא מתמקד בהכרת מונחי יסוד ובניית השפה בה העוסקים בתחום מדברים, כותבים ודנים. בסיום הקורס הלומד אמור להכיר את השפה להבין את מורכבות נושא אבטחת מידע ככלל וסייבר בכלל.

- אונטולוגיה של אבטחת מידע וסייבר: מונחים, איומים, קשרים בין המונחים השונים, תפישת NIST, תפיסת האיכות quality assurance, ואונטולוגיות אחרות. המונח dependability.
- סוגי יריבים והמוטיבציה לתקיפה.
- סוגי תקיפות לרבות תקיפת מחשב מרחוק, מתוך הארגון, חדירה פיזית למתחמי מחשב.
- Social Engineering, תקיפות משולבות, שימוש במייל, הפניה לאתרים נושאי תוכנה זדונית.
- סוגי פגיעות במערכות / במידע לרבות בהיבטי זמינות, אמינות, שלמות וסודיות.
- השלכות ומשמעויות הפגיעה - כלכליות ,מוניטין ,משמעויות מעבר לרמת הארגון.
- 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, גופים לאומיים העוסקים בתחום בישראל.
- מדיניות ונהלים של אבטחת מידע.
- אבטחת מידע בפרויקט, הטמעת היבטי אבטחת מידע במחזור החיים לפיתוח תוכנה, לרבות השלבים של הפצה ליצור וניהול שינויים.

הגנת גישה בתקשורת ואינטרנט

הקורס מתמקד במנגנוני ההגנה של רשתות המחשבים שבארגון, מוצרי אבטחה , גישה מרחוק למשאבי הארגון וההגנה על דרכי גישה אלו. היבטי אבטחה בעת קישור הארגון לאינטרנט. מנגנוני אבטחה ופרוטוקולים אפליקטיביים של השכבות הגבוהות במודל OSI. בקורס ידונו הפרוטוקולים המרכזיים, שימושם והיבטי אבטחה של הפרוטוקולים. מנגנוני אבטחה אין חובה לדעת את נבכי ה-RFC של כל פרוטוקול ופרוטוקול.

בסיום הקורס על הלומד לדעת את מנגנוני ההגנה המתאימים לכל דרך גישה למשאבי הארגון. היבטי אבטחת מידע וחולשות מרכזיות. הבעייתיות שבקישור הרשת הארגונית כולה/ או חלקה לאינטרנט, מנגנוני הגנה, סוגי הפרוטוקולים השונים המשמשים לקישור אפליקטיבי , לציין את תפקידם, היבטי אבטחת מידע וחולשות מרכזיות, מי מפעיל איזה פרוטוקול.

- מוצרי אבטחה והגנה ל- WAN/LAN, Wireless ו- Bluetooth.
- גישה מרחוק למשאבי הארגון וההגנה על דרכי גישה אלו.
- טיפול בגישה באמצעות מחשבים/ מכשירים ניידים דוגמת טלפונים חכמים, iPad.
- הגדרת VLAN.
- היבטי אבטחת המידע/ רשתות /ארגון בעת קישור הרשת הארגונית לאינטרנט,
- מוצרי אבטחה,
- בנית DMZ, (נושא זה למעשה מבצע שימוש ביידע קודם של הנושאים שנלמדו.
- תיאור הפרוטוקולים האפליקטיביים, HTML5, HTML3, WebRTC, שימושים והיבטי אבטחה – חולשות שהתפרסמו. אין חובה לדעת את נבכי הפרוטוקול כפי המופיע ב- RFC.
- השלמה לבידול בן רשתות: נושאי ה- Web Filtering, וה- WAF (web application firewall).

בידול והפרדת רשתות תקשורת

הקורס מתמקד במנגנונים ומוצרים שעניינם הפרדת רשתות. אם רשתות פנים ארגוניות ואם של הרשת הארגונית כלפי העולם החיצון.

בסיום הקורס על הלומד לדעת את מנגנוני הבידול המתאים, יתרונות חסרונות. היבטי אבטחת מידע וחולשות מרכזיות. כיצד יש להקשיח את רשת התקשורת מפני מתקפות מבחוץ.

