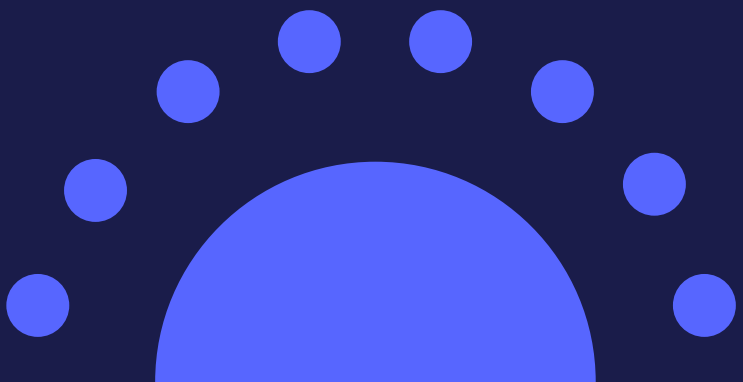
אטלס
האקדמיה הטכנולוגית
של מערכת הביטחון

הטכניון
ביה"ס ללימודי המשך
של הטכניון ע"ש עזריאלי

תוכנית מיישמי הגנה והתקפת סייבר
Cyber Security offense and Defense Practitioner Program

הכשרת סייבר למפקדי צה"ל פצועי מלחמת "חרבות ברזל"



אודות התוכנית

ישראל היא אחת מבין מעצמות הסייבר המובילה בעולם. לאחרונה התרחשו בארץ ובעולם מתקפות סייבר חסרות תקדים הן בעוצמתן והן בכמותן. במרבית המקרים מדובר במתקפות שניתן היה למנוע או להפחית את הסיכוי להתרחשותן בעזרת כלים טכנולוגיים ולמידה.

אנו מודעים לדרישה ההולכת וגוברת באנשי סייבר מוכשרים במגוון רחב של חברות וארגונים ובהתאם לכך הקמנו עבורכם בשיתוף עם הטכניון מסלול הכשרה ייחודי ומקיף המותאם לדרישות מערכת הביטחון והתעשייה. המסלול משלב לימודים תיאורטיים לצד מיומנויות מקצועיות Hands-On שימוש במעבדות וסימולטור להבנה ויישום החומר הנלמד בעולמות הסייבר ואבטחת המידע.

מנהל התוכנית, מר ישראל ברון- מומחה בהגנת סייבר, בעל ניסיון רב בהגנה על תשתיות מדינה קריטיות, בעברו ממונה ביטחון אבטחת מידע וסייבר במשרד הביטחון וכן מנהל אגף הסייבר ברכבת ישראל. בנוסף ישראל חבר בקבוצות סייבר בינלאומיות העוסקות בתקינה בתחום הסייבר ואף מרצה בכיר בארץ ובחו"ל בנושאי הגנת תשתיות קריטיות מפני מתקפות סייבר.

התוכנית

במהלך התוכנית תחשפו ל- 3 צירים שמהווים יסודות ידע לעולם הסייבר:

1. רשתות תקשורת
2. מערכות הפעלה
3. פיתוח / תכנות

בנוסף, תלמדו באופן נרחב את עולמות ההגנה וההתקפה:

1. הגנה – הכשרה של צוות כחול (הבנת וקטורים של התקפה, היכרות עם זיהוי פלילי ברשת, הבנת הבסיס של ניתוח תוכנות זדוניות).
2. התקפה – הכשרה של צוות אדום (איסוף מידע ברשת באמצעות מקורות רלוונטיים, בדיקת חדירה של אפליקציות אינטרנט, בדיקת חדירה לתשתיות, Using reverse engineering and binary exploitation.

התוכנית

התוכנית נועדה להכשיר למשרות ראשוניות בתעשייה
בתחומי אנליסט SOC, אבטחת מידע, בקר סייבר, ועוד.

