We Search Knowledge Different

תוכנית ותכני ההכשרה – 'מיישם סייבר ארגוני'

מדוע מיישם סייבר ארגוני?

מקצוע מיישם סייבר ארגוני הוגדר על-ידי רשות הסייבר הלאומית כמקצוע בסיס רוחב הנדרש בכל ארגון וזאת לצורך עמידת הארגון בהנחיות הרגולציה הממשלתית של ממשלת ישראל. כל מיישם סייבר יעבור בחינת הסמכה על-ידי הרשות ויוכל לשמש בתפקידי מיישם סייבר כן בארגונים פרטיים וכן הממשלתיים. בנוסף לזה, קורס מיישם סייבר הנו קורס חובה מקדים לקורסים מתקדמים כמו בודקי חדירות, טכנולוגיה ומתודולוגיה של הסייבר וקורס חקירות הסייבר שגם אלה הוגדרו ומונחים על-ידי רשות הסייבר הלאומית.

תוכנית הלימודים:

<u>המכינה</u>: התוכנית בנויה על מכינה מקוונת של חומרי חובה של רשות הסייבר הלאומית. במהלך המכינה החניכים לומדים פרקים של חומר עיוני בשיטת לימוד עצמי עם מבדקי הבנה וידע באינטרנט. הלימוד מלווה באופן רציף על-ידי מדריך כך שגם הוא וגם החניך יוכלו לראות את ההתקדמות ואת השיגים אישיים וגם יחסיים לקבוצה. בסיום החלק העיוני ולפני הכניסה לאינקובטור נערך מבחן הבנה.

נושאים נלמדים - מבוא לאבטחת מידע והגנת הסייבר, תקני אבטחת מידע וניהול סיכונים ,מבנה מחשב, יסודות מערכות הפעלה, יסודות תקשורת מחשבים , תוכנות זדוניות וזיהוי אנומליות (תיאורטי) ,הגנת גישה בתקשורת ואינטרנט (תיאורטי),אבטחת מידע במערכות הפעלה והקשחת שרתים (תיאורטי),בקרת גישה (תיאורטי),חוק ואתיקה (סה"כ בהיקף שוו"ע 120 שעות לימוד).

שלב #1: שגרת הגנה ארגונית וזיהוי האירוע

במהלך שבועיים הראשוניים של הקורס החניכים לומדים את סביבת הרשת הארגונית על מרכיביה הרשתיים ואנושיים, משאבי מידע העיקריים והיקרים שברשת ואופן הגנתם, דרכי חדירה ואופני הפעולה של האקרים. במהלך השבועיים הללו החניכים ילמדו לאבחן מהי אנומליה בפעילות בסביבת סייבר.

הפרק מסתיים בבחינה מעשיית של המדריך את אופן הזיהוי בסביבה ארגונית.

נושאים נלמדים - *אבטחה פיזית* ,אבטחה אפליקטיבית ,שינוע מידע מ/אל הארגון ,הצפנה ואימות ,תוכנות זדוניות וזיהוי אנומליות (מעשי) ,מחשב ענן, שרתי אירוח, וירטואליזציה ,הגנת גישה בתקשורת ואינטרנט (מעשי), (סה"כ בהיקף שוו"ע 54 שעות לימוד).

שלב #2: ביצוע אבחון לאירוע/זיהוי - בחירת אופן הטיפול

אירוע לימודי של יום אחד – במהלך האירוע הארגון של החניך יותקף בשורה של מתקפות טוריות ומקבילות ועל החניך יהיה לזהותן ולאבחנן.

נושאים נלמדים - *היבטי אבטחת מידע במסדי נתונים*, דלף מידע, היבטי אבטחת מידע בציוד תקשורת (הקשחה) ואבטחת מידע, היבטי אבטחת מידע במערכות הפעלה והקשחת שרתים (מעשי) **,** (סה"כ בהיקף שוו"ע 44 שעות לימוד).

שלב #3: טיפול באירוע סייבר

נלמד ונתרגל אופני הטיפול באירועי הסייבר לפי סוגים.

נושאים נלמדים - טיפול באירועי אבטחת מידע, מתודולוגית ביצוע ניסיונות חוסן (תשתית ואפליקציה),בידול והפרדת רשתות תקשורת, בקרת גישה (מעשי) **,** (סה"כ בהיקף שוו"ע 48 שעות לימוד).

שלב #4: תחקיר, הפקת לקחים וסגירת אירוע

נושאים נלמדים - ניהול ורישום אירועי אבטחת מידע (Audit),המשכיות עסקית (BCP/DRP) **,** (סה"כ בהיקף שוו"ע 16 שעות לימוד).

ימים רביעי וחמישי בשבוע האחרון יושקעו במבחן סופי של הקורס שיהיה במתכונת של סימולטור מעשי לתרגול כל מה שנלמד בקורס.

מתכונת התוכנית?

הלימודים מתקיימים במתכונת של יום שלם במשך 3 שבועות באופן מאד אינטנסיבי:

<u>שבוע מס' 1</u> -08:30-19:00

19:00 – 22:00 תרגולים/חזרות/למידה עצמית עם מרצה מלווה (שעות תרגול).

<u>שבוע מס' 2</u> - 08:30- 16:30

בערב בכל יום בשעות 17:00-2300 יועבר קורס הכנה להסמכה בינלאומית מקבילה מוכרת כ"קפסולה" מלאה באנגלית <u>(בתשלום נוסף למעוניינים לרכוש גם את ההסמכה הבינלאומית)</u>.

<u>שבוע מס' 3</u> – 08:30-19:00

19:00 – 22:00 יהיו תרגולים/חזרות/למידה עצמית עם מרצה מלווה (שעות תרגול).