המרכז הבינלאומי למקצועות הסייבר

שיתוף פעולה ייחודי בין היחידה ללימודי חוץ
ומפעל הסייבר- אלתא מערכות.

חוברת מידע למועמדים

מגוון תכניות למידה משולבות ופורצות דרך, המציעות, בשיתוף פעולה ייחודי הכשרות מקצועיות ואימונים מעשיים בסימולטור מתקדם למקצועות הסייבר.
התקדמו עוד היום לקריירה מבוקשת, המשלבת אתגרים טכנולוגיים, חשיבה יצירתית ופיתוחים חדשניים באחד הענפים המבוקשים כיום בעולמות ההייטק והטכנולוגיה.

היחידה ללימודי חוץ

TAME™ Range

אלתא מערכות בע"מ IAI

לפרטים נוספים והגשת מועמדות:

*3068 דרך מאיר וויסגל 2, פארק המדע, רחובות www.ash-limudim.co.il

מקצועות הסייבר- ביקושים

בזמן המשבר: עלייה של 7% בביקוש למומחי סייבר; השכר במקצועות הדאטה - 32 אלף שקל בממוצע
(כלכליסט | 6.9.20 | מעין מנלה)

ברבעון השני של 2020 חלה עלייה של 7% בביקוש לאנשי מקצוע בתחום אבטחת סייבר. "תקופת הקורונה היא גן עדן לפשיעת סייבר, רבים עובדים מהבית ומתחברים מרחוק למערכות רגישות של החברה, מה שמקל מאוד על עבודתם של ההאקרים. בנוסף, תקופות של אי ודאות, פחד וחרדה מאז ומתמיד היו בסיס טוב לפיתיונות הונאה, במיוחד פגיעים אנשים מבוגרים חסרי ניסיון והבנה במערכות אונליין. כמובן, אנשי מקצוע בתחומי הסייבר היו מבוקשים מאוד גם לפני כן, אבל הצורך במומחי סייבר הפך בתקופה הזאת לאקוטי".

"...השכר הממוצע במקצועות הסייבר עומד על כ-36 אלף שקל בחודש, כאשר אנשים במקצועות כמו Security Researcher יכולים להגיע לשכר של 40 אלף שקל לחודש ויותר."

76% of Cybersecurity Leaders Face Skills Shortage
(security | 6.5.20)

"The latest findings of the Stott and May Cyber Security in Focus research reveal that leaders are still struggling with the skills gap and access to talent. Most respondents (76 percent) believe there is a shortage of cybersecurity skills in their company, which represents an improvement on 2019 (88 percent), however, the problem still seems more potent for mid-market and large enterprise businesses. Organizations are still struggling to source cybersecurity talent (72 percent) with no material improvement around time-to-hire from 2019".

בשנים האחרונות, עם ההתפתחות הטכנולוגית המואצת, בשילוב משבר הקורונה, אשר יצר קרקע פורייה למתקפות רשת שונות, העלולות להתרחש בכל רגע נתון כנגד אנשים פרטיים, גופים אזרחיים וממשלתיים, חברות וארגונים, הפכו חטיבות הסייבר לחיוניות וקריטיות, בכל חברה וארגון, אשר זקוקים להם כחלק ממערכי הגנה קבועים ששומרים על בטחון המידע והמשתמשים.
יחידות אלו הפכו לחוד החנית באותן חברות, אשר מחזרות ומחפשות אחר עובדים בתחום בו קיים חוסר של מעל 10,000 עובדים (!). ביקושים רבים אלו, יצרו מצב, בו כבר לא חייב תארים מתקדמים בהנדסה, מחשבים או טכנולוגיה, והגיוס הינו מהיר וכמעט מיידי, מול בוגרי קורסים מקצועיים שונים, אף ללא ניסיון בתחום.
בהתאמה, השכר במקצועות אלו מגיע לעשרות אלפי שקלים, לעובדים מתחילים, שמחוזרים תמידית למשרות שונות ונהנים מתנאים נחשקים, במקביל לנחיצותם הרבה בשמירה על מאגרי המידע השונים- שנמצאים תמיד- ויותר מתמיד, בסכנות כגון חשיפה ופריצה, שעלולות לגרום לנזקים של מיליארדי שקלים ואף למוטט חברות, טכנולוגיות, רשתות וארגונים.

המרכז הבינלאומי למקצועות הסייבר של היחידה ללימודי חוץ ומפעל הסייבר של אלתא מערכות

בשל המציאות שנוצרה מול איומים שונים, בשילוב הביקושים הרבים בתחום הסייבר, מובילות היחידה ללימודי חוץ ומפעל הסייבר של אלתא, את המרכז הבינלאומי למקצועות הסייבר בשילוב מאמן (סימולטור) הסייבר. המרכז מציע מגוון הכשרות מבוקשות, ויעניק לבוגריו הכשרה משולבת, מהמתקדמות בישראל, ותעודה מקצועית נדרשת, כולל ליווי לתעסוקה בתחום.

שלל ההכשרות הפרונטליות והמקוונות בשילוב הסימולטור, כחלק מהפרקטיקה המעשית בקורס, יאפשרו לסטודנטים ללמוד, להתמחות ולרכוש ניסיון מעשי, ולבוגרים, ליהנות מתעודות מקצוע מתקדמות, ומגוון אפשרויות תעסוקתיות, המותאמות לתחומי העניין שלהם.

סוגי ההסמכות

- קורס סייבר ואבטחת מידע בשילוב מאמן הסייבר. מכין למבחני ההסמכה הבינלאומיים CEH
- הסמכת מיישם הגנת סייבר בשילוב מאמן סייבר.
- קורס הכשרת מדריכים גלובליים להוראת הסייבר- בשילוב מאמן סייבר
- קורס מודיעין עסקי שיווקי והגנת סייבר בארגונים - בשילוב מאמן סייבר
- הכשרת חוקרים פרטיים -התמחות בתחום הסייבר.
- קורס מנתח אבטחת סייבר- בשילוב מאמן סייבר. מכין למבחני הסמכה בינ"ל מטעם IBM

2021 למידה פורצת דרך

משולבת אימוני סימולטור TAME™ Range במפעל מיומנויות הסייבר של אלתא מערכות.

הלמידה בכלל הקורסים וההכשרות הינה משולבת, ומכילה לימודים עיוניים ומעשיים, פרקטיקה ואימונים בסימולטור המתקדם, אשר מציע שלל תרחישי הגנות והתקפות מציאותיות.

אימונים אלו בסימולטור, משמשים במקביל גם חברות ממשלתיות, אזרחיות וארגונים פרטיים (כגון גופים פיננסיים, מרכזים רפואיים, חברות ביטוח ועוד) ומותאמים לתרחישים מורכבים בהתאם לאיומים הקיימים על אותם ארגונים.

