

מניהול חולשות לניהול חשיפה מקומו המשתנה של המודיעין בעידן ה-CTEM

רס"ן (מיל') יונתן קלר¹

התפתחות ההגנה האזרחית בסייבר אינה רק סיפור טכנולוגי או ארגוני, אלא גם אתגר מושגי עבור עולם הביטחון כולו. היא מלמדת כי בעידן בו יריבים פועלים במהירות, באופורטוניזם ובמגוון רחב של נתיבי פעולה, לא די בהבנת האויב כשלעצמה. לאחר 7 באוקטובר קשה להימנע מן התהייה אם גם המערכת הביטחונית והצבאית נדרשת לתמורה דומה. אין פירוש הדבר שאפשר להעתיק בפשטות את תפיסת ה-CTEM מן הסייבר הארגוני אל שדה הביטחון הלאומי. אולם ההיגיון המארגן עשוי להיות רלוונטי: נדרש מעבר מן השאלה "מה האויב מתכוון לעשות?" לשאלה משלימה (ולעיתים מקדימה): "באלו תנאים אנו בעצמנו חשופים לפגיעה?"

מבוא

בשנים האחרונות מתרחש שינוי עמוק בעולם ההגנה בסייבר. במשך זמן רב אורגנה פעולת ההגנה במבט החוצה – זהות התוקף, כוונותיו והטכניקות שלו; אולם בהדרגה, ובייחוד בעולם הסייבר האזרחי, עברה נקודת הכובד מהבנת האיום אל הערכת הפגיעות. השאלה אינה עוד מי עלול לתקוף את הארגון ומתי, אלא כיצד הארגון עצמו נעשה חשוף לתקיפות אפשריות. שינוי זה התפתח מתוך התחום של ניהול חולשות, אך חרג ממנו. תחום זה העניק לארגונים דרך מעשית לזהות, לדרג ולתקן חולשות, אך לנוכח התפתחות ה-AI המתקדם, הוא נקלע לאחרונה למשבר בשל קפיצה במספר החולשות החדשות, קיצור חלון הזמן לניצול חולשות והתרחבות שטח התקיפה). על רקע זה עלתה קרנה של תפיסה ל"ניהול מתמשך של חשיפה לאיומים" (CTEM – Continuous Threat Exposure Management) – אשר מבקשת לגבש תהליך רחב יותר המחובר בין נכסי הארגון, רמת חשיפתם, בקורות ההגנה, מידת הניצול בפועל של החולשות וסדרי העדיפויות העסקיים. הצלחת התפיסה אינה נמדדת עוד במספר הליקויים שתוקנו, אלא ביכולתו של הארגון לצמצם באופן שיטתי את הנתיבים הריאליים לתקיפה שלו.

יודגש, חשיבותה של תפיסת ה-CTEM אינה רק בשיפור תהליך העבודה, אלא גם בניסיון לארגן את האבטחה בסייבר כמערכת הגנתית: איגוד של פעולות מקומיות טקטיות לתוכנית פעולה מתמשכת המתכתבת עם ההיגיון הארגוני הרחב. מהבחינה הזו, היא מסמנת שינוי פרדיגמטי באופן שבו הגנת הסייבר מבינה ומתארת את עצמה.

לכאורה מדובר בהתפתחות פנימית של תעשיית הסייבר המסחרית, אולם בפועל היא מעלה שאלה רחבה הרבה יותר על האבולוציה של מערכות ההגנה ועל מקומו של המודיעין בתוכן. בראש ובראשונה תפיסת ה-CTEM מספקת הזדמנות עבור מודיעין הסייבר, משום שהיא "דוחפת אותו" אל הרמה המערכתית. במשך שנים מודיעין הסייבר דיבר בשפה טקטית, טכנית ומקצועית מאוד, וכעת הוא נדרש לעסוק בתהליך קבלת ההחלטות ובשאלות שעניינן סיכון עסקי, איומי ייחוס, תרחישי תקיפה ותעדוף משאבים. יחד עם זאת, אותה ההזדמנות כרוכה גם בשינוי של מעמד המודיעין ומקומו בתהליכי קבלת ההחלטות: המודיעין אינו ניצב עוד בראשית הדרך של המעשה ההגנתי והסיכולי, אלא הופך גורם מכונן המטמיע הבנות של איומים חיצוניים בתהליכים אשר מופנים פנימה ומתמקדים בניית פגיעותו של הארגון.

המאמר פותח בבירור מעמדו של מודיעין הסייבר כמקצוע שהתפתח על התפר בין שתי סביבות: המערכת הביטחונית – זו שהורשה לו את שפת המודיעין, את המושג "התרעה" ואת ההתמקדות ביריב; והתעשייה האזרחית – זו שעיצבה אותו סביב נתונים, כלים טכנולוגיים, וחקירות תקיפה. לאחר מכן, נבחן את המעבר ההדרגתי "מאדום לכחול", המפנה את המבט פנימה: מן המאמץ להבין את התוקף כשלעצמו, אל הצורך להבין את התנאים הפנימיים המאפשרים לו לפעול באופן אפקטיבי. בהקשר הזה נדון התחום של ניהול החולשות – תחילה כמענה שיטתי לשאלת הפגיעות הארגונית, ובהמשך כמודל שנקלע לקשיים. לבסוף דן המאמר בהתבססותה של תפיסת ה-CTEM ובתמורה העמוקה שהיא מביאה לידי ביטוי: עידוד מעבר לגישה מערכתית בנושא הטיפול בסיכוני הסייבר. חלק זה מראה כיצד מודיעין הסייבר משתלב במערכת לא רק כגורם מתריע, אלא ככוח המסייע לקשור בין איומים חיצוניים, פגיעות פנימיות וקבלת החלטות המובילים לתעדוף סדרי פעולה.

איזה סוג מודיעין הוא "המודיעין לאומי סייבר"? מודיעין בצילה של תעשייה

בשני העשורים האחרונים התקבע הסייבר כממד פעולה עצמאי – הן במערכות הביטחוניות המדינתיות, הן בעולם ההגנה הארגונית. בד בבד עם התפתחותן של יחידות סייבר צבאיות, מפקדות ייעודיות ויכולות מבצעיות חדשות, נולד מקצוע מודיעיני ששמו מוכר לכאורה: מודיעין לאומי סייבר. אולם דווקא הדמיון הלשוני למודיעין המסורתי עלול להטעות. השאלה אם מודיעין לאומי סייבר הוא אכן "מודיעין" אינה סמנטית בלבד, והיא משפיעה על האופנים שארגונים מבינים איום, מנהלים סיכון, מתעדפים משאבים ומגדירים את תכלית פעולת ההגנה שלהם. היא פותחת פתח לשאלה רחבה יותר בדבר מקומו של המודיעין במערכת הגנה אשר מתמקדת בניהול של חשיפות, פגיעויות ונתיבי תקיפה פנימיים.

במערכות הביטחוניות ההמשגה הזרועית של ממד הסייבר באה לידי ביטוי בהקמה של מפקדות וגופי מטה ייעודיים, כמו למשל פיקוד הסייבר האמריקני (CYBERCOM). המשגה זו השפיעה גם על עיצובם של גופי המודיעין החדשים, ומודיעין הסייבר נתפס רבות כתחום משנה של המודיעין הלאומי-ביטחוני: כשם שפעלו אנשי מודיעין בזרועות הים, האוויר והיבשה, כך אנשי מודיעין היו אמורים לפעול גם בסייבר. אף שברי היה כי מודיעין הסייבר מצריך בקיאות ומומחיות טכנית בעולם התוכן הרלוונטי, נטען כי אין בכך ייחוד – כישורים דומים הרי נדרשו מאנשי למד"ן (להק מודיעין בחיל האוויר) או מד"ן (מספן מודיעין בחיל הים). בהתאם לכך גופי מודיעין הסייבר התבקשו לספק תפוקות מודיעיניות מסורתיות, החל במודיעין למבצע וכלה במודיעין הנדרש לגיבוש אסטרטגיה צבאית, למשל עת מודיעין הסייבר מילא תפקיד חשוב בגיבוש וביישום של אסטרטגיית המב"ם (המערכה בין המלחמות) בעימות עם איראן.

