

סקירת פתרון



ESET INSPECT

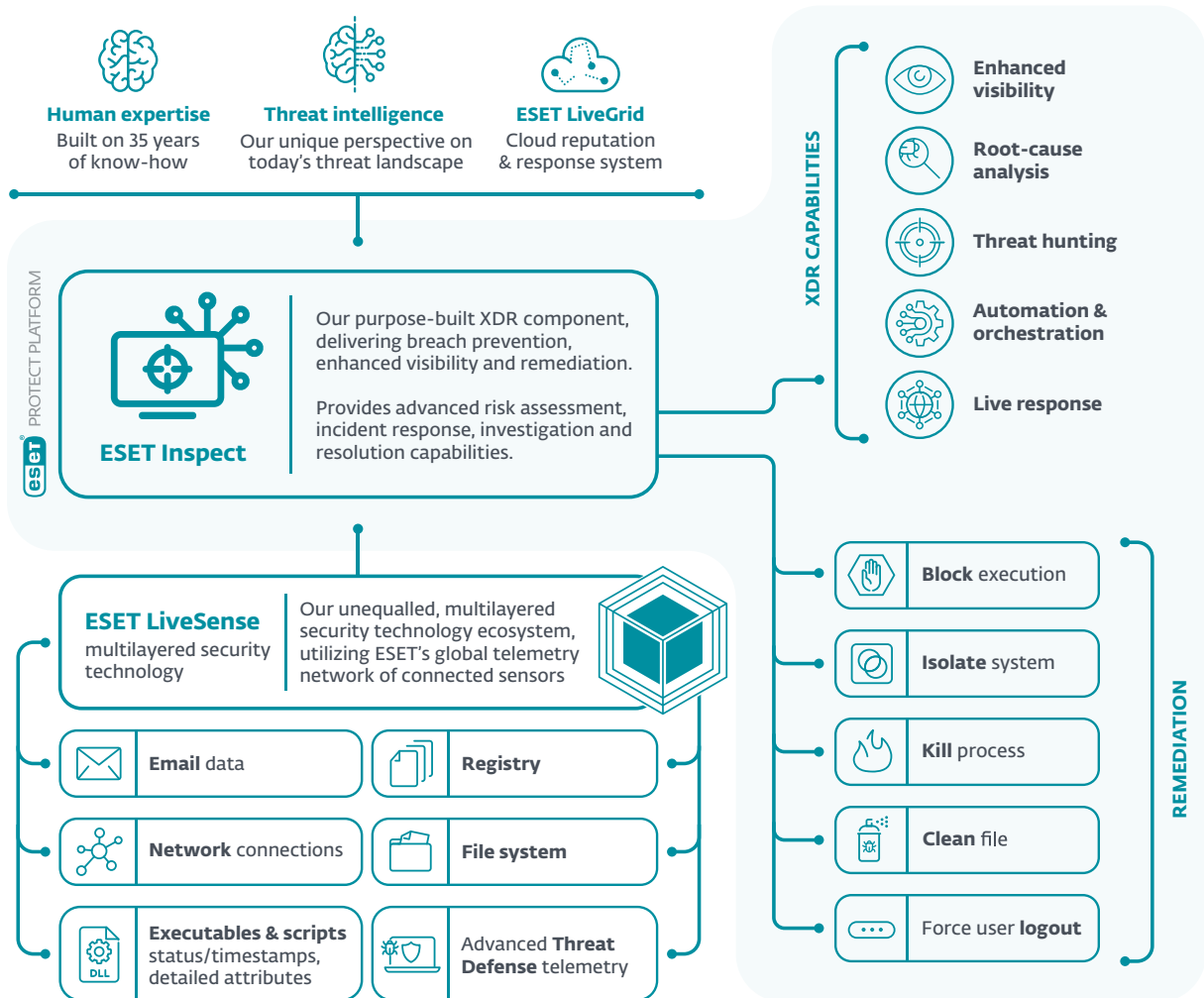
פתרון המהווה רכיב ב-XDR של פלטפורמת
ESET PROTECT, המספק מניעת דליפות, שקיפות
מוגברת וטיפול באירועי אבטחה

Progress. Protected.

