



הסמכת

Cyber Defense Professional Track

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



אודות מסלול ההסמכה

מסלול ההכשרה המקצועי להגנת סייבר (Cyber Defense Professional Track) בשילוב הסמכת Certified Cybersecurity Associate מספק חוויית למידה מקצה לקצה בתחום אבטחת המידע. המסלול תוכנן במיוחד כדי להוביל אנשי מקצוע ומשתתפים ללא רקע טכני קודם, שלב אחר שלב, מרמת הבנה בסיסית ועד למיומנות טכנית גבוהה המוכרת בשוק העבודה, ומכין אותם ישירות להשתלבות בתפקידי מרכזי SOC ומודיעין סייבר. התוכנית משלבת בין לימוד תיאורטי מונחה, מעבדות תרגול Hands-On מתקדמות והערכות מבוססות תרחישים, המעניקות עמידות מקצועית מוכחת בשטח ומתעדפות יכולות עבודה אמיתיות על פני שינון יבש.

נתוני המסלול ודרישות קדם

רמת מיומנות 
מתחילים ללא רקע קודם.

היקף שעות והשקעה 
400 שעות של למידה ממוקדת ומעבדות יישומיות מתקדמות.

לאילו תפקידים המסלול מכין אתכם?

התוכנית מותאמת באופן מלא לדרישות השוק הגלובליות ומכינה אתכם להשתלבות מהירה במגוון רחב של משרות מבוקשות בעולמות הצוות הכחול (Blue Team) ומודיעין האיומים:

Cyber Analyst / Cybersecurity Operations Technician 

Cyber Threat Researcher 

Cyber Defense Analyst 

Threat Intelligence Analyst 

Cybersecurity Associate 

Cybersecurity Intern 

Tier 1 SOC Analyst 

Tier 2 SOC Analyst 

תקינה בינלאומית: תוכנית הלימודים והתכנים במסלול ממופים ומותאמים באופן מלא לסטנדרטים הבינלאומיים המחמירים ביותר של הארגונים המובילים בעולם:

NIST

NICE



למי המסלול מתאים?

המסלול מיועד לאנשי מקצוע ומעוניינים בהסבת מקצוע המחזיקים באוריינות מחשב בסיסית וללא שום רקע קודם בעולם הסייבר. המסלול בנוי במתכונת של פיתוח מיומנויות הדרגתי ופרוגרסיבי, המתחיל בבניית יסודות מוצקים ומתקדם בהדרגה לעבר רמות ניסיון טכניות ומבצעיות מורכבות.

המבנה הייחודי של התוכנית: תעודות שמצטברות לקריירה

התוכנית מורכבת מ-4 הסמכות מלאות ו-12 מיקרו-הסמכות נפרדות המשתלבות זו בזו:

Certified SOC Analyst 3

- תפעול SOC וניטור איומים
- זיהוי איומים וניתוח לוגים
- תגובה לאירועים וניהול חולשות

Certified Cybersecurity Associate 1

- יסודות (Foundations)
- מערכות (Systems)
- תפעול (Operations)

Certified CTI Analyst 4

- יסודות מודיעין האיומים
- ציד איומי תשתית
- ציד איומים אסטרטגי ואוטומציית AI

Certified Cybersecurity Analyst 2

- יסודות הגנת הסייבר (Fundamentals)
- מיומנויות ליבה (Essentials)
- אנליזה (Analysis)

כל מיקרו-הסמכה מתמקדת ביישום פרקטי בשילוב למידה מונחת, ומסתיימת במבחן הסמכה יישומי. עם השלמת שלושת השלבים של כל קורס ומעבר המבחנים בהצלחה, תהיו זכאים לכל מיקרו-הסמכה בנפרד ול-4 ההסמכות המלאות של המסלול.

