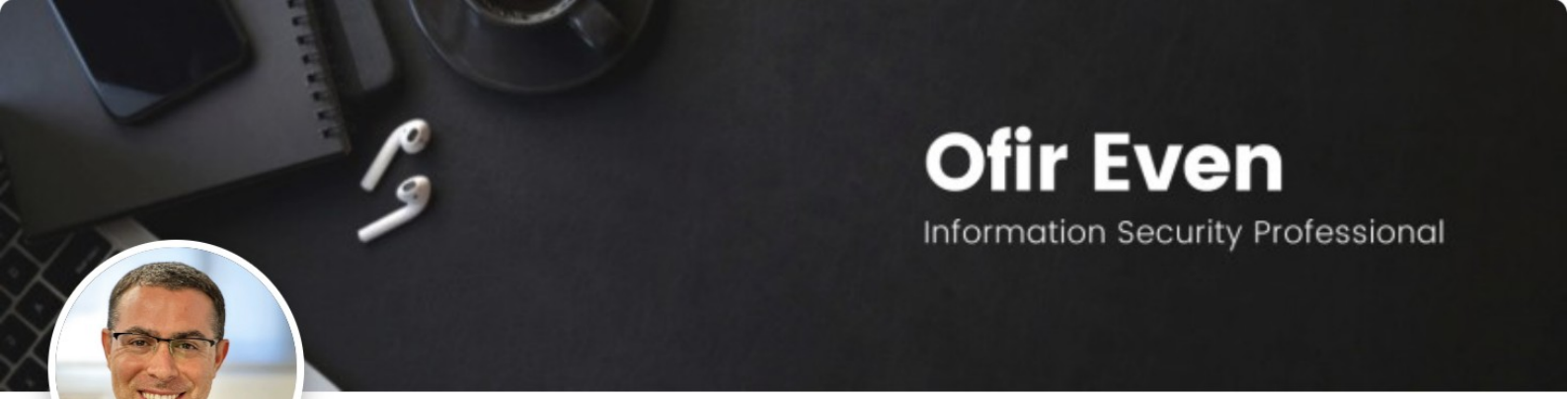

Ofir Even
CISO at Citadel | Cybersecurity Professional | OfirEven.com
X-CCNP | ISC2 - Certified in Cybersecurity

צ׳קליסט הקשחת כלים ותשתיות קריטיות לארגונים

(רכיבי גיבוי EDR, RMM, DFIR, API, Backup ועוד..)

🔑 הרשאות, גישה וניהול שינויים

- העניקו לכלי הרשאות מינימליות בלבד (Least Privileged).
- בצעו בדיקה תקופתית: מי מחזיק גישה? אילו הרשאות יש בפועל?
- הסירו משתמשים/אינטגרציות לא רלוונטיים או לא פעילים.
- ודאו שכל שינוי בהרשאות, גישה או יצירת מפתחות API מתועד ונעשה אך ורק באמצעות Ticketing System מסודר (Jira, ServiceNow וכו׳), כולל אישורים, תיעוד ומעקב.
- מיפוי הרשאות: הגדירו עבור כל משתמש/אינטגרציה – מה מותר, לאיזה צורך, ולאיזה פרק זמן.
- הטמיעו אימות דו-שלבי (MFA) לכל חשבון ניהולי וממשק רגיש.

🔌 API ואינטגרציות חיצוניות

- בחנו את הצורך לכל מפתח API ואינטגרציה — הסירו כל מה שלא הכרחי.
- ודאו שלכל מפתח/אינטגרציה מוקצות רק ההרשאות ההכרחיות.
- בצעו רוטציה/החלפה תקופתית של מפתחות גישה, ומחקו מפתחות שלא בשימוש.

🔒 ניהול סיסמאות ושחזור

- ודאו שהממשק לשחזור סיסמה מאובטח: פרטי השחזור עדכניים, מוגנים, ואינם זמינים לגורמים לא מורשים.
- קבעו Session Timeout קצר יחסית – במיוחד בכלי ניהול מרכזיים.
- אכפו שימוש בסיסמאות חזקות, כולל חידוש תקופתי ואכיפת מורכבות.

🛡️ ניטור, לוגים והתראות

- הפעילו לוגים על כל גישה, פעולה ושינוי מהותי.
- שלחו את הלוגים ל-SIEM/אחסון מרוחק, לא לוקאלי בלבד!
- ודאו שהתרעות קריטיות נשלחות גם לרשימת תפוצה ייעודית — ובדקו שהמנגנון פועל בפועל (ולא רק מוגדר תאורטית!).
- קבעו התראות על:
  - גישה/שימוש חריג (שעה, מדינה, פרוטוקול)
  - שינוי בהרשאות אדמיניסטרטור
  - ניסיונות שחזור/איפוס לא שגרתיים

⚙️ הגדרות, תפעול ובקרות

- עברו על כל הגדרות הכלים – חפשו "דלתות פתוחות" ופרצות ב-Default.
- הגבילו גישה לממשקי ניהול רק מכתובות IP של הארגון או מרשתות VPN מאובטחות.
- בטלו גישה מרחוק (Remote Access) ככל שניתן – והפעילו אותה רק במקרי צורך מוגדרים ומבוקרים.
- השביתו פיצ'רים מיותרים/שאינם נדרשים.
- הקפידו על עדכוני אבטחה שוטפים; בצעו ידנית כשאין Auto-Update.
- תעדו כל שימוש ביכולות חריגות (למשל: חקירה, שליפה, ניטור רוחבי).

📑 תחקור, ביקורת ובדיקות

- הגדירו נוהל ברור להפעלת כלים רוחביים בזמן אירוע – מי? מתי? איך?
- בצעו Audit רבעוני/חצי שנתי לכלל מערכות הניהול:
  - עברו על הלוגים
  - בדקו היסטוריית הרשאות
  - אשרו/סגרו הרשאות זמניות/מיוחדות
- תרגלו תרחישי תקיפה וניצול של כלים לגיטימיים (Living Off the Land) – תעדו ושפרו בהתאם.

🔭 רישום ל-Security Advisories

- הירשמו לעדכוני אבטחה ועדכוני גרסאות של היצרנים לכל הכלים הקריטיים.
- פעלו מיידית בהתאם להמלצות שמתקבלות ב-Advisories.
- בצעו תיעוד לכל שינוי או עדכון בעקבות Advisory.

☝🏻 אל תסמכו "על אוטומט" >>

- גם הכלי הכי בטוח הופך לסיכון בקלות; כשמפסיקים לבדוק, לבקר ולעקוב.

❤️ **אהבתם את המסמך ?** עזרתי לכם במשימה ?

- עקבו אחריי ב – LinkedIn ופרגנו בתגובות 🙏🏻