- מדוע נדרש הבידול, יסודות תאורטיים של בידול והפרדה.
- כיצד מבטיחים שיחד עם ההפרדה יהיה ניתן לאפשר לעובדים לממש את תפקידם.
- מוצרים ומנגנונים המשמשים להפרדה ובידול בין סביבות – רשתות תקשורת.
- ניטור המידע העובר בין הרשתות דוגמת Firewall, מחשבי Proxy, Mail relay, Content filtering, מוצרי Air Gap.
- הקשחת רשת התקשורת הארגונית

הצפנה ואימות

הקורס מתמקד ביסודות ההצפנה ופרוטוקולי אימות. בנוסף ילמדו פרוטוקולי התקשורת המשמשים לאימות משתמשים שימושם והיבטי אבטחה של כל פרוטוקול ופרוטוקול. אין חובה לדעת את נבכי ה-RFC של כל פרוטוקול ופרוטוקול.

בנוסף הלומד יתבקש ללמוד את הקשרים בין הפרוטוקול לציוד התקשורת, והשכבות בהן הפרוטוקול פועל.

בסיום הקורס על הלומד לדעת את סוגי הפרוטוקולים השונים, לציין את תפקידם, היבטי אבטחת מידע וחולשות מרכזיות, מי מפעיל איזה פרוטוקול.

- הצפנה סימטרית – DES 3DES, א-סימטרית, דפי הלמן, RSA,
- אימות משתמשים באמצעות דפי הלמן.
- יסודות - Certificate Authority, לאימות קצוות תקשורת, זיהוי משתמשים (הנושא של זיהוי ציוד ילמד בנפרד).
- פרוטוקולי תקשורת התומכים בנושא של הצפנה ואימות דוגמת: IPSEC, SSL, HTTPS, SSH.

אבטחת מידע במערכות הפעלה והקשחת שרתים

הקורס מיועד להכיר לתלמידים את היבטי אבטחת המידע במערכות ההפעלה השונות. להכיר ללומדים את העקרונות של הקשחת השרתים והשירותים השונים המטופלים במסגרת תהליכי ההקשחה.

בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של אבטחת מידע בכל מערכת הפעלה. חולשות מרכזיות הקימות במערכת. מתקפות ידועות. תהליכי הקשחה, התהליכים השונים והשירותים הניתנים ע"י מחשב מוקשח. כיצד לאפשר שירותים שונים ע"ג מחשב מוקשח.

- מימוש אבטחת מידע במסגרת שרותי מערכות ההפעלה הבאות: Unix, Win, Android, VM.
- יסודות תהליכי זיהוי ואימות משתמשים, קרברוס. הרשאות ל- Object ו- Subject, קבצים, קבוצות משתמשים. הנושא דנן ילמד לעומק בקורס שענינו אימות וזיהוי.
- לוגים של מערכת הפעלה התומכים באבטחת המידע.
- חלק תאורטי של מדוע נידרש לבצע הקשחת שרתים. עקרונות תהליך ההקשחה.
- הקשחה תלוית סביבות ושירותים,
- פעולות בסיסיות בסביבת מערכות ההפעלה השונות Unix, Win, VM.
- עדכון תוכנה חומרה לשרתים מוקשחים.
- בדיקת קשיחות לשרת.
- מוצרים תומכים בהקשחה.
- תאום עם מוצרי אבטחה לדיווח על אנומליות.

18 תוכנות זדוניות וזיהוי אנומליות

הקורס מיועד להכיר לתלמידים את נושא התוכנות הזדוניות דוגמת: וירוס מחשב, רוגלות. הסוגים השונים, דרכי הפצה, אופני התמודדות, מניעה ומוצרי הגנה מפני תוכנה זדונית. כיצד מזהים קיום של תוכנה זדונית, שימוש במנגנונים לזיהוי אנומליות בהתנהגות רשת והתנהגות מחשב, והפעולות שיש לנקוט בעת גילוי כאמור*.

בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של נושא התוכנה הזדונית והגנת הסביבה הממוחשבת מפניהם. דרכי הפצה, מניעה והתמודדות. מוצרים, קסטומיזציה של מוצרים, תפעול שותף של מוצרי ההגנה. להכיר את נושא זיהוי אנומליות בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של נושא זיהוי אנומליות, טיפול בסיסי בהתאם לנהלי הארגון ומוצרים תומכים בתחום.

