



40 Hours – סייבר ואבטחת מידע מתקדם

על הקורס

בימינו כשכל העולם הפך ממוחשב, אין זה פלא שהאנושות הגיעה למקום שבו גם המלחמות מתנהלות בזירה הטכנולוגית והממוחשבת עם התפתחות הטכנולוגיה והאפשרויות שהיא מציעה, גדלו עמה גם האפשרויות ללוחמה מסוג חדש, משוכללת ומתוחכמת יותר, מפחידה בהרבה מכל סוגי הלוחמה שהכרנו עד העת הזו. מדובר כמובן על תחום לוחמת המידע המתרחש במרחבים הממוחשבים ובמרחבים הווירטואלים ברשת האינטרנט.

לוחמה מסוג זה מתבצעת באמצעים טכנולוגיים משוכללים ומורכבים ועיקרה הוא חדירה למערכות ממוחשבות של גופים שונים. לוחמת סייבר הוא שמה הנפוץ, ולאחרונה אנו עדים למתקפות לא מעטות של האקרים ושל ארגוני פשע שונים הפועלים במרחב הסייבר – על מדינות, על ארגונים ועל עסקים שונים שבהם מבקשים אותם ארגונים או אנשים לפגוע.

לפיכך, ההגנה הנדרשת בעידן זה גם היא הולכת ומשתכללת – בהתאם לפשעים החדשים המתבצעים כיום ולשיטות הפגיעה הקיימות. תחום לוחמת המידע, לוחמת הסייבר, הוא תחום הנמצא בהתפתחות מטאורית כיום, ונדרשים בו אנשים מיומנים המכירים אותו לעומק.

לוחמה והגנת סייבר הינה כלל המקרים בהם ישנם נסיונות חדירה למערכות ממוחשבות על ידי האקרים וארגוני פשע במטרה לפגוע במידע השמור במערכות אלה.

קהל יעד

מנהלים ואנשי מחשוב טכנולוגיה עם נגיעה בתחום הסייבר ואבטחת מידע שמעוניינים להעשיר ידע ולהעמיק בתחום.

דרישות קדם

- ראיון מקדים
- עבודה עם מחשב ואופיס
- רצון ללמוד את התחום ולהתקדם

לאחר השתתפות ומעבר הקורס נכיר ונוכל לבצע את הפעולות הבאות

- רשתות ותקשורת
- זיהוי הצורך באבטחת מידע
- IOT \ IOE
- סוגי התקפות והאקינג
- בדיקות חוסן
- שיטות הנדסה אנושיות
- פיירול ושיטות הגנה על הארגון
- סריקות ורשת פנימית/חיצונית
- תרגול סריקה ותקיפת מערכות הפעלה
- זיהוי עקבות ברשת
- סריקת חולשות באתרי אינטרנט
- הכרות עם מנועי חיפוש
- מוצרי אבטחה מתקדמים
- זיהוי וכלי התגוננות
- הסתרת מידע
- כלי בדיקה סריקה ותקיפה
- שמירה על אנונימיות ברשת
- זמינות ארגונית
- הכרת מודל IAC \ CIA
- הגנה על המידע האישי
- ווירוסים, רוגלה ונוזקות
- שלבי הפריצה
- פורטים נפוצים
- צעדי מנע
- גניבת זהויות
- כלי סריקה ואבטחה
- סריקת רשתות אלחוטיות
- הצפנות

סילבוס

- Introduction to Cyber Security
- Cyber Laws
- Network Models
- Basics of Networking
- Cryptography
- Foot printing & System Hacking
- Networking Scanning
- Malicious coding
- APT'S Attack
- Attack Surface Models
- Mobile and Web Application Security
- Firewalls
- Injection
- MITM
- Web Servers
- Security Models
- Cloud and IoT Security
- Cyber Threats and Attacks
- PT Tools
- Security Tools
- IDS/IPS
- Linux Security Distro's
- Scanning Tools
- Next Generation Firewalls
- Unified Threat Management
- Steganography