



# INSPECT

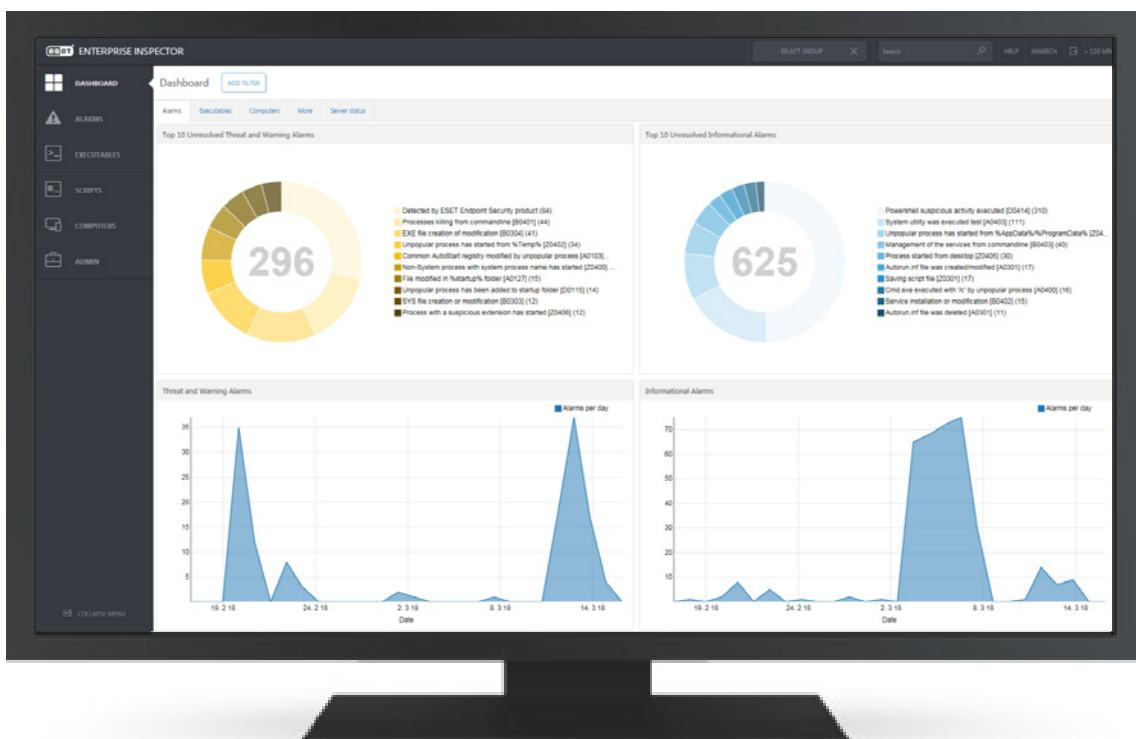
הבטיחו נראות מלאה וטיפול באירועי אבטחה  
בזמן אמת באמצעות ה-EDR של ESET

Progress. Protected.

# מהו פתרון זיהוי ותגובה לתחנות קצה (EDR)?

**ESET INSPECT** הוא כלי EDR מתוחכם המשמש לזיהוי התנהגויות חריגות ופריצות, הערכת סיכונים, תגובה לאירועים, תחקור וטיפול לאחר אירועי אבטחה.

הוא מנטר ומעריך את כל הפעילויות שקורות ברשת (כמו שינויים החלים במשתמשים, קבצים, תהליכים, ערכי Registry, זיכרון ורשת) בזמן אמת ומאפשר לכם לנקוט בפעולה מיידית בזמן אמת במידת הצורך.



# מדוע יש צורך בפתרון זיהוי ותגובה לתחנות קצה?

## דליפות מידע

חברות לא יכולות להסתפק רק בזיהוי של דליפת מידע - הן חייבות להכיל את אירוע האבטחה ולטפל בנזקים שגרם. את כל אלו יש לעשות בדיוק המירבי ומבלי לגרום להפרעה להמשכיות העסקית. רוב העסקים אינם ערוכים לביצוע תחקור, ובמקום זאת הם שוכרים את שירותיו של ספק חיצוני שסייע בכך. כיום ארגונים זקוקים לנראות מלאה של רשת המחשבים שברשותם כדי להבטיח שאיומים חדשים, התנהגות בעייתית של עובדים ותוכנות לא רצויות לא יסכנו את רווחי החברה והמוניטין שלה. התעשיות העיקריות שסובלות מדליפות מידע הן חברות שמחזיקות במידע יקר ערך, כמו חברות פיננסיות, סיטונאות, ספקי שירותי בריאות וחברות במגזר הציבורי. זה לא אומר שיתר ענפי התעשייה בטוחים - זה רק אומר שבדרך כלל האקרים בוחנים את יחס העלות-תועלת של תקיפותיהם.