זאת ועוד, בדומה לכל גוף מודיעין אחר הרעיון המארגן של גופי מודיעין הסייבר היה חובת ההתרעה. מבחינה מתודולוגית, היו ניסיונות לאמץ בגופי הסייבר שפה התרעיתית ולהעתיק אליהם מודלי התרעה ותהליכים תומכים, כמו למשל דיוני התרעה לקביעת מדרגים בסייבר.²

בד בבד עם התמסדות מודיעין הסייבר כתחום לאומי-ביטחוני, התפתח במגזר הפרטי-מסחרי מקצוע של מודיעין לאומי סייבר (CTI – Cyber Threat Intelligence). מקצוע זה צמח במהירות והיה לתעשייה ענפה ומופְּרַת בארץ ובעולם. מבחינה זו, ובניגוד למודיעין בזרועות האוויר או הים, מודיעין הסייבר התפתח לצד תמונת מראה אזרחית אשר השתכללה בהדרגה בהתאם לכלליו של שוק תחרותי. ההתכתבות בין מודיעין הסייבר הצבאי למקבילו האזרחי לא הייתה עניין משני אלא שהיא הפכה למוקד משמעותי של למידה והשתפרות בגופי הסייבר של מערכת הביטחון. למידה זו התאפשרה בין השאר הודות להסכמי שותפות בין גופים ביטחוניים לחברות מסחריות העוסקות במודיעין הסייבר. הסכמי השותפות הללו מאפשרים הפריה הדדית, שממדיה חורגים בהרבה מאלו המקובלים בעסקאות רכש טכנולוגיות בתחומים אחרים. נוסף על הטכנולוגיה עצמה, גופי הסייבר הביטחוניים למדו מעמיתיהם במגזר הפרטי תהליכי עבודה וחשוב מכך – שאבו ממנו מומחיות יקרת ערך, כזו שהתפתחה מתוך חיכוך מתמשך עם אלפי מקרים של תקיפות סייבר.

משטח התקיפה הסייברי הוא במהותו אזרחי וגלובלי, ולמידה מבצעית מצריכה התמודדות ישירה עם היריב במרחב האינטרנטי וחקירות של מקרי תקיפה ופריצה. בשני הרכיבים האלו – סיכול ברשת האינטרנט וחקירות של אירועי תקיפה – היה לחברות המסחריות יתרון תחרותי מובהק על הגופים הביטחוניים. אף שלאחרונים נכסים משלהם, היה ברור כי למידה מבצעית מחייבת ייבוא של תובנות ומומחיות מגופים מסחריים. בהתאם לכך השפעתן של חברות מסחריות על המתודולוגיה של גופי מודיעין הסייבר הביטחוניים הייתה למאפיין בולט, ואולי ייחודי, של ממד הסייבר. אמנם, נכון שגם בדיסציפלינות מודיעיניות נוספות נוצרו שיתופי פעולה עם השוק, אך קשה למצוא תחום מודיעיני נוסף בו הם נהיו לגורם מעצב כה מרכזי בהתפתחותו. למעשה, קשה היום לדמיין יחידות מודיעין סייבר ביטחוניות שאינן מתבססות במידה ניכרת על שיתופי פעולה עם השוק הפרטי.

מאפיין נוסף המבדיל את מודיעין הסייבר מדיסציפלינות מודיעיניות אחרות הוא רשת האינטרנט. בענפים ביטחוניים רבים האינטרנט נחשב למקור איסופי נוסף המסייע בהרכבת תמונת המודיעין, אולם במודיעין הסייבר אינטרנט הוא העיקר: הן מקור מידע ראשי, הן זירת המערכה עצמה אשר תוקפים ומגינים פועלים בה לצד זה. אין זה מפתיע אפוא שהתפתחו כלים מודיעיניים אזרחיים אשר אוספים כמויות עצומות של פריטי מידע ברשת האינטרנט; כך למשל VirusTotal משמש מאגר ידע גלובלי של קבצים זדוניים המשמשים תוקפים ברשת, והפלטפורמה GreyNoise מצביה "מלכודות" במוקדים רבים ברחבי האינטרנט כדי

2 HEALEY, J. (Ed.) (2013). A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012. CYBER CONFLICT STUDIES ASSOCIATION; MATTHEW S. COHEN, CHUCK FREILICH, AND GABI SIBONI, "FOUR BIG 'DS' AND A LITTLE 'R': A NEW MODEL FOR CYBER DEFENSE," CYBER, INTELLIGENCE, AND SECURITY 1, no. 2 (JUNE 2017): 21–36.

שפת המומחים של ה-CTI

ללמידה מן הסייבר האזרחי היו גם מחירים. ככל שמקצוע ה-CTI התמסד יותר בתעשייה, כך גם הלך וזנח את הרבדים האסטרטגיים והמערכתיים כדי להתמקד במודיעין טקטי-טכנולוגי.³ עולמו של איש מודיעין הסייבר התמלא במזהים, חתימות, קבצים, דומיינים, חולשות, תשתיות תקיפה וכלי ניטור. מודיעין שנועד לחולל הבנה מערכתית על איומים הסתגר וקידש שפה של מומחיות טכנית המובנת לקהילה מקצועית צרה בלבד.

תהליך זה היה במידה רבה תוצאה של התפתחות השוק ושל תנאים טכנולוגיים מאפשרים, אך גם הארגונים עצמם תרמו לצמצום זה. במשך שנים רבות הנהלות ודירקטוריונים ראו בסייבר סוגיה טכנית גרידא, העדיפו להפקיד את העיסוק בשאלת הסיכון הסייברי בידיהם של אנשי מקצוע מביני עניין והיססו להעמיק בו (בניגוד להעמקתם בבחינת סיכונים עסקיים אחרים). התנהלות זו גרמה לכך שהמודיעין התקשה להציג למקבלי ההחלטות הערכת איום עקבית ומייצרת הקשר. ביקורת נוקבת על תהליכים אלו נשמעה דווקא בספרות האקדמית, אולי כי זו הייתה חשופה יותר לדיון הרחב בתפקיד המודיעין בעת המודרנית. ב-2018 מאמר מכונן בתחום זה היה עוד מסוגל היה לשים דגש על איכות המידע הטכני, להעניק חשיבות יתרה לפרוטוקולים של שיתוף מזהים ולמפות את תכולת ה-CTI באמצעות דירוג הכולל מדדים פשוטים ותיאורים טכניים של טקטיקות התקפות.⁴ אולם, בשנים האחרונות נראה כי חל שינוי במחקר בנושא; כך למשל חוקרים מובילים התלוננו שה-CTI היה ל"מוצר ללא תהליך", הציף את מערכות האבטחה בהזנות נתונים (feeds) חסרי פשר, נכשל במימוש מעגל המודיעין ולא הצליח לתרגם מידע חיצוני למשמעויות בעלות ערך לארגון (שאלת ה-what So?).⁵ אחרים ביקרו את השתלטות נקודת המבט הטכנולוגית על ה-CTI, הצביעו על הפער בין הכלים הטכניים הרבים למחסור במיומנות ניתוח וקראו לשלב את המודיעין באופן מלא במסגרות של ניהול סיכונים.⁶

כך נוצר פרדוקס מרכזי בהתפתחותו של מודיעין הסייבר האזרחי: ככל שהתרחב בסיס המידע שלו, הצטמצמה שפתו לרבדים הטכנולוגיים; ככל שהוא התמחה יותר בטלמטריה ובחקירות אירוע, התכנס אל עולמות הזיהוי והתגובה והתרחק מן השאלות הארגוניות הרחבות שאותן נועד לשרת. המודיעין הפך עשיר יותר בנתונים, אך לא בהכרח אפקטיבי יותר בהכוונת החלטות; מדויק יותר בזיהוי סימנים טכניים, אך מתקשה להפיק מהם משמעות מערכתית. כיצד אפוא אפשר להשיב למודיעין הסייבר את תפקידו הפרשני בלי לוותר על מומחיותו הטכנית? וכיצד נכון לשלב בתהליכים שבהם ארגונים מגדירים ומנהלים סיכונים עסקיים?

