



# סילבוס



## מבוא לסייבר ואבטחת מידע

- עמוד 1 -

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

**1** ..... מבוא לסייבר ואבטחת מידע

1..... סילבוס הקורס

2..... תוכן עניינים

**3** ..... פרטי הקורס

3..... תכנית המסלול

3..... אודות סייבר סקול

3..... תיאור הקורס

3..... יעדי הלמידה

**4** ..... חלוקת הקורס

# פרטי הקורס

## תכנית המסלול

- מבוא לסייבר
- פריצה 2048
- עוגיות
- מערכת הפעלה WINDOWS
- מבוא ל-Linux
- פקודות ב-Linux
- סייבר התקפי
- XSS
- דלף מידע
- ניהול סיכונים
- היבטי אבטחת מידע
- הצפנה
- פריצת סיסמאות
- סטגנוגרפיה

## אודות סייבר סקול

חברת סייבר סקול הינה מכללה בינלאומית למקצועות הסייבר ומובילה את חזית חינוך הסייבר בישראל לבני נוער.

סייבר סקול פועלת לחינוך טכנולוגי, מצוינות אישית וחשיבה יצירתית בקרב תלמידי ישראל החל מגיל צעיר, תוך שאיפה לחנך ולהכשיר את הדור הבא של תעשיית ההייטק, היחידות הטכנולוגיות בצבא"ל, עולם האקדמיה והזירה העסקית-גלובאלית.

כל מסלולי הלימוד והתכנים נבנו באופן ייחודי ע"י צוות המחקר והפיתוח שלנו המורכב מאנשי מקצוע מובילים בתעשייה למטרת הגשת התלמידים למבחני הסמכות בינלאומיות כבר בגילאי החטיבה והתיכון.

## תיאור הקורס

נועד להכשיר את התלמידים בנושאי אבטחת מידע, תקיפה והגנה ולהקנות להם כישורים ומיומנויות טכנולוגיות ויכולות התמצאות במרחב הסייבר העומדים בסטנדרט התעשייה. קורס זה מציג מושגים ביטחוניים וכיצד הם מתייחסים לעולמנו המודרני. החומר מציג בפניך את יסודות העבודה ברשת, מערכות ההפעלה Linux ו-Windows ומושגי הווירטואליזציה. נלמד גם כיצד להריץ פקודות בסיסיות ופרוטוקולי תקשורת ממוחשבים, לפתח הבנה מוצקה של מבני מערכת ההפעלה הבסיסיים ומהו מחזור ההתקפה של Cyber.

## יעדי הלמידה

- מבוא לעולם הסייבר ותקיפות הסייבר בפרט
- סקירת סביבות העבודה הנפוצות בעולם הסייבר, לדוגמה – ווינדוס, לינוקס ועוד...
- למידה ויישום התקפות סייבר מפורסמות
- כיצד נתגונן מפני מתקפות סייבר

## חלוקת הקורס

מס	שם השיעור	נושאים כלולים	מעבדות
<b>מבוא והכרות</b>			
1	היכרות עם עולם הסייבר+2048	<ul style="list-style-type: none"> <li>הסבר כללי על מסגרת הקורס</li> <li>הכרת פיצ'רים מעניינים של גוגל</li> </ul>	
2	עקרונות הגנת סייבר	<ul style="list-style-type: none"> <li>האבולוציה של מתקפות הסייבר</li> <li>סוגי האקררים</li> </ul>	<ul style="list-style-type: none"> <li>תכנון בסיסי של DiD</li> </ul>
<b>מחקר סייבר</b>			
3	מחקר סייבר באינטרנט	<ul style="list-style-type: none"> <li>מה נדרש כדי להצליח?</li> <li>האינטרנט כמקור מידע</li> </ul>	<ul style="list-style-type: none"> <li>חיפוש מסונן בגוגל</li> </ul>
4	הסוואה וגישה	<ul style="list-style-type: none"> <li>דומיין ו-URL</li> <li>אתרי אינטרנט</li> <li>פרוקסי</li> <li>קפצ'ה</li> <li>cache,</li> <li>archive</li> </ul>	<ul style="list-style-type: none"> <li>מציאת גרסאות י</li> <li>מציאת כתובות IP</li> </ul>
5	להישאר מעודכנים - מחקר נקודות תורפה (CVE)	<ul style="list-style-type: none"> <li>להישאר מעודכנים</li> </ul>	<ul style="list-style-type: none"> <li>ניתוח CVE</li> </ul>
6	אתיקה ופרטיות	<ul style="list-style-type: none"> <li>אתיקה ברשת</li> <li>פרטיות</li> <li>סיסמאות</li> <li>הצפנה</li> <li>משתמשים פיקטיביים</li> <li>פרופילים מזויפים</li> </ul>	<ul style="list-style-type: none"> <li>תרגול קצר בנושא סיסמאות</li> <li>פענוח צופן מוצפן</li> </ul>
7	שפה זרה	<ul style="list-style-type: none"> <li>איך מתמודדים עם שפה זרה</li> <li>מילונים אונליין</li> </ul>	<ul style="list-style-type: none"> <li>תרגום אתרים</li> <li>חיפוש מידע באתרים בשפות זרות</li> </ul>
8	דרכי חשיבה במידענות	<ul style="list-style-type: none"> <li>תדרוך מודיעיני</li> <li>חשיבה מידענית ומחקר</li> <li>שרשור</li> <li>הכללה</li> <li>צמום</li> <li>נחוש תוצאה</li> </ul>	<ul style="list-style-type: none"> <li>תרגול עיבוד מידע רלוונטי</li> <li>תרגול אסטרטגיות חיפוש</li> </ul>
9	מודיעין בסייבר		<ul style="list-style-type: none"> <li>חיפוש מידע על פגיעויות דפדפן</li> </ul>