בניית תיק עבודות לעולם האמיתי

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



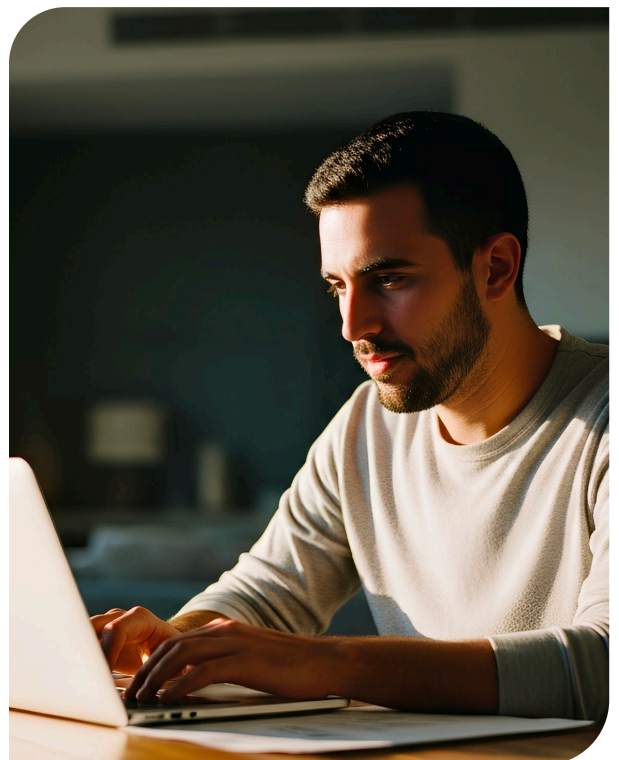
רשימת מיומנויות

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 מעשית בשטח. כל מבחן מורכב משני חלקים מרכזיים:

- **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

חלק 1: Certified Cybersecurity Associate

קורס יסודות (Foundations Course)

קורס זה מציע מבוא יסודי לעולם הגנת הסייבר ומכסה מושגי מפתח במערכות מחשב, יסודות רשתות תקשורת ומודעות לאיומי סייבר מודרניים.

מעבדות מעשיות (Labs)

- ניתוח נזקות
- מבוא לצ'אטבוט LLM מקומי
- צעדים ראשונים בהרצת פקודות ב-Windows וב-Linux
- מחקר והגנת רשת ביתית
- חקירת HTTP מול HTTPS
- חשיפת אישורי תעבורת FTP.

ניתוח אירוע (Case Study)

- מתקפת הסייבר על המשחקים האולימפיים.

מודול 1

מבוא לעולם הסייבר

היכרות עם התחום, בחינת מפת האיומים, חשיבות ההאקניג האתי והשפעת מתקפות הסייבר על חיי היומיום, לצד סקירת השפעתן של טכנולוגיות בינה מלאכותית יוצרת ומודלי שפה גדולים.

מודול 2

יסודות המחשב

בניית מיומנויות מחשב בסיסיות, הבנת יחסי הגומלין בין חומרה לתוכנה, מערכות הפעלה וממשקי שורת פקודה.

מודול 3

יסודות הרשת

הבנת עקרונות הרשת הדיגיטלית ותנועת מידע מאובטחת, ארכיטקטורה, מודל OSI, פרוטוקולי תקשורת נפוצים ושימוש ברחרחני רשת ו-Wireshark.

מודול 4

סיכום והסמכה

סיכום שלבי קורס היסודות והכנה למבחן ההסמכה של המיקרו-credential הראשון.



קורס מערכות (Systems Course)

מבוא מעשי ויישומי למערכות ליבה בהגנת סייבר הכולל ניהול רשתות, ניהול מערכות Windows ופעילויות בסביבת Linux.

מעבדות מעשיות (Labs)

- קירת קונפיגורציית DHCP
- הגדרת פונקציות ניהוליות
- הגדרת Port Security ואימותה
- הגדרת נתב ראשונית
- ניתוח תהליכים ב-Task Manager של Windows
- פקודות ניהול Windows Server
- יצירה וניהול אובייקטים ב-Active Directory
- הגדרות GPO בסיסיות
- קונפיגורציית DNS
- מדיניות סיסמאות משתמשים
- פקודות לינוקס בסיסיות
- שרשורי לינוקס
- ניהול קבוצות בלינוקס
- קינפוג שרתי אינטרנט מאובטחים.

ניתוח אירוע (Case Study)

- אבטחת גישה מרחוק לשרת קריטי.

מודול 1

ניהול רשתות

תפקיד מנהל הרשת, הגדרת כתובות IP, נתבים, מתגים, רשתות VLAN וחוקי אבטחה וגישה.

