



**בזכות הרגולציה**  
במערכת הסייבר הלאומי מסכיבים מדוע  
סדרת התחום היא אינטרס לאומי עמ' 12

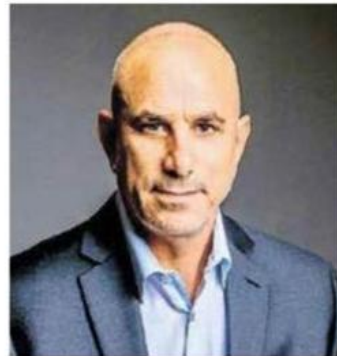
**הגנה תוך מתקפה**  
Armory Defense שוללת מהתוקף את הנכס  
הקריטי ביותר שלו: הזמן עמ' 09

**סיכול מוקדם הוא הכרחי**  
כך מאפשרת מערכת HUNTER 1  
להקדים את התוקפים עמ' 05

## "הגנה רב-שכבתית אפקטיבית מתחילה בסיכול מודיעני"

רוני רויטמן, מייסד-שותף ומנכ"ל INTENSITY GLOBAL, יזם סדרתי ומומחה סייבר, מציג את HUNTER 1, פלטפורמה שמשנה את פרדיגמת ההגנה מזיהוי תגובתי לפרואקטיבי. "ההסתכלות ההגנתית שלנו באה ממקום של התוקפים", הוא אומר. "אנו פועלים באסטרטגיה של ציד יזום: לאתר את התוקפים לפני שהם פועלים, ולהקדים אותם בכמה צעדים"

**יואל צפרי, בשיתוף INTENSITY GLOBAL**  
**מקבוצת Accel Solutions**



רוני רויטמן | צילום: שלומי פרי

מתקפת סייבר אינן עוד אירועים חריגים אלא תהליך מתמשך, שבו תוקפים מיוזמים פועלים בשקט, לאורך זמן, מתחת לרדאר של מערכת האבטחה הארגונית. במציאות הזו, תפיסת ההגנה המבוססת על חומות היקפיות והתראות טכניות נקודתיות מתיקשה לספק מענה. אמנם היא מזהה סימטומים, אך לא תמיד מציעה את הסיפור המלא של התקיפה. כאן נכנסת לתמונה HUNTER 1, פלטפורמת שמקדימה את הזיהוי - עוד לפני שהאיום מתימש. המערכת משלבת מודיעין חיצוני עם ניתוח התנהגותי של תעבורת רשת ופעילות משתמשים בארגון, כדי לחבר בין נקודות מידע מבודדות ולחשוף דפוסי תקיפה מתהווים עוד לפני שהם מתורגמים לנוק ממש.

"HUNTER 1 היא פלטפורמת AI לחיזוי איומי סייבה מודיעין סייבר וניתוח פורטני אופרטיבי של אירועים", אומר רוני רויטמן, מייסד-שותף ומנכ"ל קבוצת INTENSITY GLOBAL, שפיתח את המערכת יחד עם דן פרומוביץ, ה-CTO של הקבוצה.

"הפלטפורמה מאפשרת לארגונים לחוות איומים ולחוק משמעותית את מערך ההגנה ויכולות התגובה שלהם", הוא מוסיף. "במקום להמתין להתראה ברעב, אנחנו מנסים לזהות דפוסי תקיפה בשלב מוקדם ולבנות מהם תמונה אופרטיבית במילים פשוטות, אנחנו צדים את התוקפים ומאפשרים ללקוחות להיות שני צעדים לפניהם".

לדברי רויטמן, מרבית הארגונים כיום מתמודדים עם תופעת האיים הבודדים: מערכת האבטחה - Microsoft EDR ו-Firewall ועד לסיכנת Microsoft - 365 - פועלות מנותקות זו מזו לרוב, ללא סנכרון או שיתוף מידע רציף. הפער הזה יוצר "שטח חים מתים" היות ופעמים רבות גם מערכות כגון SIEM ו-SOC לא מצליחות להתריע בזמן על נוכחות תוקף ברשת. בשטחים מתים אלו, תוקפים מיוזמים יכולים לפעול כמעט ללא הפרעה. פלטפורמת HUNTER 1 מסייעת לגשר על הפער באמצעות תפיסה אקטיבית ואופרטיבית כוללת, השולטת על כלל הנכסים הדיגיטליים - מתנתת קצה ועד תיבות דואר - ומבצעת אינטגרציה מלאה בין המערכות השונות.

"המטרה שלנו היא להפוך את המידע המבוחר והביג דאטה, שכולל התראות רבות, לתמונה מודיעינית אחת מלאה ופעילה, שמאפשרת ראייה אחודה ותגובה מיידיית לכל איום", מציין רויטמן.