מה זה פתרון מתקדם לזיהוי ותגובה?

ESET Inspect, רכיב המהווה חלק מה-XDR בפלטפורמת **ESET PROTECT**, הוא כלי שנועד לזהות אנומליות בהתנהגות והדלפת נתונים, לבצע הערכת סיכונים, וכן להגיב לתקריות, לחקור אותן ולטפל בהן.

הוא מאפשר לצוות האבטחה לתקריות לנטר ולהעריך את כל הפעילויות ברשת ובמכשירים המחוברים אליה. בנוסף, הוא מסייע באוטומציה של תהליכי החזרה לשגרה, במידת הצורך. מספר כללי הזיהוי הגדול של ESET (מעל 1200 והמספר הולך וגדל) מאפשר ציד איומים מקיף.



היתרונות של ESET

מניעה, זיהוי ותגובה מלאים

מאפשר ניתוח זריז של כל אירועי האבטחה ברשת וחזרה מהירה לשגרה. ההגנה הרב-שכבתית של ESET (שהיא הבסיס לפתרון Inspect ESET), שכחלק ממנה כל שכבה שולחת נתונים ל-Inspect ESET, מנתחת כמויות עתק של נתונים בזמן אמת כך שאף איום לא יחמוק מזהוי.

אבטחת מידע בעדיפות הראשונה

חברת ESET נלחמת באיומי סייבר במשך יותר מ-30 שנים. כחברה שמבוססת על מדע וטכנולוגיה, היא תמיד עמדה בחוד החנית של פיתוחים כמו למידת מכונה, טכנולוגיית ענן ו-XDR.

מניעה עדיפה על טיפול

הגישה של ESET ל-XDR קשורה בקשר ישיר למוצרי המניעה זוכי-הפרסים שלה. הודות למחויבות שלה לפיתוח טכנולוגיות זיהוי באיכות גבוהה, טכנולוגיות המניעה שלה הן מהמובילות בעולם.

שקיפות מפורטת לרשת

הודות לכללי זיהוי (ל-ESET יש מעל 1200 כללים כאלה, ומספרם ממשיך לעלות), מזהים זדוניים (IOCs – Indicators of Compromise) מתקדמים ויכולת חיפוש, ניתן לבצע סריקה מעמיקה של הרשת שתאפשר לכם לזהות כל דבר חשוב.

גמישות באפשרויות ההטמעה

אנחנו נותנים לכם להחליט כיצד תרצו להטמיע את פתרון האבטחה: ESET Inspect יכול לרוץ על השרתים שלכם באופן מקומי או בהתקנה על גבי ענן של ESET, מה שמאפשר לכם להתאים את התקנת הפתרון בהתאם לנוחות וליכולות החומרה שלכם.

מוכן לפעולה באופן מיידי

הפתרון של ESET עובד ישירות לאחר ההתקנה, אך חזק מספיק כדי לאפשר התאמה של מאפיינים ספציפיים מאוד ע"י ציודי איומים מנוסים.

MITRE ATT&CK

ESET Inspect מקשר בין הזיהויים שלו לפירוט של MITRE ATT&CK™ של MITRE, כך שתוכלו לקבל מידע מקיף על האיומים בלחיצת כפתור, גם על המורכבים ביותר.

מערכת מוניטין

סינון מורחב מאפשר למהנדסי אבטחה לזהות כל אפליקציה שידועה כבטוחה, באמצעות שימוש במערכת המוניטין העוצמתית של ESET. המערכת של ESET כוללת בסיס נתונים הכולל מאות מיליוני קבצים שונים ומאפשרת לצוותי האבטחה להשקיע את הזמן שלהם בחקירת קבצים לא ידועים שעשויים להיות זדוניים, במקום לבזבז אותם על זיהויים שגויים.

אוטומציה והתאמה אישית

הגדירו את ESET Inspect בקלות כדי להגיע לרמת הפירוט והאוטומציה שאתם זקוקים לה. בחרו את רמת האינטראקציה הרצויה (ואת סוג וכמות הנתונים שאתם רוצים לאחסן) במהלך ההתקנה הראשונית באמצעות פרופילים של משתמשים מוגדרים מראש, ולאחר מכן אפשרו למצב הלמידה למפות את סביבת הארגון שלכם ולהציע כללי החרגה לזיהויים של פעולות תקינות במידת הצורך.

