קורס אבטחת מידע והגנת סייבר - ICSOC AI CONCEPT

תעודות גמר:

✓ הכנה למבחני ההסמכה הבינלאומיים:
CEH | Lpi Essential | Lpi1
PCEP | CNSS | CSA

ראש תחום מקצועי:
סהר אביטן

ICS
המרכז הארצי ללימודים

רקע על ראש התחום:

סהר אביטן- חוקר בכיר ובעלים של חברת Kayran (כלי תקיפה אוטומטי לעולמות הweb), מרצה ברחבי הארץ ובעולם, הינו בודק חוסן אפליקטיבי ותשתיתי ומתכנת יותר מעשות- אשר בהן מצא מספר רב של ליקויי אבטחה בחברות כמו:

וואטסאפ, בזק, חברת חשמל, הממשלה, הטכניון ועוד..

סהר מחזיק בהסמכות OSWE, PCEP, PCAP ועוד.

כללי

בעידן שבו הטכנולוגיה מתפתחת בקצב חסר תקדים, איומי הסייבר הולכים ונעשים מתוחכמים יותר והצורך באנשי אבטחת מידע איכותיים גובר.החלק החשוב ביותר בתחום אבטחת המידע הוא הבנת התשתית, זיהוי פגיעויות ופערי אבטחת מידע, בניית תהליכים ארגוניים והחשוב ביותר הוא יכולת התגובה לאירוע. מטרתו של אנליסט הסייבר הוא להגן על הארגון מפני איומים פנימיים וחיצוניים העלולים לשבש את פעילותו התקינה של הארגון ולגרום לו להפסדים ופגיעה במוניטין. לשם כך, איש הגנת סייבר איכותי הינו בעל ידע ברשתות, מערכות הפעלה מסוגים שונים, היכרות עם כלי תקיפה והגנה ועבודה עם מתודולוגיות, שיטות עבודה וכלים רבים בתחום. בשנים האחרונות נכנס לעולם הסייבר תחום הבינה המלאכותית (AI) בקורס זה נלמד כיצד להשתמש בטכנולוגיות אלו על מנת לשפר את מהירות התגובה לאירוע סייבר. מי שלא יכיר את הסיכונים הרבים בעולם הדיגיטלי, עלול למצוא את עצמו פגיע ולכן מחובתנו להנגיש ידע זה לקהל התלמידים ולהפוך אותם לאנשי סייבר מתוחכמים.

יעדי ההכשרה:

- ✓ הקניית כלים, טכניקות עבודה וניסיון מעשי הנדרשים להשתלבות בתפקידי תמיכה טכנית והגנת סייבר SOC.
- ✓ רכישת ידע נרחב בתחומי הגנת סייבר: עבודה עם מערכות ניטור ובקרה, היכרות עם התקפות, עבודה עם מערכות הפעלה שונות וסביבת הענן.
- ✓ היכרות עם עולם הסייבר, יכולות אוטומציה, בדגש על טכנולוגיות AI.
- ✓ שימוש בכלים מתקדמים לזיהוי התקפות ובניית יכולות תגובה לאירוע סייבר.

קהל יעד:

הקורס מיועד לאנשים ללא רקע בתחום ההייטק, לבעלי רקע בסיסי במחשבים ולאנשי IT, המבקשים להשתלב בתחום אבטחת המידע והסייבר או לעבור הסבה מקצועית לתחום זה.

פרויקט התמחות:

הקורס כולל תרגולים, פרויקט אמצע ופרויקט מסכם כמו כן לאורך הקורס יבוצעו מספר מבחנים בהתאם לכל מודול.

טבלאות שכר Cyber/אבטחת מידע

Cyber / אבטחת מידע					
תחום		דרג ניהולי	3-5 שנים	1-2 שנים	0-1 שנים
Malware analyst	◀	₪ 26-32	₪ 22-27	₪ 18-23	₪ 13-19
SOC/SIEM	◀	₪ 21-26	₪ 17-21	₪ 14-16	₪ 11-13
מומחה אבטחת מידע	◀	₪ 28-32	₪ 21-27	₪ 17-20	₪ 14-16
Reverse Engineer	◀	₪ 32-38	₪ 29-37	₪ 25-29	₪ 22-26
למשרות דרושים הייטק בתחום Cyber / אבטחת מידע ◀					

עפ"י נתוני חברות השמה בתחום הייטק

מה לומדים?

