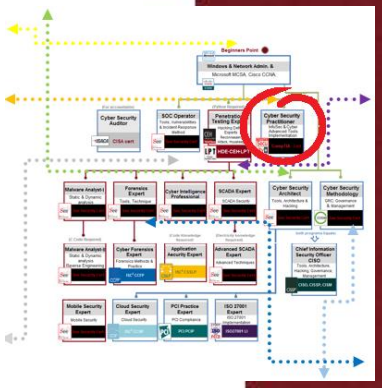


התכנית ללימודי מקצוע
מיישם הגנת סייבר
על-פי מערך הסייבר הלאומי
(אסדרת מקצועות הסייבר בישראל)

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

תכנית מפוקחת על-ידי מדינת ישראל*, כולל תעודה רשמית של מדינת ישראל למקצוע מיישם, כולל הכנה למבחני מערך הסייבר (2018) וכולל הכנה להסמכה הבינלאומית Security+,

* חוק חיילים משוחררים התשנ"ד, אישור מס' 02436069

משרד ראש הממשלה
מערך הסייבר הלאומי

תכנית זו יחידה מסוגה ברחבי העולם, ומשלבת הסמכת סייבר בינלאומית עם מעבדות ייחודיות מסוגן לתרגול Hands-on.

See
cyber security college

להיות מומחה טכנולוגיות ומתודולוגיות הגנת סייבר.

מומחה טכנולוגיות: 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.

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.

וְלֹא פָּחוֹת חָשׁוּב: נִלְמָד כְּפִי שֶׁרַק שִׂיא סֶקְיוּרִיטִי יוֹדַעַת לְלַמֵּד, עִם הַלֵּב.

תכנית הסמכה רשמית ומעבדות ללימודי מקצוע מיישם הגנת סייבר:
CSP: Cyber Security Practitioner

התוכנית נבנתה לדרישת מערך הסייבר הלאומי (ההוראה לאסדרת מקצועות הסייבר בישראל)

מנהל התכנית: המנהל האקדמי של המכללה, מר נדב נחמיאס

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 CSP – מיישמי הגנת סייבר

תכנית זו מופעלת בהתאמה לדרישות המערך למקצוע מיישם הגנת סייבר, וכוללת הכנה להסמכות הבינלאומיות **Security+** של ארגון CompTIA או **SSCP** של $(ISC)^2$, לצד עבודת Hands-on רבה.

סגנון לימודי - טכני, תיאורטי ו- Hands On.

עלות:

סך 400 ₪ דמי רישום וכן 16,500 ₪ דמי לימוד כולל מע"מ.

סגל המרצים

המרצים של תכנית זו הנם גאוות המכללה. כולם בוגרים, בגילאים 30 עד 40, מקצוענים, כולם מחויבים לציון ממוצע 9 במשובי תלמידים: יקי בן-ניסן, רן לוי, יניב אבולוב, אריאל חסון, משה פרבר, עידו הכהן, איציק משה, מיטל ברוקס, יריב הלפרן, אורן פנסו, עמי צרפתי, אלעזר בירו, אלכס ליביס, אלי טונקל, אורן מעוז, יוסי סאסי, איציק כוכב, וכן המנהל האקדמי של המכללה, נדב נחמיאס, המשמש גם כמנהל תכנית CISO הבכירה.

הסמכות בינלאומיות

- See-Security: "CSP: Cyber Security Practitioner"
- CompTIA Security+ or: $(ISC)^2$ SSCP*

מכללת See Security היא הנציגה **היחידה** של שני גופי ההסמכה הבינלאומיים $(ISC)^2$ ו- CompTIA. לכן, לימודים אלו חושפים אותך לתכנים יעודיים יקרי ערך, אשר יובילו אותך להסמכה. המכללה לא מאשרת לגופים אחרים לעשות שימוש בחומרי הלימוד המקוריים. **בבוונת מערך הסייבר למסד ב-2018 מבחן להסמכה ייחודית של מערך הסייבר בישראל, על-בסיס תכנית זו.**

CSP: CYBER SECURITY PRACTITIONER PROGRAM
(Security+ certification included)

מעבדות תרגול בינלאומיות

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

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.

