



Cyber Ops – 40 Hours

על הקורס

מטרת הקורס היא לתת למשתתפים כלים להבין את עולם התוקף, כלי ההגנה דרכי הפעולה והבנת הכלים הקיימים בשימוש כיום לתקיפות והגנות סייבר, נראה את נקודת המבט מכובע התוקף ומכובע המגן, נלמד כיצד להגן על מערכות קריטיות וסביבת העבודה שלנו ממתקפות סייבר, כיצד תוקפים חושבים ומתנהגים ואילו נקודות תורפה יכולות להיות קריטיות.

לכל משתתפי הקורס תהיה גישה למערכת לימוד וירטואלית כולל חומרי לימוד ותרגול לכל מהלך הקורס ולאחריו.

קהל יעד

אנשים טכניים המעוניינים ללמוד את תחום הסייבר בדגש על מערכות תקיפה הגנה ו Ethical Hacking.

דרישות קדם

- ראיון מקדים
- רצון ללמוד את התחום ולהתקדם

לאחר השתתפות ומעבר הקורס נכיר ונלמד את הנושאים הבאים :

- Security concepts
- Security monitoring
- Host-based analysis
- Network Fundamentals
- Defence In Depth Strategy
- Zero trust
- Whitelisting and Blacklisting
- Cyber Kill Chain Model
- Network intrusion analysis
- Security policies and procedures
- הגנת סייבר והסכנות
- מתודולוגיה של תוקף סייבר
- איסוף מודיעין
- סריקה ופריצות
- שרשרת התקיפה
- השגת אחיזה
- העלאת הרשאות
- שמירת אחיזה
- הסתרת עקבות

סילבוס

- Defense in Depth
- Kill Chain
- Linux Security Distro's
- Supply Chain Attacks
- Network Sniffing
- Credential Harvesting
- Foot printing
- Password Cracking
- Dns Enumeration
- Ddos Attacks
- Reverse Shell
- Exploits
- Payloads
- Attack Surface Reduction
- Ransomware

- Anonymity and Attribution
- Traceability Online
- Social Engineering