יישור קו טכנולוגי - תקשורת נתונים, וירטואליזציה ומערכות הפעלה			
10	יסודות התקשורת	<ul style="list-style-type: none"> <li>מבוא לרשתות</li> <li>יצירת כתובות רשת</li> </ul>	<ul style="list-style-type: none"> <li>היכרות עם קונפיגורציות רשת</li> <li>תרגול הבנה בסוגי כתובות IP</li> </ul>
11	פרוטוקולי תקשורת נתונים	<ul style="list-style-type: none"> <li>נתבים ומתגים</li> <li>פרוטוקולים ותקשורת</li> </ul>	<ul style="list-style-type: none"> <li>תרגול פקודות ping &amp; traceroute</li> </ul>
12	יסודות הווירטואליזציה	<ul style="list-style-type: none"> <li>יסודות הווירטואליזציה</li> </ul>	<ul style="list-style-type: none"> <li>התקנה והגדרת VirtualBox</li> </ul>
13	מערכת הפעלה חלונות (Windows)	<ul style="list-style-type: none"> <li>מחשבים - חומרה ותוכנה</li> <li>יסודות מערכת ההפעלה Window</li> </ul>	<ul style="list-style-type: none"> <li>התקנת Windows10</li> <li>תרגול CMD</li> <li>סוגי מתאמי רשת ב-VB</li> </ul>
14	מבוא למערכת ההפעלה לינוקס	<ul style="list-style-type: none"> <li>מבוא</li> <li>המבנה של מערכת הפעלה Linux</li> </ul>	<ul style="list-style-type: none"> <li>התקנת Kali Linux</li> </ul>
15	ניווט ופקודות בלינוקס	<ul style="list-style-type: none"> <li>ניווט ומניפולציית תוכן</li> </ul>	<ul style="list-style-type: none"> <li>עבודה בסיסית עם Terminal</li> </ul>
16	הכרות עם רשתות בלינוקס	<ul style="list-style-type: none"> <li>בניית רשתות בסיסית ב-Linux</li> </ul>	<ul style="list-style-type: none"> <li>פקודות בניית רשת</li> <li>זיהוי מערכות הפעלה</li> </ul>
בטיחות ברשת			
17	משתמשים פיקטיביים	<ul style="list-style-type: none"> <li>פרופילים פיקטיביים ולמה משמשים,</li> <li>פתיחת פרופילים פיקטיביים</li> </ul>	<ul style="list-style-type: none"> <li>חקירת פרופילים למציאת התחזות</li> <li>יצירת פרופיל פיקטיבי</li> </ul>
18	יירוסיים ואיומים ברשת	<ul style="list-style-type: none"> <li>מה הוא וירוס</li> <li>סוגי וירוסיים</li> <li>אנטי וירוס</li> <li>תקיפות רשת</li> </ul>	<ul style="list-style-type: none"> <li>בניית וירוס VBS</li> <li>הדגמה ותרגול הזרקת SQL</li> </ul>
19	שיימינג ובריונות ברשת	<ul style="list-style-type: none"> <li>מה זה בריונות</li> <li>סוגי בריונות ואיך להתמודד</li> </ul>	

