BDO

שירות התעסוקה

קורס מיישם הגנה בסייבר

BDO

קורס מיישם הגנה בסייבר

כללי

קורס מיישם הגנה בסייבר (CSRP – Cyber Security Responder & Practitioner) הינו קורס הכשרה מקצועי מקיף שנועד להקנות למשתתפים ידע מעשי, כלים טכנולוגיים ומיומנויות יישומיות הנדרשות להשתלבות בתפקידי סייבר יישומיים וניתוחיים. הקורס משלב לימוד עיוני מעמיק עם תרגולHands-On בסביבת מעבדות ייעודית (cyber school), עבודה מבוססת תרחישים וסימולציות המדמות מצבי אמת מארגונים, תוך חיבור ישיר בין ידע תשתיתי, טכנולוגיות הגנה, חשיבה התקפית, ניטור ותגובה לאירועי סייבר.

מבנה ההכשרה מאפשר העמקה הדרגתית, פיתוח חשיבה מקצועית וחיזוק יכולות יישומיות, ומסתיים בפרויקט Capstone מסכם המדמה פעילות סייבר מלאה בארגון, כהכנה להשתלבות בעולם העבודה ולבחינות ההסמכה הרלוונטיות.

קהל היעד

הקורס מיועד לדורשי עבודה בעלי אוריינטציה טכנולוגית המעוניינים להשתלב בתחום הסייבר, למועמדים המבקשים לבצע הסבה מקצועית לעולמות אבטחת המידע, וכן לבוגרי מסלולים טכנולוגיים, אקדמאים בתחומי מדעי המחשב, הנדסה או מערכות מידע, ואנשי IT בתחילת דרכם המעוניינים להעמיק ידע מקצועי ולרכוש מיומנויות יישומיות לתפקידי מיישם הגנה, SOC ואנליסט סייבר.
וניהול תפעולי בארגונים.

היקף הקורס

40 מפגשים | 160 שעות אקדמיות

קורס מיישם הגנה בסייבר

ליווי פדגוגי, מעקב התקדמות המשתתפים והבטחת איכות

במהלך הקורס יתקיים ליווי פדגוגי שוטף שמטרתו מעקב אחר התקדמות המשתתפים, חיזוק תהליכי למידה והבטחת איכות ההכשרה. הליווי יתבצע באופן שבועי – מעקב אחר ציוני המעבדה והנוכחות.

יתבצע דיווח מובנה על כל משתתף שיכלול התייחסות לנוכחות, השתתפות פעילה, ביצוע תרגולים, הבנה מקצועית והתקדמות אישית.
בנוסף, יבוצעו סקרי שביעות רצון וחוויית משתתף במהלך הקורס ובסיומו, לצורך בחינת איכות ההדרכה, רלוונטיות התכנים והפקת לקחים לשיפור מתמיד.

במהלך ההכשרה המשתתפים יקבלו:
גישה ל-LMS: פורטל למידה הכולל חומרי לימוד, הקלטות ומבחני תרגול.
מעבדות ענן: גישה 24/7 לזירת Cyber Schoolלתרגול חופשי.
העשרה: קורסי דיגיטליים ללימוד עצמי במגוון תחומים כגון בניית קורות חיים, הכנה למבחני הסמכה ועוד. כלמידה עצמית אופציונלית ולא חובה.

קורס מיישם הגנה בסייבר

עיקרי הקורס

חלק 1 – יסודות הסייבר, רשתות ומערכות הפעלה (32 שעות)
מבוא לעולם הסייבר ותפקיד המגן הארגוני, הבנת מודל ה-CIA ניהול סיכונים ואיומים מתקדמים. לימוד מעמיק של רשתות ופרוטוקולי תקשורת, שירותי ליבה ארגוניים, ניהול מערכות Windows Server ו-Linux , הקשחת מערכות וניהול זהויות בסביבת Active Directory.

