

קורס לוחמת סייבר ואבטחת מידע

לנוער בגילאים שונים



תחרות לוחמת סייבר בין הקורסים השונים לנוער!



קידום הנוער בתחומי ההייטק השונים!



קבלת תעודת בוגר "מבוא לסייבר" מטעם סייבר פור יו



בשיתוף האקדמיה של סיסקו ישראל

במסגרת התכנית, מקבלים המשתתפים את הכלים והידע העדכני ביותר על מנת להתחיל את הצעדים הראשונים שלהם בתחום הסייבר! והכל באונליין!

Python



Cyber תשתיות



Cisco



Linux



וירטואליזציה



תכנית הלימודים מתרכזת בהקניה של ארבעה צירי למידה מרכזיים:



1 הקניית ערכי למידה מתאימים ככלי להצלחה בתחום!

2 פיתוח יכולות ניתוח מערכות ממוחשבות

3 הבנת מבנה המחשב והרשת

4 למידה פעילה, חשיבה יצירתית והתנסות מעשית

קורס לוחמת סייבר ואבטחת מידע

לנוער בגילאים שונים

צוות החוקרים והמרצים שלנו מורכב מיוצאי יחידות המודיעין של צה"ל והאקדמיה ומומחי אבטחת מידע בעלי אוריינטציה פדגוגית ודידקטית עתירת ניסיון. מערך ההכשרה מבוסס על מיפוי כל תתי-הנושאים של תחום ההייטק, עקב-אחר-אגודל, עד לרמות העומק הרלוונטיות בהתאמה אישית לכל תלמיד.

בהתחשב במגבלות שעות הקורס המתקשב, החברה מספקת לתלמידיה חומרי לימוד מקוונים רבים על מנת להעמיק משמעותית את היקף הידע שלהם.

כותבי התוכניות המובילים, המרצים, שיטת הלימוד המוקפדת, והניסיון הרב אשר הוביל לנוסחאות המצליחות, הם הגורמים העיקריים ליצירת המוניטין של Cyber For you כמומחה בתחום הדרכות ההייטק בארץ ובעולם, ועכשיו - גם באונליין!

החברה חרטה על דגלה להנגיש את תחום ההייטק לנוער במדינת ישראל, תוך מתן דגש על 3 עקרונות מרכזיים:

הייטק לכולם



היכולת להצליח בתחום ההייטק תלויה בפונטציאל המתבטא ביצירתיות, חשיבה "מחוץ לקופסא" והשקעה, ללא קשר לפרמטרים המנבאים הצלחה במקצועות הקונבנציונאליים (מספר יח"ל, ציון פסיכומטרי וכדו') לכן, החברה מאפשרת קבלת תלמידים ללא תנאי קבלה מוקדמים!

עד הבית



החברה מבצעת את הקורסים באונליין ללא צורך לצאת מהבית כאשר מבנה הסילבוס מותאם ספציפית לתלמידי חט"ב ותיכון, כך שהתלמידים בגילאים השונים ילמדו על פי סילבוס המותאם להם אישית.

מחיר הוגן



על מנת להתמחות בתחומי ההייטק השונים, נדרשים נרשמי הקורסים בחברות השונות לשלם כסף רב, עקב כך, נסגרת הדלת למספר רב של מוחות פוטנציאליים המתאימים לתחום. חברת Cyber For You החליטה על מחיר אחיד, מוזל ומוסכם מראש לכל שעת קורס, המופחת משמעותית ממחיר שעת לימוד במוסדות השונים.

קורס לוחמת סייבר ואבטחת מידע

לנוער בגילאים שונים

בשנים האחרונות חלה עלייה בביקוש לאנשי האקינג מקצועיים ועקב כך עלה בהתאמה הביקוש בקרב הציבור לרכוש את המקצוע המבוקש. בוגרי הקורס נדרשים לגלות מקצועיות, יצירתיות, מיומנות בפתירת תקלות, בעיות אבטחה ופרצות באתרים שונים. קורס האקינג, מקנה ללומדים את כל הכלים הרלוונטיים להצלחה כמבוא משמעותי לתחום.