יכולות המערכת

ממשק ניהול אירועי אבטחה

ניתן לבצע שיוך בממשק זיהויים, מחשבים, קבצי הרצה או תהליכים לקבוצות, על גבי ציר הזמן, כדי לראות אירועים שעשויים להיות זדוניים, תוך כדי קישור של פעולות משתמש לרלוונטיות. ESET Inspect מציגה למנהל הממשק את כל מה שרלוונטי לאירוע ויכול לסייע בזיהוי ראשוני של האירוע, חקירה שלו ותכנון שלבי הפתרון.

אפשרויות תגובה מיידי

פתרון ESET Inspect מגיע עם כמות גדולה של תגובות אוטומטיות וגם שניתנות להפעלה בלחיצה אחת, למשל – הפעלה מחדש או כיבוי של נקודת קצה, בידוד של נקודת קצה מהרשת, הפעלה של סריקה לפי דרישה, עצירת התהליכים הפועלים, וחסימת קבצים וכל אפליקציה (על בסיס ערך ה-hash שלה). בנוסף, הודות ליכולת התגובה המיידית של ESET Inspect, המכונה Terminal, מומחי אבטחה יכולים להפיק תועלת מחבילה שלמה של אפשרויות חקירה והחזרה לשגרה באמצעות PowerShell.

ניתוח האירוע

צפו בקלות בניתוח האירוע ובעץ התהליכים המלא של כל שרשרת האירועים שעשויה להתברר כזדונית, לרדת עד לרמת העומק הרצויה בתחקיר ולקבל החלטות מבוססות-מידע המתבססות על מידע הקשרי והסברים שנכתבים ע"י מומחי הנוזקות שלנו, גם במקרים של זיהוי של פעולה לגיטימית וגם במקרים זדוניים.

API ציבורי

ESET Inspect כולל API ציבורי מסוג REST שמאפשר לגשת לזיהויים ודרכי הפתרון שלהם ולייצא אותם, כדי לאפשר אינטגרציה עם כלים כמו SIEM, SOAR, מערכות ניהול טיקטים ועוד.

מגוון סממני פריצה

צפו במודולים וחסמו אותם על בסיס יותר מ-30 מחוונים שונים, ביניהם: מחרוזת גיבוב (hash), שינויים ב-Registry, שינויים בקבצים וחיבורים לרשת.

ציד איומים

השתמשו בכלי העוצמתי לחיפוש אינדיקטורים זדוניים באמצעות שאילתות כדי למיין אותם על בסיס פופולריות הקובץ, מוניטין, חתימה דיגיטלית, התנהגות או מידע הקשרי אחר. הגדרה של מספר סינונים מאפשרת ציד איומים ותגובה לתקריות באופן קל ואוטומטי, יחד עם האפשרות לזהות ולעצור מתקפות APT ומתקפות ממוקדות.

גישה מרחוק באופן בטוח ופשוט

הפשטות של תהליכי התגובה לתקריות וניהול שירותי האבטחה תלויה בקלות הגישה לכלים המשמשים לביצוע פעולות אלה – והכוונה היא גם לחיבור בין המגיב לתקרית ובין ממשק הניהול, אך גם לחיבור עם נקודות הקצה. החיבור עובד במהירות הקרובה למהירות זמן-אמת תוך הפעלת אמצעי אבטחה רבים ככל האפשר, וכל זאת ללא צורך בכלים חיצוניים.

בידוד בקליק אחד

הגדירו מדיניות גישה לרשת במהירות כדי לעצור התפשטות של נוזקות. בודדו מהרשת מכשיר שנפגע, בלחיצה אחת מהממשק של ESET Inspect. בנוסף, ניתן להוציא מכשירים מאיזור ההסגר באותה הקלות.

