



**הסמכת**

# Certified Cybersecurity Associate

התחלה חלקה ופרקטית לעולם הסייבר – מבוססת מעבדות  
תרגול ובינה מלאכותית.

# אודות מסלול ההסמכה

תוכנית ההסמכה מיועדת למקצוענים ולמעוניינים בהסבת מקצוע, המחפשים נקודת כניסה מעשית ויישומית (Hands-on) לעולם הסייבר ואבטחת המידע. המסלול מחולק ל-3 מיקרו-הסמכות (Microcredentials) המשתלבות זו בזו, ומעניק לכם מומחיות פרקטית מקיפה: החל מיסודות המחשוב, ניהול רשתות ותשתיות, דרך אבטחת ענן והגנה מפני איומים, ועד לתפעול אירועי סייבר (Cyber Security Operations) בשילוב כלי AI מתקדמים. כל קורס בתוכנית שם דגש על למידה יישומית, עבודה עם הכלים המובילים בשטח והכנה מלאה לשוק העבודה, כדי שתצאו לשוק עם ביטחון מקצועי ויכולת מוכחת להשתלב בסביבות סייבר מודרניות.

## נתוני המסלול ודרישות קדם

**רמת מיומנות**   
מתחילים ללא רקע קודם.

**היקף שעות והשקעה**   
**100 שעות** של למידה ממוקדת ומעבדות  
יישומיות המכינות אתכם לתעשייה.

## לאילו תפקידים המסלול מכין אתכם?

התוכנית מותאמת באופן מלא לדרישות השוק ומכינה אתכם להשתלבות מהירה בתפקידי Entry-Level מבוקשים בתעשיית ההייטק והסייבר:

לסטנדרטים המחמירים של הארגונים המובילים בעולם:



Cybersecurity Associate



Cybersecurity Intern



# למי המסלול מתאים?

- כל מי שרוצה לעשות את הצעד הראשון בעולם הסייבר  
חובבי טכנולוגיה וכל מי שמרגיש שהעתיד שלו נמצא שם, ומחפש את נקודת הכניסה המהירה והנכונה ביותר לתעשייה.
  - אנשים ללא רקע טכני  
מי שעובדים כיום בתחומים אחרים ומחפשים מעבר ממוקד, יישומי ופרקטי לענף אבטחת המידע.
  - חיילים משוחררים וצעירים ללא ניסיון  
מי שרוצים לבנות מקצוע מבוקש מהיסוד ולהשתלב מהר בשוק העבודה, ללא צורך בתואר אקדמי ארוך.
- דרישות סף:**  
המסלול מותאם למתחילים ומצריך אוריינות מחשב בסיסית לצד אנגלית ברמה טובה (מאחר ועולם הסייבר, התרגול ומבחני ההסמכה מנוהלים כולם בשפה האנגלית).

## המבנה הייחודי של התוכנית: תעודות שמצטברות לקריירה

- |                               |                                                      |
|-------------------------------|------------------------------------------------------|
| 1 יסודות הסייבר (Foundations) | המסלול בנוי במודל של 3 מיקרו-הסמכות נפרדות המאפשרות  |
| 2 מערכות ותשתיות (Systems)    | לכם לבנות את היכולות שלכם צעד אחר צעד, ולתקף את הידע |
| 3 תפעול והגנה (Operations)    | שלכם באופן הדרגתי:                                   |

כל מיקרו-הסמכה כוללת תרגול פרקטי מונחה ומסתיימת במבחן הסמכה יישומי. עם השלמת שלושת השלבים ומעבר המבחנים בהצלחה, תהיו זכאים להסמכה הכוללת: **Cybersecurity Associate Certification**.

### בניית תיק עבודות לעולם האמיתי

לאורך כל המסלול תייצרו הוכחות בשטח ליכולות שלכם (Portfolio). הידע שתדגישו במעבדות ובמשימות יתועד ויוכיח למעסיקים שאתם יודעים לעבוד.