מודול 2

ניהול מערכות Windows

ניהול ואבטחת סביבות Windows ברמת הקצה ושרתים, עבודה עם תהליכים, קבצים, Active Directory, מדיניות קבוצתית ו-DNS.

מודול 3

ניהול מערכות Linux

פיתוח יכולות ניהול לינוקס, ניווט בשורת הפקודה, הרשאות קבצים, ניהול קבוצות משתמשים וקינפוג שרתים מאובטחים.

מודול 4

סיכום והסמכה

סיכום תכני הקורס והכנה מלאה לקראת מבחן המיקרו-credential השני.



קורס תפעול (Operations Course)

הכרת עולמות האבטחה המבצעיים המרכזיים הכוללים אבטחת תשתיות ענן, הגנה מונחית בינה מלאכותית וניהול איומים מורכבים.

מעבדות מעשיות (Labs)

- מבוא לוירטואליזציה
- הקמת מכונת EC2 ב-AWS
- פקודות CLI על גבי מכונת EC2
- אבטחת זהויות והרשאות ב-AWS IAM ואכיפת MFA
- עיצוב רשת VPC מאובטחת
- מחקר וניתוח חולשות במאגרי CVE
- אקספלוויטציה של חולשות VNC
- ניתוח רשת בסיכון (חלק 1 ו-2)
- קינפוג מודלי שפה
- ניתוח לוגים מונחה AI
- מניעת חשיפת מידע רגיש במערכות AI.

ניתוח אירוע (Case Study)

- זיהוי אירועי אבטחה
- פתרון נפילת רשת ב-NOC
- בלימת מתקפת כופרה ב-SOC
- מקרה בוחן MediWell
- חולשת Elysium
- ניתוח חולשת EternalBlue.

מודול 1

מחשוב ענן

יסודות הוירטואליזציה והענן, מודלי שירות, ניהול רשתות, ניטור, עמידה בתקנים והתנסות מעשית בסביבות AWS, מערכות Serverless וקונטיינרים.

מודול 2

יסודות הגנת הסייבר

סקירה יישומית של עולם פשעי הסייבר, סוגי תוקפים וחולשות מערכת, תוך בחינת מסגרת העבודה של NIST, מודל MITRE ATT&CK ו-Cyber Kill Chain ואסטרטגיות הגנה רב-שכבתית.

מודול 3

יסודות מודלי שפה עבור אנשי אבטחה

שילוב הבינה המלאכותית היוצרת בהגנת סייבר, אוטומציה של ניתוח לוגים, סריקת חולשות, כתיבת נהלים, והתמודדות עם סיכונים כמו Prompt Injection וחשיפת מידע.

מודול 4

סיכום והסמכה

סיכום שלבי קורס התפעול והכנה למבחן ההסמכה השלישי של שלב ה-Associate.



קורס יסודות ההגנה (Fundamentals Course)

הקניית בסיס מעשי בהגנת סייבר ארגונית הכוללת אבטחת רשתות, הגנת מערכות הפעלה ותהליכי עבודה במרכזי SOC.

מעבדות מעשיות (Labs)

- מודל Cyber Kill Chain
- ניתוח לוגי ניתוק מערכת
- חסימת תעבורת ICMP באמצעות חומת האש של Windows
- ניטור שלמות קבצים ומנגנוני תגובה אקטיביים ב-Wazuh
- הצפנת דיסקים ב-BitLocker
- סריקת נזקות ב-ClamAV

ניתוח אירוע (Case Study)

- פתרון נפילת רשת ב-NOC
- בלימת מתקפת כופרה ב-SOC
- זיהוי מתקפת DoS
- בלימת מתקפת אדם באמצע (MITM)
- חקירת פריצה למערכת הפעלה.

מודול 1

יסודות אבטחת סייבר ותפעול SOC

עקרונות מבצעיים של ניהול ההגנה, הכרת תפקידי ומבנה צוות ה-SOC, מסגרות עבודה מנחות כמו NIST ו-MITRE ATT&CK, ואסטרטגיות תגובה לאיומים.

מודול 2

יסודות רשתות ואבטחה

תנועת מידע מאובטחת, עיצוב רשת מאובטחת, כלי ניטור וזיהוי אנומליות, סגמנטציה וחומות אש.

