Cybersecurity Talent

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 בהבנת מנגנון התגוננות יעיל יותר כנגד התקפות שכאלו.

קורס זה נועד להכשיר את משתתפיו כמומחי אבטחת המידע בארגון הן בגישה הגנתית והן בגישה התקפית. הקורס שם דגש על דרישות מכון SANS שהינו גוף ההסמכה המוכר של מחלקת ההגנה האמריקאית (DoD) באופן שמעניק למשתתפים את הידע הנדרש לטובת מבחני ההסמכה.

הקורס מורכב ממודול של מכינה (לחסרי הרקע) ומארבעה חלקים נוספים של לימודי המשך מתקדמים :

במסגרת המכינה ירכשו המשתתפים ידע מקצועי, ומעשי בניהול רשתות תקשורת מחשבים. המסיימים בהצלחה את המכינה / בעלי הרקע בתחום ימשיכו לחלק המתקדם של הקורס הכולל כאמור 4 חלקים: בחלקו הראשון ילמדו המשתתפים את יסודות אבטחת המידע אשר ישמש אותם כבסיס למיומנות שלהם בתחום ויהווה ידע רלוונטי לעוד שנים רבות. המשתתפים יזכו להכרות מעמיקה עם אבטחת הסייבר ולהדרכה מטעם מומחי סייבר בתעשייה. החלק השני של הקורס יעסוק בסוגיות מתקדמות וטרמינולגיה של אבטחת סייבר. בחלק השלישי ילמדו המשתתפים כיצד לנהל את האבטחה ויקבלו את הידע, הכישורים והכלים החיוניים והדרושים כדי לפקח על האבטחה של הארגון. בחלק הרביעי של הקורס יזכו המשתתפים להכרות עם עולם הסייבר ברמת הניהולית .

בוגרי הקורס הארוך יוכלו במעלה הדרך להתמקם באחד מהתפקידים הבאים:

- Security Consultant
- Security Manager
- IT Director/Manager
- Security Auditor
- Security Architect

- Security Analyst
- Security Systems Engineer
- Chief Information Security Officer
- Director of Security

מטרת הקורס

- קורס מעשי במהותו המדגים טכנולוגיות המיושמות בשטח.
- הקורס היחידי בישראל המכשיר אנשי אבטחת מידע בתכנים הגנתיים והתקפיים (white hacking) תוך שימת דגש לדרישות מכון SANS ולדרישות ארגון ICS2 (Information security certification) שהינו ארגון בנ"ל להסמכות סייבר באופן שמעניק למשתתפים את הידע הנדרש לטובת מבחני ההסמכה של הארגון.
- מרצים בעלי ידע וניסיון עשיר, המובילים בתחומם.
- סביבות תרגול וירטואליות מתקדמות שהוקמו במיוחד לכל מודול.
- 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 iNT 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 המוסד לטכנולוגיה וחדשנות iNT

תעודת גמר מטעם המוסד לטכנולוגיה וחדשנות iNT 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 המוסד לטכנולוגיה וחדשנות iNT

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 ואכסון** - 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.

Institute of technology & innovation

תוכנית הלימודים המתקדמים (288 ש"ל)

☑ מודול 1 - Security Essentials (90 ש"ל)

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

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

Institute of technology & innovation

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 (80 ש"ל)**

8) **Defensive Network Infrastructure**

- Introduction to network security infrastructure as the target for attacks
- Impact of compromised routers and switches
- Escalating privileges at Layers 2 and 3
- Weaknesses in router and switch architecture
- Integrating and understanding existing network devices to defend against attacks
- Advanced Layer 2 and 3 Controls
- Filtering with access control lists
- Introduction to network admission control and 802.1x

9) Packet analysis

- Architecture design and preparing filters
- Building intrusion detection capability into a network
- Understanding the components currently in place
- Detection techniques and measures
- Understanding various types of traffic occurring on a network
- Knowing how normal traffic works
- Differentiating between attacks and normal users on a network
- Advanced IP packet analysis
- Performing deep packet inspection and understanding usage of key fields
- Event correlation and analysis
- Analyzing an entire network instead of a single device
- Building advanced snort rules
- Intrusion detection tools
- Installing and using analysis software
- Wireshark
- Building custom filters

10) Pentest

- Variety of penetration testing methods
- Frequency and use of vulnerability analysis, penetration testing, and security assessment
- Vulnerability analysis
- Tools, techniques, and methods used in testing
- Basic penetration testing
- Focus, requirements, and outputs of a successful test
- Prioritizing and remediation of issues
- Advanced penetration testing
- Understanding and mapping to an organization's infrastructure
- Application testing and system analysis

11) Malware

- Types of malware and corresponding behavior
- Dealing with malware
- Tying malware into intrusion analysis and incident response
- Windows malware
- Anti-malwares tools and analysis
- Fighting rootkits with basic and advanced tools
- Inspecting active processes
- Using online resources to get help

12) 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

13) Hands-on Exercises

- Analyze network configurations for routers
- Perform detailed analysis of traffic using various sniffers and protocol analyzers
- Identify and track attacks and anomalies in network packets
- Use various tools to perform penetration testing and network discovery
- Analyze both Windows and Unix systems during an incident to identify signs of a compromise
- Find, identify, and clean up various types of malware

☑ מודול 3 - Hacker Tools, Techniques, Exploits, and Incident Handling (80 ש"ל)

14) 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

15) Computer and Network Hacker Exploits

- Reconnaissance
- Scanning
- Intrusion Detection System (IDS) Evasion
- Network-Level Attacks
- Gathering and Parsing Packets
- Operating System and Application-level Attacks
- Netcat: The Attacker's Best Friend
- Password Cracking
- Web Application Attacks
- Denial-of-Service Attacks
- Maintaining Access
- Covering the Tracks

16) Hacker tools workshop

17) <u>Hands-on Exercises</u>

- Memory analysis
- Metasploit attack and detect
- SQL Injection
- Cross-Site Scripting
- Covert channel analysis
- Detecting an insider with built-in Windows commands
- Windows Command Line
- Working with backdoors
- Detecting Denial-of-Service attacks
- Shell history analysis
- Linux attack detection

☑ <u>מודול 4 - cyber security management (38 ש"ל)</u>

- Security and Risk Management
- Asset Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations

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.