מבוא לניהול הגנת סייבר

א. כללי

- משך הקורס: 40 שעות – שמונה מפגשים של חמש שעות.
- קהל היעד: מנהלי ואנשי אבטחת מידע, אנשים טכנולוגיים שרוצים לעבור לתחום הגנת סייבר

ב. נושאים

1. סקירה \ Landscape

- עולם הסייבר
- רשת האינטרנט
- רגולטורים, הנחיה ואסדרה
- תקנים והסמכות
- תפקידים בעולם הסייבר
- הגנת הפרטיות (GDPR, הרשות להגנת הפרטיות)
- מקורות מידע

2+3 רשתות ותקשורת מחשבים

- LAN – WAN
- מערכות הפעלה
- מרכיבי הרשת
- מודל OSI
- פרוטוקולי תקשורת
- ציוד תקשורת
- אינטרנט ואתרים
- IOT
- תשתיות ענן: IaaS, PaaS, SaaS

4. תקיפה

- שרשרת התקיפה
- סוגי תוקפים
- איום ייחוס
- תרחיש ייחוס
- מודל CIA

5+6 הגנה

- שרשרת התקיפה בהיבטי הגנה
- אבטחת מידע מול הגנת סייבר
- אמצעי הגנה ובקרות
- הגנת סייבר ע"י כלל הארגון
- אבטחת מידע פיזית

- ארכיטקטורה
- DiD
- הצפנה
- פיתוח מאובטח

7. ניהול סיכונים

- ניהול סיכונים אפקטיבי
- מונחים בניהול סיכונים
- סקר סיכונים
- דרכי התמודדות
- המשכיות עסקית

8. ניהול סייבר בארגון

- תפקידים וסמכויות, מנא"מ
- נכסי מידע – מיפוי וסיווג
- ניהול סיכונים – תפקידים, שרשרת אחריות
- שרשרת האספקה
- אסטרטגיית ניהול הגנת סייבר
- מגבלות