### לחציף את האיומים המשמעותיים

חיזוי המתקפות מבעוד מועד נעשה הן בורה הפנימית של הארגון והן בורה החיצונית. מחוץ

לה, באילו מקטעים היא עברה ומהו מצבה הנוכחי. חיבור כל הנקודות מאפשר לארגון לראות את התמונה המלאה, שהומקת מכלי סייבר אחרים.

### הוביל את הפריצה לשוק הבין-לאומי

רוני רויטמן הוא יזם הייטק עם 26 שנות ניסיון במרחב הסייבר, בהן צבר מומחיות כיועץ אסטרטגי בכיר להנהלות חברות וארגונים וכמנטור לסטארט-אפים. לפני כשמונה שנים הוא הקים את חברת INTENSITY GLOBAL, שמתמחה בסייבר התקפי והגנתי וכיועץ אסטרטגי, ורויטמן הוביל את פריצתה לשוק הבין-לאומי. כיום סדרתי, הוא הקים בנוסף את חברת Cycon Security יחד עם דן פרומוביץ, שביחד פיתחו את פלטפורמת HUNTER 1 שפועלת כאמור מנקודת ראות של התוקף והמגן. כיום, INTENSITY GLOBAL מייצגת את הפלטפורמה בישראל.

לאורך השנים הקים והיה שותף בחברות סייבר מבצעיות נוספות. השינוי המבני המשמעותי האחרון התרחש ביולי 2024, כאשר החברה הצטרפה ל- Accel Solutions רכשה 51% ממניות INTENSITY GLOBAL. בעקבות הרכישה הוקם מה קבוצת Accel Cyber Group, שמאחדת תחת קורת גג אחת את הפתרונות של חברות אבטחת המידע והסייבר של קבוצת Accel: Intensity Global (סייבר מבצעי ו-Danet, IR), Communications (אינטגרציה ואבטחת מידע) ו-SOC (שירותי SOC וניטור). כל זאת על מנת להציע פתרונות אבטחת מידע איכותיים מאוד, מקצה לקצה, ולספק ערך מוסף ממש לארגונים. "היעד המרכזי שלנו הוא להתרחב לשוקים הבין-לאומיים - תהליך שכבר החל וצור בר תאוצה", הוא מספר.

### מעטפת הגנה מלאה ורב-שכבתית

קבוצת Intensity Global מנהלת מדי שטחי אירועי תקיפה מורכבים בארץ ובעולם. היא

מספקת מעטפת הגנה מלאה ומקיפה, הכוללת צוותי IR (Incident Response) - צוותי תגובה טכנולוגיים המוקפצים לזירת האירוע כדי לבלום את התקיפה ולנהל את המשבר ברמה הניהולית והטכנולוגית כאחד. לצד ניהול המשברים, החברה מספקת שירותי "הגנה לאורך כל השנה" (Managed Services). מטרת השירות היא לחוק את הארגון מבעוד מועד, לייצג אסטרטגיית הנהלות בכירות ולמנוע מתיקפות עתידיות באמצעות ניתוח פערים ומודיעין אקטיבי.

### מהו פרופיל הלקוחות שלכם?

"קהל הלקוחות שלנו מורכב מחברות ככל הסיקט, כולל חברות אנטרפרייז ותשתיות קריטיות, המהווים את עמוד השדרה של המשק הישראלי והגלובלי. זה כולל בתי חולים ומוסדות רפואיים, חברות דלק ואנרגיה מובילות, חברות הייטק וסטארט-אפים, בנקים ומוסדות פיננסיים, וכן גופים ביטחוניים מובילים וממשלתיים".

כמומחה סייבר וכיועץ בכיר, מה המסר המרכזי שלך לשוק לקראת כנס CyberTech 2026?

"המסר שלי הוא פשוט. יש חשיבות עצומה למעטפת הגנה מלאה ורב-שכבתית. אמנם אין הגנה הרמטית, אבל המטרה שלנו היא להפוך כל התיקפה ללא כדאית עבור התוקף. ארגונים חייבים להפסיק לראות אבטחה כאיים בודדים של טכנולוגיה ולהתחיל להתבונן בתמונה המלאה. מהניסיון שצברנו בנייה אירועי סייבר, למדנו שרק שילוב של מודיעין אקטיבי, חיזוי מבוסס AI ותיגובה טכנולוגית מיידיית (IR) יכול למנוע נזקים ולבנות חוסן ארגוני לאורך זמן.

"בסופו של דבר, היכולת להקדים את התוקף ולהיבן את התמונה המלאה היא מה שמבדיל ארגון פרואקטיבי מכל מערכת תגובה נקודתית."

בשיתוף INTENSITY GLOBAL מקבוצת Accel Solutions

