



מעבדה 1



CSRP

DFIR

מבוא ל-DFIR

איתור תכניות Startup

- עמוד 1 -

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

נושאי המעבדה

השג ראיות בנוגע לגבי התוכניות המופעלות בעת הפעלת המחשב שלך.

זמן מוערך

10-15 דקות.

סביבת המעבדה

- Windows ○
- Sysinternals ○

משימת מעבדה:

נסו למצוא ראיות של תכניות מתמשכות באמצעות היישום Autoruns הכלול בערכת הכלים של Sysinternals.

- 1 הורידו והתקן Autoruns מהקישור הבא:
<https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>
- 2 השתמשו ב-Autoruns כדי למצוא תכניות המסומנות לביצוע, אך אינן מותקנות עוד.
- 3 מצאו registry keys שמאחסנים מיקומי startup (לפחות שלושה keys).
- 4 שימו לב: שה-keys יכולים להשתנות, תלוי באיזו גרסת מערכת הפעלה משתמשים. מצאו תיקיות במיקומי ה-startup.
- 5 בדקו אם "Not Verified" מופיע בטור ה-Publisher של יישום כלשהו.