מודול 3

אבטחת מערכות הפעלה

הגנה על תחנות קצה ושרתים בסביבות Windows ו-Linux, הקשחת מערכות, איתור חולשות ושימוש במערכות EDR ו-Wazuh.

מודול 4

סיכום והסמכה

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



קורס מיומנויות ליבה (Essentials Course)

תרגול של פרקטיקות מרכזיות לניטור, זיהוי איומים, ניתוח לוגים ארגוניים במערכות SIEM, אבטחת רשתות והגנת ענן.

מעבדות מעשיות (Labs)

- קינפוג שרתי לקוח ושרת OpenVPN
- הגדרת חוקי חומת האש של Windows
- הגדרת חוקי שרשרת ב-iptables בלינוקס
- הגדרת חוקי חומת אש ב-pfSense
- ניהול חוקי Snort
- פקודות Shell ומכונות Ubuntu
- ניטור פונקציות Lambda
- הקמת אפליקציות עמוד יחיד (SPA)
- יצירת קונטיינר ECS Fargate
- ניתוח וניהול לוגים והתראות בלוחות בקרה של Splunk
- אינטגרציית SIEM עם לוגי שרת Apache.

ניתוח אירוע (Case Study)

- מערכות SIEM בפעולה בזמן אמת.

מודול 1

אבטחת רשתות

שימוש בשרתי VPN, הגדרת חומות אש, מערכות גילוי ומניעת חדירות (IDS/IPS) לטובת שמירה על סודיות וזמינות המידע.

מודול 2

אבטחת ענן

הגנה על שירותי ענן וירטואליים, וירטואליזציה מעשית, ניטור תשתיות AWS, עמידה ברגולציות ומחשוב Serverless.

מודול 3

מערכות SIEM וניתוח לוגים

הניטור, זיהוי ותגובה בזמן אמת באמצעות פלטפורמות SIEM מובילות, איסוף לוגים וניהול התראות והצלבת אירועים ב-Splunk.

מודול 4

סיכום והסמכה

סיכום המודולים והכנה למבחן המיקרו-credential החמישי של המסלול.



קורס אנליזה (Analysis Course)

פיתוח יסודות חקירה ותגובה מתקדמים, ניתוח נזקות, פורנזיקה דיגיטלית, טיפול באירועים והפעלת כלי אבטחה מבוססי בינה מלאכותית (GenAI).

מודול 1

ניהול חקירת נזקות ויסודות פורנזיקה

זיהוי, ניתוח ופירוק של תוכנות זדוניות באמצעות טכניקות סטטיות ודינמיות, עבודה עם כלי Sysinternals, איסוף ראיות דיגיטליות ושימוש בפלטפורמות מודיעין איומים (TIPs) ו-OSINT.

מודול 2

תגובה לאירועי סייבר

מסגרת עבודה שלמה משלב זיהוי האירוע ועד להתאוששות ממנו, פיתוח תוכניות תגובה, ניתוח אינדיקטורים של פריצה (IOCs) ובלימת אירועים פעילים בשטח.

מודול 3

בינה מלאכותית יוצרת עבור אנשי אבטחה

כיצד מודלי שפה גדולים ולמידת מכונה משנים את עבודת האנליסט ב-SOC, אוטומציה של ניתוח התראות, תגובה לפישינג וניהול סיכונים Prompt Injection.

מודול 4

סיכום והסמכה

סיכום שלבי קורס האנליזה והכנה למבחן ההסמכה המסכם של שלב ה-Analyst.

מעבדות מעשיות (Labs)

- ניתוח נזקות היברידי
- ניתוח דינמי באמצעות כלי Sysinternals
- ניתוח נזקות סטטי ודינמי משולב
- חקירה וחיפוש במנוע Shodan
- קינפוג והגדרות מודלי שפה
- ניתוח לוגים מתקדם מונחה AI
- שימוש ב-VirusTotal ו-Code Insight
- ניתוח קבצי ואירועי פישינג בדואר אלקטרוני
- מתקפות Prompt Injection ומניעת חשיפת מידע רגיש במערכות AI.

ניתוח אירוע (Case Study)

- ניתוח מקרה בוחן נזקת Zeus
- חקירה פורנזית של נזקות בארגון.