יתרונות התוכנית

- מסלול מקיף וממוקד לדרישות המערכת והתעשייה.
- אתר קורס ייעודי המאפשר גישה לכלל חומרי הלימוד ותכנים מקצועיים.
- סדנאות : כתיבת קורות חיים ולינקדאין.
- ידע לקראת מעבר בחינות הסמכה בינלאומיות.
- Cyber War Room עם סימולטור ומעבדות וירטואליות לתרגול אונליין.
- שילוב של הרצאות אורח ממומחים בתעשייה.
- שעות קבלה ומענה פרטני מהצוות האקדמי.
- תעודת הסמכה מבית הספר ללימודי המשך במוסד הטכניון.
- כיתה קטנה ויחס אישי

מוסד הטכניון הינו הגוף המוביל בישראל בעולמות המדע והטכנולוגיה, בוגרי הטכניון זוכים להכרה בינלאומית בתחומים רבים. **העומדים בדרישות הקורס יזכו בתעודת סיום של מיישם הגנה והתקפת סייבר מבית הספר ללימודי המשך במוסד הטכניון.**

אודות הקורס

קהל יעד

- משרתים.ות שנפצעו במהלך שירותם הצבאי
- אנשי/נשות מילואים שביצעו מעל 150 ימי מילואים מאז ה- 7 באוקטובר 2023

* עדיפות למשרתים בייעוד קדמי

תנאי קבלה

- מעבר מבחן טכנולוגי אונליין המדגים את יכולות ופוטנציאל המועמד להצלחה בתחום.
- ראיון אישי עם יועץ אקדמי
- היכרות עם מחשבים ואינטרנט ברמת המשתמש.
- אנגלית ברמה טובה.

היקף הקורס

- 450 שעות לימוד אקדמיות
- 57 מפגשים
- 3 ימי לימוד בשבוע

פרקטיקה בקורס

סימולטור CYWARIA של חברת CYMPIRE

שימוש בסימולטור ייחודי שפותח על ידי צוות מנוסה המורכב ממומחי אבטחת סייבר ואנשי הדמיה ומשחקים, בעלי ניסיון מבצעי וחינוכי נרחב. ארגונים רבים בארץ ובעולם עושים שימוש בסימולטור לצורך הכשרה ושמירה על כשירות צוותי הסייבר שלהם. הסימולטור הינו מערכת המאפשרת לאנשי Cybersecurity לרכוש מיומנויות מקצועיות Hands-On ולתרגל את עצמם בתרחישים מציאותיים. בתוכנית הקורס ישולבו אתגרי סייבר ותרחישים אמיתיים שיאפשרו התנסות בזמן אמת וצבירת ניסיון מקצועי. המערכת מהווה השלמה חשובה לצד התיאורטי הנלמד בכיתה, כאשר הידע שנרכש בשיעור נדרש לבוא לידי ביטוי בעת התרגול בסימולטור. הסימולטור פותח בגישה חדשנית וייחודית בתחום אבטחת הסייבר, המשלבת סימולציה בזמן אמת, משחק ומתודולוגיה של אימוני אבטחת יישומים. הסימולטור כולל כלים רבים בהם נעשה שימוש בסביבת משחק תחרותית עם ביצועים בעלי אפקטים וירטואליים מרגשים המיועדים במיוחד לשיפור התחרותיות ואפקטיביות הלמידה.

מעבדות אינטגרליות – בתוכנית הקורס יבוצע שימוש במעבדות ייחודיות ואינטגרליות אשר פותחו במיוחד על מנת לדמות סביבה ארגונית גדולה ומורכבת. ביצוע תרחישי אמת במעבדה, שמתעדכנים בהתאם להתקדמות הלימודים, ומאפשרים לסטודנטים לחוות תהליכי תקיפה והגנה ריאליסטיים, מרובי שלבים ותלויי נסיבות בשימוש בארגז הכלים שרכשו בקורס. ניתן לגשת למעבדה בכל שעה ביממה, ומכל מקום.

פרקטיקה בקורס

הפלטפורמה תומכת בקמפיינים אדומים (התקפה) וכחולים (הגנה).