הסדק במעמדה של ההתרעה

לצד הצמצום להיבטים טכניים וטקטיים, התפתחות מודיעין הסייבר חשפה מגבלה יסודית נוספת: המתח שבין מושג ההתרעה הביטחוני הקלאסי לתנאי הפעולה של מרחב הסייבר. במילון למונחי צה"ל מוגדרת התרעה כ"ידיעה או הערכה בדבר כוונותיו של האויב לתקוף או לבצע פעולה עוינת, הניתנת זמן מספיק מראש כדי לאפשר היערכות וכדי למנוע הפתעה".⁷ ההיסטוריה הישראלית העניקה מקום של כבוד להתרעה והגדירה אותה כאחד מעמודי התווך של תפיסת הביטחון; אולם שתי נקודות האחיזה המרכזיות של מושג זה – "כוונותיו של האויב" ו"זמן מספיק" – מקבלות משמעות אחרת אם מנסים להחיל אותן על תחום הסייבר: **"כוונותיו של האויב"**. המערכה המתנהלת בעולם הסייבר מתאפיינת באופורטוניזם רב, ורובם ככולם של אירועי התקיפה בעולם זה הם עדות לכך.⁸ הזירה הסייברית אכן מורכבת ממספר רב של שחקנים אופורטוניסטיים: ב-2026 נמנו כ-160–170 קבוצות אשר עסקו בפשיעת סייבר⁹ וכ-300 התארגנויות אקטיביסטיות.¹⁰ במקרים רבים גם קבוצות שפועלות בתוך מסגרות מדינתיות, מאמצות דפוס פעולה אופורטוניסטי ובוחרות יעדים קונקרטיים בהתאם להזדמנויות בשטח. כך או כך, הדומיננטיות של

3 בהקשר הזה מעניין לבחון את השינוי בעשור וחצי האחרון בתפיסת האיומים. MANDIANT (2010). M-TRENDS REPORT: THE ADVANCED PERSISTENT THREAT; MANDIANT (2026). M-TRENDS REPORT: REAL-WORLD INVESTIGATIONS AND ACTIONABLE DEFENSE INSIGHTS

4 TOUNSI, W., & RAIS, H. (2018). A SURVEY ON TECHNICAL THREAT INTELLIGENCE IN THE AGE OF SOPHISTICATED CYBER ATTACKS. COMPUTERS & SECURITY, 72, 212-233

5 OOSTHOEK, K., & DOERR, C. (2021). CYBER THREAT INTELLIGENCE: A PRODUCT WITHOUT A PROCESS? INTERNATIONAL JOURNAL OF INTELLIGENCE AND COUNTERINTELLIGENCE, 34(2), 300-315

6 AINSLIE, S., THOMPSON, D., MAYNARD, S., & AHMAD, A. (2023). CYBER-THREAT INTELLIGENCE FOR SECURITY DECISION-MAKING: A REVIEW AND RESEARCH AGENDA FOR PRACTICE. COMPUTERS & SECURITY, 132

7 אג"ם"ת"ד (1998). המילון למונחי צה"ל, כרך א', עמ' 142. לדיון עדכני במושג "התרעה" אשר מבחין בין התרעה בסיסית להתרעה ממשית, ראו אצל איזין, ג' (2025), 20 באוקטובר). ההתרעה הבסיסית – מבחנה העליון של המודיעין האסטרטגי. המרכז למורשת המודיעין והמכון לחקר המתודולוגיה של המודיעין

8 EXPEL (2025). ANNUAL THREAT REPORT 2025

9 CROWDSTRIKE (2026, FEBRUARY 24). 2026 GLOBAL THREAT REPORT: AI ACCELERATES ADVERSARIES AND RESHAPES THE ATTACK SURFACE

10 RADWARE (2026). 2026 GLOBAL THREAT ANALYSIS REPORT

שחקנים אופורטוניסטיים מציבה סימני שאלה בנושא מחקר הכוונות. לתוקפים בסייבר יכולות להיות כוונות, אך אלו מתחלפות באופן תדיר, מתקבלות לאור תנאים מקומיים משתנים ומתורגמות לפעולה בזמן אפסי. בסופו של דבר, ממד הכוונה אינו נעדר מעולם הסייבר, אולם היכולת להתבסס עליו לצורך חיזוי דטרמיניסטי של התנהגות האויב מוגבלת.

"זמן מספיק". בעוד שבעבר איסוף על כוחות צבאיים העניק למגן חלון זמן של שבועות, מתקפת סייבר יכולה להתממש בתוך שעות. בתנאי זמן אלו, המוקד עובר באופן טבעי ממודלי התרעה למערכות ניטור רציפות.¹¹ בשנים האחרונות הצטמצם אף יותר חלון הזמן שבין קבלת ההחלטה לתקוף למימוש התקיפה: ב-2026 משך הזמן הממוצע אשר נדרש למעבר מחדירה ראשונית לרשת לתנועה רוחבית בה הוא 29 דקות בלבד;¹² בתקיפות מהירות שאיבת מידע מתחילה בתוך פחות מ-72 דקות;¹³ וניצול חולשות מקדים את פרסום התיקון בשבעה ימים בממוצע.¹⁴ התפתחות מודלים מתקדמים של בינה מלאכותית, כמו למשל Mythos או ChatGPT 5.5, עלולה אף להגביר את המגמה הזו ולאפשר בטווח הנראה לעין תקיפות אוטומטיות שיימשכו שניות בודדות.

למרות מאפיינים אלו דומה כי חלק מן העוסקים בתחום במערכת הביטחונית מנסים לשמר את מושג ההתרעה בתנאי פעולה שגורמים לו להיות פחות טבעי. כך למשל חוקרים ממכון ראנד ביקשו להחיל מודלים של סימנים מעידים על אירועי סייבר ולשכנע כי אפשר לשפר את פעילות ההגנה באמצעות הצגת תרחיש גאופוליטי, או באמצעות מיקוד ה-CTI באיסוף מקדים של מידע על היריבים;¹⁵ באופן דומה, פורום "הברית למודיעין ולביטחון לאומי" המליץ להוסיף "מזהים אסטרטגיים" למזהים הטכניים אשר בדרך כלל משרתים את אנשי ה-CTI;¹⁶ וחוקרים אחרים מנסים לשלב את הסייבר במודלים כמותיים ואיכותניים של חיזוי סיכונים מדינתיים.¹⁷ בסופו של דבר, ולמרות ניסיונות אלו תחום הסייבר מטיל ספק בשתי הנחות היסוד המרכזיות של מושג ההתרעה: היכולת לגזור חיזוי מתוך הבנת הכוונות של האויב, והציפייה כי המודיעין יספק זמן מספיק להתארגנות. האם אפשר להסיק מכך שאין מקום למודיעין בעולם הסייבר? לא בהכרח.