	<ul style="list-style-type: none"> <li>• הכרות</li> <li>• וירוס</li> <li>• משחק וסרטון וירוסים</li> </ul>	גלישה בטוחה	20
<b>סייבר התקפי</b>			
<ul style="list-style-type: none"> <li>• תרגול התקפה On path</li> </ul>	<ul style="list-style-type: none"> <li>• מונחים ומושגים</li> <li>• On-Path</li> </ul>	התקפת תקשורת - On-Path	21
<ul style="list-style-type: none"> <li>• Apache DoS</li> <li>• הפעלת תקיפת DoS</li> </ul>	<ul style="list-style-type: none"> <li>• מונחים ומושגים</li> <li>• DoS/DDoS</li> </ul>	התקפת תקשורת - DoS/DDoS	22
<ul style="list-style-type: none"> <li>• חילוף סיסמאות WPA2</li> </ul>	<ul style="list-style-type: none"> <li>• מונחים ומושגים</li> <li>• מתקפות אלחוטיות</li> </ul>	התקפות תקשורת - רשת אלחוטית	23
<ul style="list-style-type: none"> <li>• סקירת מערכות</li> </ul>	<ul style="list-style-type: none"> <li>• Cyber Kill Chain</li> <li>• Reconnaissance (סיור)</li> </ul>	מחזור התקפת סייבר - איסוף מודיעין טכני	24
<ul style="list-style-type: none"> <li>• בניית מטען תקיפה בעזרת Crunch</li> </ul>	<ul style="list-style-type: none"> <li>• Cyber Kill Chain</li> <li>• Weaponization (התחמשות)</li> </ul>	מחזור התקפת סייבר - התחמשות	25
<ul style="list-style-type: none"> <li>• EternalBlue exploit demo</li> </ul>	<ul style="list-style-type: none"> <li>• Cyber Kill Chain</li> <li>• Delivery (העברה)</li> <li>• Exploitation (ניצול)</li> </ul>	מחזור התקפת סייבר - העברה וניצול פגיעויות	26
<ul style="list-style-type: none"> <li>• אתגרי פריצת סיסמאות JS</li> </ul>	<ul style="list-style-type: none"> <li>• סוגי פריצות אבטחה</li> <li>• קובץ מקור</li> <li>• אתגרי פריצה</li> </ul>	פריצת סיסמאות	27
<ul style="list-style-type: none"> <li>• פריצה לנתוני משחק CookieClicker</li> </ul>	<ul style="list-style-type: none"> <li>• מהן עוגיות, מה המטרה של עוגיות, פריצה לעוגיות</li> </ul>	עוגיות	28
<b>סייבר הגנתי</b>			
<ul style="list-style-type: none"> <li>• זיהוי תוכנה זדונית</li> <li>• חסימת גלישה ברשת</li> </ul>	<ul style="list-style-type: none"> <li>• הגנה - סקירה כללית</li> <li>• מקרה בוחן: NotPetya</li> <li>• הגנות מתקפות סייבר</li> </ul>	אמצעי נגד והגנה	29
<ul style="list-style-type: none"> <li>• ניתוח ופיענוח HASH</li> <li>• תרגול צופן הזזה</li> </ul>	<ul style="list-style-type: none"> <li>• שלמות מידע - HASH</li> <li>• טרימינולוגיה</li> <li>• הצפנה</li> </ul>	הצפנה	30
<ul style="list-style-type: none"> <li>• הסתרת קובץ בתוך קובץ</li> </ul>	<ul style="list-style-type: none"> <li>• סטנוגרפיה</li> <li>• טכניקות שונות</li> </ul>	הסתרת מידע- סטנוגרפיה	31
<ul style="list-style-type: none"> <li>• חישוב תוכלת הפסדים כספיים לאחר תקיפת סייבר</li> </ul>	<ul style="list-style-type: none"> <li>• הגנה - סקירה כללית</li> <li>• הערכה וניהול סיכונים</li> </ul>	ניהול סיכונים	32
<ul style="list-style-type: none"> <li>• מבחן</li> </ul>	<ul style="list-style-type: none"> <li>• סקירת הבחינה</li> </ul>	תרגול וחזרה על החומר - הכרות עם עולם הסייבר	33