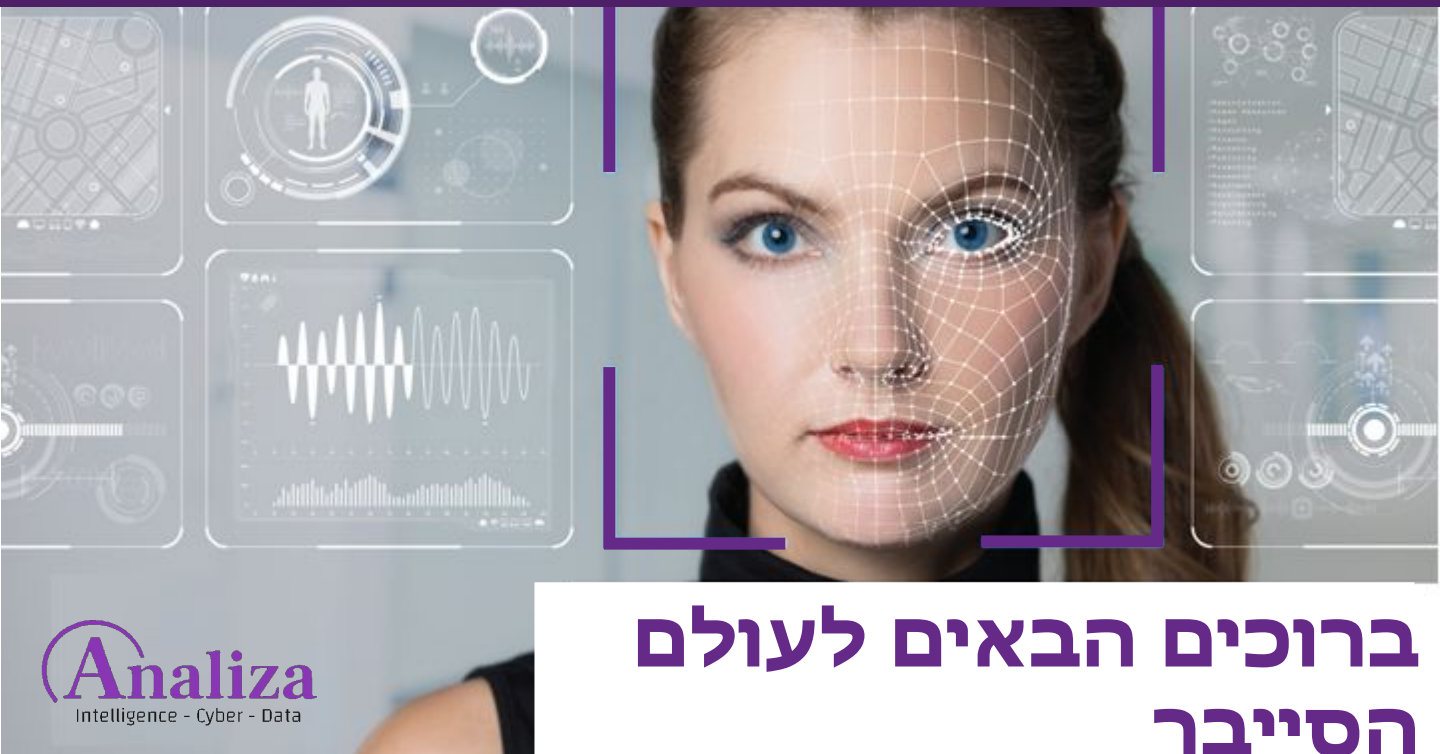




לימודי תחום הסייבר

בואו ללמוד את מקצועות הסייבר מהמומחים בתעשייה





ברוכים הבאים לעולם הסייבר

יחד עם ההתקדמות הטכנולוגית האדירה בעשורים האחרונים, תחום הסייבר החל להתפתח באופן מהיר מאוד. כיום, תחום הסייבר מהווה תחום מרכזי כמעט בכל מוסד, ארגון או חברה בעולם.

גודל שוק הסייבר העולמי צפוי להכפיל את עצמו כמעט פי 10 עד שנת 2023 ולעמוד על סכום של טריליון דולר בשנה (\$1,000,000,000,000), יחד איתו גדלים בקצב גבוהה מאוד עולמות הענן (Cloud) בדגש על שירותי ענן.