## מאמץ תקיפה מתמיד (APT) ומתקפות ממוקדות

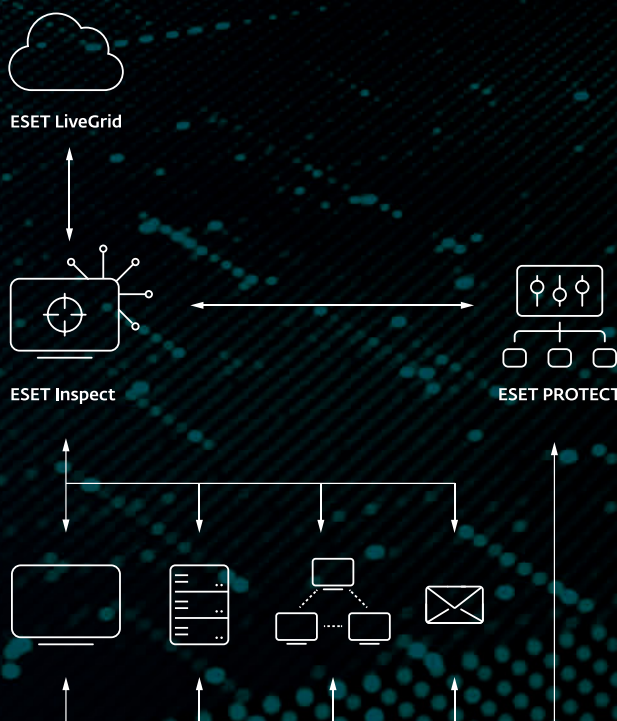
מערכות EDR משמשות בדרך כלל למטרות הבאות: זיהוי איומי APT (מאמץ תקיפה מתמיד) או מתקפות ממוקדות באמצעות ניטור איומים; הפחתת זמן התגובה לתקרית; מניעה פרואקטיבית של מתקפות עתידיות. חשיפת איומי מאמץ תקיפה מתמיד היא חשובה במיוחד לעסקים גדולים, שכן רוב העסקים כיום אינם חשים מוכנים מול המתקפות החדשות ביותר, שיכולות להימשך ברשת במשך ימים ואף חודשים מבלי שיזוהו.

מספק זיהוי ייחודי מבוסס התנהגות ומוניטין, נראות וניטור מלא לצוותי אבטחת המידע, המאפשר להם תגובה בזמן אמת על פי נתונים הנאספים מלמעלה מ-100 מיליון תחנות קצה המוגנות ע"י LiveGrid של ESET.

## נראות ושליטה מלאה על רשת הארגון

איומים פנימיים ומתקפות פשינג הן כאב ראש גדול לעסקים גדולים. מתקפות פשינג מופנות בעיקר לעסקים גדולים בשל מספר העובדים הגדול שיכולים לשמש כמטרות למתקפה. ישנו סיכוי טוב שאחד העובדים יבלע את הפיתיון ויסכן את הארגון כולו. מתקפות פנימיות הן איום נוסף שמאיים על עסקים גדולים, שכן מספר העובדים הגדול מגדיל את הסיכוי לכך שאחד מהם פועל בניגוד לאינטרסים של הארגון.

מערכות EDR מספקות את תוספת הניטור הנחוצה לארגונים כך שיוכלו לראות, להבין, לחסום ולטפל באירועי אבטחה בכל המכשירים המקושרים אליהם בזמן אמת. ESET Inspect יכול, למשל, לזהות ולעצור במהירות סקריפטים זדוניים שמסווים את עצמם כחלק ממסמך בלתי מזיק, כמו קובץ Word.



פתרון כולל המשלב מניעה, זיהוי ותגובה המאפשר ניתוח, בקרה וטיפול מהירים בכל בעיית אבטחה ברשת.

