סילבוס ותוכנית לימודים: CSRP
Cyber Security Responder & Practitioner

מסלול הכשרת מיישמי הגנה ואנליסטים בסייבר

שותפות אסטרטגית	הסמכת יעד	היקף אקדמי
זיו האפט (BDO) & סייבר סקול (Cyber School)	ISC2 Certified in Cybersecurity (CC)	160 שעות אקדמיות | 40 מפגשים 4 x שעות | היברידי

חזון התוכנית: מצוינות טכנולוגית וגישור על הפער התעסוקתי

בעידן שבו איומי הסייבר משפיעים על הביטחון הלאומי והחוסן הכלכלי, תוכנית ה-CSRP נבנתה כ"גשר מקצועי" (Professional Bridge). מטרת העל היא להעניק לתלמידים סט כלים יישומי המאפשר מעבר מהיר מהכשרה להשמה איכותית בתעשייה. התוכנית אינה מסתפקת בהעברת ידע, אלא מתמקדת בבניית יכולת ביצועית (Hands-on) מוכחת.

התוכנית מייצגת את הדור הבא של הכשרה מקצועית בסייבר - שילוב ייחודי של מתודולוגיה פדגוגית מתקדמת, ניסיון תעשייתי מוכח ופלטפורמת אימון בענן המדמה תרחישים אמיתיים. תלמידים רוכשים לא רק ידע תיאורטי, אלא גם ניסיון מעשי בכלים המדויקים שבהם משתמשים צוותי סייבר מובילים בארגונים הגדולים בישראל ובעולם.

השפעה חברתית ופריסה בינלאומית

סייבר סקול וקריית שמונה: סייבר סקול היא חברה שצמחה מהעיר קריית שמונה וחרטה על דגלה את קידום התעסוקה הטכנולוגית בצפון. אנו רואים בהכשרה זו שליחות לאומית לקידום הון אנושי איכותי מהפריפריה לחזית הסייבר העולמית.

הצלחה גלובלית: המתודולוגיה הפדגוגית של התוכנית יושמה בהצלחה ב-18 אוניברסיטאות מובילות בארה"ב, לצד גופים ממשלתיים ותעסוקתיים בישראל, מה שמבטיח תכנים ברמה בינלאומית.

פלטפורמת Cyber School: הלמידה מתבססת על זירת סייבר בענן המדמה תרחישי אמת (Scenario-based Learning) ללא צורך בהתקנות, ומאפשרת תרגול אינטנסיבי מכל מקום.

זיו האפט (BDO) – חטיבת ייעוץ הסייבר

פירמת BDO זיו האפט היא מהמובילות בישראל ובעולם בייעוץ, ניהול סיכונים וחוסן דיגיטלי. חטיבת הסייבר של BDO פועלת בחזית העשייה המבצעית ומספקת שירותים מתקדמים המשלבים מומחיות טכנית עם הבנה עסקית עמוקה.

הניסיון המעשי של יועצי BDO בשטח הוא הבסיס לתכני הלימוד, המבטיחים רלוונטיות מקסימלית לשוק העבודה. תלמידים נחשפים לאותן מתודולוגיות, כלים ותהליכים המיושמים בפרויקטים אמיתיים של ארגונים גלובליים.

סייבר התקפי

ביצוע בדיקות חדירות (Pentesting) וסקרי חולשות תשתיות ואפליקציות מתקדמות

ניהול סיכונים ו-GRC

ליווי ארגונים לתקני ISO 27001, הגנת הפרטיות וסקרי סיכונים מקיפים

SOC & MDR

הפעלת מרכזי ניטור ותגובה (Managed Detection & Response) חיצוניים לארגונים גלובליים

ניהול שרשרת אספקה

צוותי מומחים לניהול ובקרת סיכוני צד-שלישי (TPRM)

סייבר סקול (Cyber School)

המכללה הבינלאומית להכשרת מומחי סייבר, הפועלת מ-2014 ומכשירה עשרות אלפי בוגרים. כשותפה רשמית (Official Training Partner) של ארגון ה-ISC2 בישראל, סייבר סקול מובילה את תחומי ההסמכה היוקרתיים (CC, CISSP) ומפתחת דורות של אנשי מקצוע המשלבים ערכי אתיקה, אחריות דיגיטלית ומצוינות טכנית.

