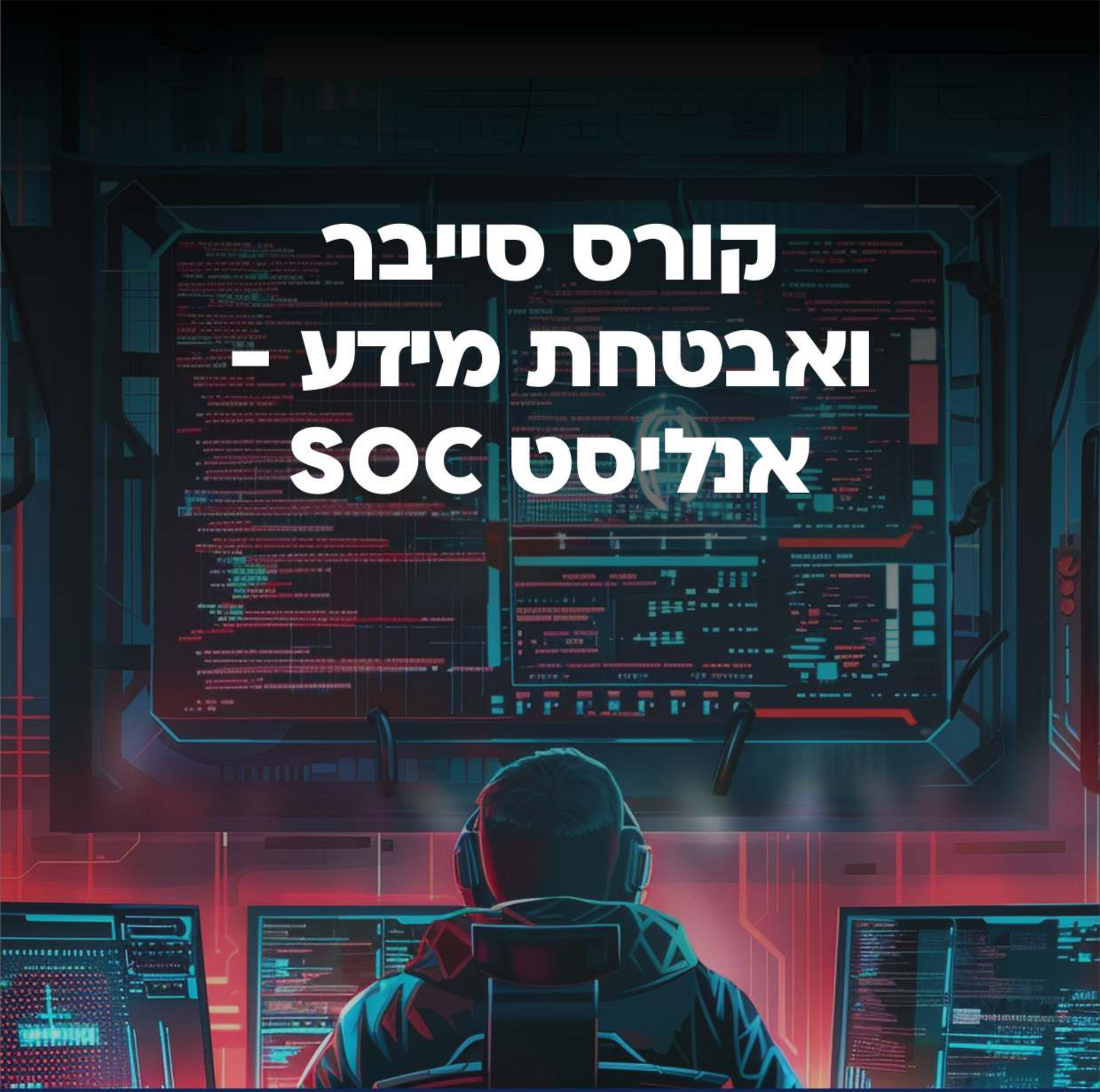


קורס סייבר ואבטחת מידע - אנליסט SOC

הקורס מכין למבחני ההסכמה הבינלאומיים הבאים

Linux Professional Institute - Linux Essentials
CompTIA - Cybersecurity Analyst (CySA+)
EC-Council - Certified SOC Analyst (CSA)

האקדמיה להייטק
Hybrid College For Life

רקע על סגל ההוראה

מרצי הקורס יהיו אליסף גליס ובן דאלל. אליסף הוא מומחה סייבר ויועץ אבטחת מידע לחברות ופרויקטים במשרד הביטחון, ששירת בחיל התקשוב וביחידה הטכנולוגית המיוחדת של חיל המודיעין כחוקר בכיר ומנהל צוותי סייבר. אליו יצטרף בן שכיום מכהן כמנהל צוות אנליסטים ומודיעין בחברת Citadel ובעברו עסק בתחומים רבים בעולמות הסייבר וכמרצה בכיר בתחום ההאקינג.

כללי

תחומי הסייבר ואבטחת המידע מתרחבים בכל יום וזאת בשל האיומים ההולכים וגוברים.
אחד המקצועות שצמחו מתוך הצורך הוא אנליסט אבטחת מידע וסייבר.