דרישות סף

- שליטה ב- Windows Servers, תקשורת, יסודות Linux.
- בוגרי 12 שנות לימוד, (או: תנאי הקבלה לחרדים מבחן מיון והתאמה למקצוע: ישיבה קטנה / ישיבה גדולה).
- ראיון אישי עם אבי ויסמן / וועדת קבלה / ועדת חריגים.

אחרי סיום הלימודים – הצעד הבא

לאחר סיום תכנית זו:

1. במישור התעסוקתי: התחל לעבוד כמיישם הגנת סייבר, העזר בבוגרים נאמנים ומרוצים מאוד של המכללה אשר משולבים בענף, ובחברת ההשמה SeeHR, וגם:
2. במישור ההתפתחותי: התחל את "***הצעד הבא***": תכנית **מומחה טכנולוגיות הגנת סייבר**: **CSTP** (**ארכיטקט**).

למידע נוסף / פגישת יעוץ:

מידע מינהלי: אלוירה אליסייב, 03-6122831, 052-8787889, elvira@see-security.com

יועץ אקדמי: אבי ויסמן, 03-5799555, 054-5222305, avi@see-security.com

שעות כיתה ומשימות אישיות

306 שעות כיתה ומעבדות, לרבות Remote Lab, וכן 320 שעות משימות אישיות.

מתכונת לימודים

הלימודים בקמפוס המכללה ברמת גן (צמוד לתחנת רכבת מרכז), מתקיימים פעמיים בשבוע בערב, 17:30 עד 21:30 במשך כ- 10 חודשים, 5 שעות אקדמיות למפגש.

זכאות לתעודה

קיימת חובת נוכחות ב-80% מהמפגשים. קבלת תעודת המכללה מותנית בעמידה במבחני מעבר, בציון 70 לפחות (מבחן חוזר ללא תשלום). לעומדים בדרישות התכנית תוענק תעודת הסמכה יוקרתית מטעם המכללה:

"מיישם אבטחת מידע CSP: Cyber Security Practitioner"

בנוסף להסמכות הבינלאומיות כמפורט (Security+ או SSCP).

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

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

תכנית לימודים (מקוצר, ראה תכנית מלאה בדפים הבאים)

נושא	שעות עיוני	שעות מעבדה
1. מבוא לאבטחת מידע והגנת הסייבר	15	
2. אבטחה פיסית	2	
3. הגנת גישה בתקשורת ואינטרנט	20	10
4. בידול והפרדת רשתות תקשורת	5	5
5. אבטחת מידע בציוד תקשורת והקשחה	10	10
6. הצפנה ואימות	10	5
7. בקרת גישה	10	5
8. אבטחה במערכות הפעלה והקשחת שרתים	20	20
9. היבטי אבטחת מידע במסדי נתונים	5	5
10. תוכנות זדוניות וזיהוי אנומליות	10	5
11. דלף מידע	5	2
12. ניהול ורישום אירועי אבטחת מידע (Audit)	5	2
13. טיפול באירועי אבטחת מידע	5	5
14. מחשוב ענן, שירותי אירוח, וירטואליזציה	5	
15. שינוע מידע מ/אל הארגון	2	
16. המשכיות עסקית (BCP/DRP)	5	5
17. אבטחה אפליקטיבית	5	
18. תקני אבטחת מידע וניהול סיכונים	10	2
19. ביצוע ניסיונות חוסן (תשתית ואפליקציה)	10	10
20. חוק ואתיקה	9	1
21. משימות תרגול אישיות		46
סך הכל:	**168**	**138**

סך הכל: 306 שעות לימוד.

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?

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.

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 SOC-IR – מומחה ניטור במרכז ניטור ותגובה לאירועי סייבר.**

A SOC-IR specialist is responsible for critical core subjects in operating cyber monitoring centers and primary response teams. The SOC operator performs the preliminary necessary actions when a cyber-event is identified.