הגישה הפדגוגית של סייבר סקול מבוססת על למידה חוויתית המשלבת תיאוריה עם תרגול מעשי אינטנסיבי. כל תלמיד עובר מסע התפתחות אישי הכולל אתגרים מדורגים, פתרון בעיות בזמן אמת והתמודדות עם תרחישים המשקפים את המציאות המורכבת של עבודת סייבר מודרנית.

מבנה המסלול: מממיישם (Practitioner) לאנליסט (Analyst)

התוכנית מחולקת לשני שלבי הכשרה מרכזיים המשקפים את מסלול ההתפתחות המקצועי הטבעי בעולם הסייבר. כל שלב בנוי על קודמו ומספק את התשתית הנדרשת לשלב הבא, תוך הבטחת רצף למידה הרמוני ומעמיק.

1	2
שלב A	**שלב B**
מיישם סייבר – התקנה והקשחה	אנליסט סייבר – גילוי ותגובה

המעבר בין השלבים מתבצע באופן מתודי ומבוסס על הצלחה בשליטה ביכולות המיישם. התלמידים מפתחים תחילה יכולות בנייה והגנה יזומה, ורק לאחר מכן עוברים ליכולות זיהוי ותגובה מתקדמות.

חלק א': מיישם סייבר

מפגשים 1-24 | 96 שעות

פוקוס: הקמה, הגדרה והקשחה של מערכות אבטחה

- יסודות תשתיות ומערכות הפעלה
- טכנולוגיות הגנה וכלי סייבר מתקדמים
- בינה מלאכותית לאוטומציה
- בניית ארגון מאובטח מאפס

חלק ב': אנליסט סייבר

מפגשים 25-40 | 64 שעות

פוקוס: ניטור, ציד איומים ותגובה לאירועים

- סייבר התקפי וניתוח חולשות
- ניטור, SOC ותגובה לאירועים
- פורנזיקה דיגיטלית בסיסית
- פרויקט Capstone מלחמתי

גישה פדגוגית ייחודית: המבנה הדו-שלבי מבטיח שתלמידים מבינים קודם כל איך לבנות מערכות מאובטחות, ורק לאחר מכן לומדים לזהות ולתקוף אותן. זו גישה המשקפת את המציאות המקצועית ומקנה הבנה עמוקה יותר של ההגנה.

פירוט 40 המפגשים (160 שעות)

מודול 1

יסודות הסייבר, רשתות ומערכות הפעלה

מיקוד: מיישם סייבר | מפגשים 1-8 | 32 שעות

מודול הפתיחה מניח את התשתית הרעיונית והטכנית לכל מסע הלמידה. תלמידים נחשפים לעולם הסייבר דרך הבנה מעמיקה של התשתיות שעליהן בנויים ארגונים מודרניים. הדגש הוא על שליטה מלאה במערכות ההפעלה המרכזיות (Windows ו-Linux), פרוטוקולי תקשורת רשת וארכיטקטורות זהויות.

התלמידים לומדים לחשוב כמנהלי מערכות מתקדמים תוך הבנת נקודות התורפה הטבועות בכל שכבה טכנולוגית. כל מפגש משלב תיאוריה מעמיקה עם תרגול מעשי בפלטפורמת Cyber School, המאפשרת התנסות בתרחישים אמיתיים ללא סיכון לסביבות ייצור.