האימונים מול התרחישים השונים, בכל אחת מההכשרות, יחזקו את הבנתם המעשית של הלומדים ואת יכולותיהם לנהל ולהפעיל מערכי הגנה, ולהקטין את הסיכויים לתקיפות שונות. במקביל, יביאו את הבוגרים לכדי ניסיון מעשי וקרוב לשטח ככל הניתן, מה שייצר עבורם יתרון משמעותי בקבלה לעבודה בתחום.

שיתוף פעולה ייחודי לתעודה מבוקשת

אלתא מערכות בע"מ היא אחת מארבע חטיבות של ה**תעשייה האווירית**, והראשונה בישראל בחברות ההגנה.
כמו כן, מובילה עולמית בתחומי המגזר הבטחוני. אלתא למעשה מפתחת פתרונות טכנולוגיים מתקדמים להגנות ביטחוניות ואזרחיות מתחומים שונים, ללקוחות ממשלתיים, ציבוריים ופרטיים. פיתוחיה כוללים פתרונות למודיעין, אבטחה, בקרת אש, מערכות קרקע, סייבר ועוד.
מפעל הסייבר הוא מרכז המצויינות של התעשייה האווירית ונועד לתת מענה לאתגרים העומדים בפני מדינות, מערכות הגנה, תשתיות ועוד באמצעות פתרונות ייחודיים להגנות סייבר- הגנה וניטור, חיזוי, זיהוי, מודיעין ונגישות.
התעשייה האווירית, באמצעות חטיבת הסייבר, מובילה את איגוד חברות הסייבר הישראלי (ic3) המציע פתרונות אבטחת סייבר שונים ונתמך ע"י מ. העבודה, מ. החוץ, מ. הבטחון, מנהלת הסייבר הלאומית הישראלית ומכון הייצוא הישראלי.

ה- TAME™ Range, הינו מרכז מיומנויות סייבר מתקדם, המציע פתרונות מתקדמים וחדשניים לניהול למידה וסייבר מקיף.
סימולטור זה מציג סביבת אימונים למלחמות סייבר מציאותיות, ונועד לשפר את חוסנם של ארגונים שונים, תוך שימוש באיומים האחרונים והעדכניים ביותר שנתגלו. סימולטור זה מציע פלטפורמות אימונים אישיות וצוותות, תרחישי תקיפה והגנה, וכולל הדרכה, מחקר וסימולציה של תרחישי סייבר בעלי רכיבים שונים כגון טופולוגית IT, סביבות OT ו- IoT ועוד.

היחידה ללימודי חוץ

היחידה ללימודי חוץ היא המכללה הגדולה בישראל להכשרות מקצועיות וכוללת את בית הספר המקוון הגדול בישראל בו מלמדים מיטב מרצי האקדמיה ואנשי המקצוע הבכירים בארץ.
מעל 30 אלף בוגרים ובוגרות כבר למדו וחוו יותר מ-100 הכשרות ומסלולי לימוד של היחידה ללימודי חוץ, אשר מפעילה גם חממת פיתוח קריירה של שירות התעסוקה, עם מעל 80% הצלחה בהשמות איכותיות!

ליחידה ללימודי חוץ שלוחות בכל רחבי הארץ. היא **מובילה את כל מערך הקורסים וההכשרות של כלל עובדי המדינה בישראל מטעם החשב הכללי, נציבות המדינה ומשרד האוצר**, וכן מובילה את בית הספר הגדול בישראל לחדשנות בקריירה ועסקים.

היחידה מציעה הכשרות בינלאומית, קורסים בפיקוח מלא של משרד הכלכלה, משרד החינוך, גמולי השתלמות, לשכת יועצי המס ועוד. זאת במטרה **לספק לבוגריה את ההסמכה המקיפה ביותר ליצירת יתרון תחרותי בשוק העבודה.**

ההחלטה לגבי בחירת מקצוע, סוג ההכשרה ו/או מוסד הלימודים, הינה החלטה מורכבת ובעלת משמעויות רבות. ביחידה ללימודי חוץ, ליווינו בשנים האחרונות, אלפי מתעניינים בדרכם לבחירה בהכשרה מקצועית, אשר תעמוד בקנה אחד עם החלומות, הכשרונות והשאיפות שלהם לגבי עתידם. גם עבורכם- אנו זמינים ונכונים להקשיב ולייעץ בכל התלבטות שתהיה טרום בחירת ההכשרה, וכמובן זמינים ללוות אתכם במהלכה.

עדיין מתלבטים?
6 סיבות טובות מדוע ללמוד את מקצועות הסייבר:

1. אחד התחומים המבוקשים והנחשקים כיום בעולם ההייטק. בין המקצועות היחידים שבשל משבר הקורונה העצימו את הדרישה לעובדים בתחום.
2. להשתלבות במרבית המקצועות בתחום- כלל לא נדרש ידע קודם.
3. השתלבות מהירה בעולם העבודה- מעסיקים יחזרו אחרייך!
4. משכורות גבוהות (מאוד) עוד בתחילת דרככם הראשונית בעבודות בתחום
5. תחום מרתק ומאתגר לפיתוח קריירה בארץ ובחו"ל
6. נחשב לאחד התחומים הלוהטים ואחד ממקצועות העתיד -2021 ניתן להמשיך לעוד ועוד הסמכות בתחום שלעולם ימציא את עצמו מחדש.

ועוד 6 סיבות מצויינות, מדוע ללמוד במרכז הבינ"ל למקצועות הסייבר- היחידה ללימודי חוץ וחטיבת הסייבר של התעשייה האווירית:

1. הכשרה מעשית בשילוב סימולטור מתקדם לאימונים בתחום- צבירת ניסיון מעשי תוך כדי ההכשרה, המתקיימת בחיבור למרכז האימון של מפעל הסייבר באלתא. החברה הגדולה והמובילה בארץ בפיתוחים בטחונים ומהמובילות בתחומה בעולם.
2. המכללה היחידה אשר מציעה מגוון הכשרות בהן תוכלו להשתלב בהתאם לתחומים המעניינים אתכם- וגם להמשיך ולהתמחות בהכשרות נוספות בתחום.
3. שיתוף פעולה של המכללה הגדולה בארץ והחברה המובילה בישראל ובעולם במגזר הבטחוני- תעודה נחשקת שתפתח לכם המון דלתות תעסוקתיות ובכלל!
4. צוות מרצים ומאמנים מומחה שיילווה אתכם לאורך כל ההכשרה והאימון המקצועי. כמו גם צוות ליווי מנהלי לכל נושא שיעלה לפני ובמהלך ההכשרות.
5. לימודים מרתקים, תכניות למידה מתקדמות ומשולבות בלמידה עיונית ומעשית, תרגולים, מקרי בוחן, סימולציות ועוד...
6. ליווי הבוגרים ע"י חממת פיתוח קריירה ייחודית. יועצי קריירה ילוו אתכם בדרככם להשתלבות בעבודה בתחום, או לפתיחת עסק משלכם במידה ותרצו.