קמפיינים כחולים – מספקים סימולציה חיה של מתקני וצוותי הגנת סייבר הפועלים לזהות ולהכיל איומי והתקפות סייבר.

קמפיינים אדומים – נועדו להעניק למשתמשים הבנה של כלי וטכניקות ההתקפה העומדים לרשות תוקפי הסייבר בנוסף לידע רלוונטי למשתמשים העובדים בצוות אדום או המיועדים לעבודה בצוות אדום.

תכנית הלימודים

	Module	Academic Hours
1	Introduction to Cyber Security	5
2	Networking Fundamentals	50
3	Operating Systems: Windows	50
4	Operating Systems: Linux	50
5	Python Fundamentals	50
6	Cyber Offensive: Ethical Hacking	75
7	Cyber Offensive: Web Hacking	45
8	Red Project	10
9	Cyber Defense: Breach prevention	75
10	Cyber Defense: Forensics	30
11	Blue Project	10
Total		**450**

סילבוס

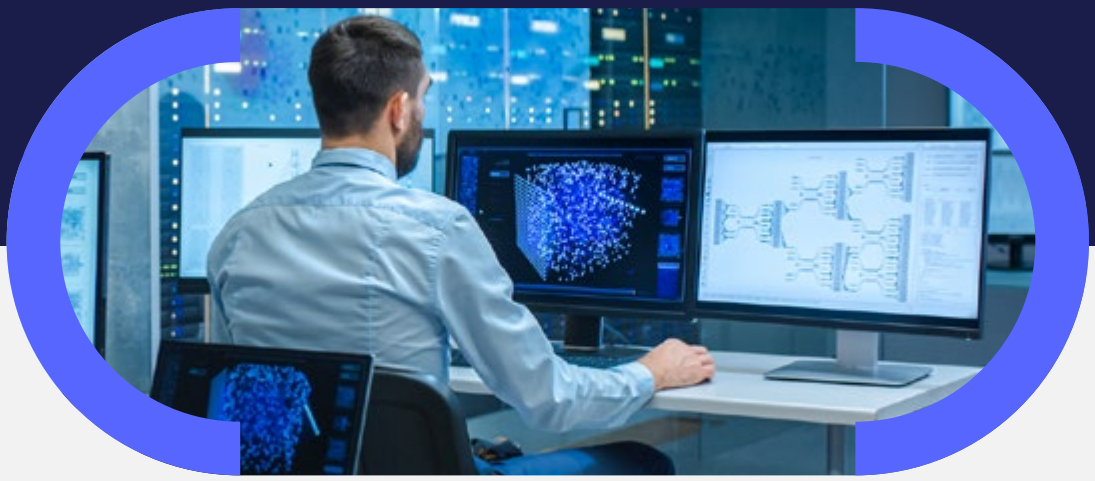
Module 1: Introduction to Cyber Security — **5 hours**

- Introduction to the Course and Learning Pathways
- Identifying Roles, Actors, and Common Mitigation Strategies
- Cyber Security Fundamentals: Concepts and Glossary
- The CIA Triad: A Fundamental Overview

Module 2: Networking Fundamentals — **50 hours**

החיבור בין תוכנה, רשתות ותשתיו תקשורת הולך ומתגבר מדי יום. בכדי להתקדם בקריירה טכנולוגית בנוף משתנה זה, הינך נדרש להכיר את טכנולוגיות הרשת החדישות בתוספת אבטחה, אוטומציה ותכנות. מודול זה של הקורס יקנה ידע בסיס, חיוני ורחב לעוסקים בתחומי ה – IT והסייבר: רשת, גישה לרשת, קישוריות, שירותי , IP ויסודות ,IP אבטחה, אוטומציה ותכנות.

