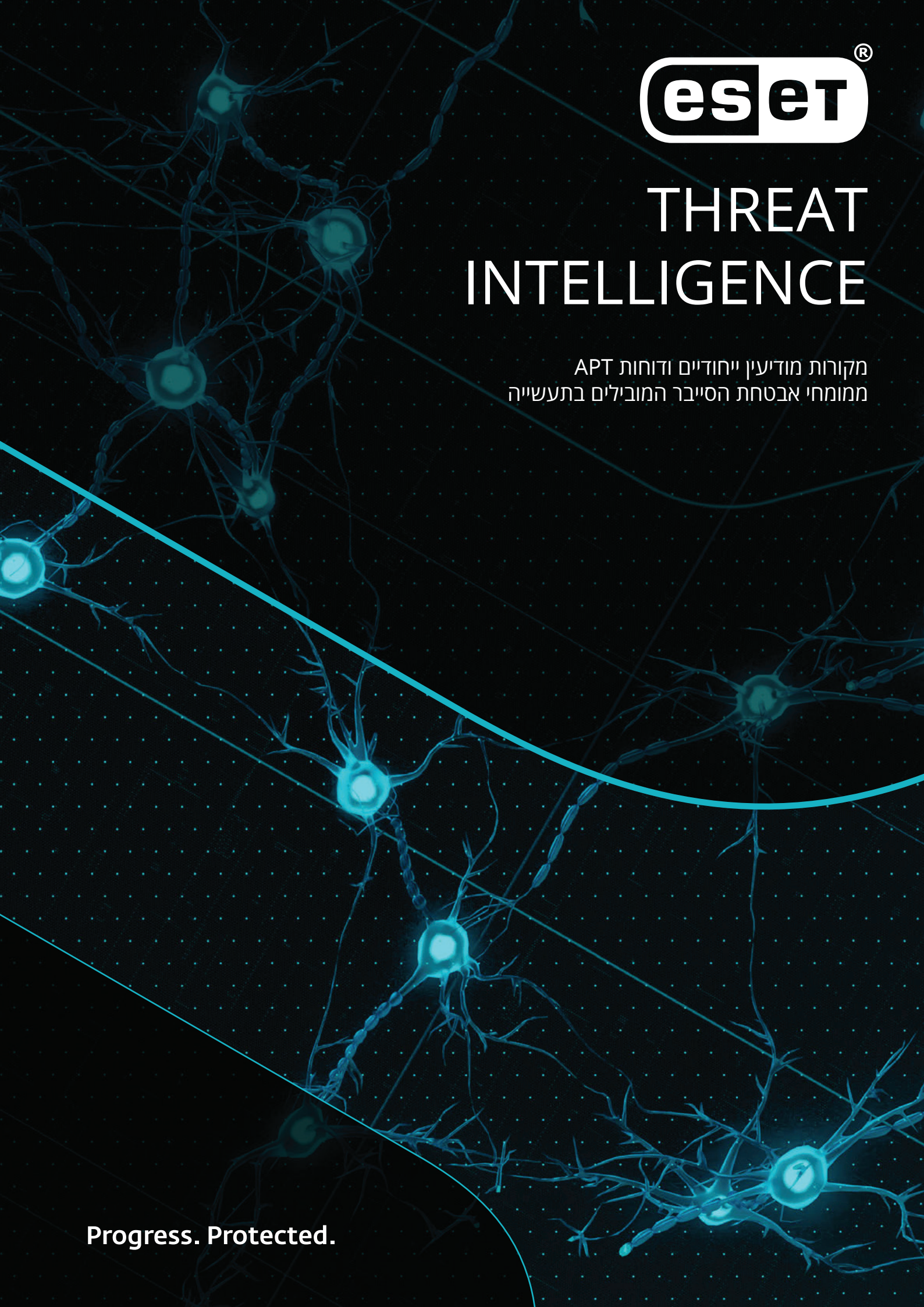


# THREAT INTELLIGENCE

מקורות מודיעין ייחודיים ודוחות APT
ממומחי אבטחת הסייבר המובילים בתעשייה

Progress. Protected.