קורס SOC משולב טכנולוגיות AI

מודול 1 - תקשורת מחשבים

- מהי תקשורת מחשבים?
- מודל ה-OSI ו-TCP/IP
- מהי כתובת IP
- לימוד IPv4
- לימוד IPv6
- מה זה Unicast & Broadcast
- פרוטוקולים
- ההבדל בין TCP ל-UDP
- איך עושים Routing
- איך משתמשים ב-Wireshark

מודול 2 - מבוא לתשתית ענן

- מהי תשתית ענן
- מה ההבדלים בין תשתית ענן לתשתית מקומית
- מודולים: Public/Private/Hybrid/Multi-Cloud
- סוגי תשתי: IaaS/SaaS/PaaS
- היכרות עם Azure
- מה זה Office365 וניהול משתמשים
- כיצד מאבטחים תשתית ענן

מודול 3 - מערכות הפעלה

עבודה עם Windows

- מה זה Windows
- משתמשים בWindows
- עבודה עם CMD
- עבודה עם PowerShell
- סוגי קבצים
- מה זה Windows Server
- איך מתקינים שרת
- מה זה דומיין ואיך מקימים אחד?
- התקנת Domain Controller
- התקנת Active Directory והסבר מקיף
- חיבור מחשב לדומיין
- משתמשים קבוצות ומחשבים
- מה זה OU ולמה הוא נועד.

עבודה עם Linux

- מה זה OpenSource
- הפצות בלינוקס
- הכרת ה-CLI
- מערכת קבצים
- עבודה עם קבצים
- לימוד WildCard & Globing
- Grep
- STDIO (STDOUT, STDIN, STDERR)
- מה זה Pipe
- עבודה עם טקסט
- רגקס
- חיפוש קבצים
- Linux Networking
- משתמשים וקבוצות

מודול 4 - פייתון

- הקמת סביבת עבודה ולימוד IDE
- עבודה עם משתנים
- מחרוזות
- תנאים
- רשימות
- לולאות
- מילון ולולאות
- ספריות ושגיאות
- פונקציות
- עבודה עם קבצים
- תכנות מונחה עצמים (OOP)
- בקשות
- רגקס

מודול 5 –
הגנת סייבר - (Soc Analyst) :

- מהו מרכז הבקרה (SOC)
- מה זה EDR
- מודיעין סייבר ואיסוף מידע מקדים
- מה זה Wazuh
- התקנת Wazuh וההגדרות של המערכת
- מה זה חוקים
- מה זה לוגים
- כתיבת חוקים
- תחקור אירועים (Malware / Ddos / Ransomware)

מודול 6 - סייבר התקפי:

- מבוא להתקפות ומבדקי חוסן
- מאפייני התוקף
- מהן השלבים בהתקפה נכונה
- מהו BugBounty
- דיוג, הנדסה חברתית ותהחזות
- עבודה עם WireShark וניתוח רשת
- Whois & DNS Enumeration
- NMAP וסריקת פורטים
- MetaSploit
- Responder
- Session Hijacking

מודול 7 - התקפה אפליקטיבית:

- לימוד HTML - בסיס
- לימוד JS - בסיס
- לימוד על XAMPP
- לימוד PHP - בסיס
- לימוד SQL - בסיס
- עבודה עם Burpsuite ולימוד מקיף עם התוכנה
- מציאת וחקירת חולשות : XSS, SQLI, CSRF, XXE, LFI, RFI, RCE
- מודל ה- OWASP TOP 10

מודול 8 - התקפה תשתיתית:

- סריקה אקטיבית ופסיבית
- עבודה עם NMAP
- ביצוע DNS Enumeration
- מה זה Metasploit FrameWork ותחילת עבודה מקיפה
- תקיפת מכונות Windows 7/10/2019
- ניצול אקספלויטים
- בניית סוס טרויאני ואיך הוא עובד מאחורי הקלעים
- לימוד להסמכת CEH.

מודול 9 - הכנה לעבודה:

- כיצד נראה דוח של בדיקות חוסן
- איסוף ממצאים, כתיבת דוח ומעקב ביצוע
- סדנת הכנה לראיונות עבודה (כללי עשה ואל תעשה)
- הכנה מנטלית לקראת הרעיון
- שאלות אישיות ורעיונות עומק
- סימולציה של ראיון פרונטלי אחד על אחד
- שימוש בכלי AI לחיפוש משרות

למען הסר ספק , מובהר כי המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכניות הלימודים , היקף שעות הלימוד, סגל המדריכים, ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

קורס מסתיים במעבר בהצלחה על המבחן המסכם,
הגשת כל הפרויקטים ואחוז נוכחות בשיעורים > 85%

הגשה למבחנים חיצוניים כרוכה בעלות של אגרת בחינה
ותשולם ישירות למעבירי הבחינה החיצונית
בחינה פנימית במכללה וקבלת תעודה מהמכללה – ללא עלות

דוגמאות לתעודות גמר בסיום הקורס: