



מעבדה 7



CSRP

DFIR

מבוא ל-DFIR תכנית תגובה לאירועים

- עמוד 1 -

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

נושאי המעבדה



תרגלו כיצד ליצור תכנית תגובה לאירוע עבור התרעות שונות.

זמן מוערך



20-30 דקות.

סביבת המעבדה



● כתבן

משימת מעבדה:

כתובו תכנית תגובה לאירוע לארבעת השלבים הראשונים:

- הכנה
- זיהוי
- הכלה
- חיסול

כללו לפחות שלוש דוגמאות לכל שלב, בתרחישים הבאים:

- 1 עובד מקבל מייל זדוני עם תוכנה זדונית עליו.
- 2 האקר מבצע התקפת השחתה על אתר החברה, בה תוכן/נראות האתר שונתה.