זיהוי התנהגות ואנומליות

בדקו את הפעולות המבוצעות ע"י קובץ הרצה והשתמשו במערכת המוניטין של ESET – LiveGrid – כדי להעריך במהירות אם התהליך שרץ הוא בטוח או חשוד. ניתן לנטר תקריות אנומליות הקשורות למשתמשים באמצעות כלים שנוצרו כך שיופעלו ע"י התנהגות ולא רק ע"י זיהוי של נוזקה או של חתימה דיגיטלית. ניתן להגדיר קבוצות מחשבים על פי משתמשים או מחלקות כדי לאפשר לצוותי האבטחה לזהות אם המשתמש רשאי לבצע פעולה מסוימת או לא.

תיוג

מערכת ניקוד מתוחכמת

צרו תעדוף של ההתראות באמצעות אפשרות ניקוד המשייכת לכל תקרית ערך מספרי המצביע על חומרתה וכך מאפשר למנהלי הרשת לזהות במהירות מחשבים שבהם קיימת סבירות גבוהה לתקרית פוטנציאלית.

איסוף נתונים מקומי

צפו בנתונים מקיפים על מודול שהורץ בפעם הראשונה, כולל מועד ההרצה, המשתמש המריץ, משך השהות של התהליך במערכת והמכשירים שהותקפו. כל הנתונים מאוחסנים באופן מקומי כדי למנוע דליפת נתונים רגישים.

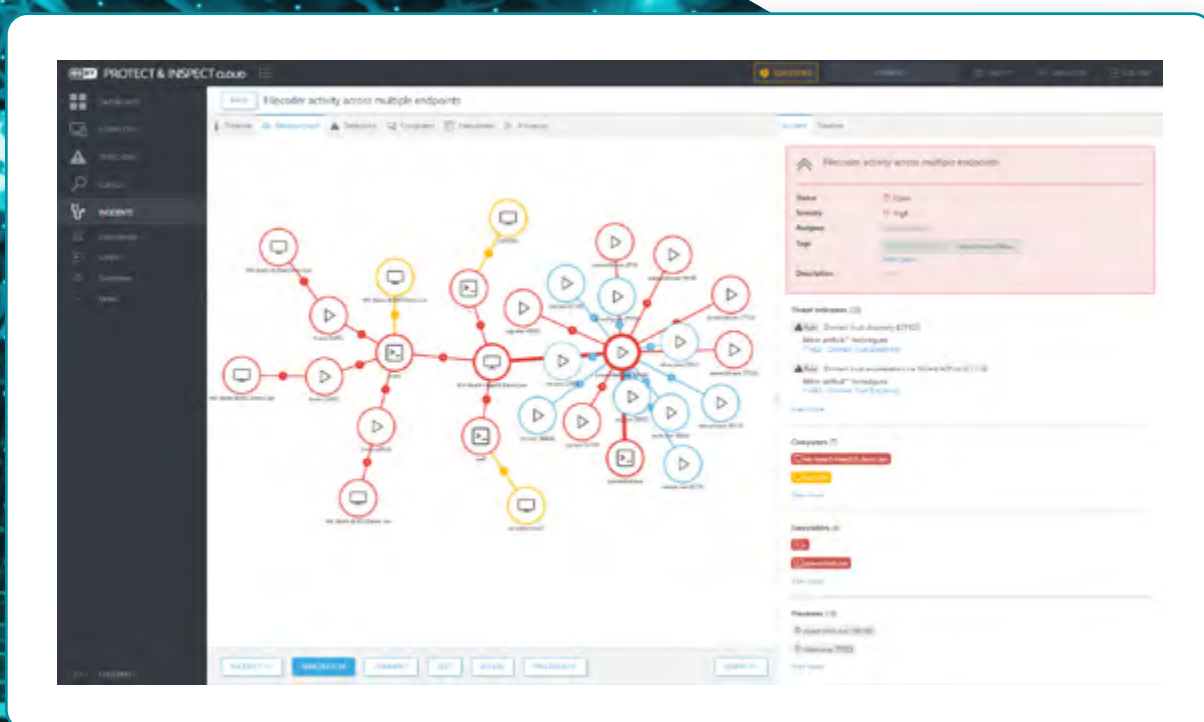
הוסיפו והסירו תוויות (תגים) כדי לבצע סינון מהיר של עצמים כמו מחשבים, התראות, כללי החרגה, משימות, קבצים ברי-הרצה, תהליכים וסקריפטים. התוויות משותפות למשתמשים, וניתן לשייך אותם לפריטים מיד לאחר שנצורו.