3. **להמשיך בצעד הבא - תכנית הלימודים CSTP – ארכיטקט הגנת סייבר.**

A person with an academic background, wide-ranging and profound theoretical knowledge, whom is in charge of:

A. Designing technological solutions for cyber protection in the organization combining technologies and security methods.
B. Adjusting cyber protection products and integrating them in the IT infrastructure, including storage and backup.
C. Accompanying the process of handling security events with a technology standpoint, acknowledging the organization activities, needs and objectives.
D. May includes International Certification such as CompTIA Security+, or $(ISC)^2$ SSCP.
E. This is in recognition of understanding of the activities, needs and corporate objectives.

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

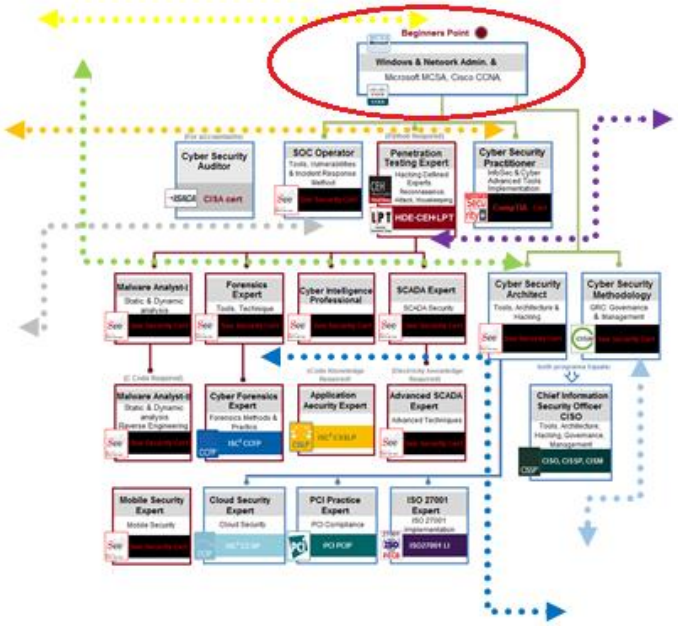
Before this course, the candidate should complete his knowledge in Linux Essentials and Python code.

An Expert with wide and up dated knowledge as well as practical abilities in vulnerabilities detection and penetration testing in cyber systems.

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	16

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.

מבנה המחשב	2

תת הקורס מיועד להכיר לתלמידים יסודות מבנה מחשב בהיבטי של חומרה, מבנה סכמתי תפקידי הרכיבים. מתקפות ידועות על חלק מהרכיבים (דוגמא מתקפה על ה-BIOS).

בסיום הקורס הלומד אמור להכיר את רכיבי החומרה העקרים ואת תפקידם. בנוסף אמור הלומד להכיר מספר תקיפות ומאפייני תקיפות מול הרכיבים הרלוונטיים.

- הכרת חלקי מחשב, לדוגמא: RAM, ROM, ALU, CPUלרבות ריבוי ליבות, GPU, אמצעי אחסון, BIOS, UEFI (Unified extensible firmware interface).
- תפקיד כל רכיב מבנה סכמתי, אופני הקישור בין הרכיבים – BUS, הקישור בין כל הרכיבים
- מתקפות ידועות על חלק מהרכיבים (דוגמא מתקפה על ה-BIOS).

אבטחה פיזית	2

סביבת המחשב הארגונית אמורה להיות מוגנת ומאובטחת מפני חדירה פיזית, גישה ע"י בלתי מורשים או אבטחה מפני אירועי קיצון דוגמת רעידות אדמה. קורס זה מציג בפני הלומד מתודולוגיות שונות ואמצעים להגנת אתרי המחשב הפיזיים, בהם מצוי המידע הארגוני והמחשבים הארגוניים, לרבות סביבת העבודה של העובדים.

בסיום הקורס הלומד אמור להכיר את אמצעי האבטחה הפיזיים, מנגנוני הניטור והבקרה והאמצעים העומדים לרשות הארגון לטיפול באירועי קיצון.