ההבחנה המושגית שהציעו הוסאק ואחרים, יכולה להיות מסגרת לניתוח.¹⁸ ראשית, גם אם פעילות ה-CTI אינה נסובה סביב מושג ההתרעה, תפקידה לספק חיזוי מגמות (forecasting) המאפשר לארגונים – צבאיים ואזרחיים כאחד – לגבש אסטרטגיה להתמודדות מושכלת עם היריב. בדומה לכל תחום מודיעין אחר, ה-CTI פועל כדי ליצור מודעות מצבית, לנתח את דפוסי הפעולה של היריב ולכוון תהליכי קבלת החלטות בתחומי ההגנה והסיכול.

שנית, ה-CTI בעל יכולת ניבוי (prediction), כלומר ביכולת לזהות תקיפות מבעוד מועד על סמך הערכות הסתברותיות (גם בהיעדר ידיעה על כוונה קונקרטית של היריב). כך למשל, פלטפורמות שונות מנטרות את תעבורת האינטרנט העולמית ומספקות תובנות ונתונים על ניסיונות של גורמי פשיעה לסרוק חולשות למיניהן. אף שסריקת חולשות אינה ערובה לניצול מוצלח שלהן, היא מדד איכותי ומהימן לרמת העניין של התוקפים בהן – בייחוד אם מזהה גידול רב בהיקף הסריקות, או בכמות התוקפים הייחודיים שמבצעים אותן.

שלישית, ה-CTI מאפשר צפיית מהלכים (projection), כלומר לזהות את התוקף או לחזות את הצעד הבא שלו בעת מתקפה פעילה. צפיית מהלכים נשענת במידה רבה על היכרות עמוקה עם הטכניקות ודפוסי ההתנהגות של היריב, ואלה ממופים במודלים דוגמת TTPs, CK&ATT, MITRE. יש חשיבות רבה גם לאיסוף "סימנים מעידים" בשטח, בין אם אלה מזהים התנהגותיים (IOA – Indicators of Attack) ובין אם הם מזהים טכניים (IOC – Indicators of Compromise).

מודיעין לאומי סייבר הוא אפוא אכן מודיעין, אך מודיעין מסוג אחר – כזה שאינו נשען בראש ובראשונה על הדיאלקטיקה הקלסית בין כוונות ליכולות, ואינו רואה במתן התרעה עיקרון מכונן. מכאן עולה שאלה רחבה יותר: אם ההתרעה אינה יכולה עוד להיות נקודת מוצא בלעדית לפעולת ההגנה, מהו הרעיון המארגן שיחליף אותה? בנקודה זו מציעה תעשיית הסייבר המסחרית תשובה מעניינת: מעבר מהתמקדות בהבנת האויב לניהול רציף של חשיפות הארגון לאיומים החיצוניים. בהתאם לכך המשך הדיון

PROCTOR, J. (2024). THE WARNING RENAISSANCE: ADVANCING THE ART AND SCIENCE OF WARNING IN THE US INTELLIGENCE COMMUNITY AND BEYOND. NATIONAL INTELLIGENCE UNIVERSITY 11

(2026) CROWDSTRIKE 12

PALO ALTO NETWORKS, UNIT 42 (2026). GLOBAL INCIDENT RESPONSE REPORT 2026 13

MANDIANT (2026) 14

HODGSON, LILLY, BILYANA, MOORE, ALYSON, AND MA, LEN (2020). RAND'S SCALABLE WARNING AND RESILIENCE MODEL (SWARM): ENHANCING CYBER WARNING AND RESILIENCE, RAND CORPORATION 15

MATTERN, T., FELKER, J., BORUM, R., & BAMFORD, G. (2014). OPERATIONAL LEVELS OF CYBER INTELLIGENCE. INTERNATIONAL JOURNAL OF INTELLIGENCE AND COUNTERINTELLIGENCE 16

RIEDL, S., & RUNGE, L. (2025). CYBER THREATS AND CRISIS EARLY WARNING. CISS MUNICH WORKING PAPERS 17

HUSÁK, M., KOMÁRKOVÁ, J., BOU-HARB, E., & ČELEDÁ, P. (2019). SURVEY OF ATTACK PROJECTION, PREDICTION, AND FORECASTING IN CYBER SECURITY. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 21(1), 640-660 18

במאמר זה עוסק בעיקר בעולם ההגנה הארגונית, שבו השפעתה של תעשיית הסייבר המסחרית על מושגי העבודה ועל תהליכי ההגנה הייתה עמוקה במיוחד.

הפניית המבט פנימה

מאדום לכחול: מהערכת אויב להערכת חשיפה

במערכת הביטחון נתפס המודיעין לא פעם כנקודת המוצא של המעשה הצבאי. עיקר המאמץ מופנה להבנת היריב: כוונותיו, יכולותיו, דפוסי פעולתו, מגבלותיו וההיגיון המארגן את החלטותיו. הבנה זו אמורה לאפשר למערכת הביטחונית לגבש התרעה, לבנות תפיסת הפעלה, להיערך למבצע ולעצב את בניין הכוח העתידי. במובן זה המבט המודיעיני מופנה בראש ובראשונה אל הצד האדום, כלומר אל האויב; המודיעין מבקש לפענח את האויב, ובהתבסס על פענוח זה להגדיר את פעולת "כוחותינו".

אולם אם מעתיקים את ההיגיון הזה אל עולם הסייבר הארגוני, מגבלותיו מתגלות במהירות. מרחב הסייבר אינו מתאפיין רק בקיומו של אויב מוגדר ובעל כוונות יציבות ויכולת פעולה הניתנת למעקב רציף, אלא בריבוי שחקנים, כלים, טכניקות והזדמנויות. חלק ניכר מן הפעילות ההתקפית במרחב זה אינו מתחיל בהחלטה מוקדמת לתקוף ארגון מסוים, אלא בזיהוי התנאים המאפשרים פעולה התקפית: נכס חשוף, חולשה בלתי מטופלת, זהות שנגנבה, תצורה שגויה, נתיב גישה פתוח. במציאות כזו השאלה "מי מתכוון לתקוף אותנו" חשובה, אך היא אינה יכולה עוד להיות בסיס מספק לתהליך ההגנה; לצידה, ולעיתים לפניו, ניצבת שאלה אחרת: באילו תנאים אנחנו חשופים לתקיפה אפשרית?

בנקודה זו מתרחש המעבר מאדום לכחול. אין מדובר בויתור על הבנת היריב, אלא בהכרה בכך שמשמעותו המעשית של האיום נקבעת רק במפגש בינו למצב החשיפה של הארגון. למודיעין על קבוצת תקיפה, על טכניקת פעולה או על חולשה מנוצלת בעולם יש ערך ממשי רק אם אפשר לברר כיצד הוא מתקשר לנכסי הארגון, למערכותיו, לזהויותיו, לבקורות ההגנה שלו ולנתיבי התקיפה האפשריים בתוכו. ללא הקשר הזה גם מודיעין חיצוני איכותי עלול להישאר יתום, נטול השפעה של ממש על פעולת ההגנה. כדי להבין את השינוי הזה יש לעבור מן הדיון במודיעין כשלעצמו אל אחת מאבני היסוד של ההגנה בסייבר הארגוני: החולשה. בעשורים האחרונים התפתח תחום מקצועי שלם העוסק בניהול חולשות שנועד לאפשר לארגונים לזהות, למדוד, לתעדף ולתקן את נקודות הפגיעות בסביבתם הדיגיטלית. אולם דווקא תחום זה, שנועד לספק מענה מסודר לשאלת החשיפה הארגונית, נקלע בשנים האחרונות למשבר עמוק.