קורס תפעול SOC וניטור איומים (SOC Operations and Threat Monitoring Course)

הבנת תהליכי העבודה, המבנה המבצעי והאחריות בתוך מרכז SOC מודרני, ניטור תעבורת רשת מתקדם ואסטרטגיות גילוי ומניעת חדירות.

מעבדות מעשיות (Labs)

- מעבר ממערכת Sigma ל-SIEM
- ניתוח דו"חות אירוע
- מעקב אחר פעילות חשודה ברשת
- ניתוח תעבורה מתקדם
- חילוץ קבצים ב-Wireshark ו-Network Miner
- קונפיגורציית SNMP בצידוד Cisco
- עבודה עם Zeek
- התקנה והגדרת Nagios
- ניטור משאבים עם Zabbix
- התקנת Suricata ב-pfSense
- זיהוי אנומליות וכתיבה ובדיקה של חוקי Suricata מול קבצי PCAP.

מודול 1

מושגים בתפעול מערך אבטחה

הבנת דרגי ה-SOC (Tiers), נתיבי אסקלציה של התראות, מדדי איכות וכתיבת דו"חות אירוע מקצועיים וברורים.

מודול 2

ניטור אבטחת רשתות

איסוף ובחינת תעבורה, זיהוי התנהגות זדונית באמצעות Wireshark, Zeek וכלי טלמטריה, וניטור תשתיות באמצעות מערכות Nagios ו-Zabbix.

מודול 3

אסטרטגיות גילוי ומניעת חדירות

ניתוח ובלית חדירות באמצעות פתרונות IDS/IPS המובילים בשוק, קונפיגורציית Suricata, פיתוח וכוונון חוקי זיהוי וביצוע בדיקת חבילות עמוקה (DPI).

מודול 4

סיכום והסמכה

סיכום התכנים והכנה למבחן המיקרו-credential השביעי של המסלול.



קורס זיהוי איומים וניתוח לוגים (Threat Detection and Log Analysis Course)

כווןון ובניית חוקי הצלבה (Correlation Rules) במערכות SIEM, ניהול והתאמת התראות, יסודות אוטומציה ב-SOAR וניתוח מתקדם של לוגי מערכת בסביבות Windows ו-Linux.

מעבדות מעשיות (Labs)

- כווןון ובדיקת חוקי SIEM
- חקירת פריצה לסביבת דומיין
- זיהוי וחקירה עם Splunk
- חקירת מתקפות SQL Injection ומתקפות הזרקת קוד לזיג
- הטמעת פלייבוק ב-Splunk SOAR
- הצלבה וניתוח לוגי Windows ב-Splunk.

ניתוח אירוע (Case Study)

- מקרה בוחן Zoom ומחירן של בקורות גישה חלשות
- פריצה ל-Heartland Payment Systems
- כיצד מערכות SOAR מיעילות את התגובה ב-SOC.

מודול 1

כווןון מערכות SIEM ותפעול התראות

ניהול מחזור החיים של התראות אבטחה, סינון אירועים (Triage), צמצום התראות שזוא וחקירת מתקפות וזב מורכבות.

מודול 2

מבוא לעולם ה-SOAR

הבנת טכנולוגיות האוטומציה והתזמור המבצעי ב-SOC, אוטומציית פלייבוקים ב-Splunk SOAR, וניהול אירועים יעיל ומהיר.

מודול 3

ניתוח לוגים מתקדם בסביבות Linux ו-Windows

כיצד מודלי שפה גדולים ולמידת מכונה משנים את עבודת האנליסט ב-SOC, אוטומציה של ניתוח התראות, תגובה לפישינג וניהול סיכוני Prompt Injection.

מודול 4

סיכום והסמכה

סיכום המודולים והכנה למבחן המיקרו-credential השמיני של המסלול.



קורס תגובה לאירועים וניהול חולשות (Incident Response and Vulnerability Management Course)

הכשרה פורנזית מעשית ברכישת ראיות דיגיטליות, תהליכי תגובה מובנים לאירועי פריצה מורכבים ואינטגרציה של סימולציות Purple Team בשילוב סוכני בינה מלאכותית (AI Agents).