=

## ESET Endpoint Protection

הגנה רב שכבתית לתחנות הקצה, בה כל שכבה שולחת נתונים ל-ESET Inspect

+

## ESET Inspect

מערכת EDR מתוחכמת המנתחת כמויות עצומות של נתונים בזמן אמת כך שכל האיומים יזוהו.

כיום, ארגונים זקוקים לנראות וניטור של המחשבים ברשותם על מנת לוודא שאיומים חדשים, התנהגויות בעייתיות של עובדים ותוכנות לא-רצויות אינן מסכנות את הרווחים והמוניטין של החברה.

# למה ESET Inspect?

## סנכרון מלא

ESET Inspect, יושב על בסיס הגנת תחנות הקצה של ESET, יוצר מערכת גומלין עקבית שמאפשרת חיבור בין כל הפריטים הרלוונטיים וטיפול מסונכרן של נזקי אירועי האבטחה. צוות האבטחה יכול לעצור תהליכים הרצים במערכות, להוריד את הקובץ שגרם לזיהוי, או פשוט להפעיל מחדש מחשבים, לכבות אותם, לסרוק אותם או לבודד אותם מהרשת, כל זה ישירות מממשק הניהול.

## ארכיטקטורה פתוחה

ESET Inspect מספק זיהוי ייחודי מבוסס התנהגות ומוניטין, בנראות מלאה לצוותי האבטחה. כל הכללים נכתבים בפורמט XML הנפוץ, וניתן ליצור ולשנות אותם בקלות כך שיתאימו לצרכים הספציפיים של סביבות העבודה הארגוניות, ביניהם אינטגרציות SIEM.

## גישה מרחוק

ESET Inspect כולל יכולת להפעלת פקודות PowerShell מרחוק, שמאפשרת למנהלי האבטחה לבחון ולהגדיר מרחוק את המחשבים שבארגון שלהם, כך שיהיה ניתן לתת תגובה מתוחכמת למתקפה מבלי להפריע לרצף העבודה של המשתמשים.

## תאימות לסביבות מרובות פלטפורמות

ESET Inspect תומך במערכות הפעלה Windows, Linux, ו-MacOS. מה שהופך אותו לבחירה המושלמת לסביבות מרובות פלטפורמות.

## API ציבורי

ESET Inspect כולל API שמאפשר גישה לזיהויים וייצוא שלהם, יחד עם טיפול בזיהויים, מה שמאפשר אינטגרציה אפקטיבית עם SIEM, SOAR, כלי ניהול קריאות וכלים אחרים רבים.

## שליטה והתאמה לרגישות הזיהויים

התאם את הזיהויים בקלות באמצעות התאמה אישית של רגישות החוקים לקבוצות משתמשים שונות או למשתמשים שונים. שלבו בין קריטריונים כמו שם הקובץ, מיקומו, ערכי Hash, שורת פקודה וחותם כדי להתאים באופן מושלם את התנאים להפעלת הכללים.

## MITRE ATT&CK™

ESET Inspect יוצר התאמה בין הזיהויים שלו ובין המסגרת של MITRE ATT&CK™, שמספקת לכם את מידע מקיף על כל האיומים, גם המורכבים ביותר, בלחיצת כפתור.

## מערכת ניהול מוניטין

הסינון המקיף של ESET מאפשר למנהלי אבטחת המידע לסנן את כל התוכנות הידועות כבטוחות באמצעות שימוש במערכת המוניטין החזקה של ESET. מערכת המוניטין שלנו כוללת בסיס נתונים של מאות מיליוני קבצים הידועים כבטוחים, כך שצוותי האבטחה יקדישו את זמנם לזיהויים הלא מוכרים שעשויים להיות זדוניים במקום לכלות את זמנם על התראות שווא.

# מקרים לשימוש זיהוי איום לעומק – כופרה

## מקרה לדוגמה

עסק מעוניין בכלים נוספים לזיהוי פרואקטיבי של כופרות, ובנוסף מעוניין לקבל התראות אם נצפתה התנהגות הדומה להתנהגות של כופרה ברשת.

## פתרון

✓ הגדרת כללים לזיהוי תוכנות הרצות מתיקיות זמניות

✓ הגדרת כללים לזיהוי קבצי אופיס (Word, Excel, PowerPoint) כאשר הם מפעילים סקריפטים או קבצים ברי-הרצה נוספים.

