Cyber Security Management - (CISO)

תאור הקורס

בשנים האחרונות הופכת אבטחת "מרחב הסייבר" של כל פרט וארגון לחיונית יותר ויותר, בפרט נוכח העולם המודרני שבו אנו חיים, ואשר בו אנו מוצאים עצמנו מוקפים בטכנולוגיות מידע, התקני ושירותי תקשורת, הקשורים לכל היבט והיבט של חיינו. מציאות זו הופכת את אבטחת הסייבר למשימה חשובה ביותר עבור הארגון, אך גם מאתגרת לא פחות, בפרט נוכח חשיבות הצורך בהבנת ההשפעות של תקיפות הסייבר על הארגון וכן יותר כנגד התקפות שכאלו בהבנת מנגנון התגוננות יעיל

במסגרת המכינה ירכשו המשתתפים ידע מקצועי, ומעשי בניהול רשתות תקשורת מחשבים. המסיימים בהצלחה את המכינה / בעלי הרקע בתחום ימשיכו לחלק המתקדם של הקורס.

מטרת הקורס

- קורס מעשי במהותו המדגים טכנולוגיות המיושמות בשטח.
- מרצים בעלי ידע וניסיון עשיר, המובילים בתחומם.
- סביבות תרגול וירטואליות מתקדמות שהוקמו במיוחד
- ליווי אישי של התלמיד לאורך המסלול וגם לאחריו.

היקף הקורס

453 שעות לימוד אקדמאיות במתכונת הבאה:

- **מכינה** (לחסרי רקע) – 165 ש"ל

- **לימודי המשך מתקדמים** - 288 ש"ל.

אוכלוסיית יעד

הקורס מתאים לבוגרי קורס MCSA ו/או CCNA ו/או לבעלי ניסיון וידע בתחום תשתיות / רשתות / מערכות הפעלה ללא הסמכה מסודרת כגון טכנאי מחשבים / מנהלי רשתות או חיילים משוחררים יוצאי תפקידי מפעילי מחשב / מנמ"ר. הקורס מתאים גם לחסרי רקע אשר ידרשו ללימודי המכינה כתנאי להמשך הלימודים בקורס

תנאי קבלה

- מבחן כניסה.
- ראיון אישי.

מתודולוגית הלמידה

הרצאה פרונטאלית, הדגמות, תרגולים וסימולציות בסביבת הלמידה.

סגל המרצים

למכללת נס טכנולוגיות סגל מרצים ומומחי הדרכה, מהמובילים בתחומם, בעלי ניסיון מעשי רב ביישום והדרכת נושאי הלימוד בתעשיית ההי-טק הישראלית והעולמית. הקורס יועבר ע"י מרצים מומחים מתחום אבטחת הסייבר בארץ ובעולם. הקורס מועבר בשיתוף עם המכון למחקרי ביטחון לאומי.

זכאות לתעודת גמר מטעם מכללת Ness College

תעודת גמר מטעם Ness College תוענק לבוגרים העומדים בכל דרישות התוכנית כמפורט:

- נוכחות בקורס לפחות ב-85% ממפגשי הקורס.
- הגשת כל מטלות החובה בקורס.

בוגרי המכינה שיסיימו את המכינה בהצלחה יהיו זכאים לקבלת תעודת בוגר מכינת סייבר מטעם Ness College

תוכנית מכינת הסייבר (165 ש"ל)

- **אנגלית טכנית –** מושגי יסוד - הכרת השפה הטכנית וידיעת מושגים חשובים.
- **מבוא להכרת המחשב האישי -** למידה על חומרת המחשב האישי: מבנה המחשב, זיכרונות, דרייברים, הגדרות ברמת BIOS , פירוק והרכבת המחשב, טיפול בתקלות חומרה, טכנולוגיות מתקדמות, רכיבי לוחות אם ומעבדים.
- **מערכות הפעלה -** התקנה, ניהול ואיתור תקלות של מערכות הפעלה נפוצות וכלים לתחזוקתן, דיאגנוסטיקה, שחזור נתונים, ניהול מחיצות, כלי Imaging, שליטה מרחוק .
- **ממשק CLI -** תרגול ולמידת ממשק שורת פקודה הפועל באמצעות הקשת פקודות.
- **סדנת רשתות -** מושגי יסוד בתקשורת נתונים, מודל 7 (4) השכבות, תשתיות, טופולוגיות, ארכיטקטורות רשת, פרוטוקולים, הקמת תשתית לרשתות תקשורת.
- **תחנת עבודה וירטואלית** - הכרות עם תוכנת הווירטואליזציה Hyper-V מבית Microsoft המאפשרת הגדרה והתקנה של מכונות וירטואליות.

