
אבטחת נקודת קצה



CYBER SCHOOL



שיעור זה מציג פתרונות אבטחת נקודות קצה, אופן פעולתם וכיצד ליצור כללים לאיתור יישומים זדוניים בנקודות קצה.

מבוא לאבטחת רשת ונקודת קצה

תקלות וסיכונים





CYBER SCHOOL

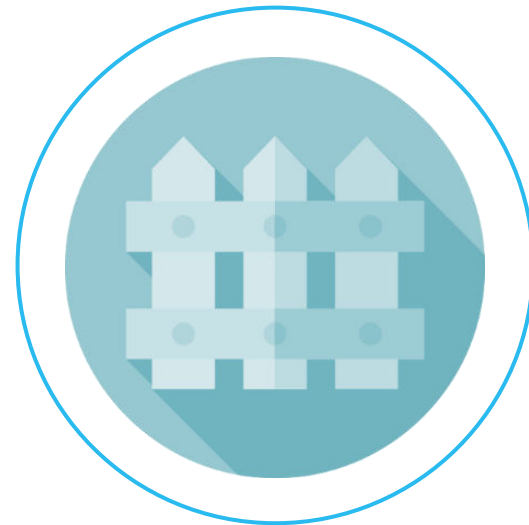
אבטחת נקודת קצה

מבוא לאבטחת רשת ונקודת קצה

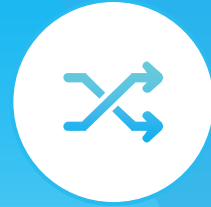
מה הוא פתרון אבטחת נקודת קצה?



מערכת כלים שמסייעת להגן על תחנות עבודה
מאבטחת מכשירים של משתמשי קצה (מחשבי שולחן,
מחשבים ניידים)
מספקת הגנה אקטיבית נגד פעילות מסוכנת ו/או
מתקפות זדוניות
פועלת כמערכת היקפית של אבטחה ארגונית ומתאימה
ביותר ל-BYOD



חבילת אבטחת נקודת קצה



הצפנת תקשורת	אנטי-וירוס
דוא"ל והגנה מפני דיוג	מניעת אובדן נתונים (DLP)
רישום וניטור	בקרת יישום/ניהול רשימות היתרים
תקשורת וחומרה מוצפנות	מערכת למניעת חדירות/גילוי מארח (HIPS/HIDS)

אנטי-וירוס -מבט מקרוב: סריקה



חתימות מחרוזת/בייט



חתימות Hash



זיהוי היוריסטי



ספקים נפוצים



Symantec
Endpoint
Protection



Check Point
Endpoint
Security



Kaspersky
Endpoint
Security



McAfee
Endpoint
Protection



CYBER SCHOOL

סריקת אנטי-וירוס מרובת מנועים



יש להתקין רק AV אחד בתחנת עבודה.
מכשירי AV שונים, מתודולוגיות ורשימות חסימות שונות
סריקה עם מספר מנועים במקביל





CYBER SCHOOL

אבטחת נקודת קצה

תקלות וסיכונים

הגדרה של False (Positive (F/P



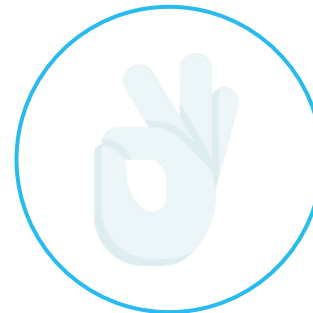
False Positive

תוצאת בדיקה המעידה בטעות על קיומו של מצב.



False Negative

תוצאת בדיקה השוללת בטעות על קיומו של מצב.



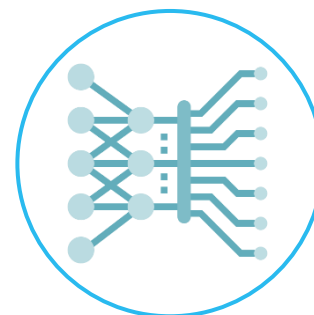
גורמים של False Positive (F/P)



היוריסטיקה: האנטי וירוסים מתפתחים, וכך גם היורוסים.



ניתוח התנהגותי: יישומים לגיטימיים המתנהגים כמו יישומים זדוניים

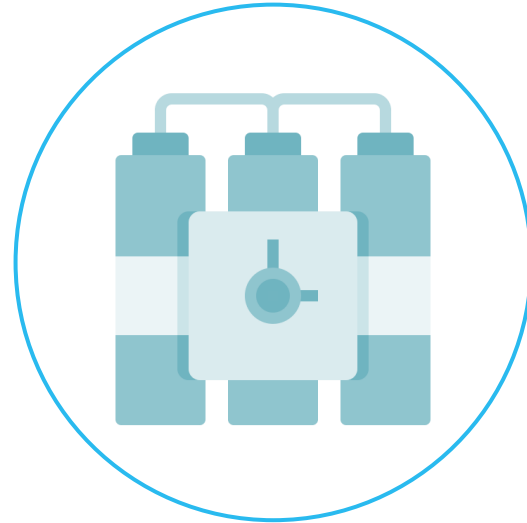


למידת מכונה: טעויות בנתוני ההכשרה המוזנים לתוכנה





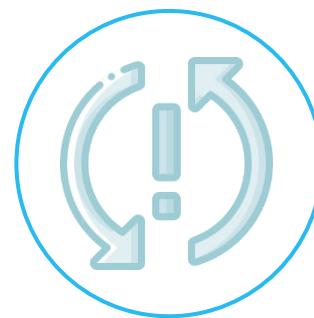
פגם חדש שהתגלה בתוכנית
מנוצל לפני שלספק יש הזדמנות לתקן אותו
פגמים של יום אפס מבוקשים מאוד הן על ידי
האקרים (עבירות) והן על צוותי אבטחה ארגונית
(הגנה).



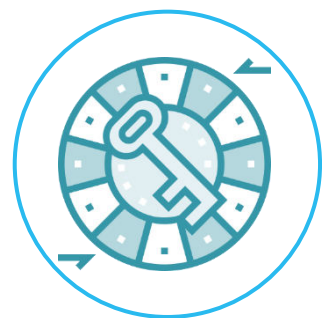
שיטות לעקיפת אנטי וירוס



מוטציית קוד



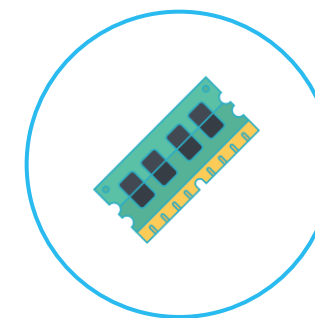
השבתת עדכוני
אנטי וירוס



אריזה והצפנה



טכניקות
התגנבות



מתקפה
נטולת קבצים



מעבדה - עקיפת אנטי-וירוס



20-30 דקות

המשימה

יש להוריד קבצי EICAR ולהצפין אותם כדי למנוע זיהוי על ידי סורקי VirusTotal.

השלבים

- יש להוריד את קבצי ה-EICAR.
- יש לסרוק אותם באמצעות VirusTotal.
- יש להצפין את הקבצים ולסרוק אותם שוב.

כלים

Windows 10
WinRAR

קבצים קשורים

[eicarcom2.zip](#) < מסמך מעבדה <
[eicar.com](#) < [eicar_com.zip](#) <



CYBER SCHOOL

אבטחת נקודת קצה



שאלות