✓ הגדירו התראה למקרה בו אחת מהסיומות הנפוצות של קושחות נראית באחד המכשירים.

✓ צפו בהתראות של Ransomware Shield מפתרונות האבטחה לתחנות קצה של ESET באותו ממשק הניהול.

כיום, כופרות מנסות לפעול ברשת מבלי להתגלות ולהפיץ את עצמן לכמה שיותר תחנות קצה ברשת. הן חודרות לגיבויי המכשירים כדי להבטיח שאפילו שחזור הגיבויים הקודמים לא ימנע את ההפעלה המוצלחת של הכופרה.

ESET Inspect מגדיל את הפונקציונליות של פתרונות ESET לאבטחת תחנות קצה ומאפשר לזהות באופן פרואקטיבי כופרות שאולי כבר קיימות ברשת הארגון. בתרחיש כופרה רגיל, משתמש מקבל הודעת דוא"ל שאליה מצורף מסמך. המשתמש פותח את מסמך ה-Word ומתבקש להריץ סקריפט מאקרו. לאחר שהמשתמש מריץ את סקריפט המאקרו, קובץ הרצה (EXE) מורד למערכת ומתחיל להצפין כל מה שהוא יכול, כולל כוננים ממופים.

ESET Inspect מאפשר לצוות האבטחה שלכם לקבל התראות להתנהגות כמו זו, ולאחר כמה לחיצות תוכלו לדעת מה הושפע מהכופרה, מתי ואיפה הופעלו קבצי הרצה (EXE), סקריפטים או פעולה זדונית אחרת, ולבצע תחקור וניתוח מעמיק.

The screenshot displays the ESET Protect & Inspect Cloud dashboard. On the left, a sidebar contains navigation options: DASHBOARDS, COMPUTERS, Detections, SEARCH, INCIDENTS, Favorites, Scripts, and Admin. The main area shows a 'Blocked by Anti-Phishing blacklist' alert for 'chrome.exe' (PE: Google Chrome) detected by ESET Endpoint Security product. Below this, there are sections for 'ESET LiveGrid®' showing reputation and popularity, and a 'Process tree' for 'userinit.exe (5008)' showing a chain of processes including 'explorer.exe (5068)', '7zj.exe (7524)', '7zj.exe (5282)', and 'chrome.exe (8092)'. A dark blue box on the right contains the text 'פירוט התהליך ומידע על התנהגות חשודה'.

# זיהוי עובדים שמפרים כללי אבטחת מידע

## מקרה לדוגמה

ברשת שלך ישנם משתמשים שעוברים שוב ושוב על החוקים הנוגעים לנוזקות. אותם המשתמשים נדבקים בנוזקות פעם אחר פעם. האם זה נובע מהתנהגות בעייתית, או שהם מותקפים יותר ממשתמשים אחרים?

## פתרון

✓ צפייה בקלות במשתמשים ומכשירים בעייתיים.

✓ השלמת ניתוח מקורות וסיבות במהירות כדי למצוא את מקור ההדבקות.

✓ טיפול בשיטות התקיפה שנמצאו, כגון דוא"ל, רשת האינטרנט או התקני USB.

במקרים רבים, החוליה החלשה ביותר במערכי אבטחה היא העובדים שיושבים ליד מקלדת, גם אם אין להם אף כוונה רעה.

ESET Inspect מזהה בקלות את החוליות החלשות האלה באמצעות דירוג המחשבים על פי מספר ההתראות הייחודיות שכל מחשב יצר. אם משתמש מעורר מספר התראות, זהו סימן ברור לכך שיש לבדוק את הפעילות שהתרחשה במחשב.

# איתור וחסמת איומים

## מקרה לדוגמה

מערכת ההתראה המוקדמת שלכם או מרכז פעילויות האבטחה שלכם (SOC) משגר אזהרה על איום חדש. מהם הצעדים הבאים שלכם?

## פתרון

✓ ניצול מערכת ההתראה המתקדמת על מנת לאסוף נתונים על איומים קרובים או חדשים.

✓ איתור האיום החדש והאם קיים בכל המחשבים בארגון.

✓ חיפוש סימנים לפריצה (IoC) בכל המחשבים בכדי לגלות באילו מחשבים האיום היה קיים לפני כן.