# נקודת מבט ייחודית על מפת האיומים

### תובנות מודיעיניות ייחודיות

ESET אוספת מודיעין איומים ממגוון מקורות ייחודיים, ומשלבת ניסיון מעשי שאין לו תחרות, כדי לסייע לכם להתמודד עם מתקפות סייבר מתוחכמות ההולכות ומשתכללות.

### להישאר צעד אחד לפני התוקפים

ESET עוקבת אחרי הכסף, ומנטרת באופן ייעודי אזורים שבהם זוהו קבוצות APT הפועלות נגד חברות מערביות - איראן, רוסיה, סין וצפון קוריאה. כך תכירו איומים חדשים לפני כולם.

### קבלת התלטות קריטיות - מהר יותר

חיזוי איומים וקבלת החלטות טובות ומהירות יותר הודות לדוחות מקיפים ולפידים (feeds) מסוננים של ESET. הפחיתו חשיפה לאיומים נפוצים בעזרת התרעה מוקדמת ממומחים.

### שפרו את רמת האבטחה בארגון

בהסתמך על מקורות המודיעין של ESET, שפרו את יכולות ציד האיומים והטיפול בתקריות, חסמו מתקפות APT וכופרות, וחזקו את ארכיטקטורת אבטחת הסייבר שלכם.

### אוטומציה של חקירת איומים

טכנולוגיית ESET מאתרת איומים באופן רציף ובמספר שכבות, משלב ה-Pre-Boot ועד מצב מנוחה, ומסתמכת על טלמטריה גלובלית מכל המדינות שבהן ESET מזהה איומים מתפתחים.

# היתרון של ESET

מומחיות אנושית הנתמכת בבינה מלאכותית ולמידת מכונה. מערכת ®LiveGrid, מבוססת על כ-110 מיליון מכשירים ברחבי העולם ונבדקת ומאומתת על ידי מרכזי המחקר והפיתוח של ESET.

### מומחיות אנושית בגיבוי למידת מכונה

השימוש בלמידת מכונה לצורך אוטומציה של קבלת החלטות והערכת איומים פוטנציאליים הוא חלק מרכזי בגישה שלנו. עם זאת, עוצמת המערכת נובעת מהאנשים שעומדים מאחוריה. מומחיות אנושית היא מרכיב קריטי ביצירת מודיעין איומים מדויק ככל האפשר, שכן גורמי האיום עצמם הם יריבים מתוחכמים ואינטליגנטיים.

### מערכת ®LiveGrid חזקה

מוצרי ה-Endpoint של ESET כוללים מערכת מוניטין מבוססת ענן, המספקת מידע רלוונטי ועדכני על איומים חדשים ועל קבצים תקינים. מערכת ®LiveGrid נשענת על כ-110 מיליון מכשירים ברחבי העולם, כאשר הנתונים שהיא מפיקה מאומתים על ידי מרכזי הפיתוח של ESET. כך יכולים הלקוחות ליהנות מרמת אמון גבוהה במיוחד בדוחות ובמידע המוצגים בקונסולת הניהול.

### שורשים אירופיים, נוכחות גלובלית

ESET פועלת מתוך האיחוד האירופי ומביאה עמה למעלה מ-30 שנות ניסיון בעולם אבטחת המידע. לחברה 22 משרדים ברחבי העולם, 13 מרכזי מחקר ופיתוח ונוכחות ביותר מ-200 מדינות וטריטוריות. פריסה זו מאפשרת ללקוחותינו לקבל נקודת מבט גלובלית ומעמיקה על מגמות ואיומי הסייבר העדכניים ביותר.

# דוחות Advanced Persistent Threat (APT)

## מיטב המחקר שלנו - בהישג ידכם

צוות המחקר של ESET מוכר ומוערך בתעשיית אבטחת הסייבר. מחקרי הצוות, סיכומי פעילות APT ומידע מעמיק נוסף זמינים ללקוחות ESET.