החולשה כאבן יסוד של ההגנה הארגונית

המכון הלאומי לתקנים וטכנולוגיה בארצות הברית (NIST – National Institute of Standards and Technology) מגדיר חולשה כ"פגם בנהלי האבטחה, בתכנון, במימוש או בבקורות הפנימיות של מערכת, אשר עלול להיות מנוצל ולגרום לפרצת אבטחה או להפרה של מדיניות האבטחה"¹⁹. במילים אחרות, חולשות תוכנה הן למעשה "באגים" המאפשרים לתוקף (שלמד לנצל אותן) לבצע מגוון פעולות זדוניות – החל בקבלת הרשאות לגשת לנכס מסוים וכלה ביכולת להריץ קוד ברשת של הקורבן.

החולשה הייתה לאחת מיחידות העבודה המרכזיות של ההגנה בסייבר, משום שהיא מעניקה לפגיעות תצורה ניתנת לניהול. כל עוד הסיכון מנוסח במונחים כלליים – תוקפים, כוונות, קמפיינים או מגמות – קשה לארגון לגזור ממנו פעולה קונקרטית; לעומת זאת חולשה אפשר לזהות, לתייג, לדרג, לשייך לנכס מסוים, להגדיר את האחריות לה, ולבסוף לטפל בה. במובן זה חשיבותה אינה טכנית בלבד, אלא נובעת מכך שהיא מתרגמת את שאלת הפגיעות הארגונית למשימת עבודה.

בהתאם לכך התפתחה שפה מקצועית שאפשרה לעשות את החולשות לאובייקט ניהולי. מנגנון להגדרת חולשות ופגיעות נפוצות (CVE)²⁰ מעניק לכל חולשה תיאור ומוזהה מוסכמים, והודות לכך חוקרים, יצרנים, ארגונים וכלי אבטחה יכולים לכוון פגם מסוים באותו השם; בד בבד הציון במערכת לדירוג חולשות נפוצות (CVSS)²¹ מדרג את חומרת החולשה בסולם שבין 0 ל-10. שני המנגנונים האלה יצרו תשתית חיונית לניהול חולשות בקנה מידה גדול, שכן הם מאפשרים השוואה, סריקה, דיווח ותעדוף ראשוני. אולם הם גם מגלמים מגבלה יסודית: מנגנונים אלה מתארים את החולשה באופן גנרי, אך אינם יודעים לקבוע את משמעותה בתוך ארגון מסוים – האם הנכס הפגיע חשוף או מוגן? האם הוא חיוני? האם הוא מצוי בנתיב תקיפה ריאלי?

הצורך בשפה משותפת זו התחדד ככל שחולשות הפכו נפוצות יותר. אף שתוקפים יכולים לחדור לארגון גם באמצעות מבצעי דיוג,

NIST COMPUTER SECURITY RESOURCE CENTER (N.D.). VULNERABILITY. IN NIST GLOSSARY. [HTTPS://CSRC.NIST.GOV/GLOSSARY/TERM/VULNERABILITY](https://csrc.nist.gov/glossary/term/vulnerability) 19

COMMON VULNERABILITIES AND EXPOSURES 20

COMMON VULNERABILITY SCORING SYSTEM 21

שימוש בפרטי הזדהות גנובים או מניפולציה על משתמשים, בשנים האחרונות ניצול חולשות היה לנתיב חדירה מרכזי; למעשה, כיום כשליש ממקרי הפרצה מתבססים על ניצול חולשות.²² הדבר נובע מהדמוקרטיזציה של הידע על גילוי וניצול של חולשות, מזמינותם של כלי תקיפה ושל קודי ניצול, ומהתחזקות אמצעי ההגנה מפני וקטורים אחרים (כמו למשל אימוץ נרחב של תהליך אימות רב-שלבי). במצב עניינים זה היכולת לזהות חולשות ולטפל בהן הייתה לתנאי בסיסי להגנה ארגונית.

לכאורה המענה לבעיה פשוט: משפורסמה חולשה, היצרן מתקן אותה, הארגון מתקין עדכון, והסיכון נסגר. אולם במציאות הארגונית הרווחת פעולה זו מורכבת הרבה יותר: לא פעם ארגונים גדולים מתקשים לדעת אלו נכסים דיגיטליים קיימים ברשותם, אלו גרסאות מותקנות בהם, מי אחראי עליהם, ואם תיקון מסוים עלול לפגוע במערכות ייצור, בתלויות תוכנה (dependencies) או ברציפות העסקית. סגירת חולשה אינה אפוא פעולה טכנית מבודדת, אלא תהליך המחייב נראות, בעלות, תיאום בין אבטחת מידע לצוותי IT, בדיקות תאימות, ולעיתים גם הכרעה בין סיכון אבטחה לסיכון תפעולי.

צורך זה היה הבסיס ללידתו של תחום ניהול החולשות (VM – Vulnerability Management). המטרה הייתה לקחת מרחב כאוטי של פגיעויות טכניות וליצור תהליך סדור: סריקה, דירוג, טיפול, אימות ודיווח. ה-VM העניק לארגונים דרך מעשית לנהל את פגיעותם העצמית – מיקוד ההגנה עבר מן האיום הכללי אל רשימת פערים קונקרטיים, והודות לכך נבנה מנגנון המאפשר למדוד התקדמות, לחלק תחומי אחריות ולהציג להנהלה תמונת מצב.

אולם דווקא הצלחתו של מודל זה חשפה את מגבלותיו: ככל שניהול החולשות התמסד והיה לפרקטיקה ארגונית מרכזית, התבררה תלותו בהנחת יסוד בעייתית – חולשה טכנית היא יחידת הסיכון המרכזית. מה שנראה תחילה כמנגנון סדור לזיהוי, לדירוג ולתיקון של פערי אבטחה, החל להתערער תחת משקלם של היקפי חולשות עצומים, סביבת תקיפה דינמית וקושי גובר להבחין בין חולשה חמורה על הנייר לסיכון ממשי לארגון.

משבר ניהול החולשות

בשנים האחרונות נקלע תחום ניהול החולשות למשבר עמוק. בבסיסו עומד פער הולך וגדל בין היקף החולשות שהארגון נדרש לנהל, ליכולתו המעשית להבין, לתעדף ולתקן אותן בזמן. ב-2025 דווח על מספר שיא של 48,185 חולשות חדשות, כלומר 132 חולשות חדשות ביום.²³ במקביל, התשתית הארגונית נעשתה מורכבת יותר בשל שימוש מסיבי בתוכנות קוד פתוח, ברכיבי צד שלישי, בשירותי ענן ובמערכות "תוכנה כשירות" (SaaS – Software as a Service); הדבר גורם לכך שחולשה אחת בספרייה נפוצה עשויה להשתכפל וליצור אלפי מופעים בתוך הארגון. התוצאה היא הצפה מתמשכת: קצב הופעת החולשות מהיר משמעותית מיכולתם של צוותי האבטחה וה-IT לספק מענה להן.

הצפה זו חשפה את חולשתו של מנגנון התעדוף המסורתי. תהליכי VM קלסיים נשענו, ולעיתים עדיין נשענים, על ציון ה-CVSS – ציון אשר מתאר חומרה טכנית גנרית, אך לא בהכרח ממחיש את הסיכון בפועל לארגון. בשל כך, אלפי חולשות מוגדרות אפוא כ"גבוהות" או "קריטיות", אף שרק חלק קטן מהן אפשר לנצל (או נמצא בשימוש פעיל של תוקפים). כך למשל סקרים הראו כי לא פחות מ-51% מכלל החולשות אשר מזוהות בארגונים מוגדרות כסיכון גבוה או קריטי. שיעור כה גבוה גורם לכך שהסיווג עצמו הופך כלי תעדוף לא אפקטיבי;²⁴ האינפלציה בציונים יוצרת ריבוי התערות, עומס תפעולי ומרדף בלתי פוסק אחר חולשות שלא בהכרח גורמות לסיכון ממשי.