✓ חסימת יכולתו של האיום לחדור לרשת העסק שלכם או לפעול בה.

היתרון המשמעותי של ESET Inspect הוא זיהוי איומים באמצעות טקטיקה של "מציאת מחט בערימת שחת".

באמצעות הפעלת מסננים על הנתונים, שממיינים קבצים על פי הפופולריות או המוניטין שלהם, החתימה הדיגיטלית שלהם, המידע ההקשרי וההתנהגותי שלהם, ניתן לזהות ולחקור כל פעילות זדונית בקלות. הגדרת מספר רב של מסננים מאפשרת להפעיל משימות לזיהוי איומים באופן אוטומטי ולהתאים את סף הזיהוי על פי הסביבה של אותו הארגון.

ניתן לזהות ולחקור  
כל פעילות זדונית בקלות

# נראות מלאה של הרשת

## מקרה לדוגמה

חלק מהארגונים מודאגים מהתוכנות שהמשתמשים מריצים על מערכות החברה. ואלו לא רק התוכנות שמותקנות באופן מסורתי שמדאיגות אתכם, אלא גם תוכנות שאינן מותקנות במחשבים עצמם. כיצד תוכלו להמשיך ולשלוט עליהם?

ESET Inspect הוא פתרון ארכיטקטורה פתוחה, מה שאומר שצוות האבטחה יכול להתאים את כללי הזיהוי כנגד טכניקות ההתקפה השונות לסביבה הספציפית של הארגון.

## פתרון

✓ צפייה בכל התוכנות המותקנות על כל המכשירים וסינון שלהן בקלות.

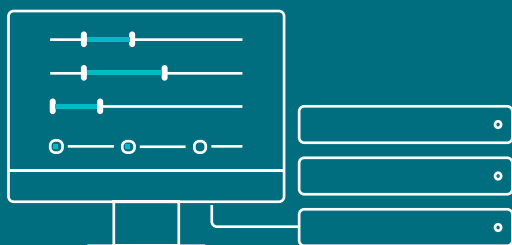
✓ צפייה בכל הסקריפטים בכל המכשירים ואפשרויות סינון.

✓ חסימה של הרצת סקריפטים או תוכנות לא רצויים בקלות.

✓ טיפול באירוע באמצעות שיגור התראה למשתמשים אודות אפליקציות לא מורשות והסרה שלהן באופן אוטומטי.

בנוסף, הארכיטקטורה הפתוחה מאפשרת גמישות רבה וכך ניתן להגדיר את ESET Inspect לזיהוי הפרות של נהלי החברה הנוגעים לשימוש בתוכנות ספציפיות כמו תוכנות טורנט, תוכנות לאחסון בענן, תוכנות לגלישה ב-Tor, הקמת שרתים על מחשבי החברה ותוכנות לא רצויות נוספות.

אלו לא רק התוכנות שמותקנות באופן מסורתי שמדאיגות אתכם, אלא גם תוכנות שאינן מותקנות במחשבים עצמם. כיצד תוכלו להמשיך ולשלוט עליהם?



צוותי האבטחה יכולים להתאים את כללי הזיהוי כנגד טכניקות ההתקפה השונות לסביבה הספציפית של הארגון.



# תחקור וטיפול באירועים על פי הקשר

## מקרה לדוגמה

הנתונים לא שווים כלום ללא ההקשר העומד מאחוריהם. כדי לקבל החלטות באופן נכון, עליך לדעת מהן ההתראות, על אלו מחשבים הן מופיעות ומיהם המשתמשים שגורמים להפעלתן.

## פתרון

- ✓ זיהוי ומיון המחשבים על פי Active Directory, חלוקה אוטומטית לקבוצות או חלוקה ידנית.
- ✓ חסימת הפעלתם של תוכנות וסקריפטים או מתן הרשאות לשימוש בהן בכל אחת מקבוצות המחשבים השונות.
- ✓ חסימת הפעלתם של תוכנות וסקריפטים או אפשר אותן לכל אחד מהמשתמשים השונים.
- ✓ קבלת התראות רק עבור קבוצות מסוימות והסרה שלהן באופן אוטומטי.

הפעילות ה"זדונית" של תהליכים מסוימים תלויה בהקשר שלה.