אבטחת מידע זהו תחום הגנה הקשור לעולם המחשבים והאינטרנט. בעידן בו ניתן בקלות לפרוץ למחשב הפרטי או העסקי שלכם, דרושים אנשי מקצוע שיילחמו בתופעה. עלינו לזכור כי האינטרנט מוצף במידע סודי רב, וגם מחשבכם האישי הנתון בסכנה עלול להיות קורבן. בימים בהם הכל מתנהל מול המחשב, אנחנו מוצאים את עצמנו חשופים להתקפות ולפריצות. זו הסיבה שאבטחת מידע היא תחום חשוב שיש להתמחות בו באופן מעמיק.



היקף שעות הקורס



כיתות ז' - ט' - 22 שעות אקדמיות.
הקורס מורכב מ-11 מפגשים.

22
שעות אקדמיות

כיתות י' - י"ב - 22 שעות אקדמיות.
הקורס מורכב מ-11 מפגשים.

22
שעות אקדמיות

מחיר



399 ש"ח

המחיר הוא בעבור כל הקורס כולל דמי הרשמה.
לא יינתן החזר בעלות הקורס מכל סיבה שהיא.

קורס לוחמת סייבר ואבטחת מידע

לנוער בגילאים שונים



תנאים מוקדמים



- 1 שליטה בסיסית במחשב
- 2 חשיבה יצירתית ומכונות להשקעה
- 3 שליטה בסיסית בשפה האנגלית

מה לומדים בקורס ?



התלמידים בקורס ירכשו את הכלים הבסיסיים לצורכי הגנה והתקפה בעולם המחשב. הנושאים בקורס כוללים את עולם ההצפנות, אסטרטגיות הגנה, חוקי האקינג ועוד. בנוסף, התלמידים בקורס יקבלו את ההכשרה המתאימה למיומנויות פריצה לרשתות תקשורת ולמערכות תקשורת של סלולריים ויישומי אינטרנט. והכל עם מרצים בעלי ניסיון רב בהכשרות אונליין לנוער!

התכנים המועברים:



פרק 1 : מבוא למחשב

- הכרת המחשב - חומרה
- הכרת המחשב - מערכות הפעלה ותכונותיהן הבסיסיות
- לינוקס



פרק 2 : הצורך באבטחת סייבר

- מידע אישי
- מידע ארגוני
- תקיפות ומומחי אבטחת מידע
- לוחמת סייבר

קורס לוחמת סייבר ואבטחת מידע

לנוער בגילאים שונים

פרק 9 : אומנות האמינות

- סוגי בקרה
- חתימות דיגיטליות
- רישיונות
- מאגרי מידע

פרק 3 : תקיפות, מושגים וטכניקות

- מבוא
- ניתוח מתקפת סייבר
- עולם אבטחת סייבר

פרק 10 : מושג חמשת התשיעיות (Five Nines)

- זמינות גבוהה (המודל)
- מדדים לשיפור זמינות
- מענה לתקריות
- התאוששות מאסון

פרק 4 : הגנה על מידע אישי ופרטיות

- הגנה על המידע האישי
- שמירה על פרטיותך במרחב הסייבר

פרק 5 : אבטחת סייבר: תקיפה והגנה

- פושעים ומומחים בעולם הסייבר
- איומים נפוצים
- התפשטות איומי סייבר

פרק 11 : הגנה על הארגון

- Firewalls
- גישות לאבטחת סייבר – זיהוי התנהגותי
- הפתרון של סיסקו לאבטחת סייבר

פרק 6 : קוביית אבטחת הסייבר

- שלושת מימדי הקובייה
- CIA (Confidentiality, Integrity, Availability)
- מצבי מידע
- אמצעי נגד