היחידה ללימודי חוץ

TAME™ Range

אלתא מערכות בע"מ IAI

/1 קורס סייבר ואבטחת מידע בשילוב מאמן הסייבר של אלתא מערכות

מכין למבחני ההסמכה הבינלאומיים של EC-Council בשם CEH

רקע כללי

בהכשרה זו, ילמדו הסטודנטים מגוון תחומים על מנת להתמקצע למגוון תחומים בענף הסייבר ולהשתלב בעבודה מבוקשת בתחום. מסלול זה הינו מסלול מקיף ומקצועי, הכולל התמחות בעולם ההאקינג, SIEM-SOC ושילוב לתקיפה והגנה של כלל התשתיות והפלטפורמות הקיימות כיום בעולם. המסלול נלמד בשילוב התנסות מעשית עם סימולטור מתקדם ממפעל הסייבר של אלתא מערכות.

בתחילתו של המסלול תתקיים מכינה מקדימה, בה יבוצע יישור קו בין המשתתפים, ויילמדו תכני המבוא והבסיס של הקורס. המכינה תתקיים כ 4 מפגשים, ולאחריה, יחל הקורס המתקדם.

בקורס ילמדו, בחלוקה למודולים מקצועיים, התכנים הרלוונטיים ביותר לעולם ותעשיית הסייבר, כגון: Infrastracture Linux, Cisco, Cyber, אבטחת מובייל, Testing Penetration, תכנות בשפת Python, התקפות והגנות בעולם הסייבר ובנוסף מרכז ניטור ואבטחת מידע-SIEM-SOC ועוד.

מלבד הלמידה העיונית במהלך המפגשים, יתנסו הלומדים ב- TAME™ Range, סימולטור מתקדם, ממפעל הסייבר של אלתא מערכות, המציג סביבת אימונים למלחמות סייבר מציאותיות, ונועד לשפר את חוסנם של ארגונים שונים, תוך שימוש באיומים האחרונים והעדכניים ביותר שנתגלו. סימולטור זה מציע פלטפורמות אימונים אישיות וצוותיות, תרחישי תקיפה והגנה, וכולל הדרכה, מחקר וסימולציה של תרחישי סייבר שונים.

קורס זה יכין את הלומדים למבחני ההסמכה הבינלאומיים של EC-Council בשם CEH

פרטים טכניים

תנאי הקבלה

1. בוגרי 12 שנות לימוד
2. ועדת קבלה.

משך ההכשרה

700 שעות לימוד עיוניות ומעשיות- כולל תרגול במאמן הסייבר בשיתוף מפעל הסייבר של אלתא מערכות.

דרישות התכנית

מעבר בחינה עיונית ומעשית בהצלחה. נוכחות של לפחות 85% במפגשים

תעודות סיום והסמכה | לעומדים בהצלחה בדרישות הקורס יוענקו התעודות:

1. בוגר קורס סייבר ואבטחת מידע - תעודה מטעם היחידה ללימודי חוץ ומפעל הסייבר של אלתא מערכות.
2. העוברים בהצלחה את הבחינה הבינ"ל, יקבלו תעודה בינלאומית EC-Council בשם CEH

תכנית הלימודים

נושאי הלימוד	שעות אקדמאיות
מכינה מקדימה -סייבר, רשתות ואבטחת מידע	20
Web application	15
Windows Server 2016	30
Linux	38
Cisco	60
Cyber infrastracture	30
SIEM- SOC	40
Cross Platform Elevation of Privileges	30
Advanced Infrastructure Attacks	55
Python Programming For Security	62
Web Application Penetration Testing	60
Mobile Security	30
Introduction To Malware Analysis & Reverse Engineering	50
C|EH הכנה לבחינה הבינ"ל	30
תרגול מעשי במאמן הסייבר	150

700 שעות סה"כ

מכינה מקדימה -סייבר, רשתות ואבטחת מידע

הכרת המחשב, מבוא למערכות הפעלה, חומרה, ציוד תקשורת, פרוטוקול IP/TCP בהרחבה, מערכות ווירטואליות + תרגול הקמת רשת ווירטואלית, הכרת מערכת ה-Linux והרצת פקודות בממשק ה- Terminal , ביצוע תקיפת שירותים פופלריים לדוגמא: SSH ו- RDP.

Web application

מודול בניית אתרים בסיסיים
מערכת ההפעלה לשרתים
CSS
HTML
Javascript
DOM

Windows Server 2016

מערכת ההפעלה לשרתים מבית Microsoft
היכרות עם סביבת DOMAIN
מבוא והתקנת שרת Server 2016
הקמת דומיין וניהול Directory Active
ניהול שירותי דומיין- DNS, DHCP
שיתוף קבצים והרשאות
יצירת מדיניות בעזרת GPO
היכרות עם מבנה רשת ארגונית

Linux

מערכת ההפעלה Linux
Linux Distros & Kali Linux
Introduction to Offensive Linux
Basic Commands
Networking
Networking
File system structure
Users & Groups
Password & shadow file
Permissions and ownership
Package management
Common Services SSH / TELNET / FTP
Task schedulers
Process management
Final Lab

Cisco

מודול זה מעניק ידע וכלים בסיסיים לטכנאי/ מנהל רשת והינו קריטי להצלחה בתפקידים בעולם הסייבר. כמו כן, מהווה הכנה לבחינת ההסמכה CCENT, הסמכהמקצועית לניהול ותפעול ציוד תקשורת מטעם חברת Cisco העולמית, אשר מעניקה לטכנאים ואנשי אבטחת מידע את היכולת לפתרון תקלות יעיל יותר בציוד הרשת והבנה מעמיקה יותר ובניית מערך הגנה יעיל תוך שימוש בציוד ברשת. תעודה זו היא שלב חיוני להשגת תעודות נוספות בעולם אבטחת המידע ורשתות שלCISCO כגון Security CCNA ו- CCNP.