## תוכן ממוקד ובר יישום

הדוחות מספקים הקשר מעמיק למה שמתרחש ומדוע. כתוצאה מכך, ארגונים יכולים להיערך מראש לאיומים עתידיים. חשוב לא פחות, מומחי ESET מקפידים להציג את המידע בצורה ברורה וקלה להבנה.

## קבלת החלטות קריטיות - במהירות

המידע מסייע לארגונים לקבל החלטות קריטיות בזמן אמת ומעניק יתרון אסטרטגי במאבק בפשיעת סייבר. הוא מספק הבנה מעמיקה של המתרחש ב"צד האפל של האינטרנט" והקשר חיוני, המאפשר היערכות ארגונית מהירה ויעילה.

## גישה ישירה לאנליסט של ESET

לקוחות חבילת APT Reports Premium נהנים גם מגישה ישירה לאנליסט של ESET - עד ארבע שעות בכל חודש. גישה זו מאפשרת להעמיק בנושאים רלוונטיים ולקבל סיוע בפתרון סוגיות פתוחות.

## עם דוחות APT תקבלו:

- גישה לניתוחים טכניים פרטיים ומעמיקים
- דוחות סיכום של פעילות APT
- סיכום מנהלים חודשי ייעודי להנהלה הבכירה
- גישה ישירה למומחה אבטחת סייבר של ESET
- גישה לשרת ה-MISP של ESET

## ניתוח טכני מעמיק

החבילה כוללת דוחות ניתוח טכניים מעמיקים המתפרסמים מדי חודש, ומתארים מתקפות עדכניות, כלי תקיפה חדשים ונושאים קשורים. בנוסף, תקבלו אחת לשבועיים דוח סיכום פעילות, המתאר את המתקפות האחרונות של קבוצות ה-APT, שחוקרי ESET עוקבים אחריהן - כולל גורמי האיום המעורבים, היעדים שלהם וכמובן גם אינדיקטורים זדוניים (IoCs) משויכים.

סקירה חודשית מרכזת את כלל דוחות הניתוח הטכני וסיכומי הפעילות שפורסמו במהלך החודש הקודם, ומציגה אותם בפורמט קצר וממוקד.

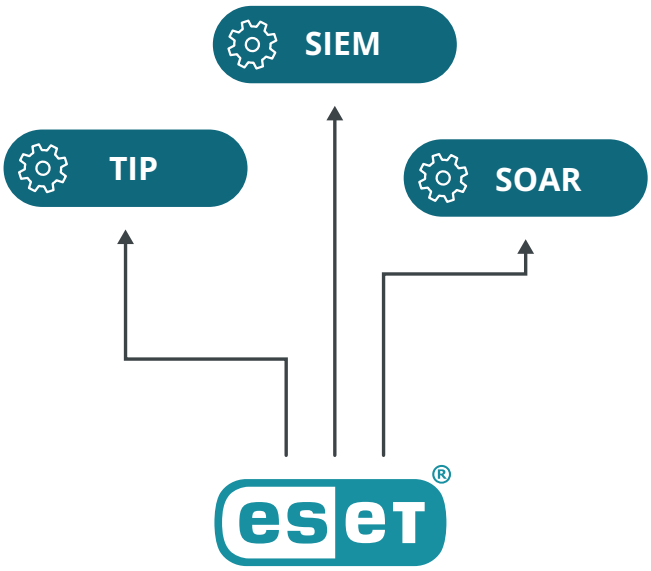
זמינות דוחות ופידי Threat Intelligence של ESET משתנה ממדינה למדינה.

למידע נוסף, מומלץ לפנות אלינו.

eset Cybersecurity Progress. Protected.

# שלבו את ESET Threat Intelligence במערכות הארגון שלכם

שילוב הטלמטריה של ESET הוא פשוט ומעשיר את פלטפורמות ה-TIP, SIEM או SOAR שלכם.
אנו מספקים API מקיף עם תיעוד מלא, המאפשר חיבור מהיר ויעיל למערכות קיימות.