01

מבוא לסייבר ומשולש ה-CIA

הבנת תפקיד המגן הארגוני והכרת וקטורי התקיפה המודרניים. סודיות, שלמות, זמינות (CIA), ניהול סיכונים, איומי APT. מעבדה: Cyber School – הכרת ממשק המעבדה ואתגר CTF ראשון.

02

מודל ה-OSI ושכבות הרשת

שליטה במודל שבע השכבות ובפרוטוקולי הקצה. Physical Layer to Application Layer, Encapsulation. מעבדה: Wireshark – ניתוח פקטות ושכבת קו הנתונים.

03

פרוטוקולי תקשורת (TCP/IP)

הבנת מנגנוני הניתוב והעברת המידע ברשת. IP Addressing, Subnetting, Routing. מעבדה: Cyber School – הגדרת רשתות וניתוב בנתבים וירטואליים.

04

שירותי ליבה ותורפות (DNS/DHCP)

איתור תורפות בפרוטוקולי השירות הארגוניים. DNS Poisoning, DHCP Starvation, HTTP/S. מעבדה: Cyber School – ניתוח אנומליות תעבורה.

05

ניהול מערכות Windows Server

יכולת ניהול משתמשים והרשאות בשרתים ארגוניים. NTFS Permissions, Services, Local Security Policy. מעבדה: Cyber School – הקשחת Windows Server 2022.

06

ניהול זהויות Active Directory

הבנת מבנה ה-Domain וניהול מרכזי של מדיניות אבטחה. OU, GPO, Kerberos vs NTLM. מעבדה: Cyber School – הקמת דומיין וניהול GPO.

07

יסודות לינוקס (Linux CLI)

שליטה מלאה בשורת הפקודה (Terminal) לניהול שרתים. Filesystem, Pipes, Basic Commands. מעבדה: Cyber School – Linux CLI Master Challenge.

08

הרשאות והקשחה בלינוקס

הגנה על שרתי קוד פתוח וניהול גישה מתקדם. chmod, chown, sudoers, SUID/GUID. מעבדה: Cyber School – Privilege Escalation Defense.

מודול 2

טכנולוגיות הגנה וכלי סייבר

מיקוד: מיישם סייבר | מפגשים 9-20 | 48 שעות

המודול השני מתמקד בארסנל הכלים המקצועיים שמהווים את עמוד השדרה של כל מערך הגנה ארגוני מודרני. תלמידים לומדים לתכנן, ליישם ולתחזק מערכות הגנה רב-שכבתיות (Defense in Depth) המשלבות חומות אש, רשתות פרטיות וירטואליות, מערכות זיהוי חדירות ופתרונות הגנה על נקודות קצה.

ארכיטקטורת Firewalls

תכנון חומות אש מבוססות מדיניות ארגונית. Stateless vs Stateful, Ruleset design, DMZ.

ניהול תעבורה NAT

שליטה בתרגום כתובות ומיפוי פורטים מאובטח. SNAT, DNAT, Port Forwarding.

פתרונות VPN ארגוניים

הקמת חיבורים מרוחקים מאובטחים. IPsec vs SSL VPN, Encryption protocols.

מערכות IDS/IPS

זיהוי חדירות ומניעה אקטיבית של סריקות רשת. Snort, Suricata, Signature-based detection.

ניהול זהויות (IAM)

יישום בקרת גישה מבוססת תפקיד (RBAC). Identity Lifecycle, Provisioning, Least Privilege.

הזדהות חזקה (MFA)

מניעת גניבת חשבונות דרך הטמעת שכבות הגנה. 2FA, OTP, FIDO2, Biometrics.

הגנת מידע (DLP)

זיהוי ומניעת דליפת קבצים רגישים. Data Loss Prevention, Regex, Data Classification.

אבטחת נקודות קצה (EDR)

הגנה על תחנות קצה באמצעות כלים מבוססי התנהגות. AV vs EDR, XDR, Threat Hunting basics.

אבטחת שרתי דואר

מניעת פישינג וזיוף כתובות מייל. SPF, DKIM, DMARC, Mail Relay.