היכרות מעמיקה עם יסודות הרשת וכללי תקשורת המחשבים (IP/TCP & OSI.)
היכרות עם רכיבי הרשת השונים ותפקידם ברשת הארגונית.
היכרות ותפעול של מערכת ההפעלה IOS
היכרות מעמיקה עם פרוטוקולי ה- v4 & v6 (IP)
היכרות עם קונספט הניתוב (Routing)בדגש על ניתוב סטטי.
הקמה וניהול רשתות וירטואליות (VLANs.)
התמחות בהגדרת הפרוטוקולים והטכנולוגיות השונות
כולל הגדרות ראשוניות ופתרון תקלות נכון לציוד רשת, בדגש על נתבים ומתגים
הגדרות אבטחה בסיסיות ומתקדמות וסינון חבילות מידע
הקמה וניהול רשת ארגונית קטנה-בינונית.

Cyber Infrastracture

האיומים בעולם הדיגיטלי
מבוא לאבטחת מידע וסייבר
ניתוח תעבורה וסריקות
ביצוע סריקות רשת פנימית
ניתוח תעבורה עם Wireshark
חקירת קבצי PCAP
OSINT
ביצוע סריקות רשת חיצונית
סריקת מערכת, סריקת שירות, סריקת אפליקציה
איסוף מידע ברשת הפתוחה
Dictionary/Password Attacks
התקפת כוח ברוטלי כנגד שירותים
פיצוח קבצים מוצפנים
Wi-Fi
הכרות עם עולם האינטרנט האלחוטי
מבוא לקריפטוגרפיה
תקני הגנה והצפנות ברשתות Wi-Fi
חולשות מוכרות וניצולם
הנדסה חברתית
מבוא ל- SE
SEToolKit
HiddenEYE
הקמת דפי נחיתה לטובת Phishing
Network Annonymity
Dark Net & Deep Web
Proxy & VPN
Proxychains
MITM
מבוא ל"איש שבאמצע"
טכניקות שונות לביצוע MITM
ירוט תעבורה מוצפנת
HTTPS Downgrade
Metasploit and known CVE
Metasploit & Exploit-DB & Shodan
CVE & BugBounties
חיפוש ומציאת חולשות מוכרות
יצירת נוזקה וניצול חולשה
יצירת שרת שליטה CNC
Bind / Reverse Shell

SIEM-SOC

מרכז ניטור אבטחת מידע SOC
שימוש במערכת SIEM לזיהוי והתמודדות עם מתקפות בזמן אמת.
SOC lifesycle
Security measures
SIEM Implementation and configuration
Log analysis and attack detection
Filtering the right way
Using SIEM for Incident respons

Cross Platform Elevation of Privileges

שיטות אסקלציה מתוחכמות המאפשרות להפוך לאדמין בכל מערכות ההפעלה, גם כאשר לא קיים משתמש באותה מערכת.
Privilege Escalation Techniques
Local & Remote Privilege escalation
Credential Dumping & Pass The Hash
Privilege Escalation Using Common exploits
Local & Remote Privilege escalation in Linux
Privilege Escalation Using Automated Tasks
Permission misconfiguration &
Post Exploitation Techniques in Windows & Linux

Mobile Security

מערכות ההפעלה Android ו- iOS, כיצד בנויות, חולשותיהן ואיך לנצלן.
תכנות מחדש אפליקציות קיימות על מנת שיאפשרו לבצע פעולות חדשות ולעקוף לוגיקות קיימות, ואיך ניתן לתפוס תעבורה של אפליקציות, לשתול בהן באגים ולנצל חולשות. כיצד ניתן ליצור אפליקציה זדונית ולהחדירה לטלפון היעד לטובת השתלטות על המכשיר.

Android

Introduction to Android
Android Security Architecture
Android Permissions
Reversing Android Applications
Analyzing Android Traffic
Analyzing Android Malwares
Introduction to Drozer
SSL Pinning and ways to bypass it
Lab configuration for application

iOS

Introduction to iOS Security
Setting up Hackingtosh enviornment
Jailbreaking iOS
Exploiting iOS Applications
Dynamic runtime analysis

Advanced Infrastructure Attacks

תשתיות, איסוף נתונים על הלקוח,עקיפת מערכות הגנה, ביצוע אסקלציות במערכת ההרשאות ותנועה ברשת ועוד.

Lateral Movement Methodology & Internal
Cyber attack cycle
Enumerating an Organization
Exploiting Services & Ports ו
SMB Relay & Responder
PowerShell as a Weapon
Kerberoasting & Pass The Ticket
Get The Domain Admins
Veil-Framework & Obfuscation techniques
Office Exploitation

Python Programming

פיתוח וכתיבה בשפה המתפתחת ביותר בעולם אשר משמשת באופן יום-יומי אלפי אנשי אבטחת מידע.

Python introduction
Data types
Conditions & Loops
Code Handling
Functions
Sockets
Using Python For Hacking
Final project

Web Application Penetration Testing

ההתקפות החזקות ביותר ברשת האינטרנט, אשר מאפשרות לתוקף להשתלט על האתר עצמו ואף על המחשב המארח.

Web Technologies
OWASP Top 10
Burp Suite / ZAP
XSS
CSRF
SQL/NOSQL Injection
LFI\RFI
XML Injections
Path Traversal ו Exploiting Upload Mechanisem
Bypassing Authentication
Clickjacking
Web Shells
Report Writing

Introduction To Malware Analysis & Reverse Engineering

חקירה סטטית ודינמית, סוסים טרויאנים וחקירתם
שיטות שונות לתכנות לאחור ושינוי קוד ע"י תוקפים
Static Malware Analysis
Dynamic Malware Analysis
Assembly Registers
Debugging Using OllyDbg & Immunity Dbg
Debugging Using Ida
Anti Debugging
Packing & Unpacking
Manual Packing & Assembly Editing
Understand The CODE
Software & Hardware Breakpoints
AntiVirus Evasion
Reversing Challenges
Memory Corruption Attacks
Final Lab

הכנה לבחינה בינ"ל CEH

לימוד הנושאים המרכזיים בהסמכת CEH הבינלאומית של EC-COUNCIL. הכוללים מתדולוגיית התקפה, שיטות התקפה מגוונות לאפליקציה ותשתית ועוד.
אנשי אבטחת מידע וסייבר המחזיקים בתעודה זו הינם בעלי יתרון משמעותי על פני מועמדים אחרים לאותם התפקידים, מבחינת ידע תיאורטי ופרקטי. נושאי הבחינה:

Introduction to Ethical Hacking
Footprinting and Reconnaissance
Scanning Networks
Vulnerability Analysis Enumeration
System Hacking
Malware Threats
Sniffing
Social Engineering
Denial-of-Service
Session Hijacking
Evading IDS, Firewalls, and Honeypots
Hacking Web Servers
Hacking Web Applications
SQL Injection
Hacking Wireless Networks
Hacking Mobile Platforms
IoT Hacking
Cloud Computing
Cryptography

תרגול מעשי משולב בסימולטור הסייבר TAME™ Range

אימוני סימולטור TAME™ Range במפעל מיומנויות הסייבר של אלתא מערכות.