חלק 2 – טכנולוגיות הגנה וכלי סייבר (48 שעות)
תכנון והטמעה של מערכי הגנה רב־שכבתיים (Defense in Depth), חומות אש, VPN, מערכות IDS/IPS, ניהול זהויות והרשאות(IAM, MFA) הגנת מידע(DLP), אבטחת תחנות קצה(EDR) , אבטחת דואר וגלישה, רגולציה ותקני אבטחת מידע, ויישום אבטחה בסביבות ענן.

חלק 3 – בינה מלאכותית(AI) בעולם הסייבר (16 שעות)
שילוב טכנולוגיות AI ו-Machine Learning באבטחת מידע, זיהוי אנומליות ואיומים, היכרות עם איומי AI מתקדמים (Adversarial AI , Deepfakes) והגנה על מודלי בינה מלאכותית בסביבות ארגוניות.

חלק 4 – סייבר התקפי וניתוח חולשות (32 שעות)
פיתוח חשיבה התקפית לצורך חיזוק ההגנה: מחזור חיי תקיפה(Cyber Kill Chain), איסוף מודיעין(OSINT), סריקות רשת וחולשות, Exploitation, פגיעויות אפליקטיביות(Web Security) , הנדסה חברתית ופיצוח סיסמאות בסביבות מבוקרות ואתיות.

חלק 5 – ניטור, SOC ותגובה לאירועים (32 שעות)
היכרות עם עבודת SOC, מערכות SIEM (Splunk), ניתוח לוגים, ניטור והתראות, תגובה לאירועי סייבר((Incident Response פורנזיקה דיגיטלית בסיסית, וניהול אירועים מקצה לקצה. החלק כולל פרויקט Capstone מסכם המדמה תרחיש סייבר ארגוני מלא. חישים ואתגרי אספקה, ולבסוף פרויקט מסכם יישומי המחבר בין כלל נושאי הקורס.

מרצי הקורס

עומרי סגרון

מנהל הטכנולוגיות (CTO) של חטיבת ייעוץ הסייבר ב- BDO ומייסד Cyber School

מוסמך CISSP ומדריך מוסמך של ארגון ISC2.
בעל ניסיון של כ-18 שנים בהובלה, פיתוח והדרכת תוכניות סייבר מתקדמות בישראל ובעולם. יוצא יחידות טכנולוגיות מובחרות (ממר"ם), בעל ידע מעמיק בעולמות ההגנה הארגונית, ניהול סיכונים, אבטחת תשתיות והכשרת כוח אדם מקצועי לתפקידי סייבר מתקדמים.

אסף ששון

ארכיטקט אבטחת מידע בכיר

מרצה באקדמיה, בעל ניסיון מקצועי רחב בתכנון והטמעת פתרונות אבטחת מידע בארגונים מורכבים. מומחה בתשתיות תקשורת, אבטחת ענן (AWS, Azure) ואבטחה התקפית, עם ניסיון רב בהכשרת והובלת הדור הבא של אנשי ולוחמי הסייבר במסגרת צה"ל ותוכניות הכשרה ייעודיות.

אלכס טימוכוב

יועץ סייבר ב- BDO

מרצה מוסמך המתמחה בפיתוח תוכן טכנולוגי, אוטומציית אבטחה ופיתוח ב-Python. בעל ניסיון בליווי ארגונים בביצוע סקרי סיכונים, הטמעת תהליכי אבטחה והעברת הדרכות מתקדמות לקראת הסמכות סייבר בינלאומיות, תוך שילוב ידע טכנולוגי מעשי עם אוריינטציה פדגוגית יישומית.

קורס מיישם הגנה בסייבר

מפגש 1: מבוא לסייבר ומשולש ה-CIA

הבנת תפקיד המגן הארגוני והכרת וקטורי התקיפה המודרניים. סודיות, שלמות, זמינות (CIA), ניהול סיכונים ואיומי APT .