אבטחת גלישה (Web Proxy)

סינון תכנים והגנה על גלישת המשתמשים. Transparent Proxy, URL Filtering, SSL Inspection.

רגולציה ותקנים

הכרת עולם הציות והתקנים הבינלאומיים. ISO 27001, SOC2, חוק הגנת הפרטיות.

יסודות אבטחת ענן

הגנה על תשתיות ענן ציבורי. Shared Responsibility Model, Security Groups, IAM in Cloud.

מודול 3

בינה מלאכותית (AI) בעולם הסייבר

מיקוד: מיישם סייבר | מפגשים 24-21 | 16 שעות

המודול החדשני הזה מציב את התלמידים בחזית המהפכה הטכנולוגית. בינה מלאכותית משנה באופן יסודי את נוף הסייבר - הן בצד ההגנה והן בצד התקיפה. תלמידים לומדים כיצד למנף יכולות AI לאוטומציה של משימות אבטחה, זיהוי אנומליות וניתוח התנהגות משתמשים.

במקביל, הם נחשפים לאיומים החדשים שמביאה האינטליגנציה המלאכותית - מהתקפות Deepfake ועד Prompt Injection. זהו מודול ייחודי המשקף את המציאות המשתנה של עולם הסייבר ומכין את התלמידים לעתיד המקצוע.

בינה לאוטומציה של אבטחה

שימוש ב-AI לייעול עבודת ה-Security Practitioner. כתיבת סקריפטים עם LLM, אוטומציית ניטור לוגים. מעבדה: כתיבת סקריפטים הגנתיים (Python+AI).

זיהוי אנומליות באמצעות Machine Learning

הבנת השימוש ב-ML לזיהוי חריגות ברשת. Behavior Analysis, UEBA, ML Models. מעבדה: ניתוח תעבורה חריגה באמצעות מודל AI.

איומי AI ו-Adversarial ML

זיהוי התקפות המנצלות בינה מלאכותית. Deepfakes, AI-driven Phishing. מעבדה: Cyber School – זיהוי התקפות הנדסה חברתית ב-AI.

הגנה על מודלי AI

אבטחת כלי ה-AI בארגון מפני ניצול זדוני. Prompt Injection, Jailbreaking, LLM Security. מעבדה: Cyber School – אתגר הגנת Prompt Injection.

חדשנות בחזית הטכנולוגיה: תלמידי CSRP נחשפים לטכנולוגיות המתקדמות ביותר בשוק. הבנת AI בסייבר היא כבר לא יתרון תחרותי אלא דרישה בסיסית להצלחה בתעשייה.

מודול 4

סייבר התקפי וניתוח חולשות

מיקוד: אנליסט סייבר | מפגשים 25-32 | 32 שעות

נקודת המפנה בתוכנית - המעבר מתפיסת "מיישם ומגן" למחשבת "תוקף ומגן". מודול זה מלמד את התלמידים לחשוב כאויב כדי להגן טוב יותר. באימוץ פרספקטיבה התקפית, תלמידים מפתחים הבנה עמוקה יותר של נקודות התורפה במערכות שהם יידרשו להגן עליהן.

המודול מכסה את מלוא מחזור החיים של תקיפה - מאיסוף מודיעין ראשוני, דרך סריקות רשת וזיהוי חולשות, ועד לניצול מעשי של פרצות אבטחה. תלמידים עובדים בסביבות מבוקרות ואתיות, רוכשים מיומנויות שהם חיוניות הן לעבודת בוחני חדירות והן לאנליסטי SOC שצריכים להבין את דרכי החשיבה של התוקפים.

1

מחזור התקיפה (Cyber Kill Chain)

אימוץ חשיבה של תוקף כדי לשפר את ההגנה. Recon, Weaponization, Delivery, Exploitation. מעבדה: Cyber School – תרחיש תקיפה מלא שלב אחר שלב.