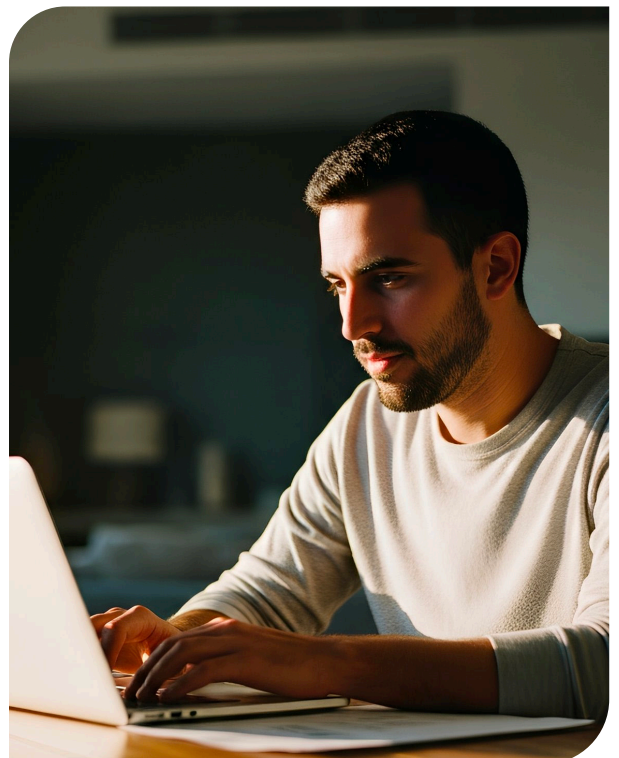
### רשימת מיומנויות

ככל שתשלימו יותר מעבדות בפלטפורמת התרגול של TechDX, המערכת תעדכן אוטומטית רשימת כישורים טכנולוגיים שתוכלו לשתף ברשתות החברתיות (כמו לינקדאין) כדי להציג את ההתקדמות שלכם בזמן אמת.



### דו"חות הישגים

לאחר כל 5 מעבדות, תקבלו דו"ח מסכם המפרט את התרחישים שפתרתם, הכישורים שהפגנתם והתוצאה המעשית שהשגתם.



# מידע על מבחני ההסמכה

המבחנים שלנו לא בודקים שינון – הם בודקים יכולת. כל מבחן נמשך בין 2.5 ל-6 שעות ומורכב משני חלקים:

- **הערכה ורבליט:** הסבר של מושגים והפגנת יכולת תקשורת מקצועית וברורה של ידע טכני (אלמנט קריטי בראיונות עבודה).
- **אתגר מעשי ודו"ח מסכם:** פתרון תרחיש סייבר מורכב בזמן אמת והגשת דו"ח מקצועי המפרט את הממצאים ודרכי הטיפול.

## מידע טכני על הבחינות:

✓ **שפת הבחינה**  
אנגלית (שפת הסייבר העולמית).

✓ **חלון גישה למבחן**  
14 ימים מרגע הפתיחה.

✓ **משך המבחן**  
2.5 עד 6 שעות.

✓ **מיקום**  
אונליין, ישירות בתוך פלטפורמת הלמידה של TechDX.

✓ **פורמט הבחינה**  
יישומי / מעשי (Applied).

✓ **ציון עובר**  
70 מתוך 100 (מבוסס Pass/Fail).

## אודות HackerU by TechDX

HackerU היא ה'חממה' המובילה בישראל להכשרת מיומנויות סייבר והייטק בישראל ובעולם. כחלק מקבוצת TechDX הגלובלית, אנחנו מנגישים תוכניות למידה חדשניות מבוססות בינה מלאכותית, ומספקים פתרונות הכשרה והסמכה מתקדמים בתחומי הסייבר עבור למעלה מ-60,000 סטודנטים ברחבי העולם.