מעבדה: היכרות עם Cyber School ואתגר CTF ראשון.

מפגש 2: מודל ה-OSI ושכבות הרשת

שליטה במודל שבע השכבות ובפרוטוקולי הקצה.

מעבדה: ניתוח פקטות ושכבת קו הנתונים – Wireshark.

מפגש 3: פרוטוקולי תקשורת TCP/IP

הבנת מנגנוני הניתוב והעברת המידע ברשת. IP Addressing , Subnetting , Routing

מעבדה: הגדרת רשתות וניתוב בנתבים וירטואליים – Cyber School.

מפגש 4: שירותי ליבה ותורפות (DNS/DHCP)

איתור תורפות בפרוטוקולי השירות הארגוניים.

מעבדה: ניתוח אנומליות תעבורה.

מפגש 5: ניהול מערכות Windows Server

הכולת ניהול משתמשים והרשאות בשרתים ארגוניים.

מעבדה: הקשחת Windows Server 2022.

מפגש 6: Active Directory וניהול זהויות

הבנת מבנה ה- Domain וניהול מרכזי של מדיניות אבטחה.

מעבדה: הקמת דומיין וניהול GPO.

מפגש 7: יסודות לינוקס (Linux CLI)

שליטה מלאה בשורת הפקודה (Terminal) לניהול שרתים.

מעבדה: Linux CLI Master Challenge.

קורס מיישם הגנה בסייבר

מפגש 8: הרשאות והקשחה בלינוקס

הגנה על שרתי קוד פתוח וניהול גישה מתקדם.
מעבדה: Privilege Escalation Defense.

מפגש 9: ארכיטקטורת Firewalls

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

מפגש 10: ניהול תעבורה – NAT

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

מפגש 11: פתרונות VPN ארגוניים

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

מפגש 12: מערכות IDS/IPS

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

מפגש 13: ניהול זהויות (IAM)

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

מפגש 14: הזדהות חזקה (MFA)

מניעת גניבת חשבונות דרך הטמעת שכבות הגנה. FIDO2, OTP.

מפגש 15: הגנת מידע (DLP)

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

קורס מיישם הגנה בסייבר

מפגש 16: אבטחת נקודות קצה (EDR)

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

מפגש 17: אבטחת שרתי דואר

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

מפגש 18: אבטחת גלישה (Web Proxy)

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

מפגש 19: רגולציה ותקנים

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

מפגש 20: יסודות אבטחת ענן

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

מפגש 21: בינה לאוטומציה של אבטחה

שימושי AI לייעול מערכות אבטחה, Security Automation, שילוב AI-וPython.

מפגש 22: זיהוי אנומליות באמצעות ML

Behavior Analysis , UEBA , ML Models, זיהוי חריגות בסביבות ארגוניות.

מפגש 23: איומי AI-Adversarial ML

Deepfakes , Adversarial Phishing, התקפות הסוואה על מודלים.

מפגש 24: הגנה על מודלי AI

Prompt Injection , Jailbreaking , LLM Security מנגנוני הגנה מתקדמים.

קורס מיישם הגנה בסייבר

מפגש 25: מחזור התקיפה (Cyber Kill Chain)

היכרות עם שלבי תקיפה מלאים – מאיסוף מידע ראשוני ועד לניצול בפועל. הבנת דרך החשיבה של תוקפים לצורך חיזוק מערכי ההגנה הארגוניים. תרגול תרחיש תקיפה מלא בסביבה מבוקרת.

מפגש 26: איסוף מודיעין (OSINT)

זיהוי נכסים חשופים של ארגונים באמצעות מידע פומבי, חיפוש מתקדם ברשת, ניתוח מטא־דאטה ואיתור נקודות תורפה ראשוניות. תרגול מעשי בסביבת מעבדה.