בעיה זו מתחדדת עוד יותר לנוכח הצטמצמות חלון ההגנה. פרק הזמן שבין פרסום חולשה לתחילת ניצולה התקצר מאוד, ותוקפים מודרניים יכולים להתחיל לסרוק אחר חולשה בארגון דקות בודדות לאחר פרסומה. לפי נתוני חברת התקשורת ורייזון (Verizon), הזמן החציוני אשר חולף מרגע פרסומה של חולשה עד שתוקפים מתחילים בניצול המוני שלה הוא שעות בודדות; לעומת זאת לארגונים נדרשים במוצע 43 ימים כדי לתקן חולשה קריטית שהתגלתה.²⁵ בעידן המתאפיין בכך שקצב האוטומציה בצד התוקף גבוה הרבה יותר מקצב ניהול העדכונים בצד המגן, ארגונים מצויים בנחיתות מובנית.

לכך מצטרף שינוי עמוק בשטח התקיפה עצמו. מודל ה-VM עוצב במידה רבה עבור ארגונים אשר עיקר נכסיהם היו שרתים ותחנות עבודה הנמצאים בתוך רשת סגורה ומנוהלת; אולם בעידן הענן, ה-SaaS, הזהויות המבוזרות והעבודה מרחוק שטח התקיפה משתנה ללא הרף. סריקות תקופתיות מספקות תמונת מצב נקודתית אחת לשבוע, או אחת לחודש, ואינן מצליחות לשקף את

MANDIANT (2026) 22

/GAMBLIN, J. (2026). 2025 CVE DATA REVIEW. <https://jerrygamblin.com/2026/01/01/2025-cve-data-review> 23

MUKERY, A. (2026, FEBRUARY 24). IN-DEPTH LOOK INTO DATA-DRIVEN SCIENCE BEHIND QUALYS TRURISK. <https://blog.qualys.com/qualys-insights/2022/10/10/in-depth-look-into-data-driven-science-behind-qualys-trurisk> 24

VERIZON (2025). 2025 DATA BREACH INVESTIGATIONS REPORT 25

הדינמיות הזו: הן מתארות את הארגון כפי שהיה ברגע הסריקה, אך לא בהכרח את חשיפתו בפועל בזמן אמת. הבעיה הגדולה ביותר היא שניהול החולשות המסורתי נוטה לטפל בחולשות כאירועים בדידים. הוא יודע לזהות חולשה בשרת מסוים, אך מתקשה להבין אם אותו השרת מחובר למידע רגיש, אם הוא נגיש מבחוץ, אם קיימות בקורות הממתנות את הסיכון, או אם הוא חוליה בנתיב תקיפה רחב יותר. התוקפים, לעומת זאת, אינם מחפשים חולשות כשלעצמן אלא נתיבים: הם מצרפים חולשות, זהויות, תצורות שגויות והרשאות עודפות כדי ליצור מסלול פעולה המוביל לנכס בעל ערך. לנוכח היגיון פעולה זה ה-CTEM המסורתי מתקשה לחבר בין פגיעויות טכניות בודדות וליצור תמונת סיכון עסקי כוללת. הצטברות משברים הובילה את קהילת הסייבר העולמית לתובנה כי מודל ה-CTEM המסורתי חדל להיות מסגרת מספקת לניהול סיכונים סייבר. התפיסה החדשה מתרחקת מן השאיפה "לתקן הכול" (patch everything) ומאמצת במקומה היגיון הוליסטי יותר השואף לניהול מתמשך של החשיפות לאיומים: ה-CTEM.

מודיעין הסייבר בעידן ה-CTEM ה-CTEM כתפיסה מערכתית

CTEM (ניהול מתמשך של חשיפה לאיומים, Continuous Threat Exposure Management) הוא מסגרת עבודה שצמחה בשנים האחרונות על רקע המשבר אשר פקד תפיסות ניהול מסורתיות בסייבר, כמו למשל תפיסת ניהול החולשות. מסגרת עבודה זו אינה מסתכמת בתהליכי ניהול יעילים יותר, אלא מסמנת תמורה מתודולוגית חשובה: מעבר מגישה תגובתית הממוקדת בקטלוג ליקויים אל מודל פרואקטיבי של ניהול סיכונים המבוסס על חשיפה ממשית. ה-CTEM רואה בהגנת הסייבר חלק בלתי נפרד מהאסטרטגיה העסקית, והיא מטמיעה אותה תוך כדי יצירת שפה משותפת עם הנהלת הארגון ורתימתה לתהליך. הודות לכך הטיפול בחשיפות אינו מסתכם עוד בפעולות של "היגיינה" טכנית, או של עמידה ברגולציה, אלא הופך רכיב מפתח בחוסן הארגוני. חברת המחקר והייעוץ Gartner הגדירה את ה-CTEM כ"גישה פרגמטית ושיטתית [...] להערכה מתמשכת של נגישותם, חשיפתם ויכולת הניצול של נכסים דיגיטליים, תוך התאמת המענה לווקטורי התקיפה המשתנים".²⁶ במילים אחרות, הגישה החדשה שואפת לאמוד את פוטנציאל המימוש האמיתי של החשיפות השונות ולהציע דרכים יעילות לצמצום הסיכון בהתאם ליעדי הארגון. מתודולוגיית ה-CTEM מסמנת במידה רבה את עלייתה של הגנת הסייבר לרמה המערכתית: היא מארגנת מחדש טיפולים נקודתיים בממצאים לכדי מאמץ מתמשך בעל היגיון רחב, והיא שוזרת מבצעים טקטיים של זיהוי, תיקון ואימות לכדי תכלית אסטרטגית רחבה - תוך הכתבת קצב עבודה, סדרי עדיפויות והקצאת משאבים דינמית. מנקודת מבט זו, המערכה ההגנתית אינה נאמדת לפי מספר הליקויים שנסגרו, אלא לפי מידת הצלחתו של הארגון לצמצם באופן שיטתי את נתיבי התקיפה הריאליים נגדו. תפיסה זו מושרשת במחקרים עדכניים אשר ממשיגים את ההגנה בסייבר כתחרות של למידה והסתגלות המצריכות "מנטליות של מערכה";²⁷ קוראים לאמץ אנלוגיות צבאיות ולנסח תפיסה של "הגנת סייבר מבוססת משימה";²⁸ ומקדמים את הרעיון של "הגנת סייבר הוליסטית" באמצעות סנכרון בין פונקציות ארגוניות מגוונות לשם יצירת סינרגיה הגנתית לאורך זמן.²⁹ בפועל המעבר מ-CTEM ל-CTEM בא לידי ביטוי בכמה תמורות מרכזיות - חלקן מושגיות, חלקן תהליכיות:

הראשונה היא מעבר מחומרה טכנית לסיכון ארגוני. גישת ה-CTEM אינה מסתפקת בציון גנרי לתיאור חומרת החולשה, אלא מבקשת להעריך את הסיכון בהתבסס על ניתוח הקשרי של מיקום הנכס ברשת, הקושי המעשי לנצל בו חולשה, חשיבותו העסקית וקיומם של נתיבי תקיפה המקשרים בינו לליבת המידע של הארגון.