לאור הגידול המהיר בגודל שוק, נוצר מחסור הולך וגדל באנשי טכנולוגיה מקצועיים בשוק העבודה. כיום מדובר על מחסור של לפחות 40% במומחי טכנולוגיה בשוק, מחסור זה צפוי להמשיך ולגדול בשנים הקרובות יחד עם הגידול המשמעותי הצפוי בשוק הטכנולוגי העולמי.

השילוב בין תחום מרכזי, שוק אשר גדל במהירות ומחסור גדל בעובדים מוסמכים יוצר הזדמנות משמעותית ביותר עבורכם, הסטודנטים - ומאפשר לכם (לאחר קורס ייעודי) להיכנס לתחום המבוקש ביותר כיום בשוק ההי-טק העולמי, להתפתח אישית ומקצועית ולקבל שכר מהטובים במשק.

צוות אנליזה מציע לכם מסלול לימודים איכותי וממוקד אשר תוכנן ונבנה בקפידה על-ידי צוות מומחים מיחידת 8200, חיל האוויר ויחידות טכנולוגיה מובילות נוספות – בשיתוף חברות טכנולוגיה מובילות בתעשייה.

לימודי תחום הסייבר

הקורס נמשך כ- 320 שעות אקדמיות (140 מול מדריך / 180 תרגול עצמי):

אופרציה



שעות 80

נושאים:

• פורנזיקה

• Incident response

• מבוא למערכות SIEM

• כתיבת חוקי SIEM

• תפקידי אנליסט סייבר

• משחקי מלחמה

טכנולוגיה



שעות 120

נושאים:

• תקשורת מחשבים

• סייבר הגנתי

• סייבר התקפי

• שימוש ב FIREWALL

• מבוא למחשוב ענן

מבואות



שעות 120

נושאים:

• הכרת המחשב

• חומרה ותוכנה

• וירטואליזציה

• מ"ה WINDOWS*

• מ"ה LINUX*

• ניהול רשתות

מערכת הפעלה*

לאחר מעבר מבחן מסכם בהצלחה, הבוגרים יקבלו תעודת בוגר קורס

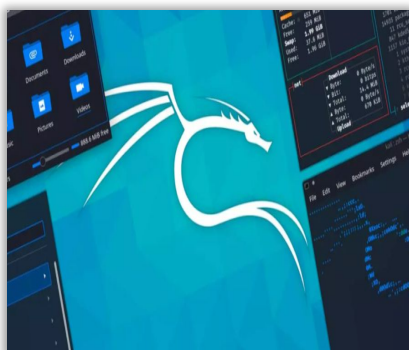


פרק המבואות

"נושאי הבסיס שכל איש טכנולוגיה חייב להכיר"

מילה מהתעשייה

מערכת ההפעלה Kali Linux



נחשבת להפצת הלינוקס המועדפת על אנשי הסייבר בעולם, מכילה מספר רב של כלי בדיקה ותקיפה. במהלך הקורס נלמד על המערכת זו לעומק.

הכרת המחשב

- מהו מחשב
- סוגי מחשבים
- מבנה המחשב
- רכיבים מרכזיים

חומרה ותוכנה

- מבוא לחומרה
- מבוא לתוכנה
- סוגי תכונות
- תוכנות קוד פתוח/ סגור

ניהול רשתות

- מבוא לשרתים וניהול רשתות
- התקנת שרת Windows Server
- הקמת Domain והתקנת DC ו AD
- יצירת אובייקטים ברשת (כולל GPO)
- התקנה וניהול שירותים (DNS, DHCP)
- תפקידי מנהל הרשת בתעשייה

מערכת ההפעלה Linux

- גרסאות, מבנה, תהליכים ושירותים
- עבודה מלאה באמצעות ה Terminal
- יצירה וניהול קבצים ותיקיות
- יצירה וניהול משתמשים והרשאות
- יכולות חיפוש מתקדמות
- ניתוח ופקודות מתקדמות בתקשורת
- צפיה וניתוח מערכת ה Logs