לכל אורכה של ההכשרה, הלמידה הינה משולבת, ומכילה במקביל ללימודים העיוניים, אימונים בסימולטור מתקדם, אשר מציע שלל תרחישי הגנות והתקפות מציאותיות.

האימונים מול התרחישים השונים, יכללו תרחישים המותאים לנושאי הלימוד במודולות השונות ויחזקו את הבנתם המעשית של הלומדים ואת יכולותיהם לנהל ולהפעיל מערכי הגנה, ולהקטין את הסיכויים לתקיפות שונות. במקביל, יביאו את הבוגרים לכדי ניסיון מעשי וקרוב לשטח ככל הניתן, מה שייצר עבורם יתרון משמעותי בקבלה לעבודה בתחום.

2/ מיישם הגנת סייבר בשילוב מאמן הסייבר מבית אלתא מערכות

רקע כללי | מתוך: מדיניות הסדרת מקצועות הגנת הסייבר במדינת ישראל-מערך הסייבר הלאומי.

מיישם הגנת הסייבר הינו בעל ידע תיאורטי בסיסי ויכולת יישומית, האחראי על יישום הגנת הסייבר בארגון בהיבטים שונים: התקנה, ניהול תפעול ותחזוקה של מוצרי הגנת הסייבר, יישום תהליכי אבטחה שגרתיים- ניהול חשבונות והרשאות משתמשים, ניהול סיסמאות, ניהול גישת משתמשים למחשבים ולמידע, ניהול ציוד קצה והתקנים ניידים בהיבטי אבטחה, זיהוי וטיפול ראשוני/בסיסי באירועי אבטחה בהסתמך על הכרת סוגי איומים ותקיפות, אופן הטיפול בתקיפות שהתגלו ועוד, כל זאת תוך הכרת והבנת הפעילות, הצרכים והמטרות של הארגון.

נושאי הלימוד

1. מבוא לאבטחת מידע והגנת הסייבר
2. תקני אבטחת מידע וניהול סיכונים
3. מבנה מחשב + יסודות מערכות הפעלה
4. יסודות תקשורת מחשבים-א' + ב'
5. הגנת גישה בתקשורת ואינטרנט
6. בידול והפרדת רשתות תקשורת
7. היבטי אבטחת מידע בציודי תקשורת (הקשחה) ואבטחת מידע
8. אימות והצפנה
9. בקרת גישה
10. היבטי אבטחת מידע במערכות הפעלה והקשחות שרתים
11. היבטי אבטחת מידע במסדי נתונים
12. תוכנות זדוניות וזיהוי אנומליות
13. דלף מידע
14. ניהול ורישום אירועי אבטחת מידע (Audit)
15. טיפול באירועי אבטחת מידע
16. מחשוב ענן, שירותי אירוח, וירטואליזציה
17. שינוע מידע מ/אל הארגון
18. המשכיות עסקית (BCP/DRP)
19. אבטחה אפליקטיבית
20. מתודולוגית ביצוע ניסיונות חוסן
21. חוק ואתיקה
22. אבטחה פיסית

פרטים טכניים

תנאי הקבלה

1. בוגרי 12 שנות לימוד
2. בגרות באנגלית ובמתמטיקה, ברמה של 3 יחידות או מבחנים ברמה מקבילה.
3. תעודת הסמכה בינלאומית בסביבות תקשורת Networking
4. ועדת קבלה.

משך ההכשרה

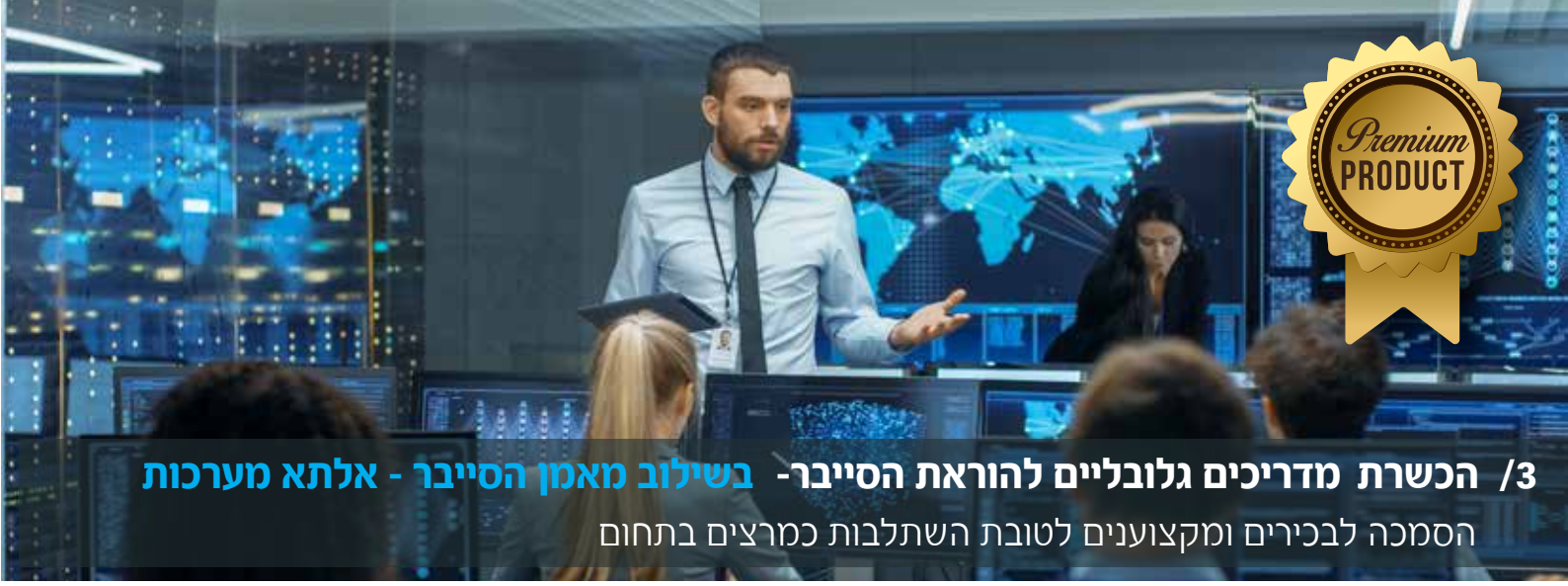
306 שעות לימוד עיוניות ומעשיות+ מודול תרגול במאמן הסייבר בשיתוף מפעל הסייבר של אלתא מערכות.