תפקידים פוטנציאליים

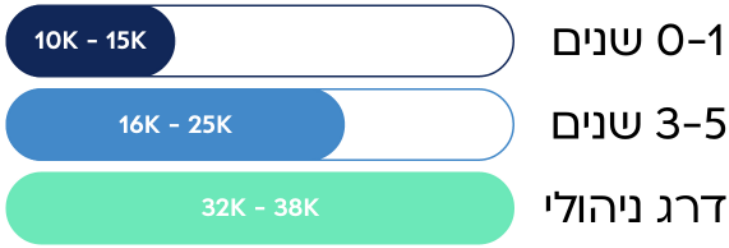
הקורס מכוון למספר תפקידים וביניהם: אנליסט סייבר, איש צוות SOC או NOC, אנשי רשתות ואדמיניסטרציה, ועוד.

מה הידע המדרש מאנליסט סייבר

דרישות התפקיד כוללות היכרות עם מערכות הפעלה, מערכות תקשורת, ידע באבטחת מידע ותקיפה, תשתיות וסקריפטינג.

שכר בתחום

שכר ממוצע לתפקיד אנליסט אבטחת מידע על פי טבלאות שכר המפורסמות ברשת



תפקידו של אנליסט סייבר

מרכז ניתוח האבטחה בארגון (SOC – Security Operating Center) זהו מרכז הניטור והבקרה של אבטחת המידע בארגון. בדרך כלל מרכז זה פועל במתכונת רציפה במשך כל שעות היממה ובכל ימות השנה במטרה לספק הגנה בלתי פוסקת לנכסי המידע של הארגון. במרכז זה פועלים כל בעלי התפקידים בתחום אבטחת המידע בארגון כולל האנליסטים שלו.

תפקידו של אנליסט אבטחת מידע מתמקד בהגנה על המידע הארגוני מפני סיכונים החורבים לו מחוץ לארגון. ניתוח אבטחת הרשת הפנימית בארגון ובדיקת חריגות של מחלקה מסוימת או של הארגון כולו.

הכנה להסמכות בינלאומיות

Linux Professional Institute - Linux Essentials
CompTIA - Cybersecurity Analyst (CySA+)
EC-Council - Certified SOC Analyst (CSA)

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.

דרישות סף

נדרשת יכולת קריאת טקסט באנגלית ברמה סבירה. רצוי אך לא חובה ידע קודם במחשבים.

מה לומדים?

קורס סייבר ואבטחת מידע

מודול 1 - מבוא לסייבר

- מבוא לעולם הסייבר + סקירת טרנדים
- תפקידים וצוותים
- סוגי תוקפים ואינטרסים
- סוגי נוזקות ופוגענים
- מכונת פון נוימן
- חומרה, תוכנה וקושחה
- מערכות האתחול וה- BIOS
- הבסיס הבינארי
- הבסיס ההקסדצימלי
- תהליכים, קבצים, שירותים ופעולות

מודול 2 - יסודות התקשורת

- רשתות תקשורת מסוג IT + קינפוג הגדרות
- ארכיטקטורה, טופולוגיה וסגמנטציה
- מוצרי ורכיבי תקשורת
- כתובות תקשרות, IP וסאבנטינג
- מודל OSI ו- TCP/IP
- אנקפסולציה ומולטיפלקסינג
- פרוטוקולי תקשורת פופולרים
- פקודות תקשורת ב- CMD
- הצפנות
- עבודה עם Wireshark וכלים נוספים

מודול 3 - Windows

- עקרונות מערכת ההפעלה וה- Kernel
- וירטואליזציה ו- Hypervisor
- תהליך האתחול ומערכת הקבצים
- עבודה עם Registry, Logs, Scheduler ועוד
- ממשקי הפקודה CMD ו- PowerShell
- סוגי קבצים ו- Executables
- אבטחה וניהול הרשאות
- היכרות עם מעגלי ההגנה ומוצרי Built-In
- הכרת סביבת Domain ו- AD Objects
- פרוטוקולי אימות Kerberos ו- NTLM

מודול 4 - Linux

- עקרונות מערכת ההפעלה וה- Kernel
- היכרות עם מערכת הקבצים
- היכרות עם Open Source ו- Git
- פקודות Shell שונות
- קבצים מיוחדים
- ניתוח לוגים
- עבודה עם cron, deamon ואלמנטים נוספים
- הרשאות משתמשים וקבצים
- ניתוח טקסטים ו- regex
- היכרות עם package manager
- שירותי תקשורת

מודול 5 - פורמיקה

- מבוא לחקירות סייבר
- חקירה סטטית ודינאמית
- מנגנוני reputation וסנדבוקסים
- הקמת סביבת חקירה
- חקירת תקשורות
- חקירת קבצים ומטאדאטה
- חקירת מערכת הפעלה ומערכת קבצים
- חקירת תהליכים וזיכרון
- חקירת נתונים מוחבאים
- סקירת מוצרי הגנה ומתודולוגיות

מודול 6 - האקינג

- היכרות עם MITRE Attack
- סריקות ו- reconnaissance
- עבודה עם Metasploit
- ביצוע Privilege Escalation
- ביצוע Post-Exploitation
- התקפות פישינג
- ביצוע Brute Force
- היכרות עם התקפות web
- התקפות דומיין ושתית
- דוחות חקירה / דוחות התקפה