- Networking devices
- TCP three-way handshake and UDP protocol
- LAN/WAN, network topologies
- Application layer: HTTP, SSH, DNS
- The OSI reference model, TCP/IP
- IP routing
- Physical layer and ethernet
- DHCP and NAT
- ARP and ICMP
- Network monitoring with Wireshark
- IP addressing: IPv4, VLSM, IPv6



Module 3: Operating Systems - WindowsSecurity **50 hours**

Windows היא מערכת ההפעלה הנפוצה בעולם, החיבור בין תוכנה, רשתות ותשתיות תקשורת הולך ומתגבר מדי יום. מודול זה יקנה לך את הידע והמיומנות הנדרשת על מנת להכיר ולתפעל את מערכת ההפעלה, הקמת שרתים וירטואליזציה ועוד. יכולות אלו יסייעו לך כמגן לזהות איומים פוטנציאלים.

• Introduction to Windows	• Windows and cloud networking and security
• Introduction to Windows, domains, and the Azure cloud	• Microsoft Active Directory and identity
• Building a Windows client machine and cloud computing	• Group policies
• Cloud services, resources and solutions	• Windows services (RDP, DNS, DHCP, File and printer sharing)
Managing processes and services	• Intro to CMD and PowerShell scripting

Module 4: Operating Systems – Linux — **50 hours**

Linux הינה מערכת הפעלה שרבים מכלי האבטחת מידע הם מבוססים .Linuxיתרה מכך, רוב מארחי הענן מבוססים על גרסה מסוימת של אותה מערכת ההפעלה. מקצועני הסייבר צריכים להיות מסוגלים לפעול בסביבה זו. המודול יעניק לך את הידע הבסיסי הנדרש לעשות זאת.

• Introduction to Linux and Linux distributions	• Searching for specific files
• Building a Linux virtual machine	• Linux networking
• The Linux file system	• Managing processes
• Text processing and regular expressions	• Installing programs and services (webserver, mysql, ssh, dhcp)
• Access control and file permissions	• Bash scripting

Module 5: Python Fundamentals — **50 hours**

פייתון היא שפת תכנות הפופולרית ביותר בתחום הסייבר. היא עוצמתית, פשוטה לשימוש וניתנת להרחבה. רבים מכלי האבטחת מידע כתובים בפייתון, וזהו כלי שיאפשר ביצוע אוטומציה ושיפור תהליכי עבודה.

• Introduction to programming	• Functions and modules
• Python environment	• String handling and regular expressions
• Introduction to Python	• Working with files
• Expressions, variables, data and types	• Introduction to the Requests library for HTTP requests and responses
• Loops and conditionals	

Module 6: Cyber Offensive - Ethical Hacking **75 hours**

זהו המודל הראשון שמוקדש לפעילויות צוות האדום, תלמד את הכלים הבסיסיים והתהליכים הדרושים לביצוע בדיקות חדירה ולפיתוח כצוות אדום בסביבת רשת מקומית.

• OSINT, WHOIS and DNS enumeration	• The Metasploit database
• Discovering live hosts	• Brute force attacks
• Network, port scanning and OS fingerprinting (Nmap)	• Privilege escalation: Windows
• Vulnerability analysis	• Privilege escalation: Linux
• Remote control	• Lateral movement

Module 7: Cyber Offensive - Web Hacking **45 hours**

כיום הדרך הנפוצה לחדור לתוך ארגונים היא דרך אפליקציות הענן והאינטרנט. המודול יקנה יכולת הבנה בבדיקת חדירות של אפליקציות אינטרנטיות. במהלך המודול תחשפו לטכניקות ניתוח ותקיפת אפליקציות מבוססות רשת.

• HTTP and the web stack	• OS command injections
• OWASP top 10	• Denial of Service
• SQL injection	• Local File Execution (LFI) and Remote File Inclusion (RFI)
• Client-side injections (XSS, CSRF)	• Working with Burp Suite

Module 8: Red Project — **10 hours**

Module 9: Cyber Offensive - Web Hacking — **75 hours**

המודול יקנה ללומד כלים תיאוריטיים ופרקטיים איך להגן על תשתית ולנטר אירועי סייבר באמצעות מרכז הבקרה (SOC).