פרק 7 : איומים, הונאות ותקיפות

- תוכנה זדונית
- הונאות
- תקיפות

פרק 8 : אומנות ההגנה על סודות

- קריפטוגרפיה
- בקרת גישה
- הסתרת מידע



קורס לוחמת סייבר ואבטחת מידע

לנוער בגילאים שונים



רשימת נושאים כללית - חלק מן הנושאים יילמדו עצמאית

פירוט	נושא	1
את המחשב וחלקיו עלינו להכיר על מנת שנוכל ללמוד להגן על עמדת העבודה.	הכרת המחשב – חומרה	1
הכרת סוגי <u>מערכות ההפעלה</u> שקיימים היום: מיקרוסופט, לינוקס, אנדרואיד, IOS. <u>ותכונות בסיסיות של המערכות</u> : מנהל התקנים, ניהול דיסקים, איחוי דיסק ועוד.	הכרת המחשב – מערכות ההפעלה ותכונות בסיסיות שלהן.	2
<ul style="list-style-type: none"> הכרה מעמיקה יותר של מערכת ההפעלה לינוקס המשרתת את תחום אבטחת המידע היכרות עם סביבת Bash 	הכרת המחשב – מערכת הפעלה - לינוקס	3
<ul style="list-style-type: none"> מה זה אבטחת סייבר <u>מידע אישי</u>: הזהות שלנו און ליין ובחיים, המידע שלנו, היכן נמצא המידע באינטרנט שלנו, המכשירים שלנו ומה מחפשים ההאקרים. <u>מידע ארגוני</u>: סוגי מידע ארגוני, מערכות מידע ו-IoT, משמעות פירצת אבטחה לארגון, דוגמאות לפרצות אבטחה. 	הצורך באבטחת מידע: רקע, מידע אישי ומידע ארגוני	4
<ul style="list-style-type: none"> <u>פרופיל התוקף</u>: סוגי תוקפים, איומים פנימיים וחיצוניים קצת על <u>חוק ואתיקה</u> בתחום אבטחת סייבר <u>לוחמת סייבר</u>: מהי לוחמת סייבר ומה מטרותיה 	הצורך באבטחת מידע: תקיפות ומומחי אבטחת מידע ולוחמת סייבר	5
<ul style="list-style-type: none"> פרצות אבטחה וניצול סוגי פרצות אבטחה סוגי תוכנות זדוניות וזיהוין אופני חדירה חסימה לשירות 	תקיפות, מושגים וטכניקות – ניתוח תקיפה	6
<ul style="list-style-type: none"> תקיפה מעורבת הפחתת הנזק של תקיפה – פעולות שניתן לבצע כדי להפחית נזקי תקיפה סיכום 	תקיפות, מושגים וטכניקות – עולם הסייבר	7
<ul style="list-style-type: none"> הגנה על מכשירים הגנה על תקשורת תחזוקת מידע שמירה על הפרטיות במרחב הסייבר: סיסמאות, עודף מידע 	הגנה על מידע אישי ופרטיות	8
<ul style="list-style-type: none"> דומיינים (Domains) באבטחת סייבר – היכרות ודוגמאות פושעי אבטחת סייבר מומחי אבטחת סייבר איומים נפוצים: זירות, אופן הפצה, מורכבותם 	אבטחת סייבר: תקיפה והגנה	9