הנתונים מועברים בפורמטים סטנדרטיים, כגון JSON ופידי STIX באמצעות TAXII - כך שניתן לבצע אינטגרציה כמעט עם כל כלי אבטחה בארגון.

למערכות IBM QRadar, Anomali, ThreatQuotient ו-Logpoint קיימים מדריכי אינטגרציה מפורטים שלב-אחר-שלב, המאפשרים הטמעה מהירה וקלה - ואנו ממשיכים להוסיף אינטגרציות נוספות באופן שוטף.

# כיצד מודיעין האיומים שלנו קורם עור וגידים?

# מחזור החיים של ESET Threat Intelligence

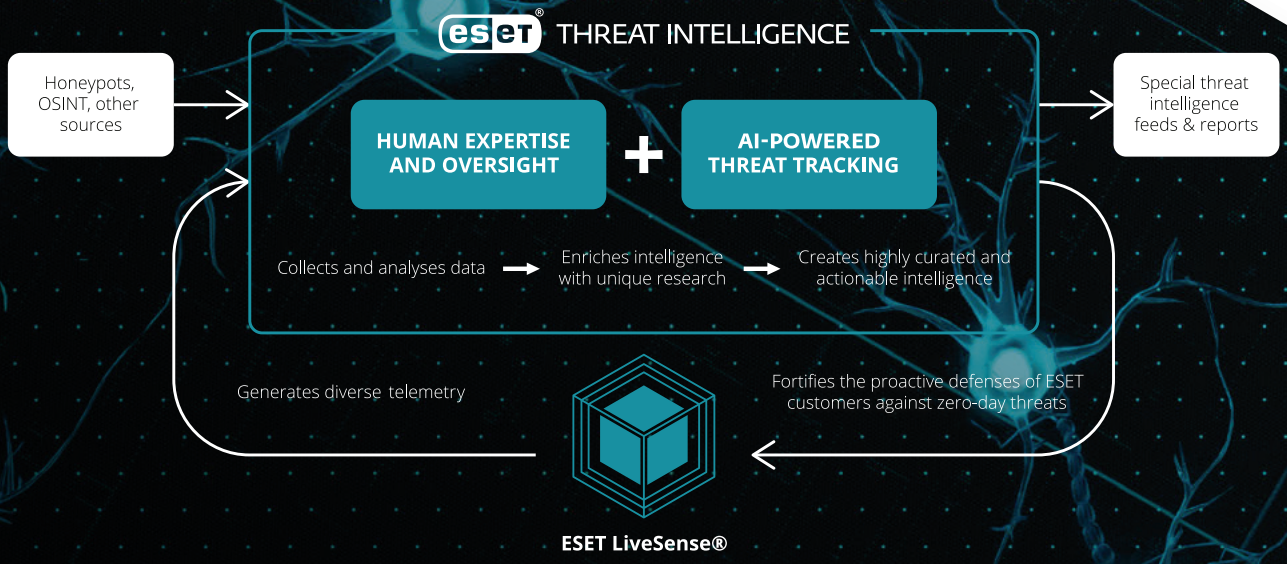
יצירת מודיעין האיומים של ESET מבוססת למעשה על מחזור עבודה מתמשך שמחזק את עצמו.

הוא נשען על מגוון רחב של טלמטריה המופקת על ידי ESET LiveSense® - טכנולוגיית האבטחה הרב-שכבתית של ESET, המשולבת בפלטפורמת ESET PROTECT.

הטלמטריה הנאספת מועשרת במקורות נוספים, כגון שרתי פיתיון (Honeypots), OSINT ומקורות חיצוניים אחרים.

בהמשך, הנתונים מעובדים באמצעות מערכות מתקדמות למעקב וניתוח נוזקות, המשלבות בינה מלאכותית (AI). מערכות אלו מסוגלות לחשוף ולהוסיף הקשר רחב ומשמעותי, המעשיר את נתוני המודיעין.

כמרכיב קריטי בתהליך, מומחי מודיעין האיומים של ESET מפקחים על התוצר הסופי ודואגים לכך שהוא יהיה מסונן, מדויק ועדכני - כדי לסייע לכם לקבל החלטות נכונות ומהירות יותר.




