



# מעבדה 4



CSRP

DFIR

## מבוא ל-DFIR בוחר מתודולוגיית DFIR

- עמוד 1 -

כל הזכויות שמורות © סיבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

## נושאי המעבדה

נתחו מספר תרחישי התקפה על ארגון, ובחרו במתודולוגיית ה-DFIR הטובה ביותר לכל תרחיש.

## זמן מוערך

20-30 דקות.

## סביבת המעבדה

- סביבה וכלים
  - כתבן

## משימת מעבדה:

ענו על השאלות הבאות והסבירו איזה סוג אירוע קרה ואיך לטפל בו. שימו לב שאין תשובות מוחלטות לתרגיל זה, התכלית של מעבדה זו היא לעודד חשיבה לוגית.

הסבירו וקטלגו כל אחד מהתרחישים הבאים. בכל תרחיש, תחשבו על מה צריך לעשות כדי לאסוף כמה שיותר מידע וכדי להתמודד עם האירוע. השאלות דורשות ממכם לחשוב "מחוז לקופסה".

### תרחיש א'

אדם קורא לצוות האבטחה בחברה גדולה, אומר שהוא ממחלקת ה-IT, ואומר שהוא צריך להתחבר למחשב ספציפי כדי לעדכן משהו. קצין האבטחה בודק עם מחלקת ה-IT אם מי שהתקשר הוא עובד החברה, ומגלה כי הוא לא חלק מהחברה.

הקצין מדווח את האירוע לצוות ה-IR כשהאדם שהתקשר עדיין על הקו.

- 1 לאיזו קטגוריה ניתן לשייך את אירוע זה?
- 2 אילו צעדים ניתן לנקוט כדי להשיג מידע נוסף אודות ההתקפה?
- 3 אילו צעדים ניתן לנקוט כדי לטפל באירוע?

### תרחיש ב'

צוות ה-NOC של חברה מקבל התרעה שאתר החברה שונה לפוסטר תעמולת בחירות, כנראה עבודה של כמה האקרים אקטיביסטיים (hacktivists). צוות ה-NOC מדווח על האירוע לצוות ה-IR.

- 1 לאיזו קטגוריה ניתן לשייך את אירוע זה?
- 2 אילו צעדים ניתן לנקוט כדי להשיג מידע נוסף אודות ההתקפה?
- 3 אילו צעדים ניתן לנקוט כדי לטפל באירוע?

## תרחיש ג'

רועי מקבל אימייל מחברתו לעבודה יערה, עם קישור שנראה חשוד. כאשר הוא שואל את יערה לגבי האימייל, היא אומרת שהיא לא שלחה אותו, ואינה יודעת איך השתמשו במייל שלה. רועי ויערה יוצרים קשר עם צוות ה-IR ומודיעים להם לגבי האירוע.

- 1 לאיזו קטגוריה ניתן לשייך את אירוע זה?
- 2 אילו צעדים ניתן לנקוט כדי להשיג מידע נוסף אודות ההתקפה?
- 3 אילו צעדים ניתן לנקוט כדי לטפל באירוע?