## השוואת תכונות מלאה: Velociraptor לעומת Trellix Endpoint Security HX (לסביבה מקומית)

### 🔧 פריסה והתקנה

| תכונה | Velociraptor | Trellix Endpoint Security HX | הסבר |
| --- | --- | --- | --- |
| תמיכה בסביבה מקומית | ✅ נתמך באופן מלא | ✅ נתמך באופן מלא | האם ניתן לפרוס ולנהל את המוצר כולו בתוך הארגון ללא תלות בענן? |
| מתאים לרשת מנותקת (Air-Gap) | ✅ כן, לא דורש אינטרנט | ✅ כן, אך דורש עדכונים ידניים | האם הכלי פועל ללא חיבור לאינטרנט? |
| סוכן נדרש | ✅ סוכן קל משקל | ✅ סוכן HX | האם נדרש סוכן מקומי במחשבי הקצה? |
| משאבי מערכת | 🟢 מאוד קל | 🔴 צורך גבוה במשאבים | כמה משאבים (CPU/RAM) דורש הסוכן? |
| מורכבות התקנת השרת | ⚠️ בינונית | ⚠️ בינונית-גבוהה | כמה מורכב להקים את השרתים (DB, UI וכו’)? |
| תמיכה במערכות הפעלה | Windows, Linux, macOS | בעיקר Windows, תמיכה חלקית ב-Linux | אילו מערכות הפעלה נתמכות? |
| עדכונים אוטומטיים | ❌ לא, רק ידני | ✅ כן (עם ePO או קבצים ידניים) | האם ניתן לעדכן את המערכת והחתימות בצורה אוטומטית? |
| תמיכה בריבוי לקוחות | ⚠️ בעייתי | ✅ נתמך מובנה | האם ניתן לתחזק מספר מחלקות או ארגונים באותה מערכת? |
| אינטגרציה עם Active Directory | ⚠️ ידנית | ✅ מלאה דרך ePO/HX Server | האם הכלי משתלב עם AD? |
| ניהול הרשאות משתמשים | ✅ כן | ✅ כן | האם ניתן לנהל הרשאות לפי תפקידים? |
| הגנה עצמית של הסוכן | ❌ לא | ✅ כן | האם ניתן למנוע השבתת הסוכן ע”י תוקף? |

### 🔍 גילוי וציד איומים

| תכונה | Velociraptor | Trellix Endpoint Security HX | הסבר |
| --- | --- | --- | --- |
| מנוע ציד איומים | ✅ שפת VQL מותאמת | ✅ שפת שאילתות HX | באיזו שפה/כלים משתמשים לציד איומים? |
| זיהוי IOC בזמן אמת | ✅ ידני (IOC/YARA) | ✅ כן, כולל חוקים פנימיים | האם ניתן לזהות אינדיקטורים של תקיפה בזמן אמת? |
| זיהוי התנהגותי | ❌ אין, רק ידני | ✅ כן (EDR מובנה) | האם הכלי מזהה התנהגות חשודה כמו תהליכים חריגים? |
| זיהוי תקיפות ללא קבצים | ⚠️ אפשרי עם סקריפטים | ✅ כן | האם הכלי מזהה תקיפות שמבוצעות רק בזיכרון או PowerShell? |
| מיפוי למטריצת MITRE | ⚠️ דורש הגדרה ידנית | ✅ כן | האם הכלי ממפה איומים לפי מסגרת ATT&CK? |
| אינטגרציה עם מודיעין איומים | ❌ לא | ✅ כן, דורש עדכון ידני | האם יש מודיעין איומים מובנה או ניתן לשילוב? |
| תמיכה ב-YARA | ✅ כן | ⚠️ חלקית | האם ניתן להשתמש בחוקי YARA? |
| תמיכה ב-IOC מותאם | ✅ כן (קבצים, דומיינים וכו’) | ✅ כן (רשימות או חוקים) | האם ניתן להזין IOC ידני לזיהוי? |
| בניית ציר זמן | ✅ כן (אירועים, לוגים, prefetch וכו’) | ⚠️ חלקי | האם ניתן לבנות ציר זמן של פעילות חשודה? |
| ניתוח לוגים | ✅ כן | ⚠️ מוגבל | האם הכלי מאפשר חיפוש ולמידה מלוגים חיים? |