עם ניסיון של למעלה מ-30 שנה בתחום, אנחנו משמשים כשותף האקדמי הרשמי של אוניברסיטאות ומכללות מובילות במעל ל-10 מדינות, ביניהן ארצות הברית, אוסטרליה, סינגפור, הודו ופולין.

פלטפורמת סימולציית הסייבר הייחודית שלנו נבחרה כסטנדרט המקצועי להכשרת כוחות ביטחון, צבאות, משטרות וגופי ממשל גלובליים, ומציידת את הסטודנטים בידע מעשי Hands-On ושליטה מלאה בכלים המתקדמים ביותר שנדרשים כיום בתעשיית אבטחת המידע.



# פירוט המודולים ותוכנית הלימודים

## יסודות הסייבר (Foundations Course)

המבוא הרשמי שלכם לעולם אבטחת המידע. נלמד איך מחשבים חושבים, איך רשתות מתקשרות ואיך מזהים איומים בשטח.

### מודול 1

#### אוריינטציה ופתיחה

היכרות עם פלטפורמת הלמידה, הגדרת פרופיל אישי, ניווט בחומרי הלימוד וחיבור לקהילת הסטודנטים כדי להתחיל ברגל ימין.

### מודול 3

#### יסודות המחשב

בניית בסיס טכנולוגי חזק: הבנת רכיבי חומרה ותוכנה, מערכות הפעלה וממשק שורת הפקודה (CLI).

##### נושאים נלמדים

- החיים בעידן הדיגיטלי
- רכיבי המחשב
- מערכות הפעלה.

##### תוצרי למידה

- ניווט מלא במערכת הקבצים של Linux וניהול קבצים ותיקיות דרך הטרמינל.

### מודול 2

#### מבוא לעולם הסייבר (Introduction to Cyber)

היכרות עם פלטפורמת הלמידה, הגדרת פרופיל אישי, ניווט בחומרי הלימוד וחיבור לקהילת הסטודנטים כדי להתחיל ברגל ימין.

##### נושאים נלמדים

- צעדים ראשונים בסייבר
- עולם אבטחת המידע
- איומי סייבר
- האקינג אתי
- מתקפות בחיי היום-יום
- Gen AI & LLMs
- מגמות ומפת איומי ה-AI בסייבר.

##### תוצרי למידה (מה תדעו לעשות)

- הנדסת פרומפטים מול עוזר AI מקומי לפתרון בעיות קוד וסייבר.
- ניתוח קבצים חשודים ב-VirusTotal לזיהוי נזקות.

### מודול 4

#### יסודות הרשת (Network Fundamentals)

איך מידע נע ברשת בצורה מאובטחת? היכרות עם ארכיטקטורת רשתות, מודל OSI, פרוטוקולי תקשורת נפוצים ושימוש ברחרחני רשת (Sniffers).

##### נושאים נלמדים

- הרשת הדיגיטלית
- בניית ארכיטקטורת רשת
- כתובות פיזיות ולוגיות
- מודל OSI
- פרוטוקולי תקשורת
- Network Sniffers
- ניתוח תעבורת רשת.

##### תוצרי למידה

- ניתוח פרקטיקות אבטחה ברשת הביתית והמלצה על הגנות; ניתוח תעבורת HTTP לעומת HTTPS ב-Wireshark והבחנה בין סיסמאות חשופות למוצפנות.
- ניתוח תעבורת FTP/SFTP להשוואת מידע חשוף מול מוצפן.

### מעבדות מעשיות (Labs)

- ניתוח נזקות (Malware Analysis)
- עבודה עם Local LLM Chatbot
- הרצת פקודות ראשונות ב-Windows CLI וב-Linux
- מחקר והגנת רשת ביתית
- חקירת תעבורת HTTP/HTTPS ופענוח סיסמאות חשופות ב-FTP.

### מודול 4

#### סיכום והסמכה

סיכום תכני הקורס והכנה למבחן המיקרו-credential הרביעי של המסלול.