מעבדות מעשיות (Labs)

- הפקת אימג' פורנזי באמצעות FTK Imager
- חקירת תהליכים ורכישת זיכרון במעבדת MemorizeMe
- עבודה מעשית וניתוח ממצאים ב-Autopsy
- ניתוח קבצים מצורפים באימיילי פישניג
- פיתוח והרצת סוכן ה-AI הראשון שלכם.

מודול 1

רכישת ראיות דיגיטליות

מבוא יישומי לפורנזיקה דיגיטלית וטיפול בראיות, איסוף ושימור זיכרון נדיף (RAM) ושאינו נדיף באמצעות כלי תעשייה מובילים כמו FTK Imager, Autopsy ו-Volatility.

מודול 2

תגובה לאירועי סייבר

פיתוח מיומנויות יסוד הנדרשות לניהול אירועי אבטחה, הבנת מודל ה-Incident Response של NIST, ופרקטיקות מיטביות לשלבי המוכנות, הזיהוי, הבלימה וההתאוששות מחדירה או פישניג.

ניתוח אירוע (Case Study)

- חקירת הפריצה ל-Equifax (2017)
- פריצת National Public Data
- ניתוח מתקפת הסייבר הגלובלית על CDK Global (2024)
- ניתוח תרחישים וכוונות חוקי זיהוי (חלק 1 ו-2).

מודול 3

Purple Teaming והגנה מונחת בינה מלאכותית

גישור בין עולמות התקיפה וההגנה (צוותים סגולים), בחינת תפקידם של סוכני AI (AI Agents) במערך ה-SOC, והערכת השפעתם על סקילביליות ויכולת התאמה של פונקציות אבטחה.

מודול 4

סיכום והסמכה

סיכום שלבי הקורס והכנה למבחן ההסמכה התשיעי של המסלול.



קורס יסודות מודיעין האיומים (Threat Intelligence Foundations Course)

הקניית בסיס מעשי רחב בתפעול מערכי מודיעין סייבר, מחזור חיי המודיעין (CTI Lifecycle), עבודה עם פלטפורמות ייעודיות, שיתוף מידע וניתוח קבצי נזקה ותשתיות תוקפים.

מעבדות מעשיות (Labs)

- בניית פרופיל יריב באמצעות חקירות OSINT
- יצירת פרופיל תוקף מתוך מקרה בוחן | איסוף וניהול מודיעין איומי סייבר
- מחקר קבוצות APT
- יצירת חוקי YARA וביצוע ציד איומים מבוסס חתימות
- ניתוח דגימות נזקה לזיהוי טקטיקות ניצול.

ניתוח אירוע (Case Study)

- חקירת פעילות קבוצת התקיפה Volt Typhoon.

מודול 1

מבוא למודיעין איומי סייבר

עקרונות היסוד ומטרות ה-CTI, הפיכת נתונים גולמיים לתובנות מעשיות, ניתוח התנהגות תוקפים וטכניקות שיוך (Attribution) ופרופילינג.

מודול 2

פלטפורמות מודיעין איומים

היכרות עם כלי המפתח, הזנות הנתונים (Feeds) ומסגרות עבודה מובנות כגון MITRE ATT&CK ו-D3FEND למיפוי התנהגות יריב ותמיכה במערך הבטחה הארגוני.

מודול 3

ניתוח נזקות ותשתיות

מיקוד בניתוח אינדיקטורים של פריצה (IOCs), תהליכי חקירת נזקות וטכניקות דיווח מודיעיני, וצלילה עמוקה לכתובה ויישום של חוקי YARA בתהליכי עבודה מודיעיניים.

מודול 4

סיכום והסמכה

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



קורס ציד איומי תשתית

(Infrastructure Threat Hunting Course)

פיתוח יכולות ציד איומים פרואקטיבי (Threat Hunting) המשלים את הניטור המסורתי ב-SOC, גיבוש היפותזות, ניתוח לוגים מתקדם בסביבות מגוונות וניטור אנומליות בסביבות ענן.

מעבדות מעשיות (Labs)

- הגדרת ELK לאיסוף נתונים
- חקירה ואימות שאילתות ב-Elastic
- חקירת טכניקות עמידות (Persistence) במערכת Windows
- ציד בתחנות קצה עם Velociraptor
- פקודות ובקרה (C2) מבוססות Mythic
- חקירת DNS Tunneling ב-Wireshark
- הקמת פתיון Cowrie Honeypot וניתוח הלוגים שלו
- שאילתות על נתוני האבטחה שלכם.