- Vulnerability management
- Risk management
- Security controls
- Network segmentation
- Network monitoring and malware detection
- Security Incident and Event Management (SIEM)
- Security Operation Centers (SOC)
- Introduction to Check Point technologies
- Monitoring traffic and connections with Check Point

Module 10: Cyber Defense – Forensics **30 hours**

כאשר מתרחש אירוע סייבר, חיוני להיות מסוגל לאסוף ראיות ולהיות מסוגל לנתח אותן.
זה יאפשר לארגון להבין בדיוק את הפעולות שביצע התוקף ויאפשר יצירת כלים והגנות למניעת אירוע חוזר.

- Network forensics and packet analysis
- Creating timelines
- Extracting files
- Malware analysis
- Memory forensics with Volatility
- Windows memory forensics
- Disk and filesystem analysis
- Linux memory forensics

Module 11: Blue Project **10 hours**

הסמכות בינלאומיות

הקורס מסייע לבוגריו לגשת להסמכות שונות של עולם הסייבר, חלק מההסמכות יילמדו באופן עצמאי במהלך הקורס ולחלקן יזדקק התלמיד בהשלמת חומר נוסף ללמידה באופן עצמאי. מדריכי הקורס יכוונו את הסטודנט/ית לחומרי העזר הנדרשים כהכנה למבחן לפי ביקוש. עלות מבחני ההסמכה, מועדיהם ודרישות הקדם הינם באחריות הגוף המסמיך בלבד ועל כן יכול אותו גוף לערוך שינויים או עדכונים למבחני ההסמכה או לתנאי הקדם הנדרשים. האחריות לבירור פרטים אלו היא על הנבחן בלבד.

הידע הנרכש בקורס יסייע למשתתפיו לגשת לבחינות הסמכה מקצועיות של גופים בינלאומיים מובילים:

הסמכת Linux Essentials מאמתת את הבנת יישומי קוד פתוח והיחסים ליישומי קוד סגור מקבילים. מושגים בסיסיים של חומרה, תהליכים, תוכניות ורכיבי מערכת ההפעלה לינוקס. כיצד לעבוד בשורת הפקודה ועם קבצים, ליצור ולשחזר גיבויים וארכיונים דחוסים. אבטחת מערכת, משתמשים/קבוצות והרשאות קבצים עבור ספריות ציבוריות ופרטיות.

הסמכת Security+ 601 מבססת את הידע המרכזי הנדרש מכל תפקיד אבטחת סייבר ומספקת קרש קפיצה למשרות בתחום. ההסמכה משלבת שיטות עבודה מומלצות בפתרון בעיות מעשית, ומבטיחה שלמוסמכים יש כישורים מעשיים לפתרון בעיות אבטחה שונות.

הסמכת CySA+ היא הסמכה למקצועני סייבר העוסקים בזיהוי מניעה ותגובה לאירועי סייבר באמצעות ניטור אבטחת מידע רציף.

הסמכתeJPT היא הסמכה מעשית (לא בחינה) שמאמתת את הידע והיכולות למלא את כל המטלות של מבצע מבחני חדירה. ההסמכה כוללת ביקורת על מחשבים, רשתות ויישומי רשת.

סטודנטים יוכלו להתכונן להסמכות הבאות באמצעות הידע הנכלל בקורס בנוסף לחומרים חיצוניים שיועמדו לרשותם:

הסמכת Azure Fundamentals היא הזדמנות להוכיח ידע בסביבת שירותי הענן של מייקרוסופט – Azure שירותים, עומסי עבודה, אבטחה ופרטיות, תמחור ותמיכה. על המועמדים להכיר את המושגים הטכנולוגיים הכלליים, לרבות מושגי רשת, אחסון, מחשוב, תמיכה באפליקציות ופיתוח יישומים.

הסמכת CCNA מכסה מגוון רחב של נושאים, כולל יסודות וגישת רשת, קישוריות ושירותי IP, יסודות אבטחת מידע, אוטומציה ותכנות. הבחינה כוללת את הטכנולוגיות העדכניות ביותר אשר יעניקו למוסמכים את הבסיס לו הם זקוקים על מנת לקדם את הקריירה שלהם בתחום הסייבר.