זיהוי הפרה של מדיניות החברה

חסמו הרצה של מודולים זדוניים על כל אחד מהמחשבים ברשת הארגון. הארכיטקטורה הפתוחה של ESET Inspect גמישה מספיק כדי לאפשר זיהוי הפרה של מדיניות שנוגעות לשימוש בתוכנות ספציפיות כמו תוכנות הורדות מבוססות טורנט (torrent), אחסון בענן, גלישה דרך דפדפן טור (Tor) או כל תוכנה לא-רצויה אחרת.

ארכיטקטורה פתוחה ואינטגרציות

פתרון ESET Inspect מספק זיהוי ייחודי המבוסס על התנהגות ומוניטין אשר מופיע בשקיפות מלאה לצוותי האבטחה. ניתן לערוך את כל הכללים בקלות באמצעות XML כדי לאפשר כוונן עדין של כללים או יצירה של כללים חדשים כך שיתאימו לצרכים של הסביבה הארגונית הספציפית, כולל אינטגרציות ל-SIEM.



מקרים לדוגמה

זיהוי התנהגות ומפרים סדרתיים

הבעיה

ברשת שלכם ישנם משתמשים שמפרים את ההנחיות הנוגעות לנוזקות פעם אחר פעם. אותם המשתמשים גם ממשיכים להידבק בנוזקות. האם זה נובע מהתנהגות מסוכנת, או שיותר מתקפות מכוונות אליהם לעומת משתמשים אחרים?

הפתרון

✓ צפו בקלות במשתמשים ומכשירים בעייתיים.

✓ בצעו ניתוח סיבת שורש באופן מהיר כדי למצוא את מקור ההדבקה.

✓ טפלו בווקטורי ההתקפה שזוהו – כמו דוא"ל, רשת האינטרנט או התקני USB.

✓ אם הקובץ התגלה כזדוני, ESET Mail Security משמיד באופן אוטומטי את הודעת הדוא"ל שמכילה את התוכן הזדוני.

התקנה ותגובה בקלות – ללא צורך בצוות אבטחה

הבעיה

לא לכל העסקים יש צוותי אבטחה ייעודיים, והיצירה וההטמעה של כללי זיהוי מתקדמים עשויים להפוך לאתגר.

הפתרון

✓ מעל ל-1200 כללים מוגדרים מראש.

✓ הגיבו בקלות בלחיצת כפתור, כדי לחסום מכשיר, לכבות אותו או להכניס אותו להסגר.

✓ ההתראות על התקריות מגיעות יחד עם הצעות לצעדים לטיפול בתקרית.

✓ ניתן לערוך את הכללים באמצעות שפת XML כדי לאפשר כוונן עדין של כללים או יצירה של כללים חדשים באופן פשוט.

ציוד וחסמת איומים

הבעיה

מערכת ההתרעה המוקדמת או מרכז פעולות האבטחה (SOC) שלכם שלח התרעה על איום חדש. מה יהיו הצעדים הבאים שלכם?

הפתרון

✓ השתמשו במערכת ההתראה המוקדמת כדי לקבל נתונים על איומים צפויים או חדשים.

✓ בצעו חיפוש כדי לבדוק אם האיום קיים בכל המחשבים.

✓ בצעו חיפוש של אינדיקטורים זדוניים כדי לזהות מחשבים שבהם קיים האיום לפני התרחשות המתקפה.

✓ חסמו את האיום כך שלא יוכל לחדור לרשת הארגון או להיות מורץ במכשירי הארגון.

שקיפות לרשת

הבעיה

חלק מהעסקים מודאגים בגלל האפליקציות שהמשתמשים מפעילים על המערכות שלהם. לא רק שעליכם לדאוג מאפליקציות שמותקנות באופן מסורתי, אלא גם מאפליקציות שאינן מותקנות על המחשב עצמו. כיצד תוכלו להיות בבקרה עליהם?

