מבוא ל- CISO

קורס 71550 – 56 שעות

אודות הקורס

בעולם בו מערכות המחשוב הפכו לחלק בלתי נפרד מחיינו, בעולם בו פגיעה במערכות מחשוב גורמות לנזקים פיננסים בחברות תחום הגנת המידע הפך להיות תחום פעילות בעל חשיבות עליונה עבור כל חברה. מטרתה של הגנת המידע היא להגן על המערכות הממוחשבות מפני כל הסיכונים האפשריים העלולים לאיים עליהן. בהגנת המידע יש להתחשב בשלושה גורמים עיקריים: חיסיון המידע, זמינות המידע ואמינות המידע.

מטרות הקורס

- מטרת הקורס להקנות למשתתפים את הכלים הניהוליים והטכנולוגים בעולם הגנת המידע, להסביר את עקרונות הגנת המידע, תקני אבטחת המידע הנהוגים העולם ובארץ ואת הטופולוגיות אשר משתמשים בהם בהגנת המידע,

קהל יעד

- הקורס מיועד לבעלי רקע מעמיק ברשתות Windows או Linux ותקשורת, מנהלי מערכות מידע, יועצי אבטחת מידע ומבקרי מערכות מידע או לבעלי רקע בפתוח תוכנה.

דרישות קדם

- ידע ברשתות תקשורת
- ידע במערכות הפעלה

או

- ידע בפיתוח תוכנה

תכני הקורס

יעדי אבטחת מידע CIA:

- עקרונות הגנה על מידע ומטרות אבטחת המידע: חשאיות, שלמות וזמינות.
- דוגמאות לאירועים מרכזיים בעולם האבטחה והגדרות מושגים בסיסיים בתחום.

מדיניות אבטחת מידע

- סיווג מידע. תפקידים בצוות אבטחת מידע. עקרונות לקביעת מדיניות. סוגים של מדיניות -CISO. , מדיניות אבטחת מידע ככלי להשגת יעדי ה
- דוגמאות למדיניות בארץ ובעולם ISO, . מדיניות לפי תקן
- תרגיל עבודה בקבוצות: כתיבת מדיניות אבטחה

תכנית עבודה ל -CISO

- הגדרת פרוייקטים באבטחת מידע וניהולם בתכנית עבודה שנתית
- הכנה לביקורת ,ניהול הרשאות ,מיפוי נכסים ,ניטור ,פיתוח מאובטח,ניתוח סיכונים ,ועוד.

בקרת גישה

- עקרונות בקרת גישה AAA
- אימות הרשאות ו- accountability
- אמצעים ובקרות ליישום בקרת גישה בארגונים ,דוגמאות עם Active Directory

תקן אבטחת מידע ISO 27001

- סקירת תקן ISO 27001 כתקן אבטחה ארגוני ומסגרת לביקורת אבטחת מידע
- הכנת הארגון לביקורת ISO
- הטמעת שיפור מתמיד

תקן PCI

- סקירת תקן PCI כתקן אבטחה טכנולוגי המחויב ע"י חברות אשראי
- הכנה לביקורת PCI, מו"מ עם המבקר
- כלים טכניים לבדיקות

SANS Top 20

- SANS 20 של Critical Controls כתקן חדש עם דגש על תוצאות וצמצום סיכונים ע"י יישום מספר קטן של בקרות אשר יעילותן הוכחה בארגונים רבים.

OWASP

- סקירת תקן OWASP כתקן מוביל בעולם ה – Web ובעולם הפיתוח המאובטח
- הטמעת פיתוח מאובטח בארגון ובחינת ספקים לפי הערכת אבטחת תהליך הפיתוח שלהם.

מודלים לניתוח איומים

- סקירת מודלים לניתוח איומים כגון STRIDE ו- DREAD
- היכרות עם איומים לפי מודל CVE, CWE, מודיעין סייבר
- היכרות עם כלים לניתוח איומים.

ניהול סיכונים

- אסטרטגיות לניהול סיכונים ,קביעת מדיניות סיכונים ,גיוס תמיכה בארגון ,בחירת אמצעים לפי שיקולי עלות מול תועלת ,ניהול סיכוני ספקים.

הגורם האנושי

- הגורם האנושי כחולייה החלשה בשרשת האבטחה
- דוגמאות להתקפות אפשריות של עובדים וספקים
- שילוב של משאבי אנוש במדיניות האבטחה
- סיווג עובדים לפי רמת סיכון

הדרכת עובדים והעלאת רמת המודעות

- הדרכה כאמצעי הגנה
- שיטות להעלאת המודעות אל עובדים
- התאמת ההדרכה לסוגי תפקידים בארגון
- תרגיל בקבוצות :העלאת רמת המודעות.

הערכות לשעת חירום/המשכיות עסקית

- מבוא ל- BCP/DRP
- אמצעי שרידות והמשכיות עסקית
- התקפות DDOS
- מדיניות ונהלי תגובה וטיפול באירועי
- גיבוי כאמצעי התאוששות

טכנולוגיות באבטחת מידע

- היכרות עם טכנולוגיות לסינון מידור ,זיהוי חריגות ,הצפנה:
  - VLAN
  - WAF
  - Proxy
  - Firewall
  - אנטי וירוס
  - DLP
  - IDP/IPS