### ניתוח אירוע (Case Study)

- מתקפת הסייבר על המשחקים האולימפיים.

## מערכות ותשתיות (Systems Course)

**השלב הפרקטי:** ניהול, אבטחה ופתרון תקלות בסביבות ה-IT הארגוניות המובילות בשוק (Cisco, Windows Server, Linux).

### מודול 1

#### ניהול רשתות (Network Administration)

היכרות עם ארגז הכלים של מנהל הרשת: הגדרת נתבים (Routers), מתגים (Switches), חלוקה ל-VLANs והטמעת חוקי גישה ואבטחה (ACLs).

##### נושאים נלמדים

- יסודות סיסקו (Cisco)
- ניהול כתובות IP
- מנגנוני DHCP & NAT
- אבטחת פורטים (Switch Port Security)
- ניטור ופתרון תקלות רשת.

##### תוצרי למידה (מה תדעו לעשות)

- הטמעת שרת DHCP בסימולטור Cisco
- Packet Tracer
- הגדרת Port Security על מתגי סיסקו לחסימת גישה לא מורשית.

### מודול 2

#### ניהול מערכות Windows הארגונית

ניהול ואבטחת סביבת מיקרוסופט ברמת תחנת קצה וברמת שרת (Server). עבודה מעשית עם Active Directory (AD), מדיניות קבוצתית (GPO), ניהול שירותי DNS והקשחת שרתים.

##### נושאים נלמדים

- ניהול תהליכים ושירותים
- Windows Registry
- שורת הפקודה
- Active Directory
- הגדרות GPO
- חומת אש (Firewall) ומדיניות סיסמאות.

##### תוצרי למידה (מה תדעו לעשות)

- ניתוח תהליכים ב-Task Manager לזיהוי אנומליות
- הגדרת שרת Windows Server, יצירה וניהול של אובייקטים ב-Active Directory
- החלת מדיניות סיסמאות ארגונית מאובטחת.

## מעבדות מעשיות (Labs)

- הגדרת DHCP וקינפוג נתבים ב-Packet Tracer
- ניתוח תהליכים ב-Windows Task Manager
- ניהול אובייקטים ב-Active Directory ויישום GPO
- הקמת שרת DNS
- כתיבת פקודות ושרשורי קוד (Pipelines) בלינוקס
- אבטחת שרתי Web בלינוקס. ניתוח אירוע (Case Study): מערכות SIEM בפעולה בזמן אמת.

## ניתוח אירוע (Case Study)

- מערכות SIEM בפעולה בזמן אמת.

## מודול 3

### ניהול מערכות Linux

שליטה במערכת ההפעלה שהיא הלב של עולם הסייבר. מניווט מתקדם ועד ניהול הרשאות, משתמשים והקשחת שרתי ווב (Web Servers).

#### נושאים נלמדים

- מבנה מערכת הקבצים
- פקודות לוגיות ושרשור פקודות (Pipelines)
- ניהול קלטים ופלטים (I/O Redirection)
- ניהול חבילות (Package Management) ואבטחת שרתים.

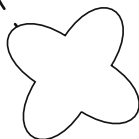
#### תוצרי למידה

- הרצת Pipelines לעיבוד נתונים יעיל
- ניהול הרשאות קבצים (Permissions) וקבוצות משתמשים לאכיפת בקרת גישה (Access Control)
- הגדרת שרתי אינטרנט מאובטחים בלינוקס לצמצום חולשות.

## מודול 4

### סיכום והסמכה

סיכום תכני הקורס והכנה למבחן המיקרו-credential הרביעי של המסלול.



# תפעול והגנה (Operations Course)

מעבר לחזית ההגנה: נלמד על אבטחת תשתיות ענן (AWS), ניתוח איומים מבוסס AI, ועבודה עם מודלים ומתודולוגיות בינלאומיות של הגנת סייבר.