- הנחיות החוק בדבר אבטחת סביבת המחשוב.
- על מה מגנים
- אמצעי אבטחה וניטור למניעת גישה ע"י בלתי מורשים.
- אמצעים לטיפול בפני אירועי קיצון שונים דוגמת הפסקת חשמל, רעידת אדמה, מלחמה.

הגנת גישה בתקשורת ואינטרנט — 30

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 — 8

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 — 16

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 — 40

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.

היבטי אבטחת מידע במסדי נתונים 10

הקורס מיועד להכיר לתלמידים את היבטי אבטחת המידע – גישת משתמשים, הגנה על מידע נייח, במערכות מסדי נתונים וב- Storage systems. חולשות ואופני הגנה.

בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של אבטחת מידע במסדי נתונים כאמור לעייל, חולשות מרכזיות הקימות במערכת, אופני ההגנה, ומוצרים משלימים, ומתקפות ידועות.

- יסודות מסדי נתונים: SQL, Relational DB, MongoDB, ארכיטקטורה.
- היבטי אבטחת מידע במערכות הנ"ל, הגנת גישה, הגבלת מידע לצפייה/ עדכון פעולות תוכנה נדרשות (לדוגמא: בדיקת אורכי שדות קלט) חולשות ידועות, ומתקפות ידועות.
- תמיכת מערכת ההפעלה בשמירה על מסדי הנתונים, תמיכת תוכנת מסד הנתונים בנושאי אבטחה.
- Referential integrity,
- מוצרים משלימים שמעבר לאשר ניתן ע"י מ"ה, מערכות Storage systems ואבטחת המידע בהם.

המשכיות עסקית (BCP/ DRP) 8

הקורס מיועד להכיר לתלמידים את נושא הגיבוי, השחזור והתאוששות מאסון על היבטיו וברמות השונות של גיבוי ושחזור. תמיכת מערכת ההפעלה בנושא ומוצרים משלימים. היבטי אבטחת מידע בנושא.

בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של נושא הגיבוי השחזור וההתאוששות מאסון, תמיכת מערכת ההפעלה ומוצרים משלימים.

- תאוריה של DRP and BCP, מתודולוגית לגיבוי ושחזור - גיבוי מלא, חלקי, שימוש בלוגים כגיבוי.
- שיטות תלויות סביבה – אתרי מחשב מפוצלים, מערכות הפעלה שונות.
- שרותי מערכות ההפעלה לגיבוי ושחזור.
- מוצרים חיצוניים משלימים
- היבטים אירגוניים של התאוששות מאסון
- היבטי אבטחת מידע של נושא הגיבוי והשחזור . לדוגמא: הרשאות יתר למשתמשים המבצעים פעולות אלו, היכולת לעיין במידע שאינם מורשים לו.
- מוצרי Storage systems אופני הגנה על המידע האגור בהם, גיבוי והתאוששות ואופני הגנה במוצרים אלו.

תוכנות זדוניות וזיהוי אנומליות 18

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: APT ,Trojan.
- 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 20

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 ארגוני לזיהוי ציוד תקשורת.

דלף מידע — 6

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) — 8

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 — 16

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 — 5

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

שינוע מידע מ/אל הארגון — 2

הנושא יחשוף ללומד את העקרונות המתודולוגיות הנהוגות בנושא שינוע מידע מ/אל הארגון באמצעים פיזיים דוגמת מצאי מידע מגנטיים ואופטיים. מטבע הדברים נושא זה הינו תלויי ארגון, המידע שבארגון והנחיות החוק.

בסיום הקורס הלומד אמור לדעת ולהכיר את היבטי אבטחת המידע והסיכונים הקיימים בעת שינוע מידע מ /אל הארגון והשיטות המקובלות להגן על מידע זה.

- היבטי אבטחת המידע בעת הכנסת מידע לארגון באמצעות מצעי מידע מגנטיים ואופטיים.
- שינוע גיבויים.
- נהלים ומתודולוגיות.
- תחנות "הלבנה"
- תהליכי "השחרה"

אבטחה אפליקטיבית — 8

התלמיד יחשף לעקרונות ולמתודולוגיות הנהוגות בנושא הטמעת היבטי אבטחת מידע בתוכנה, ניהול שינויי תוכנה והיבטים של מבדקי אבטחת מידע בתוכנה. הקשר בין איכות תוכנה לאבטחת מידע ואמינות תוכנה. בסיום הקורס הלומד אמור להכיר את התהליכים השונים למימוש בעת מחזור החיים של פיתוח תוכנה ושינויים בתוכנה.