השנייה היא מעבר מסגרת חולשות לניהול סיכון. במקום לראות בכל חולשה ממצא אשר מחייב "סגירה", ה-CTEM בוחן את הסיכון בהקשר רחב יותר ומבקש למנוף בקורות אבטחה קיימות. בבסיס גישה זו מצויה הבנה שאפשר לנהל סיכונים סייבר - חלק מהסיכונים אפשר לקבל, באחרים יש לטפל באמצעות השקעת משאבים, ולשאר אפשר למצוא בקורות מפצות או פתרונות חלופיים. השלישית היא מעבר מאחריות של צוותי IT לרתימת הארגון כולו. ה-CTEM מחייב חיבור בין העוסקים באבטחת המידע, צוותי ה-IT, הנהלת הארגון ומנהלי הסיכונים העסקיים. הוא ממיר דוחות טכניים לשפה ניהולית משותפת שבמרכזה הסכמה על רמות סיכון קבילות וגיבוש תכנית פעולה כלל-ארגונית. הרביעית היא מעבר מסריקות תקופתיות לניהול מחזורי ורציף. ארגונים רבים עדיין

GARTNER (2025, AUGUST 26). STRATEGIC ROADMAP FOR CONTINUOUS THREAT EXPOSURE MANAGEMENT 26

WILLARD, G. N. (2015). UNDERSTANDING THE CO-EVOLUTION OF CYBER DEFENSES AND ATTACKS TO ACHIEVE ENHANCED CYBERSECURITY. JOURNAL OF INFORMATION WARFARE, 14(2), 27 27

D. L., YOO, E., WELTE, J. J., & SINCLAIR, P. (2025). PULLING THE THREAD: A CAMPAIGN APPROACH TO MISSION THREAT DEFENSE OF FORCE PROJECTION. THE CYBER DEFENSE REVIEW, 10(2), 81-97 28

DE NOBREGA, K. M., RUTKOWSKI, A. F., & SAUNDERS, C. (2024). THE WHOLE OF CYBER DEFENSE: SYNCING PRACTICE AND THEORY. THE JOURNAL OF STRATEGIC (INFORMATION SYSTEMS, 33(4) 29



מחזור ה-CTEM

פועלים במתכונת של סריקות שבועיות, אולם ה-CTEM מציע תהליך מתמשך המותאם לקצב השינוי של שטח התקיפה. ולבסוף היא מעבר מהסתכלות דיכוטומית על פנים וחץ להסתכלות על רצף מרחבי. במקום החלוקה המיושנת בין הגנה על הרשת הפנימית לניטור האיומים החיצוניים, ה-CTEM מאגד את "האדום" ו"הכחול" למרחב "סגול" אחד. הודות לכך אפשר לראות את הארגון בעיניו של התוקף ולנהל את הסיכון כרצף מתמשך. בהקשר זה נהוג להגדיר את שלבי מחזור ה-CTEM:

תיחום (scoping). קביעת סדרי העדיפויות העסקיים וגבולות הגזרה של התהליך. בשלב הזה הארגון מזהה ומתעדף את הנכסים, התהליכים העסקיים והתשתיות שחיוני ביותר להגן עליהם. לשם כך נדרשת הבנה של ההקשר העסקי ושל סדרי העדיפויות הארגוניים, כמו גם סימון של "נכסי יהלום" ומרחבים הנמצאים מחוץ לטווח העשייה.

גילוי (discovery). סריקה מקיפה ומיפוי של כלל החשיפות הרלוונטיות – לרבות חולשות תוכנה, נכסים לא מנוהלים, שירותים שיצאו משירות, שגיאות בהגדרות מערכת, או סוגיות של הרשאות וזהויות.

תעדוף (prioritization). זיהוי ודירוג של האיומים הממשיים באמצעות ניתוח רכיבים דוגמת פוטנציאל הניצול (exploitability), רמת החומרה הטכנית והחשיבות העסקית של הנכס שעלול להיפגע.

אימות (validation). בחינת האפשרות לטפל בחשיפות באמצעות מערכי ההגנה הקיימים. השלב הזה כולל תיקוף של יעילות אמצעי האבטחה, ומסנן החוצה את אותן החשיפות אשר אינן עלולות לסכן בפועל את הארגון.

הנעה לפעולה (mobilization). יישום של צעדים לשיפור האבטחה, תוך כדי התמקדות בשיתוף הפעולה בין צוותי האבטחה לצוותי ה-IT והתפעול ובגיבוש תוכנית פעולה ארגונית לצמצום סיכונים.

בעולמות האבטחה בסייבר, ה-CTEM היא פרדיגמה חדשה לניהול חשיפות, אך לענייננו, הוא גם הזדמנות להחזיר את מודיעין הסייבר למקום שהוא נדחק ממנו בהדרגה. אם במשך שנים ה-CTI התכנס לשפה טכנית המנותקת מההקשר העסקי, הרי ה-CTEM מחייב את המודיעין לשוב ולדבר בשפה ארגונית-מערכתית על אודות מושגים רלוונטיים: סיכונים עסקיים, תרחישי תקיפה, סבירות מימוש, סדרי עדיפויות, הקצאת משאבים. כמו כן ה-CTEM משנה את תפקיד המודיעין בשרשרת הערך: המודיעין אינו נתפס עוד כנקודת מוצא עצמאית והכרחית לסיכול ולמניעה, אלא כרכיב הקשרי אשר משולב בתהליכי קבלת החלטות וחיוני להזנת שלבים במחזור ההגנה הארגוני (בפרט בשלבי התיחום והתעדוף).

המודיעין כתשתית לתיחום איום הייחוס הארגוני

בשלב התיחום – שלב הגדרת המערכת לפי המינוח הביטחוני – המודיעין ממלא תפקיד חשוב של מתן היגיון והקשר המאפשר לארגון לגבש אסטרטגיית פעולה. כך התיחום אמור לשקלל גם איומים חיצוניים בבואו להגדיר גבולות גזרה. העניין מחייב את הארגון להתעמק בספקטרום האיומים העדכניים: מי הם התוקפים הפוטנציאליים, באלו טכניקות הם משתמשים, מה הן מטרותיהם, ואלו נכסים או תהליכים הם נוטים לתקוף. אולם, נוסף על אלו, חשובה גם היכרות עם הארגון עצמו, על התהליכים העסקיים והנכסים שלו: מאלו תרחישי תקיפה הוא חושש, היכן נשמר המידע הרגיש שלו או כיצד פועלים השירותים החיוניים שהוא מספק. שילוב זה בין "צד אדום" ל"צד כחול", כלומר בין הבנת התוקפים הפוטנציאליים להבנת החששות וסדרי העדיפויות של הנהלת הארגון, הוא המפתח לתיחום מוצלח.

בשלב הזה אפשר, ולעיתים רצוי, להתמקד ביריבים ספציפיים. ארגון יכול להימצא "על הכוונת" של תוקפים בשל שיוכו המגזרי, מיקומו הגאופוליטי או הנכסים הייחודיים שהוא מחזיק. כך למשל חברת תקשורת עשויה לסמן שחקנים מדינתיים סיניים כאיום רלוונטי, ואילו ארגון המספק שירותים אינטרנטיים יחשוש בייחוד משחקנים המתמחים בתקיפות מניעת שירות (DoS – Denial of Service). למעשה, הצבעה של אנשי המודיעין על תוקפים רלוונטיים לארגון בעת נתונה, מסייעת

לקבוע את איום הייחוס הארגוני בתחום הסייבר. מכאן, פעולות הסריקה, החקירה והתיקון יכולו לנוכח איום ייחוס זה. כך למשל, תחת איום של ריגול תעשייתי, תתמקד האסטרטגיה בהגנה על קניין רוחני ומניעת דליפת מידע; לעומת זאת, למול איום שיבוש תסיט את המוקד לתשתיות קריטיות ולהבטחת רציפות תפעולית. תיחום מוכוון-איום מבטיח כי כל שלבי מחזור ה-CTEM יהיו ממוקדים ויעילים יותר, כשהם מספקים מענה ישיר לתרחישי ייחוס המבוססים על מודיעין.