מס' מפגש	נושא	פירוט
10	מודל קוביית אבטחת הסייבר – שלושת המימדים ומודל ה-CIA	<ul style="list-style-type: none"> שלושת המימדים: עקרונות אבטחה, נתונים, הגנות CIA Confidentiality – עקרונות, הגנה על פרטיות מידע, שליטה בגישה, החוק Integrity – עקרונות, צורך ומדידה Availability – עקרונות, חמשת התשיעיות (99.999%), הבטחת זמינות
11	מודל קוביית אבטחת הסייבר – מצבי מידע ואמצעים שכנגד	<ul style="list-style-type: none"> מצבי מידע / נתונים (דטה): מנוחה, העברה, עיבוד אמצעי נגד: טכנולוגיות, חינוך, מודעות, תרגול ותקנות
12	איומים הונאות ותקיפות – תוכנות זדוניות	<ul style="list-style-type: none"> סוגי Malware תקיפה של דואר אלקטרוני ודפדפן
13	איומים הונאות ותקיפות – הונאות	<ul style="list-style-type: none"> אומנות ההונאה שיטות הונאה והגנות מפניהן
14	איומים הונאות ותקיפות – תקיפות	<ul style="list-style-type: none"> סוגי תקיפות סייבר תקיפות מובייל ו- תקיפה באמצעות אפליקציות והגנות כנגד תקיפות אלו
15	אומנות ההגנה על סודות: קריפטוגרפיה	<ul style="list-style-type: none"> רקע: מהי קריפטוגרפיה, היסטוריה, יצירת טקסט מוצפן הצפנת מפתח פרטי הצפנת מפתח ציבורי השוואת הצפנה סימטרית וא-סימטרית
16	אומנות ההגנה על סודות: בקרת גישה	<ul style="list-style-type: none"> סוגי גישה: מוחשיים, לוגיים ומנהלתיים אסטרטגיות בקרה זיהוי שיטות אימות הרשאות סוגי פקדי אבטחה
17	אומנות ההגנה על סודות: הסתרת מידע	<ul style="list-style-type: none"> סיכך נתונים: הגדרה וטכניקות סטגוגרפיה: הגדרה, טכניקות ואיתור "האפלט" מידע: הגדרה, אפליקציות ושימושים
18	אומנות האמינות – סוגי בקרה וחתימות דיגיטליות	<ul style="list-style-type: none"> סוגי בקרת אמינות נתונים חתימות דיגיטליות



קורס לוחמת סייבר ואבטחת מידע

לנוער בגילאים שונים

מס' מפגש	נושא	פירוט
19	אומנות האמינות – רישיונות ומאגרי מידע	<ul style="list-style-type: none"> רישיונות: מהו אישור דיגיטלי וכיצד משתמשים, תהליך הבניה של אישור דיגיטלי. מאגרי מידע: אמינות מאגר, אימות נתונים ודרישות
20	חמשת התשיעיות (Five Nines) – המודל ומדדים לשיפור	<ul style="list-style-type: none"> המודל: מהם חמשת התשיעיות, סביבות הדורשות קיום המודל, איזמים על זמינות הנתונים מדדים לשיפור זמינות: ניהול, הגנה וגמישות המערכת
21	חמשת התשיעיות (Five Nines) – מענה לתקריות והתאוששות מאסון	<ul style="list-style-type: none"> מענה לתקריות: שלבים, וטכניקות התאוששות מאסון: תכנון ההתאוששות והמשכיות העבודה תוך כדי
22	הגנה על הארגון - Firewalls	<ul style="list-style-type: none"> סוגי Firewalls מכשירי אבטחה זיהוי תקיפה בזמן אמת זיהוי תוכנות זדוניות אבטחה – שיטות מומלצות
23	הגנה על הארגון – זיהוי התנהגותי	<ul style="list-style-type: none"> Botnet Kill chain אבטחה מבוססת זיהוי תבניות התנהגויות במערכת Netflow
24	גישת סיסקו ואבטחת סייבר	<ul style="list-style-type: none"> CSIRT Security Play Book כלי מניעה וזיהוי IDS & IPS
25	שיח ומבחן סיכום	<ul style="list-style-type: none"> יערך מבחן על החומר שנלמד ותוענק תעודה למי שעבר את הבחינה יתקיים שיח – "האם העתיד שלנו / שלכם נמצא בעולם אבטחת הסייבר" – יוצגו הכשרות ומקצועות בתחום.

* תוכני הליבה המקצועית וסדר העברתם ניתנים לשינוי על פי שיקולים מקצועיים, בהתאם לרמת הכיתה





Cyber For You
Cyber Security Training

03-5114066

www.cyberforyou.co.il

סניף רמת גן - החילזון 3, מתחם הבורסה סניף תל אביב - יגאל אלון 65
טל': 03-5114066 www.cyberforyou.co.il Info@cyberforyou.co.il

החברה שומרת לעצמה את הזכות לערוך את תוכנית הלימודים לפי שיקול דעתה לרבות סגל המרצים ושעות הלימוד.