עמידות סייבר

קורס עמידות סייבר למקצועני המשכיות עסקית

משך: 4.5 ימים (4 ימי הדרכה מלאים בין השעות 08:30-17:00), שלאחריהם חצי יום של בחינה בנושא עמידות סייבר (08:30-12:00)

תיאור

ארגונים נדרשים כיום להתמודד עם מגוון רחב של מתקפות סייבר, וארגונכם אינו יוצא מן הכלל. קיימות אינספור דרכים ושיטות שבהם האקרים יכולים לעשות שימוש על מנת לפגוע בארגון. למול המתקפות נדרשת תגובה מתאימה מצד הארגון. קורס עמידות סייבר למומחי המשכיות העסקית הנו קורס בן ארבעה וחצי ימים, המלמד כיצד ניתן לטפל בשיבושים הנובעים ממתקפות סייבר במסגרת ההמשכיות העסקית של הארגון.

הקורס יסייע לכם להבין מדוע חייבים לשלב בין המשכיות עסקית לאבטחת סייבר, וכיצד לבצע זאת, בכל ארגון, תוך שימוש בחמשת האלמנטים של עמידות סייבר: הערכה / זיהוי, הגנה, גילוי, תגובה והתאוששות. מושגים אלה ותוכניות הפעולה הנובעות מהן יסייעו בפיתוח אסטרטגיה לתגובה יעילה למול אירועים בלתי צפויים, ותאפשר לארגונכם לפעול במהירות לשם התמודדות מיטבית עם שיבושים שנגרמו. אבטחת סייבר והמשכיות עסקית חייבים להיות משולבים יחדיו. קורס זה מלמד מהם הצעדים שיש לנקוט על מנת שהדבר יקרה גם בארגונכם. השילוב בין אבטחת סייבר להמשכיות עסקית ייעל את הזיהוי והתגובה למתקפות סייבר ולזליגת מידע, ימזער עלויות, יגן על המוניטין של הארגון ויעניק לכם את הידע והכישורים להתמודד עם אירועי סייבר בראיית ההמשכיות העסקית של הארגון.

מטרות

1. לספק ללומדים הוראות מפורטות, מסגרת, והנחייה ליישום המושגים החיוניים לשילוב בין אבטחת סייבר להמשכיות עסקית לשם יצירת תכנית עמידות סייבר אפקטיבית.
2. לתת בידי התלמידים כלים שיאפשרו להם להציג להנהלת הארגון המלצות מקצועיות (בעלות ערך) ואשר יסייעו בשכנוע ההנהלה להשקיע בבניית תכנית עמידות סייבר הולמת.
3. תרגול הלומדים בתרגילי סייבר/המשכיות עסקית לשם העמקת ההבנה בנושאים עימם נדרש להתמודד.
4. שיתוף ידע עם מומחי המשכיות עסקית אחרים.
5. הכנה לבחינת עמידות סייבר, לשם קבלת ההסמכה מומחה עמידות סייבר (Certified Cyber Resilience Professional) של DRI International.

מתווה הקורס

יום 1

- הצגת המושג עמידות סייבר
- סוגי אירועי איום
- כיצד אירועי סייבר משפיעים על המשכיות עסקית
- שילוב אבטחת סייבר בהמשכיות העסקית
- שיקולים ארגוניים
- עליית מדרגה מאבטחת סייבר והמשכיות עסקית להשגת עמידות סייבר

יום 2

- פיתוח תכנית אפקטיבית לתגובה לאירועים
- כיצד לשלב בין התכנון של אבטחת הסייבר וזה של ההמשכיות העסקית
- תכנון אסטרטגיות להפחתת נזק במקרה של אירוע אבטחת סייבר
- זיהוי פעילויות IT קריטיות והערכת ההשפעות של פגיעה בהן על הארגון
- פירוט אסטרטגיות התאוששות חיוניות שיאפשרו אישוש הטכנולוגיות והמשכיות הפעילות של תהליכים חיוניים לארגון
- יתרונות בזיהוי סיכוני סייבר ושילובם וניהולם במסגרת תכנית כלל ארגונית

יום 3

- יצירת מסגרת אבטחת סייבר
- בחינת מסגרות סייבר עדכניות
- סקירת רגולציה קיימת לנושא הגנת סייבר (הגנה ודיווח)
- הסבר כיצד לפתח וליישם הגנות לתשתיות ושירותים טכנולוגיים במטרה להתמודד עם השפעות של מתקפת סייבר
- דיון כיצד לגלות ולנטר מתקפות רשת באמצעות גורמים שמזהים וזאת בכדי להבטיח יעילות של ההגנות
- הסבר לגבי חשיבות אימון מודעות לסייבר שיועבר באופן סדיר
- ניטור אירועי אבטחה פנימיים וקישורם לאיומים חיצוניים (בצוע קורלציה)

יום 4

- יצירת תכנית תגובה אפקטיבית
- כיצד לשחזר נתונים ושירותים שהושפעו במהלך התקפת סייבר
- הבנה כיצד אבטחת סייבר והמשכיות הארגון מסייעים בניהול המוניטין של הארגון
- ניטור אבטחת סייבר
- יצירת תכניות אפקטיביות לתקשורת בשעת משבר לאירועי סייבר
- רשימת המלצות להכנת ספקי מפתח למקרה של מתקפת סייבר
- דיון כיצד יש ליישם יוזמות אימון והגברת המודעות לשם שילוב אבטחת סייבר במסגרת הארגון ולהבטיח שהסגל מכיר את תכניות התגובה

שלום דוד
מנהל פעילות DRII בישראל
0504-916155
shalom@dri-israel.co.il

נורית דוד
מתאמת הדרכות DRII בישראל
0506-916156
nurit@dri-israel.co.il