- תאוריה וסוגים של תוכנות זדוניות, לדוגמא: Trojan, APT.
- תוכנה זדונית מוכוונת מטרה ויעד.
- שימוש בתוכנה זדונית לתקיפה, דוגמאות לדרכי הפצה.
- מוצרי אנטי וירוס, לשרתים, מחשבים אישיים, שרתי דואר, סביבת אינטרנט.
- התקנה, קסטומיזציה, עדכון.
- הבדלה בין מוצרים מבוססי חתימה למוצרים מבוססי התנהגות ומוצרים היברידיים.
- מתודולוגיות להתמודדות עם תוכנות זדוניות.
- מהי אנומליה, כיצד מזהים אנומליה ברשתות, במחשבים.
- טכניקות לזיהוי אנומליות - תלויות חוקים, תלויות זמן, תלויות משתמש, בניית פרופילים.
- מוצרים לזיהוי אנומליות. תהליכים ושיטות לטיפול באירוע .
- מוצרי IDS (intrusion detection systems)
- IPS (intrusion prevention systems)
- התקנה קסטומיזציה, תפעול שוטף ובדיקת לוגים.
- התראות שווא מול התראות אמת.
- זיהוי אנומליה מחייבת "הרמת דגל" והפניה לדרג בכיר

בקרת גישה

הקורס מיועד להכיר לתלמידים את נושא בקרת הגישה. הקורס מחולק לשני חלקים

בחלק הראשון ילמדו הנושאים של בקרת גישה של משתמשים, תוכנות לרכיבים, מידע במערכות המחשב ורכיבים שונים ברשת הארגונית. מוצרים שונים בתחום.

בחלק השני של הקורס ילמד התחום של מערכות ארגוניות לזיהוי ואימות משתמשים וחומרה.

בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של בקרת הגישה, תהליכים, התמודדות עם תקלות, וטיפול בחריגים, מערכות ארגוניות לזיהוי ואימות משתמשים.

חלק ראשון

- זיהוי ואימות משתמשים תאוריה, חזרה קצרה על המנגנונים הקיימים במערכת ההפעלה לזיהוי ואימות משתמשים.
- המושג של Multifactor authentication
- תוכנה/ חומרה נוספת לזיהוי ואימות משתמשים דוגמת: Tokens, Smart cards,
- ו- Biometric devices
- תהליכי קישור רכיב החומרה למשתמש ספציפי, טיפול בחריגים – אובדן, משתמש חדש במערכת, משתמש העוזב את הארגון. התפיסה של שימוש ביותר מרכיב אחד לזיהוי משתמש לדוגמא שימוש במוצר ביומטרי לזיהוי המשתמש + סיסמא.

חלק שני

- הגדרה ושימוש במערכות Identity management, כלל ארגוניות לזיהוי ואימות משתמשים והרשאותיהם במערכות השונות, Credentials.
- התממשקות עם DNS לניהול משתמשים כאמור.
- התראה על אירועים.
- זיהוי גישה של מכשירים ניידים מותרים (גישת BYOD),
- ניהול האפליקציות והגישה אליהן – מוצרי MAM (Mobile application management)
- פעולות למניעת התחברות של ציוד בלתי מורשה דוגמת מחשב נייד לרשת הארגונית.
- מוצרים וטכנולוגיות בתחום, שימוש ב- certificate אירגוני לזיהוי ציוד תקשורת.

דלף מידע

הקורס מיועד להכיר לתלמידים את נושא דלף המידע הארגוני, הסכנות שבו, תהליכי מניעה/ צמצום/ גילוי. מוצרים התומכים בהגנת המידע הארגוני מפני דלף מידע. בהתנהגות רשת והתנהגות מחשב, והפעולות שיש לנקוט בעת גילוי כאמור.

בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של נושא דלף המידע וכיצד ניתן לפעול למניעתו/ צמצומו/ גילוי עובדת קיום דלף מידע.

- הגדרת המושג, מהיכן יכול לדלוף, ערוצים, כיצד מזהים, אמצעים ושיטות קיימות למניעה/ צמצום התופעה, לזיהוי ואיתור.
- היבטי חוק בנושא דלף מידע.
- הגנה / מניעה/ צמצום של דלף מידע במסדי נתונים, storage systems.

- הגנה / מניעה/ צמצום של דלף מידע בהתקנים ניידים דוגמת טלפונים חכמים, מחשבים ניידים.
- התקני זיכרון נתיקים – disk-on-key, דיסק נתיק.
- מוצרים וטכנולוגיות למניעה/ גילוי/ זיהוי – דוגמת מוצרי content filtering

ניהול ורישום של אירועי אבטחת מידע (Audit)

הנושא מיועד להכיר לתלמידים את נושא רישום וניהול אירועי אבטחת מידע על סוגיהם השונים. לדוגמא זיהוי ממוכן של וירוס, ניסיון חדירה למערכות הארגון, ניסיון להוציא מידע אל מחוץ לארגון ע"י בלתי מורשה – דלף מידע, וכו'. בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של ניהול ורישום של אירועי אבטחה אופן ההתמודדות - מותנה בנהלי הארגון.