דרישות התכנית

מעבר בחינה עיונית ומעשית בהצלחה. נוכחות של לפחות 85% במפגשים

תעודות סיום והסמכה | לעומדים בהצלחה בדרישות הקורס תוענק התעודה:

מיישם הגנת סייבר תוך ביצוע שעות אימון בסימולטור סייבר- תעודה מטעם היחידה ללימודי חוץ ומפעל הסייבר של אלתא מערכות.



3/ הכשרת מדריכים גלובליים להוראת הסייבר- בשילוב מאמן הסייבר - אלתא מערכות

הסמכה לבכירים ומקצוענים לטובת השתלבות כמרצים בתחום

רקע כללי

כיום, בכירים במגוון רחב של תחומים מהווים את סגלי ההוראה המובילים במוסדות לימוד שונים, כאשר תחומי הסייבר נמצאים בהאצה משמעותית מול הביקושים הרבים במשק הישראלי והגלובלי, לכח אדם מיומן במקצוע. בוגרי הכשרות מקצועיות במקצועות הסייבר, ולאו דווקא בוגרי תארים, משתלבים בחברות וארגונים בתחום, **וישנו ביקוש רב למדריכים בתחומים אלו, במגוון מוסדות לימוד**. היחידה ללימודי חוץ בשיתוף מפעל הסייבר- אלתא מערכות, מציעות מסלול הכשרה ייחודי, אשר יכשיר את המועמדים המתאימים כמרצים מהשורה הראשונה, בתחומי הסייבר. **המסלול כולל הכנה משמעותית וישירה לתעסוקה בתחום, כאשר המצטיינים ישולבו בסגלי ההוראה של היחידה ללימודי חוץ בארץ ובעולם, והודות לשעות תרגול רבות על מאמן הסייבר- יהפכו למעשה למומחי סייבר ברמה עולמית.**

מסלול זה הינו מסלול פרימיום במרכז להוראת הסייבר ומתאים ל:

- סגלי הוראה בבתי ספר ,מכללות ואקדמיה בארץ ובעולם
- המעוניינים להשתלב כראשי מגמה בארץ ובעולם בתחום
- מנהלי IT בכירים בארץ ובארגונים בעולם
- המעוניינים להקים עסק כמטמיעי סייבר בעסקים קטנים ,בינוניים וארגונים

נושאי הלימוד

1. הכרות ותפקיד המרצה - מיון, בדיקת התאמה והצלבה למסלול העתודה.
2. מקצועות הסייבר בארץ ובחו"ל. הכרות עם מגוון האפשרויות להשתלבות תעסוקתית כמרצים.
3. קורסים מפוקחים, ממשלתיים, ובנ"ל. סוגי הכשרות והכרות עם מושגים הכרחיים כמרצים בתחום.
4. הכיתה כקבוצה, לימוד שלבי ההתפתחות האוניברסליים בהתפתחות קבוצה קבלת כלים לניהול תוכן השיעור
5. מעולם האימון - הכרות עם מודלים מרכזיים בתקשורת, ניהול זמן, מיומנות עמידה מול כיתה ועוד
6. המרצה כמנחה, מה בין הנחייה להוראה, שילוב כלים מתחום הנחיית קבוצות בשירות הוראה.
7. כלים טכנולוגיים לבניית אביזרי הוראה - מצגות, סקרים, בחינות, חוברות קורס, חומרים טכנולוגיים ייחודיים ועוד.
8. הכרות ולמידה של מאמן הסייבר בחברת אלתא, יצירת סביבה טכנית ללמידה בסימולטור ובניית מערכים מציאותיים נלווים.

תנאי הקבלה

בוגרי תארים ו/או קורסים מקצועיים מוכרים בתחום הסייבר+ ועדת קבלה ממיינת

משך ההכשרה

100 שעות לימוד עיוניות ומעשיות. כולל שעות תרגול במאמן הסייבר בשיתוף מפעל הסייבר של אלתא מערכות.

דרישות התכנית

מעבר בהצלחה של סימולוצית הדרכה מסכמת

תעודות סיום והסמכה | לעומדים בהצלחה בדרישות הקורס תוענק התעודה:

בוגר/ת הכשרת מדריכים גלובליים להוראת הסייבר-בשילוב מאמן סייבר תעודה מטעם היחידה ללימודי חוץ ומפעל הסייבר של אלתא מערכות.

/4 קורס מודיעין עסקי שיווקי והגנת סייבר בארגונים

בשילוב מאמן הסייבר של התעשייה האווירית

רקע כללי

בעידן התחרות העסקית הבלתי מתפשרת, מודיעין עסקי הינו תחום מקובל בעולם הרחב, כאשר בישראל גוברת המודעות לתחום, וחברות שואפות להיעזר בשירותי ייעוץ חיצוניים או להקים יחידה אינטגראלית בתוך ארגונן.
הכשרה זו תעניק ללומדים ידע רחב על מנת להשתלב במקצועות המודיעין העסקי ולהגיע למידע חיוני על שחקנים, איומים, שיתופי פעולה והזדמנויות עסקיות. המשתלבים בתחום זה יוכלו לתת להשתלב בחברות וארגונים שונים על מנת לשפר את האסטרטגיה העסקית של העסק, לשווק באפקטיביות, להתכונן למשברים, ולסייע בהשגת יתרון תחרותי על פני היריבים העסקיים בתחומם.

מוביל ההכשרה הינו אמיר פליישמן, מקים ומנכ"ל סיקום גלובל, מרצה בינ"ל לשיווק ומודיעין תחרותי באקדמיה, בסקטור הציבורי ובסקטור הפרטי. מומחה עולמי בתחום המודיעין העסקי, אשר ביוני 2019, נבחר למרצה השנה בעולם בתחום המודיעין ע"י הארגון הבינלאומי המוביל ללימודי מודיעין IAFIE

נושאי הלימוד- חטיבת מודיעין עסקי

גיבוש אסטרטגיה תחרותית לבית העסק/הארגון
טכניקות יעילות לאיתור מידע עסקי באינטרנט
מודיעין עסקי-תחרותי בקהילות וירטואליות
מאגרי מידע בישראל ובעולם: ספקים, מוצרים/שירותים
איתור אנשי מפתח בארגונים
כלי מעקב אחר פעילות אתרים
זיהוי איומים והזדמנויות על העסק:
ניטור וחיזוי פעילות מתחרים וביצועיהם בזמן אמת
מעקב אחר התנהגות צרכנים/לקוחות פוטנציאליים
איתור מידע עסקי באמצעות איגודים מקצועיים, מחקרי שוק, עיתונות וכד'
השפעת המודיעין תחרותי על האסטרטגיה
והטקטיקות העסקיות של בית העסק/הארגון
השגת מידע והתנהלות בכנסים ותערוכות

משך ההכשרה

100 שעות לימוד עיוניות ומעשיות.
כולל שעות תרגול במאמן הסייבר בשיתוף מפעל הסייבר של אלתא מערכות.