ניתוח אירוע (Case Study)

- ניצול לרעה של פישניג ב-Microsoft Teams
- ו-Quick Assist (שנת 2024)
- ציד איומים מעשי באמצעות פתיונות.

מודול 1

שיטות לציד איומים

מושגי ליבה ומתודולוגיות ציד, איסוף וניהול נתוני ציד, שימוש בכלים אנליטיים והטמעת ELK Stack לאיסוף, אחסון וויזואליזציה של טלמטריית רשת.

מודול 2

מודיעין איומים וקבוצות תקיפה מתקדמות

מינוף מודיעין איומים לטובת זיהוי קבוצות APT ודפוסי תקיפה מורכבים, ציד בתחנות קצה (Endpoints) עם Velociraptor, זיהוי תקשורת שרת חלופי (C2), ושימוש בפתיונות (Honeypots) וניתוח התנהגותי (UEBA).

מודול 3

אסטרטגיות ציד וזיהוי בענן

הרחבת פרקטיקות הציד אל תוך סביבות ענן וירטואליות והיברידיות, ניטור אנומליות, שימוש בכלי ויזואליזציה מתקדמים כמו PowerBI והגברת הנראות (Visibility) בתשתית הענן.

מודול 4

סיכום והסמכה

סיכום המודולים והכנה למבחן המיקרו-credential האחד-עשר של המסלול.



קורס ציד איומים אסטרטגי ואוטומציית AI (Strategic Threat Hunting AI Automation Course)

שילוב חזית הטכנולוגיה בפעולות הגנה מורכבות: ניתוח מודל בשלות הצייד (THMM), יישום אוטומציית בינה מלאכותית ולמידת מכונה (ML) להרחבת היקף הזיהוי, העשרת IOCs והאצת התגובה לאירועים.

מעבדות מעשיות (Labs)

- הבנת THMM וביצוע הערכות בשלות
- מסגרות עבודה של סיכונים ותפיסות טיפול
- סימולציית יריב ואמולציית מתקפות באמצעות Caldera
- ציד איומים מתקדם באמצעות פלטפורמת MISP
- חקירת אנומליות מתקדמת באמצעות Elastic ML

מודול 1

מודל בשלות ציד האיומים

הבנת שלבי האבולוציה של תוכניות הצייד הארגוניות מזיהוי ריאקטיבי לפעולות פרואקטיביות מונחות מודיעין, וביצוע תרגילי סימולציית יריב לטיוב בקורות ההגנה.

ניתוח אירוע (Case Study)

- מחקרי מקרה מיוחדים של אנומליות ברשת ובתחנות קצה.

מודול 2

אוטומציית AI עבור מודיעין איומים

שימוש בריצת תהליכי Python NLP לחילוץ ואיסוף נתונים אוטומטי, דירוג ותיקוף אוטומטי של IOCs מתוך מודיעין איומים לא מובנה (Unstructured Data) להאצת קבלת החלטות.

מודול 3

אוטומציית AI עבור ציד איומים

שילוב אלגוריתמים של למידת מכונה (ML) לניתוח UEBA, קביעת קווי בסיס (Baselines) זיהוי אנומליות, ותזמור (Orchestration) של תהליכי עבודה רציפים מונחי שיתוף פעולה אנושי-AI.

מודול 4

סיכום והסמכה

סיכום תכני הקורס והכנה למבחן ההסמכה השנתי-עשר והמסכם של המסלול כולו.





סיום המסלול והסמכה

סטודנטים שישלימו בהצלחה את כלל המעבדות, משימות הסימולציה ויעברו את מבחני ההסמכה היישומים של פלטפורמת TechDX, יזכו ב-12 מיקרו-הסמכות נפרדות ובארבע ההסמכות הרשמיות של המסלול: Certified Cybersecurity Associate, Certified Cybersecurity Analyst, Certified SOC Analyst ו-Certified CTI Analyst. זהו תיקוף היכולות המקיף ביותר בעולמות ה-Cyber Defense, המעניק לכם ידע פרקטי מוכח, ביטחון מקצועי ויתרון תחרותי עצום בשוק העבודה להשתלבות מהירה בחברות המובילות בתעשייה.