הפעולות שמבוצעות במחשביהם של מנהלי הרשת שונות מאוד מאלו המבוצעות למשל במחלקת הכספים. באמצעות חלוקה נכונה של מחשבים לקבוצות משתמשים, צוותי האבטחה יכולים לזהות במהירות האם המשתמש רשאי לבצע פעולה ספציפית במחשב שלו. הסנכרון בין קבוצות תחנות הקצה של ESET PROTECT ובין הכללים שמוגדרים ב-ESET Inspect מביאים לתוצאות חסרות תקדים מבחינת מידע הקשרי.

## התקנה קלה ותגובה מהירה – אין צורך בצוות אבטחה

## מקרה לדוגמה

לא לכל העסקים יש צוותי אבטחה ייעודיים, וכך הזנת והטמעת כללי זיהוי מתקדמים עשויה להפוך למשימה קשה מאוד.

## פתרון

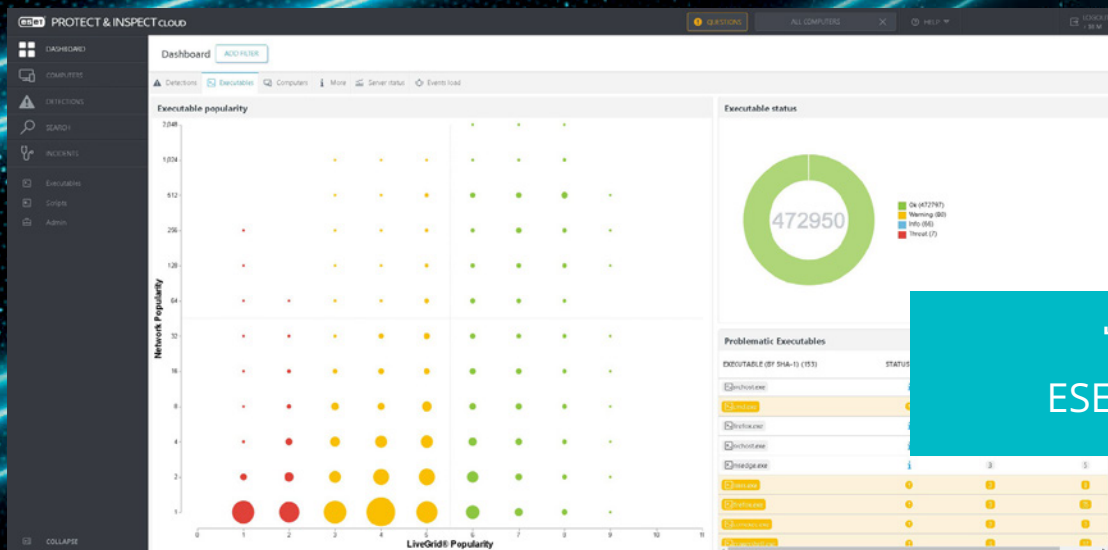
- ✓ מעל ל-800 כללים מובנים שהוגדרו מראש.
- ✓ תגובה בקלות באמצעות חסימת אפליקציות, הפסקת פעולתן או הכנסת מחשב להסגר בלחיצת כפתור אחת.
- ✓ תוכניות פעולה מוצעות הן חלק מובנה מההתראות.
- ✓ ניתן לערוך את הכללים בשפת XML וכך לאפשר כוונן עדין של הכללים הקיימים או יצירת כללים חדשים.

גם אם לחברה יש צוותי אבטחה ייעודיים, לעיתים קרובות קשה לקבוע סדר עדיפויות ולהחליט על הצעדים הבאים באופן מהיר בזמן שהתראות האבטחה ממשיכות להופיע.

לכן, עבור כל התראה ניתן ליצור תוכנית פעולה מוצעת לטיפול באירועים. כש-ESET Inspect מזהה איום, הוא מספק אפשרות לתגובה מהירה. ניתן לחסום קבצים ספציפיים על פי ערכי ה-Hash שלהם ולבודד מחשבים מהרשת או לכבות אותם מרחוק.

הפעילות ה"זדונית" של תהליכים מסוימים תלויה בהקשר שלה. הסנכרון בין קבוצות תחנות הקצה של ESET PROTECT ובין הכללים שמוגדרים ב-ESET Inspect מביאים לתוצאות חסרות תקדים מבחינת מידע הקשרי.

