מיישם Cyber Security

קריירה פורצת דרך.

מיישם אבטחת מידע - תפקיד חשוב מאוד, בייחוד בימים אלו, בהם הטכנולוגיה מתקדמת ונמצאת בכל תחום.

בישראל חסרים הרבה אנשי אבטחת מידע מקצועיים ומטרת קורס זה לשלב אותך כאיש אבטחת סייבר.

תפקיד מיישם סייבר: הגנה מפני גישה, שימוש, חשיפה ,ציתות ,שיבוש, העתקה או השמדה של מידע ומערכות מידע מצד גורמים שאינם מורשים או זדוניים ולספק סודיות, שלמות וזמינות של המידע ללא תלות בסוג המידע או בצורת האחסון, פיזית או אלקטרונית.

מערכות המידע חשופות באופן יום יומי בפני גורמים המאיימים על ביטחונן ושלמותן. ההגנה על מערכות המידע כוללת מספר שכבות ועומקים:

- אבטחה פיזית של המבנה שבו נמצאות מערכות המחשב.
- אבטחה של מערכות החומרה והתוכנה.
- אבטחת רכיבי התקשורת ואבטחת המידע הנאגר בהן.

שלושת המטרות העיקריות של אבטחת מידע הן:

- **סודיות** (confidentiality). הגבלת גישה או חשיפה לא מורשית של מידע, כולל הגנה על פרטיות וזכויות קנייניות במידע.
- **שלמות** (Integrity). הגנה מפני שינוי זדוני של המידע או השמדתו, כולל הבטחת אי התכחשות ואימות זהויות בעלי המידע.
- **זמינות** (availability). שמירה על זמינות ויעילות הגישה אל המידע בכל זמן נתון.

חלק מהמטרות מושגות באמצעות קריפטוגרפיה: כתב סתרים על רבידה השונים של אבטחת המידע כדי להסתיר את המידע ולהבטחת אמינותה, באמצעות שיטות כמו: הצפנה, חתימה דיגיטלית, קוד אימות סתרים, פונקציית גיבוב ועוד.

בוגרי הקורס יידעו לזהות נקודות תורפה אותם מנצלים תוקפים ויידעו להשתמש בטכניקות אבטחה שונות בכדי להגן על משאבי הרשת.

<u>דרישות סף</u>:

- יכולת קריאת טקסט באנגלית ברמה סבירה.
- ידע בניהול שרתים של Microsoft.
- ידע בניהול ציוד תקשורת (CCNA).

<u>קהל היעד</u>:

מנהלי רשתות שרוצים להתקדם לתחום ה- Cyber Security.

על הקורס:
מטרת הקורס הינה קידום מתחום הרשתות תקשורת לפיתוח קריירה מצליחה בתחום אבטחת הסייבר.
הקורס משמש כקרש קפיצה למשרות אבטחה.

הלימוד בקורס כולל: אבטחת מידע, תקיפה, פריצה והגנה - לוחמת סייבר.
מומחה Cyber Security.

קורס זה משלב שיטות עבודה מומלצות בפתרון בעיות מעשיות, ומיומנויות מעשיות לפתרון בעיות אבטחה מרכזיות.

ההסמכות:
- LPI Linux Essentials
- CompTIA Security +
- Cybersecurity Analyst – CompTIA CySA+
- Cisco CyberOps Associate

בקורס אנו שמים דגש רב על הפן המעשי בכדי שבוגרינו יהיו בעלי ניסיון בתחום אבטחת המידע, ויוכלו להשתלב בשוק העבודה.

להלן חלק מנושאי המעשיים בקורס:

- Advanced Tools and Techniques - Wireshark
- Check Point Next Generation Security Gateway Solution
- FortiGate Next-Generation Firewall
- Nmap Security Scanning
- Vulnerability Management with Nessus
- GNS lab
- Incident Response Lab
- VPN Lab
- Kali Linux - Wireless Attacks

<u>תוכנית הקורס</u>:
קורס זה כולל ספרות מקורית בעברית וחומר לימוד רשמי באנגלית של Cisco Network Academy.

בנוסף, הקורס מכין את התלמידים להסמכות בינלאומיות.

<u>ימי הלימוד</u>:
מתכונות דו-שבועית.

ימים: ג, ו'. שעות: יום ג' - 17:30-21:30, יום ו - 09:00-13:00.

<u>דרישות פדגוגיות וזכאות לתעודת גמר</u>:
1. נוכחות ב- 80% מהשיעורים (היעדרות עד 20% מהמפגשים תתאפשר כל עוד היא אינה רצופה).
2. הגשת כל פרוייקטי הגמר (4 פרוייקטים) וקבלת ציון עובר.
3. תעודות הסמכה בינלאומיות (במידה ועוברים את מבחני ההסמכה).
4. עמידה בתקנון התלמידים.

Ben Nissan CYBER Consulting

סילבוס הקורס

כמות השעות	שם המודול
40	LPI Linux Essentials
15	Threats, Attacks, and Vulnerabilities
15	Secure Code Design and Implementation
15	Cryptography Design and Implementation
5	Identity and Access Management Design and Implementation
10	Physical Security Design and Implementation
20	Cloud Security Design and Implementation
15	Endpoint Security Design and Implementation
35	Network Security Design and Implementation
15	Operations and Incident Response
15	Governance, Risk and Compliance
200	סה"כ שעות אקדמאיות

(40 ש"א) LPI Linux Essentials

- The Shell - Linux Command Line
- ניהול קבצים
- Archive and Compression
- טיפול בקבצי טקסט ובפלט
- ניהול חשבונות משתמשים וקבוצות
- ניהול הרשאות גישה
- Package Management Systems
- Process Management
- Shell Scripts
- TCP-IP Network Management

(15 ש"א) Threats, Attacks, and Vulnerabilities

- Malware
- Understanding Attackers
- Threat Intelligence
- Social Engineering Attacks
- Common Attacks
- Understanding Vulnerability Types
- Vulnerability Scanning
- Penetration Testing and Exercises

(15 ש"א) Secure Code Design and Implementation

- Software Development Lifecycle
- Software Quality Assurance
- Application Attacks
- Secure Coding Practices

(א"ש 15) Secure Code Design and Implementation

- Encryption
- Symmetric Cryptography
- Asymmetric Cryptography
- Key Management
- Public Key Infrastructure
- Cryptanalytic Attacks
- Cryptographic Applications

(א"ש 5) Identity and Access Management Design and Implementation

- Identification
- Authentication
- Authorization Account Management

(א"ש 10) Physical Security Design and Implementation

- Data Center protection
- Hardware and Data Security
- Business Continuity
- Disaster Recovery

(א"ש 20) Cloud Security Design and Implementation

- Cloud Computing
- Virtualization
- Cloud Reference Architecture
- Cloud Security Controls

(15 ש"א) Endpoint Security Design and Implementation

- Host Security
- Hardware Security
- Configuration Management Embedded Systems Security
- Scripting and Working at the Command Line

(35 ש"א) Network Security Design and Implementation

- TCP/IP Networking
- Secure Network Design
- Network Security Devices
- Network Security Techniques
- Transport Encryption
- Wireless Networking
- Network Attacks
- Mobile Device Security
- Network Tools

(15 ש"א) Operations and Incident Response

- Incident Response Programs
- Attack Frameworks
- Incident Investigation
- Forensic Techniques

(15 ש"א) Governance, Risk and Compliance

- Risk Analysis
- Risk Management
- Supply Chain Risk
- Security Policies
- Privacy and Compliance
- Privacy and Enhancing Technologies
- Security Awareness and Training