וירטואליזציה

- מבוא לוורטואליזציה
- מהם קבצי ISO, OVA, VMDK
- בניה וניהול מכונה וירטואלית
- בניה וניהול רשת וירטואלית

מערכת ההפעלה WINDOWS

- מבנה וגרסאות
- איתור וניהול תהליכים
- ניהול שירותים מרכזיים
- ניתוח ואבחון ביצועים
- ניתוח וניהול ה Registry
- צפיה וניתוח מערכת ה Logs
- ביצוע פעולות ב CMD

פרק הטכנולוגיה

"טכנולוגיה, ציוד ושיטות בסייבר"

מילה מהתעשייה

Wireshark



התוכנה המובילה בעולם לתיעוד וניתוח תעבורת רשת. במהלך הקורס נשתמש רבות בתוכנה הזו הן כדי ללמוד ולנתח תעבורת רשת והן לנתח מתקפות בזמן אמת

שימוש ב FIREWALL

- ייעוד, סוגים ואופן פעולה
- עקרונות בהפעלת FIREWALL
- ACL לעומק כולל White/Black list
- ניתוח חוקים וחריגות ב Logs
- כתיבת חוקים מורכבים

מבוא למחשוב ענן

- מהו למעשה ענן - Cloud
- היתרונות בשימוש במחשוב ענן
- נושאי בסיס במחשוב ענן

תקשורת מחשבים

- מודלים ופרוטוקולים
- ציוד רשת
- תהליך ה Encapsulation
- כתובות ו Subnetting
- DNS, DHCP, HTTP
- תוכנת ה Wireshark
- ניתוח תעבורת רשת

סייבר הגנתי

- עקרונות הגנת סייבר
- סוגי ציוד הגנת סייבר
- מתודולוגיות ושיטות הגנה
- מבוא לחומת אש ו ACL
- הגנת תחנות קצה באמצעות AV
- הגנת תשתית ומידע: IDPS, DLP
- הגנה אפליקטיבית: WAF

סייבר התקפי

- עיקרון ה CIA בסייבר התקפי
- סריקת רשתות ותחנות
- פריצת סיסמאות Online/Offline
- מתקפות הנדסה חברתית
- מתקפות MITM
- מתקפות מניעת שירות (DDOS)
- מתקפות אפליקטיביות (OWASP)

פרק האופרציה

"הופכים את הידע והיכולות לתפקיד בתעשייה"

מילה מהתעשייה

מערכת SIEM



ממערכות הגנת הסייבר החשובות ביותר. מסנכרנת ומאחדת מגוון פתרונות הגנה באופן מרכזי ומאפשרת ניהול אחיד ומסודר של כל אירועי הסייבר בארגון.

תפקידי אנליסט סייבר

- משימות שוטפות
- ממשקי עבודה בצוות
- ממשקי עבודה חיצוניים

משחקי מלחמה

- מבוא לסימולציות סייבר
- צוות כחול וצוות אדום
- בניה וניהול תרגולי סייבר
- תרחישי הגנה-התקפה מתקדמים
- תחקור תרחישים והפקת לקחים

הכנה לתעשייה

- קובץ קו"ח, פרופיל לינקדאין ועוד
- פיתוח כישורים אישיים
- סימולציית ראיונות עבודה

פורניקה

- עקרונות הניתוח הפורנזי
- שלבי הניתוח הפורנזי
- פורניקה למחשבי קצה
- פורניקה לאמצעי איכסון
- פורניקה לדואר אלקטרוני
- פורניקה לרשתות תקשורת
- סיכום ממצאים ודיווח

Incident response

- עקרונות ניטור מערכות
- שיטות לאיתור מתקפות
- ניתוח וקטורים של מתקפות
- ביצוע תהליך Mitigation
- מקרי False-Positive\ Negative
- ניהול לקוח ושליטה באסקלציה
- דו"חות וסיכום מתקפות סייבר

מערכות SIEM

- מבוא ושימוש בתוכנה
- פתרונות מובילים בשוק
- מבוא לתוכנה QRadar
- הקמת תשתית למערכת SIEM
- ממשקים עם מערכות הגנה
- תחזוקת המערכת לאורך זמן
- ניהול וטיפול בהתראות בזמן אמת