עבור כל התראה ניתן ליצור תוכנית פעולה מוצעת לתיקון הנזקים.



דשבורד של  
ESET Inspect

# יכולות הפתרון

## מערכת לניהול אירועים

ניתן לצפות בקבוצות נתונים כמו זיהויים, מחשבים, קבצי הפעלה או תהליכים חשודים בתצורת יחידות לוגיות המאפשרות זיהוי אירועים זדוניים פוטנציאליים על ציר זמן, עם הצעות לפעולה למשתמש. ESET Inspect מציע אוטומטית את התקריות הקשורות לאירוע הרלוונטי ומשמש כלי לסיוע במיון, חקירה ופתרון אירועי האבטחה.

## גישה מרחוק בטוחה וחלקה

תגובה לאירועים ושירותי אבטחה עובדים בצורה חלקה בהתאם לקלות של הגישה אליהם - הן מבחינת ההתחברות לממשק הניהול והן מבחינת החיבור לתחנות הקצה. ההתחברות עובדת קרוב למהירות בזמן אמת עם אמצעי אבטחה מרביים שהופעלו, והכל ללא צורך בכלים של צד שלישי.

## בידוד בלחיצה אחת

הגדרת מדיניות נישה לרשת כדי לעצור במהירות את התפשטות הנוזקה. ניתן לבדוד מכשיר נגוע מרשת האינטרנט ומהרשת הארגונית בלחיצה אחת בלבד בממשק של ESET Inspect. בנוסף, ניתן להוציא את כל המכשירים בקלות ממצב ההסגר לאחר מכן.

## תגובה בזמן אמת

ESET Inspect מאפשר בקלות ובלחיצה אחת פעולות תגובה כמו אתחול או כיבוי תחנת קצה, בידוד תחנת קצה משאר הרשת, הפעלת סריקה לפי דרישה, עצירת כל תהליך שרץ ברקע, וחסימת כל יישום המבוסס על ערך ה-Hash שלו. בנוסף, הודות לתשדורת בזמן אמת של ESET Inspect, צוותי האבטחה יכולים להפיק תועלת מאפשרויות חקירה ותיקון עם PowerShell ישירות לתחנה.

## זיהוי אנומליות והתנהגות

בדיקת פעולות שבוצעו ע"י קובץ בר הרצה והשתמשו במערכת המוניתין LiveGrid כדי להעריך במהירות אם התהליכים שהופעלו הם בטוחים או חשודים. ניתן לנטר אירועים חריגים הקשורים למשתמשים מסוימים באמצעות כללים ספציפיים המוגדרים לפעול לפי התנהגות מסוימות, ולא רק על פי זיהוי בסיסי של נוזקה או חתימה זדונית. חלוקת המחשבים לקבוצות על פי משתמשים או מחלקות מאפשרת לצוותי האבטחה לזהות האם המשתמש מורשה לבצע פעולה מסוימת או לא.

## ניתוח שורש הבעיה

תצוגה פשוטה וברורה כתרשים הזרימה של כל שרשרת אירועים שעלולה להיות זדונית, עם אפשרות לירידה לרמת הפירוט הרצויה. מקל משמעותית על קבלת החלטות המבוססות על ההקשר העשיר שההסברים מספקים למשתמש.

## תיוג

הוספת והסרת תגים לסינון מהיר של עצמים כמו מחשבים, התראות, כללי החרגה, משימות, קבצי הרצה, תהליכים וסקריפטים. ניתן לשתף את התיוגים בין המשתמשים, ולאחר שתיוג נוצר ניתן לשייך אותו לאובייקט הנבחר בשניות ספורות.

## ממשק תכנות יישומים פומבי (Public API)

ESET Inspect כולל API REST ציבורי המאפשר ניהול וייצוא של זיהויים ואת התגובות והתיקונים שלהם המאפשרים אינטגרציה יעילה עם מערכות כגון SIEM, SOAR, מערכות טיקטים ועוד רבים אחרים.

## הנגשת פגיעויות בצורה ברורה

ניתן לצפות ולחסום קבצים, סקריפטים ופעילות חשודה על בסיס למעלה מ-30 אינדיקטורים הכוללות שינויים ב-Registry, ערכי Hash, שינויים בקבצים וחיבורי רשת בצורה קלה ופשוטה.