## מודול 1

### מחשוב ענן (Cloud Computing)

איך בונים ומאבטחים תשתית ענן מודרנית? היכרות עם מודלי שירות, וירטואליזציה ושרתים, לצד התנסות מעשית חיונית בסביבת AWS.

#### נושאים נלמדים

- ארכיטקטורת רשת בענן
- אבטחת סביבת AWS
- ניהול זהויות והרשאות (IAM)
- תתי-רשתות מאובטחות (VPC)
- ניטור ענן
- קונטיינרים (Containerization) ו-Serverless.

#### תוצרי למידה (מה תדעו לעשות)

- הקמת מכונת EC2 ב-AWS
- ניהול משתמשי AWS IAM
- החלת פוליסיז ואכיפת אימות דו-שלבי (MFA)
- עיצוב ותכנון VPC מאובטח לבקרת תעבורת הרשת בענן.

## מודול 3

### בינה מלאכותית לאנשי סייבר (The Foundations of LLMs for Security Professionals)

איך ה-AI משנה את חוקי המשחק? נלמד לרתום מודלי שפה גדולים (LLMs) לאוטומציה של ניתוח לוגים, סריקת חולשות וכתובת נהלי אבטחה, לצד הבנת איומי AI ממוקדים כמו Prompt Injection ופגיעה בפרטיות מידע.

#### נושאים נלמדים

- סודות ה-ML וה-AI
- ניתוח אבטחה אוטומטי
- ניהול משימות אבטחה באמצעות LLM
- סיכוני אבטחה במודלי שפה
- ואתיקה ב-AI.

#### תוצרי למידה (מה תדעו לעשות)

- התנסות בפרמטרים של מודלי שפה להתאמת תשובות סייבר מדויקות
- ניתוח לוגים מבוסס AI לזיהוי אנומליות ושלילת ישויות אבטחה
- סימולציית מתקפת Prompt Injection על צ'אטבוט לחשיפת מידע רגיש.

## מודול 2

### יסודות הגנת הסייבר (Cybersecurity Fundamentals)

הבנת עולמם של התוקפים והמגינים. נלמד למפות איומים באמצעות המסגרות (Frameworks) המובילות בתעשייה: NIST, MITRE ATT&CK, ו-Cyber Kill Chain, ונלמד ליישם אסטרטגיית הגנה רב-שכבתית (Defense in Depth).

#### נושאים נלמדים

- סוגי האקרים ותוקפים (Threat Actors)
- חולשות (Vulnerabilities)
- אקספלויטים (Exploits) וסוגי נזקות.

## ניתוח אירוע (Case Study)

- זיהוי אירועי אבטחה
- פתרון נפילת רשת ב-NOC
- בלימת מתקפת כופרה ב-SOC
- מחקרי מקרה מיוחדים (MediWell, Elysium, CVE-2024-19876, EternalBlue).

## מודול 4

### סיכום והסמכה

סיכום תכני הקורס והכנה למבחן המיקרו-credential הרביעי של המסלול.

## מעבדות מעשיות (Labs)

- הקמת מכונות EC2 ב-AWS וניהולן מרחוק (RDP)
- אבטחת זהויות ב-AWS IAM ואכיפת MFA
- עיצוב רשת VPC מאובטחת
- מחקר מעשי של חולשות במאגרי CVE
- אקספלוויטציה של חולשות VNC
- ניתוח לוגים מונחה AI
- מתקפות סימולציה על מודלי בינה מלאכותית (Sensitive Information Disclosure).



## סיום המסלול והסמכה

סטודנטים שישלימו את כלל המעבדות, המשימות ויעברו בהצלחה את מבחני ההסמכה היישומים של TechDX, יוסמכו רשמית כ-Certified Cybersecurity Associate – התואר והיכולות המעשיות שיפתחו לכם את הדלת לתפקידי ה-Entry Level הנחשקים בתעשייה.