2

איסוף מודיעין (OSINT)

איתור נכסים חשופים במרחב הציבורי. Google Dorking, Shodan, Whois, Metadata. מעבדה: Cyber School – אתגר OSINT.

3

סריקת רשתות ופורטים (Nmap)

מיפוי שירותים ופורטים פתוחים ברשת היעד. Scanning techniques, Service detection, NSE Scripts. מעבדה: Cyber School – סריקת רשת מורכבת.

4

סריקת חולשות תשתיות

ביצוע סריקות אוטומטיות וניתוח דוחות. Nessus, OpenVAS, CVSS Scoring. מעבדה: Cyber School – הרצת סריקת Nessus וניתוח תוצאות.

5

עקרונות ה-Exploitation

הבנת שלב הפריצה המעשי. Metasploit Framework, Payloads, Reverse Shells. מעבדה: Cyber School – ניצול חולשות Windows/Linux.

6

פגיעויות אפליקטיביות (Web Security)

זיהוי פרצות באתרים ואפליקציות ווב. OWASP Top 10, SQLi, XSS. מעבדה: פריצה לאתר פגיע בסביבת מעבדה.

7

הנדסה חברתית

הבנת וקטורי תקיפה מבוססי הגורם האנושי. Phishing, Pretexting, SET. מעבדה: Cyber School – הקמת קמפיין פישינג מבוקר.

8

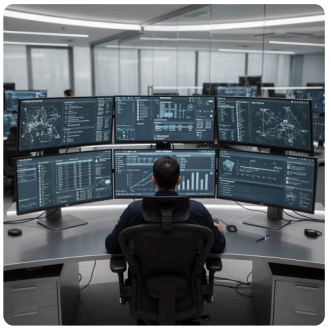
פיצוח סיסמאות ו-Hashes

הבנת חולשת מנגנוני הצפנה וסיסמאות. Brute Force, Dictionary Attack, Hashcat. מעבדה: Cyber School – פיצוח Hash של סיסמאות.

מודול 5

ניטור, SOC ותגובה לאירועים

מיקוד: אנליסט סייבר | מפגשים 33-40 | 32 שעות



המודול הסופי והמשמעותי ביותר - הכניסה לעולם המבצעי של מרכזי הגנת הסייבר (SOC). כאן התלמידים רוכשים את המיומנויות היומיומיות של אנליסטי סייבר מקצועיים: ניטור לוגים, זיהוי אנומליות, ניהול אירועים ותגובה מהירה לאיומים.

המודול משלב למידה תיאורטית של מתודולוגיות תגובה לאירועים עם תרגול מעשי אינטנסיבי במערכות SIEM מובילות כמו Splunk. התלמידים לומדים לבנות דאשבורדים, להגדיר התראות חכמות ולבצע חקירות פורנזיות בסיסיות. שיא התוכנית הוא פרויקט Capstone בן שני חלקים המדמה תרחיש מציאותי מלא.

מבוא לעולם ה-SOC

הכרת סביבת העבודה של אנליסט הסייבר. SOC Layers (L1-L3), Ticketing Systems, SLA. מעבדה: Cyber School – תרגול ניהול אירוע בכלי Ticketing.

מערכות SIEM (Splunk Basics)

יכולת חיפוש וניתוח לוגים בזמן אמת. Log collection, Splunk Search Processing Language (SPL). מעבדה: Cyber School – ניתוח אירוע ב-Splunk.

ניטור התראות ודאשבורדים

יצירת כלי בקרה ויזואליים לאיתור איומים. Alerting logic, Trends, Dashboards. מעבדה: Cyber School – יצירת Alert על סריקת רשת חריגה.

תגובה לאירועים (Incident Response)

שליטה במתודולוגיית התגובה לבלימת אירוע. NIST IR Lifecycle: Containment, Eradication, Recovery. תרגול: סימולציית IR לרנסומוור (Tabletop).