- חלק תאורטי מהו הנושא מדוע נידרש ניהול ידני לחצי ידני
- מוצרים תומכים מוצרי SOC (security operation center)
- מוצרי SIEM (security information event management),
- מוצרי NAC (network access control)
- סנסורים – התקנה וקונפיגורציה. תהליך הגדרה של חוקים במוצר, התראות שווא למול התראות אמת, מעקב, עדכון, תחזוקה.
- שילוב מוצרים אלו בארגון, קביעת מסלולי דיווח.
- אופן התייחסות למידע התרעתי המתקבל ממקור חיצוני לארגון, ניסיון חדירה מבחוץ.
- אופן ההתייחסות למידע הרתעתי המתקבל ממקור פנימי, מיתוך הארגון המתקבל מכל מחשב וציוד המותקן בארגון ו/או הרשאי לגשת למשאבי הארגון.

היבטי אבטחת מידע בציוד תקשורת והקשחה

חלק תאורטי המבהיר מדוע נידרש לבצע הקשחת נתבים:

- עקרונות תהליך ההקשחה.
- הקשחה תלוית ציוד תקשורת (לדוגמא נתב של CISCO לעומת נתב של חברה אחרת)
- עדכון תוכנה, firmware, לציוד התקשורת.
- בדיקת קשיחות לציוד.
- מוצרים תומכים בהקשחה.
- תאום עם מוצרי אבטחה לדיווח על אנומליות.

מחשוב ענן, שירותי אירוח, וירטואליזציה

נושא זה בא להכיר בפני הלומד את העקרונות הללו. הסיבה המרכזית לאיחוד הנושאים בנקודה אחת היא היותם נושאים תלויי ארגון והמידע שבארגון, ותלויי חוק.

מחשוב ענן

- הכרות, הסוגים השונים של מחשוב ענן. קבלת דיווחים מהלוגים השונים והבנתם. היבטי חוק. זיהוי אנומליות, מוצרים תומכי אבטחה של האורח והמארח.

שירותי אירוח

- הכרות, הסוגים השונים של משירותי אירוח. קבלת דיווחים מהלוגים השונים והבנתם. היבטי חוק. זיהוי אנומליות, מוצרים תומכי אבטחה של האורח והמארח.

וירטואליזציה

- הכרות וצורך בסביבת VM, לסוגיו, היבטי אבטחה מהיבט החוק מפני שהנושא דנן נלמד מהיבטים טכניים בעבר

טיפול באירועי אבטחה

10

בקורס זה מציג בפני הלומד את העקרונות של טיפול באירועי אבטחה. הבנת הסיטואציה של קיום מתקפה, שלבי המתקפה וכיצד לטפל באירוע. קורס זה מהווה אינטגרציה של הידע הנלמד בקורסים שונים.

בסיום הקורס הלומד אמור להבין כיצד נושאים שונים שלמד מתממשקים, ויסודות הטיפול באירוע אבטחה. ברור כי נושאים אלה הם תלויי ארגון והמידע שבארגון, ותלויי חוק.

- הכרת סוגי תקיפות דוגמת: DoS/ DDoS, Spear Phishing, וכו

- הבנת תהליך ביצוע התקיפה, שלבי המתקפה, משך המתקפה – לדוגמא: התקיפה מתחילה במשלוח דואר תמים המכיל קובץ עם תוכנה זדונית.
- הבנת הנזק (impact) הנגרם מהתקיפה.
- אמצעים העשויים לסייע לארגון לזיהוי קיומה של תקיפה.
- אמצעים העשויים לסייע בבלימת התקיפה.
- הכרות עם הנושא של התראות שווא, false positive ו-false negative.
- אופן הטיפול בתקיפות שהתגלו (גישות ומוצרים)
- הפעלת מנגנונים בולמים ובדיקת יעילותם,

- בדיקת נזקים, מימוש תהליכים פורנזיים
- תהליכי שחזור,
- בדיקת הפתרון שניתן
- הפקת לקחים ברמות הארגוניות השונות.
- הרחבת בסיס הידע הארגוני
- פניה דיווח לרשויות החוק.

<u>הצהרת תלמיד בלימודי CSP</u>

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

שם הנרשם: _____ תאריך: _____ חתימה _____

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

נא לרשום אותי לתוכנית הלימודים ברמת גן

קורס CSP

<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