## זיהוי איומים

ניתן לעשות שימוש במנוע חיפוש עוצמתי המבוסס על מזהים זדוניים (IOC) ולסנן נתונים גולמיים לפי פופולריות של הקובץ, המוניתין שלו, החתימה הדיגיטלית שלו והמידע ההתנהגותי או מתוך ההקשר שלו. הגדרת סננים מרובים מאפשרת זיהוי, עצירה וחסימת איומים, הכולל גם איומי תקיפה מתמשכים (APT) ומתקפות ממוקדות בצורה קלה ופשוטה.

# יכולות הפתרון

## ארכיטקטורה פתוחה

ESET Inspect מספק זיהוי ייחודי מבוסס התנהגות ומוניטין, בנראות מלאה לצוותי האבטחה. כל הכללים נכתבים בפורמט XML הנפוץ וניתן ליצור ולשנות אותם בקלות כך שיתאימו לצרכיהם הספציפיים של סביבות העבודה הארגוניות, ביניהם אינטגרציות SIEM.

## זיהוי הפרה של מדיניות ונהלי הארגון

חסימת פעילויות זדוניות לפעול ברשת הארגון. הארכיטקטורה הפתוחה של ESET Inspect מאפשרת גמישות בזיהוי הפרות של מדיניות המתייחסות לשימוש בתוכנות ספציפיות כמו תוכנות טורנט, תוכנות לאחסון בענן, תוכנות לגלישה ב-Tor, הקמת שרתים על מחשבי הארגון ותוכנות לא רצויות נוספות.

## ניקוד מתוחכם

יכולת תיעדוף התראות באמצעות מערכת ניקוד ודירוג של חומרת ההתראה, אשר מאפשרת למנהל הרשת, לזהות בקלות מחשבים שבהם הסיכון להיווצרות אירוע אבטחה הוא גבוה יותר.

## איסוף דאטה מקומי

ניתן לצפות בנתונים מקיפים על האירוע החשוד הכוללים זמן ביצוע, מידע על המשתמש, משך הפעולה החשודה והמכשירים שהותקפו. כל המידע מאוחסן באופן מקומי כדי למנוע דליפת מידע רגיש.

# קצת על ESET

ותוך מינימום צריכת משאבים. בין לקוחותינו בישראל ניתן למנות משרדי ממשלה ועיריות, מוסדות חינוך ובריאות, חברות היי-טק ועסקים במגוון תחומים רחב.

[www.eset.com/il](http://www.eset.com/il)

ESET היא חברת תוכנה בינלאומית ויצרנית אבטחת המידע מס' 1 באיחוד האירופי. עם ניסיון של 30 שנים, אנחנו מפתחים פתרונות הגנה לתחנות קצה המצטיינים במניעה, זיהוי ותגובה לאירועי סייבר, ומאפשרים לארגונים להתמקד במטרותיהן מבלי לעצור

## ESET במספרים

**1 מיליארד**  
משתמשים  
ברחבי העולם

**400k+**  
לקוחות עסקיים

**200+**  
נציגויות  
בעולם

**13**  
מרכזי מו"פ  
עולמיים

## בין לקוחותינו



מוגנת ע"י ESET  
מאז 2017;  
מעל 14,000 תחנות קצה



מוגנת ע"י ESET  
מאז 2016;  
מעל 4,000 תיבות דוא"ל



מוגנת ע"י ESET  
מאז 2016;  
מעל 32,000 תחנות קצה



ספק שירותי אינטרנט,  
שותף אבטחה מאז 2008;  
למעלה מ-2 מיליון לקוחות

## מחויבים לרמת האבטחה הגבוהה ביותר



ESET זכתה בחותמת איכות במבדק שבדק פתרונות עסקיים בדצמבר 2021 על פתרון ההגנה שלה לארגונים



ESET באופן עקבי מדורגת במיקומים גבוהים בביקורות של פלטפורמת G2 הבינלאומית והפתרונות של ESET מוערכים על ידי משתמשים מכל העולם



פתרונות ההגנה של ESET זוכים להכרה באופן עקבי על ידי גופים עצמאיים מובילים. לדוגמה בדו"ח של Forrester הבודק יכולות זיהוי ותגובה של איומי Zero-day לשנת 2021



**eset**<sup>®</sup> Digital Security  
Progress. Protected.