פורנזיקה דיגיטלית בסיסית

איסוף וחקירת ראיות ממערכות מחשב. Memory Forensics, RAM Dumping, File recovery. מעבדה: Cyber School – ניתוח Dump של זיכרון.

פרויקט Capstone – חלק א'

יישום מיומנויות ה"מיישם" להקמת ארגון מאובטח. Hardening, Firewalling, IAM Setup. מעבדה: בניית תשתית מאובטחת בזירת הסייבר.

פרויקט Capstone – חלק ב'

התמודדות עם מתקפה חיה כאנליסט סייבר. Real-time monitoring, Detection, Containment. מעבדה: זיהוי ובלימת מתקפה חיה על הארגון שהוקם.

סיכום והכנה ל-CC

הכנה סופית למבחן ההסמכה והצגת תוצרים. ISC2 CC Domains review, Exam strategies. סימולציה: מבחן דמה מלא ISC2 CC.

פרויקט Capstone - המבחן האמיתי: הפרויקט המסכם מדמה תרחיש מציאותי מלא: תחילה בניית ארגון מאובטח מהיסוד, ולאחר מכן התמודדות עם מתקפה מורכבת בזמן אמת. זהו המבחן האולטימטיבי ליכולות שנרכשו לאורך התוכנית.

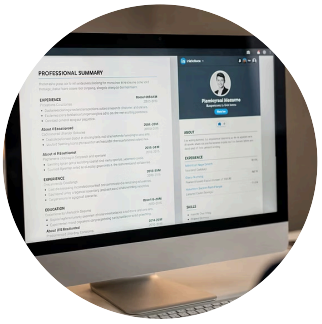
חבילת מעטפת תעסוקתית

תוכנית CSRP אינה מסתיימת בהשלמת 160 שעות הלימוד. ההשקעה האמיתית בהצלחת התלמידים ממשיכה דרך חבילת מעטפת תעסוקתית מקיפה המלווה את הבוגרים עד להשמה מוצלחת בשוק התעסוקה. זהו "הגשר האמיתי" שהופך הכשרה טכנית למסלול קריירה מוצלח.

החבילה כוללת הכנה להסמכות בינלאומיות מובילות, פיתוח מיומנויות רכות והשמה אקטיבית באמצעות רשת הקשרים הנרחבת של BDO וסייבר סקול. כל בוגר מקבל ליווי אישי המותאם לפרופיל המקצועי שלו ולשאיפות הקריירה האישיות.

מרכז הסמכות

קורסי הכנה מקיפים למבחנים בינלאומיים מובילים: **ISC2 CC** | **LPI Linux** | ו-**Python PCAP** . ההכנה כוללת מבחני דמה, חומרי לימוד ייעודיים וליווי עד להצלחה.



סדנאות קריירה

פיתוח מיומנויות השמה מקצועיות: כתיבת קורות חיים, אופטימיזציית פרופיל Linkedln, וסימולציות ראיונות עבודה טכניים עם מנהלי גיוס מהתעשייה.

ליווי השמה

גישה בלעדית לרשת הקשרים הנרחבת של BDO זיו האפט וסייבר סקול. חיבור ישיר למעסיקים מובילים בתעשייה, הכרות עם מנהלי גיוס, והמלצות מקצועיות.

160

שעות אקדמיות

תוכנית מקיפה המשלבת תיאוריה ותרגול

40

מפגשים

מפגשי למידה אינטנסיביים של 4 שעות כל אחד

3

הסמכות בינלאומיות

ISC2 CC, LPI Linux, Python PCAP

"תוכנית CSRP מייצגת את העתיד של הכשרה מקצועית בסייבר - שילוב מושלם של מצוינות טכנית, ניסיון תעשייתי ותמיכה תעסוקתית מלאה. אנו משקיעים בהצלחה ארוכת הטווח של כל תלמיד."

הירשם עכשיו לתוכנית CSRP

הורד את הסילבוס המלא