הפתרון

✓ צפו בכל האפליקציות המותקנות על כל המכשירים והפעילו סינונים בקלות.

✓ צפו בכל הסקריפטות בכל המכשירים והפעילו סינונים בקלות.

✓ חסמו הרצה של סקריפטות או אפליקציות לא מורשות בקלות.

✓ טפלו בתקרית באמצעות שליחת התראה למשתמשים על אפליקציה לא מורשית והסירו אותה באופן אוטומטי.

✓ חסמו את האיום כך שלא יוכל לחדור לרשת הארגון או להיות מורץ במכשירי הארגון.

חקירה וטיפול מבוססי-הקשר

הבעיה

הנתונים חשובים, אך ההקשר שלהם לא פחות חשוב. כדי לקבל החלטות נכונות, עליכם לדעת אילו התראות הופיעו, על אילו מכשירים הן הופיעו ומי המשתמשים שגרמו להופעתן.

הפתרון

✓ זהו ומיינו את כל המחשבים על פי Active Directory או על פי שיוך אוטומטי/ידני לקבוצות.

✓ אפשרו הרצה של אפליקציות וסקריפטים או חסמו הרצה שלהם לפי קבוצות המחשבים.

✓ אפשרו הרצה של אפליקציות וסקריפטים או חסמו הרצה למשתמשים ספציפיים.

✓ הגדירו קבלת התראות אליכם רק מקבוצות ספציפיות (תמיכה מלאה בניהול מאוחד).

זיהוי איומים מעמיק – כופרות

הבעיה

העסק מעוניין בכלים נוספים לזיהוי פרואקטיבי של כופרות בנוסף להתראות מיידית על זיהוי של התנהגות הדומה להתנהגות של כופרה שמזוהה ברשת.

הפתרון

✓ צרו כללים לזיהוי הרצה של אפליקציות המורצות מתוך תיקיות זמניות.

✓ צרו כללים לזיהוי קבצי Microsoft Office (כמו Word, Excel ו-PowerPoint) שזוהו אם הם מפעילים סקריפטים או קבצי הרצה נוספים.

✓ קבלו התרעה לאחר זיהוי של הרחבה של אחת מהכופרות הפופולריות באחד המכשירים.

✓ צפו בהתראות של Ransomware Shield המגיעות מ-ESET Endpoint Security מתוך אותו ממשק ניהול.

אודות ESET

כשאלה משולבים עם חקר ומודיעין האיורים הטובים בעולם, מוצרי ESET מציעים את האיזון המושלם בין יכולות מניעה, זיהוי ותגובה. קלות השימוש והמהירות חסרת התחרות מוכיחות שיש לנו מטרה אחת – להגן על ההתקדמות של לקוחותינו באמצעות מתן ההגנה הטובה ביותר האפשרית. www.eset.com/il

ESET בעלת ניסיון של יותר מ-30 שנים של חדשנות טכנולוגית ומספקת את פתרונות הגנת הסייבר המתקדמים ביותר בשוק. ההגנה המודרנית שלנו לתחנות הקצה מתבססת על טכנולוגיות האבטחה הרב-שכבתיות של ESET LiveSense, יחד עם שימוש מתמשך ב-Machine Learning ובמחשוב ענן.

ESET במספרים

1 מיליארד
משתמשים
ברחבי העולם

400k+
לקוחות
עסקיים

195
נציגויות
בעולם

13
מרכזי מו"פ
עולמיים

בין לקוחותינו



מוגנת ע"י ESET
מאז 2017,
מעל 9,000 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 מאז 2008, למעלה
מ-2 מיליון לקוחות

מחויבים לרמת האבטחה הגבוהה ביותר



ESET זכתה בחותמת איכות במבדק שבדק פתרונות עסקיים בדצמבר 2022 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



ESET זכתה להכרה כ"Top Player" בשנה הרביעית ברציפות בדו"ח לשנת 2023

קומסקיור בע"מ - הנציגה הבלעדית של ESET בישראל

1 מיליון משתמשים בישראל



מערך מומחים טכני בעברית
המספק שירות ללקוחות פרטיים
ועסקיים