- זיהוי הסיכונים העומדים בפני מערכת התוכנה/ אפליקציה.
- קביעת דרישות אבטחת מידע ממערכת התוכנה/ אפליקציה.
- הפעילויות השונות, בהיבטי אבטחת מידע, שיש לבצע בכל שלב של מחזור חיי פיתוח התוכנה/ אפליקציה.
- הוספת Control Gates לאיכות תוכנה ולאבטחת מידע.
- מבדקי אבטחת מידע, Testing.

תקני אבטחת מידע וניהול סיכונים — 10

הנושא עוסק בתקני האבטחה ו- Best practices מקובלים בתחום אבטחת המידע והסייבר. יסודות סקר סיכונים, סוגי סקרים, כיצד מתבצע, מטרות, פעילויות להקטנת סיכון, מושגים של סיכון וסיכון שיורי. בסיום הנושא הלומד יכיר תקנים, Best practices, יבין מה הסיבה והיתרון המתקבל מקיומם, כיצד הם משפרים את ההגנה על הארגון, מהם חסרונותיהם, וההבדלים בין התקנים, מושגי הסיכון, תהליך ומטרות ביצוע סקר סיכונים, ופעילות להקטנת סיכונים.

- תקני ISO27K, ותקנים של סקרי סיכונים.
- מתודולוגיות לביצוע סקרי סיכונים
- השלבים השונים של סקר סיכונים.
- היעדים של סקרי סיכונים
- סוגים – כמותי איכותי משולב.
- נשוא הסקרים – אפליקציות, תשתיות, למערכות האבטחה, שילוב סקרים.

מתודולוגיות ביצוע בדיקות חוסן – תשתיות ואפליקציות — 18

הנושא יחשוף בפני הלומד את העקרונות המתודולוגיות הנהוגות בנושא מבדקי חוסן לתשתיות הארגון – תקשורת, אבטחת מידע, אתר אינטרנט, ואפליקציות ומערכות מחשב.

בסיום הקורס הלומד אמור להכיר את הנושאים השונים בתהליכי ביצוע מבדקי עמידות.

- מתודולוגיות לביצוע מבדקי עמידות.
- הרכיבים השונים של מבדקי העמידות.
- זיהוי חולשות פוטנציאליות במערכות.
- הכרות עם כלי תוכנה מקובלים בתחום.
- תהליכי דיווח הממצאים.

חוק ואתיקה — 9

הקורס בנוי משלושה חלקים:

החלק הראשון מתמקד בהכרת חוקי מדינת ישראל העוסקים בתחומי הגנת הפרטיות ומחשבים, תקינה, החלטות ממשלה ואסדרה בנושא הגנת הסייבר.

החלק השני של הקורס יעסוק באתיקה של העוסקים במקצוע דוגמת מומחי הקשחת ציוד ובודקי עמידות מערכות.

החלק השלישי של הקורס יעסוק בחוקים בינלאומיים בנושא סייבר, הגנת הפרטיות בעולם – אירופה, ארה"ב .

בסיום הקורס הלומד אמור להכיר החוקים, התקנות וההנחיות בארץ, להבין מהיכן נובעים השינויים בהנחיות השונות, להבין את המשמעויות של פעולות שאינן עולות בקנה אחד עם החוק. להבין את מחויבותו האתית למקצוע ולמקום העבודה.

- חוקי מדינת ישראל: חוק הגנת הפרטיות, חוק המחשבים, הנחיות בנק ישראל, הנחיות הבורסה לני"ע, וכו'. החלטות ממשלה ואסדרה בנושא הגנת הסייבר.
- אתיקה מקצועית.

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.

We invented a methodology for cyber education,

because nobody else did it.