



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



תרגל 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.

פתרון:

הכנה:

- אמנו עובדים שלא לפתוח מיילים ממקורות שהם לא מכירים.
- צרו Blacklist של שולחים זדוניים ולחסום אותם.
- צרו Whitelist של הרחבות קבצים שמותר לקבל אותם.

זיהוי:

- צרו dashboard שמראה את שולחי המיילים המובילים בארגון.
- תנו לעובדים לפנות ל-SOC ולהודיע להם לגבי אימיילים ותוכנות זדוניות כאלו.
- צרו התרעות של תקשורת חשודה עבור המו"פ.

הכלה:

- בודדו עמדות עבודה נגועות.
- שמרו את יומני האירוע.
- חקרו את האירועים ולחלץ IOCs (indicators of compromise) – סימנים של פגיעה).
- בדקו אם מחשבים נוספים קיבלו את אותה ההודעה.
- מחקו את האימייל הזדוני מתיבות הדואר הנכנס של העובדים.

חיסול:

- אם נמצאה חולשה או פגיעות, תקנו אותה.
- מחקו את התוכנה הזדונית מהמחשב.
- שחזרו את המערכת מהגיבוי, אם יש צורך בכך.

2 האקר מבצע התקפת השחתה (defacement) על אתר החברה, בה תוכן/נראות האתר שונתה.

פתרון:

הכנה:

- צרו גיבוי של האתר.
- התקינו IDS/IPS/WAF כדי לזהות ולהתגונן מפני בקשות זדוניות.
- הורידו כלים ייעודיים שמפקחים על שינויים בדפי הרשת.
- צרו Dashboard שבודק בקשות URL חריגות.

זיהוי:

- כלי פיקוח שמתריע כשקורה שינוי.
- עובד מזהה שינוי באתר.
- ה-dashboards מזהה בקשת URL חריגה.

הכלה:

- צרו Blacklist של שולחים זדוניים ולחסום אותם.
- השתמשו ביומנים כדי לזהות איך השינויים נעשו.
- נתבו תעבורה לשרתים כושלים (failover) או כבו את שרת הייצור.
- גבו את השרת למטרות Forensics.

חיסול:

- תקינו את הקוד האחראי לפגיעות.
- חסמו את כתובת ה-IP שביצעה את ההתקפה.
- הסרירו את הדף/סקריפט הזדוני.