ESET Cybersecurity
Progress. Protected.

# פידי מודיעין ייחודיים של ESET

העשירו את תמונת האיומים הגלובלית שלכם באמצעות טלמטריה ייחודית.

פידי המודיעין של ESET נאספים ממרכזי המחקר שלנו ברחבי העולם, מספקים תמונה הוליסטית של מפת האיומים ומאפשרים חסימה מהירה של IoCs (Indicators of Compromise) בסביבה הארגונית.

הפידים זמינים בפורמטים: JSON ו-STIX 2.1.

### פיד קבצים זדוניים (Malicious Files Feed)

פיד זה מספק מידע בזמן אמת על דגימות נוזקה שהתגלו לאחרונה, מאפייניהן ו-IoCs משויכים. הוא מאפשר להבין אילו קבצים זדוניים פעילים "בשטח" ולחסום אותם באופן פרואקטיבי לפני שיגרמו לנזק. הפיד כולל מידע כגון דומיינים זדוניים, Hash-ים של קבצים, חותמות זמן, סוג האיום שזוהה ופרטים טכניים נוספים.

### פיד דומיינים (Domain Feed)

פיד זה מאפשר חסימה של דומיינים המוגדרים כזדוניים. הוא כולל שמות דומיין, כתובות IP ותאריכים רלוונטיים. הדומיינים מדורגים לפי רמת חומרה, כך שניתן להתאים את מדיניות התגובה - למשל, לחסום רק דומיינים ברמת סיכון גבוהה.

### פיד כתובות (IP Feed)

פיד זה משתף כתובות IP הנחשבות לזדוניות והמידע המשויך אליהן. מבנה הנתונים דומה לפידי Domain ו-URL. מקרי השימוש העיקריים כוללים זיהוי כתובות IP זדוניות פעילות, חסימה של כתובות חמורות במיוחד, סימון איומים ברמת סיכון נמוכה יותר והעמקה בחקירה.

### פיד כתובות (URL Feed)

בדומה לפיד הדומיינים, פיד ה-URL מתמקד בכתובות ספציפיות. הוא כולל מידע מפורט על ה-URL עצמו, לצד נתונים על הדומיינים המאחסנים אותו. כל המידע מסונן כך שיוצגו רק ממצאים בעלי רמת אמינות גבוהה.

### פיד Botnet

מבוסס על רשת המעקב הייחודית של ESET אחר Botnets. הפיד כולל שלושה תתי-פידים: Botnet, C&C ו-Targets. הנתונים כוללים, בין היתר, זיהויים, Hash-ים, פעילות אחרונה, קבצים שהורדו, כתובות IP, פרוטוקולים, יעדים ופרטים נוספים.

### פיד APT

פיד זה כולל מידע על פעילות APT המבוסס על מחקרי ESET. לרוב מדובר ביצוא נתונים משרת ה-MISP הפנימי של ESET. כל הנתונים הכלולים בפיד מוסברים בהרחבה גם בדוחות APT.

פיד ה-APT הוא חלק מחבילת APT Reports, אך ניתן לרכישה גם בנפרד.

## בפידים של ESET תקבלו:

- ✓ נתונים מסוננים ואיכותיים במיוחד
- ✓ תוכן אופרטיבי ובר יישום
- ✓ שיעור נמוך של זיהויי שווא (False Positives)
- ✓ עדכונים תכופים
- ✓ API מקיף לאינטגרציה מלאה

# על ESET

## אבטחה דיגיטלית מתקדמת לעסקים

### אנחנו לא רק עוצרים פריצות - אנחנו מונעים אותן מראש

בניגוד לפתרונות מסורתיים המתמקדים בתגובה לאיומים לאחר מימושם, ESET מציעה גישת Prevention-First מתקדמת, מבוססת בינה מלאכותית, הנשענת על מומחיות אנושית, מודיעין איומים גלובלי מוביל ורשת מחקר ופיתוח רחבה בהובלת חוקרים מהשורה הראשונה.