### 🧪 תגובה וחקירה

| תכונה | Velociraptor | Trellix Endpoint Security HX | הסבר |
| --- | --- | --- | --- |
| הרצת פקודות מרחוק | ✅ כן | ✅ כן | האם ניתן להריץ פקודות על תחנות קצה מרחוק? |
| העברת קבצים | ✅ כן | ✅ כן | האם ניתן להעלות ולהוריד קבצים מהתחנה? |
| ניתוק התחנה מהרשת | ⚠️ אפשרי עם סקריפטים | ✅ כן, תכונה מובנית | האם ניתן לנתק תחנה שנמצאה חשודה מהרשת? |
| גישה לרג’יסטרי | ✅ כן | ✅ כן | האם הכלי תומך בקריאת ועריכת הרג’יסטרי? |
| ניתוח זיכרון חי | ✅ חזק מאוד | ⚠️ חלקי | האם ניתן לאסוף ולנתח זיכרון מהרצה חיה? |
| תהליכים ומשימות מתוזמנות | ✅ כן | ✅ כן | האם הכלי מאפשר סקירת services, jobs וכו’? |

### 📊 ניהול ואינטגרציה

| תכונה | Velociraptor | Trellix Endpoint Security HX | הסבר |
| --- | --- | --- | --- |
| ממשק ניהול אינטרנטי | ✅ בסיסי | ✅ מתקדם (כולל ePO) | האם יש UI גרפי לניהול? |
| API ואוטומציה | ✅ API מלא (REST) | ✅ כן, מוגבל | האם ניתן לחבר לכלים אחרים או לאוטומציה? |
| שילוב עם SIEM | ✅ Webhook או JSON | ✅ Syslog ו-ePO | האם ניתן לשלוח נתונים ל-SIEM כמו Splunk או Elastic? |
| מערכת התראות | ⚠️ דורש סקריפטים | ✅ כן, תכונה מובנית | האם הכלי שולח התראות בזמן אמת? |
| הפקת דוחות | ⚠️ בסיסי | ✅ כן, מובנה | האם יש יכולת להפיק דוחות מתוך המערכת? |
| דשבורדים וטרנדים | ⚠️ מצריך תוספים | ✅ כן, מובנה | האם יש דשבורדים להצגת נתונים וסטטיסטיקות? |

### 🛠 תחזוקה ותמיכה

| תכונה | Velociraptor | Trellix Endpoint Security HX | הסבר |
| --- | --- | --- | --- |
| תמיכה טכנית | ❌ קהילה בלבד | ✅ תמיכה רשמית Trellix | האם יש תמיכה רשמית מהספק? |
| קהילה ודוקומנטציה | ✅ חזקה מאוד (GitHub, Discord) | ⚠️ מוגבלת | האם יש פורומים, מדריכים, מדריכי משתמש? |
| מודל רישוי | ✅ קוד פתוח, חינם | ❌ דורש רישוי מסחרי | האם המוצר בתשלום או חינמי? |
| עדכונים ברשת מנותקת | ✅ תומך ברשת מנותקת | ✅ נתמך עם עדכונים ידניים | האם אפשר לעדכן את המערכת ללא חיבור לאינטרנט? |

### 📋 המלצות לפי שימוש

| שימוש/צורך | הכלי המומלץ |
| --- | --- |
| ציד איומים גמיש וקל משקל | ✅ Velociraptor |
| גילוי התנהגות בזמן אמת | ✅ Trellix HX |
| חקירה מלאה ברשת מנותקת | ✅ Velociraptor |
| EDR מבוסס מודיעין איומים | ✅ Trellix HX |
| SOC עם תקציב מוגבל | ✅ Velociraptor |
| ניהול GUI מלא בארגון | ✅ Trellix HX |
| תגובה אוטומטית וסקריפטים מותאמים | ✅ Velociraptor |
| מערך הגנה ארגוני מתקדם | ✅ Trellix HX |