מפגש 27: סריקת רשתות ופורטים (Nmap)

מיפוי רשתות ארגוניות, זיהוי שירותים פעילים ופורטים פתוחים, והבנת המשמעויות האבטחתיות של ממצאי הסריקה. תרגול סריקות רשת מורכבות.

מפגש 28: סריקות חולשות תשתיות

ביצוע סריקות אוטומטיות לאיתור חולשות בתשתיות, ניתוח דוחות סריקה והבנת רמת הסיכון של כל ממצא לצורך תיעדוף טיפול.

מפגש 29: Exploitation - עקרונות

היכרות עם שלב הפריצה המעשי, הבנת אופן ניצול חולשות במערכות הפעלה, והקשר בין חולשה טכנית להשפעה ארגונית. תרגול מבוקר בסביבה ייעודית.

מפגש 30: פגיעויות אפליקטיביות (Web Security)

זיהוי חולשות נפוצות באתרים ובאפליקציות, הבנת דרכי תקיפה מקובלות והשלכות אבטחת מידע על מערכות ווב. תרגול פריצה לאתר פגיע בסביבת מעבדה.

מפגש 31: הנדסה חברתית

הבנת תקיפות המבוססות על הגורם האנושי, זיהוי שיטות נפוצות להטעיה והשפעה, ותרגול בניית תרחיש פישינג מבוקר לצורכי הגנה.

קורס מיישם הגנה בסייבר

מפגש 32: Hashes - פיצוח סיסמאות

הבנת חולשות במנגנוני אימות וסיסמאות, שיטות נפוצות לפיצוח סיסמאות והשלכות אבטחתיות של ניהול סיסמאות לא תקין. תרגול מעשי בסביבה מבוקרת.

מפגש 33: מבוא לעולם ה-SOC

היכרות עם מרכזי ניטור ובקרה(SOC) , תפקידי צוותי SOC, שכבות עבודה (רמה 1–3), ותהליכי טיפול באירועי סייבר בארגון. הבנת מחזור חיי אירוע אבטחת מידע.

מפגש 34: מערכות ניהול אירועים ולוגים

היכרות עם מערכות לניהול וריכוז לוגים, איסוף מידע ממקורות שונים בארגון וניתוח נתונים לצורך זיהוי אירועים חריגים. תרגול עבודה בסביבת ניטור ייעודית.

מפגש 35: ניטור התראות ודשבורדים

בניית התראות, ניתוח מגמות, עבודה עם לוחות בקרה והבנת הקשר בין אירועים בודדים לאירועי אבטחה מורכבים. תרגול ניתוח אירועים בזמן אמת.

מפגש 36: תגובה לאירועי סייבר

תהליכי תגובה לאירועי אבטחת מידע: הכלה, טיפול, התאוששות והפקת לקחים. סימולציות תרחישים ותרגול קבלת החלטות בזמן אירוע.

מפגש 37: פורנזיקה דיגיטלית בסיסית

היכרות עם עקרונות חקירה דיגיטלית, איסוף ראיות ממערכות מחשוב, ניתוח מידע מזיכרון ומדיסקים לצורך הבנת מקור האירוע והיקפו.

מפגש 38: פרויקט מסכם – שלב א'

תכנון והקמה של סביבה ארגונית מאובטחת, יישום בקרות אבטחה, הקשחת מערכות והגדרת מנגנוני ניטור.

קורס מיישם הגנה בסייבר

מפגש 39: פרויקט מסכם – שלב ב'

ניתוח תרחיש תקיפה בסביבה המדמה ארגון אמיתי, זיהוי אירועים, תגובה מבצעית ותיעוד תהליך הטיפול באירוע.

מפגש 40: סיכום והכנה להסמכה

סיכום תכני הקורס, חזרה על נושאים מרכזיים, חיזוק מוכנות מקצועית והכנה לקראת בחינת ההסמכה הרלוונטית (אין חובה לגשת, תלוי במשתתף).

*אורך המפגשים והתכנים ניתנים לשינוי בהתאם לצורך