תעודות סיום והסמכה

לעומדים בהצלחה בדרישות הקורס תוענק התעודה:
בוגר/ת קורס מודיעין עסקי שיווקי והגנת סייבר בארגונים
כולל שעות אימון בסימולטור סייבר.
תעודה מטעם היחידה ללימודי חוץ ומפעל הסייבר של אלתא מערכות.

נושאי הלימוד - חטיבת הסייבר- בשילוב תרגולים מעשיים במאמן הסייבר

מבוא להגנת סייבר
סייבר, אבטחת מידע ופרטיות בראי החוק
הטכנולוגיה מאחורי הסייבר
מערכות להגנת סייבר
אירוע סייבר
אתיקה מקצועית
לינוקס
מודיעין
הערכת פגיעות ותוכנות זדוניות
Hacking
ניתור רשתות
הזרקת קוד זדוני
תקיפת שרתי אינטרנט
תיעוד הבדיקה
חקירת ארוע סייבר
תהליך חקירת עבירת מחשב
המידע הדיגיטלי
בחינת מכשיר סלולארי והתקן USB
בחינת רשת תקשורת
ציוד תקשורת

/5 הכשרת חוקרים פרטיים- בהתמחות סייבר בשילוב מאמן הסייבר של התעשייה האווירית

רקע כללי

קורס זה יכשיר את הסטודנטים לתפקידי חקירות וביטחון בסקטור האזרחי והציבורי, בהתמחות חקירות סייבר- פתיונות הונאה, פישינג, פריצות למאגרי מידע, התקפות טכנולוגיות ועוד. זאת במטרה להכשיר את החוקרים להתמודד כנדרש עם איומי וארועי סייבר, ולהבטיח את הרמה המקצועית, המהימנות והאתיקה של העוסקים בתחום.
במהלך ההכשרה יעמיקו הסטודנטים בהכרת החוק והמשפט, וילמדו את הנושאים למעבר בחינת ההסמכה של מ. המשפטים להשתלבות בתחום החקירות הפרטיות: בתחומי האבטחה, חקירות ותשאול ובמגוון האמצעים העומדים לרשות החוקר. במקביל, יעמיקו בלימוד חטיבת הסייבר כהכנה להשתלבות תעסוקתית והתמחות בתחום.

נושאי הלימוד- חטיבה משפטית

חוק ותקנות חוקרים פרטיים, חוק האזנות סתר - השיטה
חוק כבוד האדם והגנת הפרטיות - סוגיות נבחרות
חוק העונשין + סוגיות נבחרות
חוק אבטחה במקומות ציבוריים
חוק המרשם הפלילי ותקנות נמלים
חוק איסור לשון הרע - הפלילי, האזרחי
פקודת סדר הדין הפלילי + פקודת הפרוצדורה הפלילית (עדות)

נושאי הלימוד- חטיבה מעשית

איסוף מודיעין עסקי , מודיעין רשת- תהליך המודיעין, סוגי מקורות
גיוס סוכן ויצירת קשר
סדנא- תרגילי חקירה, שפת גוף וגרפולוגיה
חקירות ביטוח, חקירות נזקי גוף ורכוש, גניבה והונאה
חקירת תאונת דרכים - עקרונות ופרקטיקה (ניתוח מקרה בוחן)
תרגיל שטח, איסוף ראיות, פרופילאות
ציוד בילוש-צילום ומצלמות סמויות
חקירות כלכליות

משך ההכשרה

100 שעות לימוד עיוניות ומעשיות.
כולל שעות תרגול במאמן הסייבר מפעל הסייבר של אלתא מערכות.

נושאי הלימוד - חטיבת הסייבר- בשילוב תרגולים מעשיים במאמן הסייבר

מבוא להגנת סייבר
סייבר, אבטחת מידע ופרטיות בראי החוק
הטכנולוגיה מאחורי הסייבר
מערכות להגנת סייבר
אירוע סייבר
אתיקה מקצועית
לינוקס
מודיעין
הערכת פגיעות ותוכנות זדוניות
Hacking
ניתור רשתות
הזרקת קוד זדוני
תקיפת שרתי אינטרנט
תיעוד הבדיקה
חקירת ארוע סייבר
תהליך חקירת עבירת מחשב
המידע הדיגיטלי
בחינת המחשב
בחינת מכשיר סלולארי והתקן USB
בחינת רשת תקשורת
ציוד תקשורת

תעודות סיום והסמכה

לעומדים בהצלחה בדרישות הקורס תוענק התעודה:
בוגר.ת הכשרת חוקרים פרטיים בהתמחות ארועי סייבר- כולל שעות אימון בסימולטור הסייבר
תעודה מטעם היחידה ללימודי חוץ ומפעל הסייבר של אלתא מערכות.

/6 תכנית הכנה לבחינות הסמכה - מנתח אבטחת סייבר- בשילוב מאמן הסייבר

הסמכה בינ"ל - IBM Cybersecurity Analyst Professional Certificate

רקע כללי

הכשרה זו, תעניק ללומדים את הכישורים הטכניים לקבלת תעודה בינ"ל מטעם IBM על מנת להשתלב בתפקידי אנליסט אבטחת סייבר. תוכן עיוני, הדרכה מעשית ושימוש במעבדות ובסימולטור הסייבר המתקדם של אלתא מערכות, יקדמו אתכם להכרת מושגים הכוללים אבטחת רשת, הגנה על נקודות קצה, תגובת אירועים, מודיעין איומים, בדיקות חדירה והערכת פגיעות וניתוח אבטחת סייבר, ולקבלת תעודה בינ"ל נדרשת על מנת להשתלב באופן מהיר ואיכותי בעבודה בתחום.

מטרות ההכשרה

פיתוח ידע בכלים אנליסטיים באבטחת סייבר הכוללים הגנה על נתונים; נקודות קצה; SIEM; ומערכות יסוד ורשת.
העמקה בנושאים עיקריים בתחום איומי מודיעין בנוף אבטחת הסייבר של ימינו.
קבלת מיומנויות לתגובות אירועים פלילים באמצעות מחקרי מקרה אבטחת סייבר בעולם האמיתי.
התנסות מעשת ופיתוח מיומנויות באמצעות כלי אבטחה ספציפיים ותעשייתיים עם קוד פתוח.

