אבטחת מידע וסייבר בסיסי

<u>תיאור הקורס:</u>

יחד עם ההתקדמות הטכנולוגית האדירה בעשורים האחרונים, תחום הסייבר התפתח בקצב מהיר והפך לאחד התחומים המרכזיים בעולם הטכנולוגיה. כיום, הסייבר מהווה רכיב חיוני כמעט בכל מוסד, ארגון או חברה ברחבי העולם.

לאור הגידול המהיר בהיקף שוק הסייבר, נוצר מחסור הולך וגובר באנשי סייבר מקצועיים בשוק העבודה. נכון לשנת 2021, קיים מחסור של לפחות 40% במומחי סייבר, ומגמה זו צפויה להחריף בשנים הקרובות, במקביל לצמיחה המשמעותית של שוק הסייבר העולמי.

השילוב בין תחום מרכזי, שוק הצומח במהירות ומחסור באנשי מקצוע מוסמכים יוצר הזדמנות משמעותית עבור הסטודנטים. קורס ייעודי מאפשר כניסה לאחד התחומים המבוקשים ביותר כיום בשוק ההיי-טק העולמי, לצד אפשרויות להתפתחות אישית ומקצועית ושכר מהגבוהים במשק.

אין צורך בידע מקדים.

סילבוס נושאים

מודול 1: מבואות (5 ש"א)

יסודות עולם המחשוב

- מבוא לחומרה
- מבוא לתוכנה
- השילוב בין חומרה לתוכנה

וירטואליזציה

- עקרונות הווירטואליזציה
- שימושי וירטואליזציה בתעשייה
- בניית מכונה וירטואלית
- בניית מעבדה וירטואלית

מודול 2: מערכת ההפעלה Linux (10 ש"א)

מבוא ל־Linux

- מבנה מערכת ההפעלהLinux
- מערכתKali Linux

הטרמינל(Shell)

- מהו טרמינל (Shell)
- עקרונות ממשק הפקודות
- ניווט בסיסי במערכת Linux

ניהול קבצים ותיקיות

- יצירה ועריכה של קבצי טקסט
- ניהול בסיסי של קבצי טקסט
- ניהול מתקדם של קבצי טקסט

ניהול משתמשים והרשאות

- יצירה וניהול משתמשים
- ניטור משתמשים פעילים
- חשבון המשתמש Superuser

חיפוש ועזרה

- פקודות חיפוש וסינון מתקדמות
- תפריטי עזרה בסיסיים ומתקדמים

שירותים ותהליכי מערכת

- צפייה וניהול תהליכים
- שירותי מערכת בסיסיים
- הפעלה וכיבוי שירותי מערכת

תקשורת ואבטחה

- פקודות תקשורת בסיסיות
- ניהול DNS ו־Routing
- צפייה וניהול לוגים
- ניהול מערכת חומת אש

מודול 3: תקשורת מחשבים (10 ש"א)

מודלים

- מודל שבע השכבות (OSI)
- מודל ארבע השכבות (TCP/IP)
- תהליכי Encapsulation ו־Decapsulation

פרוטוקולים

- פרוטוקולי תעבורה: TCP / UDP
- פרוטוקולים אפליקטיביים: DNS, HTTP, DHCP, FTP ועוד
- פורטים מרכזיים

ציוד תקשורת

- מתג (Switch)
- נתב (Router)
- ציוד הגנת תקשורת (Firewall)

ניתוח תעבורת רשת

- מבוא לתוכנתWireshark
- ניתוח מתקדם של תעבורת רשת באמצעותWireshark
- מבוא לניתוח מתקפות סייבר בתחום תעבורת הרשת

מודול 4: סייבר הגנתי (15 ש"א)

<u>מבוא לעולם הסייבר</u>

- ההבדל בין סייבר לאבטחת מידע
- מתקפות הסייבר הראשונות
- מבוא לסייבר הגנתי

<u>עקרונות הגנת סייבר</u>

- שיטות איתור וגילוי מתקפות
- שיטות הגנה נפוצות
- עקרונות הגנה

<u>אמצעי הגנת סייבר</u>

- הגדרה וניהול חומת אש(Firewall)
- הגנה על רשתות ועמדות קצה באמצעותIDPS
- הגנתDOS / DDOS
- הגדרה וניהול חומת אש אפליקטיבית (Web Application Firewall – WAF)
- הגנה מפני תוכנות זדוניות (Anti-Virus)

<u>ניהול אופרציית סייבר</u>

- צוות SOC
- צוות NOC
- מערכת SIEM

<u>ניהול וסקר סיכוני סייבר</u>

- חוקים ורגולציה בעולם הסייבר
- תקנים רלוונטיים לעולם הסייבר
- סקר סיכונים בעולם הסייבר