כל זאת כדי להמשיך ולחדש בטכנולוגיית האבטחה הרב שכבתית שלנו.

ESET מספקת הגנה חסרת פשרות מפני מתקפות כופר, פישינג, איומי Zero-Day ומתקפות ממוקדות - באמצעות פלטפורמת XDR עטורת פרסים, מבוססת ענן, המשלבת מניעה מתקדמת, זיהוי וציד איומים פרואקטיבי. הפתרונות שלנו ניתנים להתאמה גבוהה, כוללים תמיכה מקומית, פועלים עם השפעה מינימלית על ביצועי תחנות הקצה, מזהים ומנטרלים איומים מתפתחים עוד לפני מימושם, מבטיחים המשכיות עסקית ומצמצמים את עלויות ההטמעה והניהול.

בעולם שבו טכנולוגיה מאפשרת התקדמות - הגנו על העסק שלכם עם ESET.

## ESET במספרים

**1bn+**
**מעל מיליארד משתמשי אינטרנט מוגנים**

**500k+**
**לקוחות עסקיים**

**200+**
**מדינות וטריטוריות שיש בהן נוכחות**

**13**
**מרכזי מחקר ופיתוח גלובליים**

## הוקרה תעשייתית

ESET זכתה בפרס Tech Cares 2023 מטעם TrustRadius על תרומתה לקהילה

ESET זוכה להכרה בזכות למעלה מ-700 חוות דעת שנאספו ב-Gartner Peer Insights

## הוקרה מצד אנליסטים

ESET היא אחת מחברות אבטחת הסייבר העצמאיות המובילות בתרומת ידע וכלים, ומדורגת בין 10 המובילות מתוך 354 תורמים לפרויקט MITRE ATT&CK

ESET הוכרה כ-"Top Player" זו השנה הרביעית ברציפות בדוח

בשנת 2023, IDC דירגה את ESET בין חמשת ספקי מודיעין האיומים המובילים והדגישה את פרופיל ESET Threat Intelligence

Cybersecurity
Progress. Protected.

## עמידה בתקנות אבטחת מידע - ISO

ESET עומדת בתקן ISO/IEC 27001:2022 - תקן אבטחת מידע בינלאומי מוכר ומוביל ליישום ולניהול אבטחת מידע בארגונים. ההסמכה ניתנה על ידי גוף הסמכה חיצוני ומוסמך (SGS), ומעידה על עמידה מלאה של ESET בסטנדרטים ובשיטות העבודה המובילות בתעשייה.

## חלק מלקוחותינו

שותפת אבטחה ל-ISP מאז 2008
בסיס לקוחות של כ-2 מיליון משתמשים

מוגנת על ידי ESET מאז 2016
למעלה מ-32,000 תחנות קצה

מוגנת על ידי ESET מאז 2017
למעלה מ-9,000 תחנות קצה

## חלק מהפרסים המובילים שלנו

Cybersecurity Champion 2022

G2- LEADER 2026 חורף

Approved Corporate Endpoint Protection

דירוג AAA להגנת Endpoint ארגונית

Approved Security Product 2024

"THE IMPLEMENTATION WAS VERY STRAIGHTFORWARD. **IN COOPERATION WITH ESET'S WELL-TRAINED** TECHNICAL STAFF, WE WERE UP AND RUNNING OUR NEW ESET SECURITY SOLUTION IN A FEW HOURS."

IT Manager, Diamantis Masoutis S.A., Greece, 6,000+ seats

"WE WERE MOST IMPRESSED WITH THE SUPPORT AND ASSISTANCE WE RECEIVED. IN **ADDITION TO BEING A GREAT** PRODUCT, THE EXCELLENT CARE AND SUPPORT WE GOT WAS WHAT REALLY LED US TO MOVE ALL OF PRIMORIS' SYSTEMS TO ESET AS A WHOLE."

Joshua Collins, Data Center Operations Manager, Primoris Services Corporation, USA, 4,000+ seats