ההכשרה מחולקת ל 8 קורסים:

1/ מבוא לכלי אבטחת סייבר ותקיפות סייבר

נושאים באבטחת סייבר בסיסית: היסטוריה של אבטחת הסייבר, סוגים ומניעים של התקפות סייבר, איומים הנוכחיים על ארגונים ואנשים פרטיים, טרמינולוגיה מרכזית, מושגי מערכת בסיסיים וכלי מבוא לתחום הסייבר. נושאים נוספים בקורס זה: חשיבה ביקורתית וחשיבותה, ארגונים ומשאבים, אבטחת סייבר בעידן המודרני ועוד.

2/ תפקידים, תהליכים ואבטחת מערכות הפעלה ברשת

הבנת תפקידי המפתח לאבטחת סייבר בארגון, תהליכי אבטחת סייבר מרכזיים ודוגמה לכל תהליך, ארכיטקטורה, מערכות הקבצים והפקודות הבסיסיות למספר מערכות הפעלה כולל Windows, Mac / OS, Linux ו- Mobile, וירטואליזציה בכל הקשור לאבטחת סייבר, ארגונים ומשאבים וחקר סוגיות אבטחה ברשת בעידן המודרני.

3/ מסגרת תאימות לאבטחת סייבר ומינהל מערכות

קורס זה יעניק ללומדים את כל הרקע הדרוש להבנת המפתח לפתרון בתחום אבטחת סייבר ותקני התעשייה. פקודות בסיסיות לניהול משתמשים ושרתי אבטחה, פגיעות במערכות ההפעלה של הארגון, אבטחת נקודות קצה וניהול תיקונים, הצפנה, מיומנויות מעמיקות סביב הצפנה ועוד.

4/ פגיעויות באבטחת רשת ובסיסי נתונים

רשתות מקומיות, TCP / IP, מסגרת OSI ויסודות ניתוב, כיצד רשת משפיעה על מערכות אבטחה בארגון, רכיבי הרשת השומרים על ארגון מפני התקפות אבטחה ברשת, נקודות תורפה של מסדי נתונים והכלים / ידע הדרושים לחקר פגיעות מסד נתונים למגוון בסיסי נתונים, כולל SQL Injection, Oracle, Mongo ו- Couch. סוגי הפרות אבטחה שונים הקשורים למאגרי מידע וארגונים המגדירים תקנים ומספקים כלים לאנשי מקצוע בתחום אבטחת הסייבר.

5/ בדיקת פריצה לשרתים, תגובת אירוע וגורמים פליליים

שלבים שונים של בדיקות הפריצה, כיצד אוספים נתונים וכלים פופולריים לבדיקת פריצה. השלבים של תגובת אירוע, תיעוד חשוב לאיסוף, ומרכיבים של מדיניות תגובה וצוות. שלבים מרכזיים בתהליך הפלילי ונתונים חשובים לאיסוף. קורס זה יעניק למשתתפים גם מבט ראשון על סקריפטים ועל החשיבות למנתח מערכות.

6/ מודיעין איומי סייבר

טקטיקות הגנת רשת, הגדרת בקרת גישה לרשת ושימוש בכלי ניטור רשת. סיכוני הגנה על נתונים ותחקור הגנה על נקודות קצה ניידות. זיהוי טכנולוגיות סריקה שונות, פרצות אבטחת יישומים ופלטפורמות מודיעין איומים, כלי אבטחת סייבר החשובים לאנליסט מערכות, סווג נתונים בסביבת מסד הנתונים שלך, טכנולוגיות וכלים לסריקת פגיעות אבטחה, זיהוי איומי אבטחה של אפליקציות ופגיעות נפוצות.

7/ אבטחת סייבר: מקרים של תגובת הפרות

תחקור מתודולוגיות של תגובת אירועים ומודלים ביטחוניים. הכרות וסיווג סוגים מרכזיים של נקודות תורפה והתקפות נלוות נגד הארגונים של ימינו. חקר מקרי בוחן של הפרות כדי ללמוד כיצד זוהו ומה נעשה או שהיה יכול להיעשות כדי להפחית את הסיכון האיומי לארגון. בדיקת העלויות של הפרות נתונים באמצעות מחקרי מחקר והפרות ידועות.
בקורס זה יבחרו ויחקרו הסטודנטים, פרצת אבטחת סייבר ויישמו באמצעות חקר את הידע והמיומנויות מקורס זה ומקורסים קודמים כדי לנתח את סוג ההתקפה, ציר הזמן של ההתקפה, מערכות פגיעות וכל ההזדמנויות שהוחמצו.

8/ קורס מסכם- מנתחי אבטחת סייבר של IBM

זהו הקורס הסופי הנדרש להערכת הידע והמיומנויות הנרכשים כדי להיות מוכן לתפקיד אנליסט אבטחת סייבר.
בקורס זה יועברו בחינות הערכה סופיות לכל אחד משבעת הקורסים הקודמים בתעודת המקצוע של IBM Cybersecurity Analyst. לאחר סיום מוצלח של הבחינות, תוכלו לרכוש את תעודת המקצוע של IBM Cybersecurity Analyst.

תנאי הקבלה
ידע בשפה האנגלית

משך ההכשרה
130 שעות לימוד עיוניות ומעשיות.
+ 20 שעות תרגול במאמן הסייבר בשיתוף מפעל הסייבר של אלתא מערכות

דרישות התכנית
מעבר בהצלחה של בחינות הסיום בכל אחד מהקורסים

תעודות סיום והסמכה |

מידה בהצלחה בדרישות הקורס תזכה את הבוגרים בתעודת גמר מקצועית: IBM Cybersecurity Analyst Professional Certificate

IBM Cybersecurity Analyst Professional Certificate

IBM הינו תאגיד רב-לאומי אמריקאי, שמרכזו במדינת ניו יורק, ומהווה את אחד התאגידים הגדולים והוותיקים בעולם המחשוב, כאשר במשך שנים רבות היה הגדול בתחום זה. התאגיד עוסק במגוון תחומי חומרה, תוכנה ושירותים: מעבדים, מערכות מחשב שלמות בגדלים שונים, ציוד היקפי, תוכנות, בסיסי נתונים, שרתי יישומים, כלי פיתוח, ייעוץ ועוד. והינו המעסיק הגדול בעולם של עובדים בתחום טכנולוגיית המידע.
הכשרה זו נלמדת באופן מקוון, מול הקורסים ותוכנית הלימודים ב IBM, ובליווי צוות מומחי תוכן לתחום מהיחידה ללימודי חוץ. הבוגרים, אשר יעמדו בדרישות הקורסים ויעברו בהצלחה את פרוייקטי הסיום, יקבלו תעודות הסמכה מטעם IBM ויוכלו להשתלב באחד התחומים החזקים והמובילים היום בתעשיית הסייבר.