- **WINDOWS 10** - הכרת מערכת ההפעלה החדשה מבית Microsoft ומאפייניה החדשים. ניהול, יישום ואיתור תקלות ב- Windows 10 כמערכת המותקנת ב-Client.
- **עבודה עם Server 2016 – התקנה ואחסון** - התקנה, שדרוג והעברה של שרתים ועומסי עבודה, פתרונות אחסון ארגוניים, מרחבי אחסון ומניעת כפילות נתונים, איזון עומסים, פריסה,
- **יישומים ב- Server 2016** -IPv4, DHCP, IPv6 , DNS, IPAM, גישה מרחוק, DirectAccess, VPN.
- **ניהול תצורת רשת עם Server 2016** - בקרי תחום, Active Directory, AD DS, AD CS, AD FS, GPO, AD RMS.

תוכנית הלימודים המתקדמים (288 ש"ל)

מודול 1 – Security Essentials

1) Networking Concept (quick overview)

- Network types (LANs, WANs)
- Network topologies
- LAN protocols
- WAN protocols
- Network devices
- IP Concepts

2) Defense in Depth (quick overview)

- Information Assurance Foundations
- Computer Security Policies
- Contingency and Continuity Planning
- Access Control
- Password cracking for Windows and Unix
- Incident Response (IR)
- Offensive and Defensive Information Warfare (IW)
- Attack Strategies and Methods

Institute of technology & innovation

3) Internet Security Technologies

- Vulnerability Scanning and Remediation
- Web Security
- Firewalls and Perimeters
- Honeypots
- Host-based Protection
- Network-based Intrusion Detection and Prevention

4) Secure Communications

- Cryptography
- Steganography
- Critical Security Controls
- Risk Assessment and Auditing

5) Windows Security

- Security Infrastructure
- Service Packs, Patches, and Backups
- Permissions and User Rights
- Security Policies and Templates
- Securing Network Services
- Auditing and Automation

6) Unix/Linux Security

- Linux Landscape
- Permissions and User Accounts
- Linux OS Security
- Maintenance, Monitoring, and Auditing Linux
- Linux Security Tools

7) Hands-on Exercises

- Setup of virtual lab environment
- Windows/Linux tutorial
- TCP dump analysis
- WireShark decoding of VoIP traffic
- Password cracking
- Host-based discovery with Dumpsec

- Hashing to preserve digital evidence
- Analyzing networks with hping and nmap
- Event correlation with Splunk
- Use of steganography tools
- Securing a Windows system with MBSA and SCA

מודול 2– Advanced Security Essentials

8) Data loos prevention

- Risk management
- Understanding insider threats
- Data classification
- Managing and maintaining portable data classification
- Digital rights management
- Balancing digital rights with data classification
- Managing access across the enterprise
- Balancing functionality and security
- Data loss prevention (DLP)
- Identifying requirements and goals for preventing data loss
- Identifying practical DLP solutions

מודול 3– Hacker Tools, Techniques, Exploits, and Incident Handling

9) Incident Handling Step-by-Step and Computer Crime Investigation

- Identification
- Containment
- Eradication
- Recovery
- Special Actions for Responding to Different Types of Incidents
- Incident Record-keeping
- Incident Follow-up

10) Cyber security management

- Security and Risk Management
- Asset Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- laws, Regulations, Compliance
- Cloud security
- Intro to Cyber security products – solutions categories:
    - SIEM
    - FW – NG+web proxy
    - IPS
    - WAF
    - VPN
    - CASB
    - SSO and IDP (identity providers)
    - IDM
    - MFA (OTP)
    - AV (+cloud+multi engine)
    - SAND BOX
    - EPS
    - DLP
    - NAC
    - DAM
    - FAM
    - MDM
    - GRC
    - PKI
    - Permissions review (by state/usage)
    - Change management (Tufin,Algosec)
    - Anti spam
    - One way link
    - UBA – user behavior analytics
    - Forensic (EnCase)
    - E-Discovery and data classification& labeling
    - Disk encryption

- File encryption
- Traffic encryption
- HIPS
- Honey pots – deception tools
- Compliance scanners
- Vulnerability scanners
- Secure Code review
- Anti Phishing
- User Awareness tools (ironscale)
- Anti Fraud (Actimize)
- User Activity recording
- SCADA and IOT security NAC and FW
- Cyber Intelligence
- Privileged user management

מובהר כי המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

תל אביב | ירושלים | באר שבע | רחובות | רח' ראול ולנברג 36, קריית עתידים, תל אביב | טל: 6377 * | פקס: 03-3723480