מעבר להתעדכנות שוטפת, מודיעין על סביבת האיומים מחייב יצירתיות ויכולת תרחוש. פונקציות מודיעין סייבר הפועלות בארגונים מסחריים מתמודדות עם מידע חלקי ביותר, כשהן נעדרות היסטוריה חיכוך עם אויב מוגדר (בניגוד למקביליהם במערכת הביטחונית). הצבעה על אויב פוטנציאלי נעשית תוך כדי גישוש באפלה: על איש המודיעין לדמיין את נתיב התקיפה העתידי אשר רלוונטי ביותר לארגונו בהיבט של סבירות התקיפה, כמו גם בהיבט של השלכותיו האפשריות. אין מדובר במודל קשיח של "מקרים ותגובות" - שכן הממד הריאקטיבי מול התוקף נעדר כאן - אלא בדרישה מאנשי המודיעין להפעיל דמיון ולשרטט תרחישי תקיפה פוטנציאליים, לצקת לתוכם הקשר וסימנים, ולזקקם לכדי סיפור (narrative) עבור מקבלי ההחלטות האמונים על הגדרת מרחב החשיפה הארגוני.

כמו כן, עבודת המודיעין בשלב התיחום אינה מוגבלת לסימון תוקפים פוטנציאליים, אלא מצריכה גם תיאור של שיטות הפעולה ההתקפיות אשר מחייבות תשומת לב. כך למשל אם תמונת המודיעין מצביעה על קבוצות כופרה המתבססות על גניבת זהויות ופועלות נגד מערכות גיבוי, ראוי שמחזור ה-CTEM יכלול את המרחבים בהם תרחיש זה עשוי להתממש: מנגנוני גישה חיצונית, חשבונות עם הרשאות גבוהות, או נכסים ללא מנגנון אימות רב-שלבי (Authentication Factor-Multi – MFA). גבולות הגזרה צריכים אפוא להיות מוגדרים בהתאם לדרך ההתפתחות הצפויה של האיום בתוך הארגון, ולא להיגזר רק מן הסיווג הטכני של הנכסים.

הבנה עמוקה של הטקטיקות והטכניקות אשר התוקפים הפוטנציאליים נוקטים, גם מסייעת "להציף" רכיבים שחשיבותם בהקשר של מימוש תרחישי תקיפה גבוהה מכפי שהיה דומה תחילה. מערכות ניהול, סביבות בדיקות, חשבונות שירות, מכשירים ניידים, תחנות עבודה של אנשי IT וממשקים פנימיים עשויים להיראות כרכיבים תומכים בלבד, אך בתרחישי תקיפה מסוימים הם עלולים להיות מנוצלים למעבר, להסלמה או לאחיזה מתמשכת. מודיעין איכותי מאפשר להכניס רכיבים אלו לתוך גבולות הבחינה ולהגדיר מחדש את תפיסת ההגנה.

כיצד המודיעין מבחין בין חולשה לסיכון

תרומתו של המודיעין ניכרת במיוחד בשלב התעדוף של מחזור ה-CTEM. בשלב הזה מתגלה ההבדל בין מודיעין התרעתי למודיעין מתעדף: הראשון מבקש להצביע על תקיפה קרובה, ואילו השני מסייע להבחין באלו מבין אלפי החשיפות יש לטפל תחילה. התעדוף נשען תחילה על הקשר פנימי: מיקום הנכס ברשת, נגישותו מן האינטרנט, חשיבותו העסקית, הקושי המעשי לנצל את החולשה בסביבה מסוימת, וקיומן של בקורות אבטחה שעשויות לצמצם או למנוע את מימושה. אולם למשתנים אלה מצטרף רובד של מודיעין טקטי, הבוחן את "ביוגרפיית הניצול" של החולשה בעולם האמיתי - אם נוצלה בעבר, באיזה היקף, על ידי אלו שחקנים, נגד אלו מגזרים; ואם קיימים סימנים להתעניינות מחדשת בה. ההנחה היא סטטיסטית: ככל שחולשה כבר נוצלה בפועל, ובייחוד אם נוצלה על ידי שחקנים מתוחכמים או בהיקף רחב, גדלה הסבירות שהיא תנוצל שוב.

איסוף מידע זה מורכב, משום שאין חובה רגולטורית אחידה לדווח אלו חולשות שימשו עבור נתיבי תקיפה. לפיכך המידע מפורז ונמצא במקורות רבים - דוחות אבטחה, דיווחים בעיתונות, פרסומים ממשלתיים, טענות של יצרנים, ולעיתים אף הצהרות של התוקפים עצמם. גם מאגרי ידע רשמיים אינם מספקים תמונה מלאה: קטלוג ה-KEV (Known Exploited Vulnerabilities) של הסוכנות לאבטחת סייבר ותשתיות של ארצות הברית (CISA – Cybersecurity and Infrastructure Security Agency) הוא כלי חשוב, אך אינו מקור מודיעיני שלם. למעשה, מוטלת ביקורת על כלי זה בשל גישתו המצמצמת וקצב עדכונו האיטי. היחס בין מספר החולשות הידועות כמנוצלות בפועל לבין אלו אשר נכללות בקטלוג גבוה מאחד לשלוש, והדבר ממחיש את הצורך בעבודת מודיעין עצמאית ומשלמה.³⁰

נוסף על היסטוריית הניצול נבחנת גם זמינותן של הוכחות היתכנות (PoC – Proof of Concept), קטעי קוד - שמאפשרות להדגים את ניצול החולשה בפועל. פרסום כזה מנמיך מאוד רף הכניסה של התוקפים, משום שהוא מאפשר להם לנצל חולשות ללא מחקר עצמאי מעמיק; אולם גם כאן נדרש שיקול מודיעיני: לא כל PoC הוא קוד יציב, נגיש או מתאים להפעלה מבצעית. לפיכך השאלה

30 מעריכים שבפועל נוצלו כ-4,500 חולשות, אך הרשימה בקטלוג ה-KEV כוללת כ-1,250 בלבד - פחות משליש מההיקף האיומים הממשיים בשטח. VULNCHECK (2026). THE 2026 VULNCHECK EXPLOIT INTELLIGENCE REPORT

אינה רק אם פורסם קוד אלא גם מה רמת בשלותו, עד כמה קל להפעילו, ואם הוא עלול להיות לכלי תקיפה מעשי. מדד נוסף המסייע לתעדוף הוא מערכת הניקוד לחיזוי ניצול (EPSS – Exploit Prediction Scoring System), אשר מעניקה לכל חולשה ציון הסתברותי המשקף את הסיכוי שחולשה זו תנוצל ב־30 הימים הקרובים. המדד הזה נשען על מודל של למידת מכונה ומשקלל משתנים רבים, כמו למשל עדויות לניצול פעיל, זמינות PoC, מאפייני המוצר והדיון הציבורי בחולשה; בכך הוא מגלם היטב את המעבר ממדד חומרה סטטי למודיעין הסתברותי. עם זאת, גם EPSS אינו התרעה במובנה הקלסי: הוא אינו מזהה יריב מסוים, מועד תקיפה או מתווה פעולה, אלא מספק הערכת סבירות גלובלית. יתרה מכך, הוא עלול לסבול מהטיות: משקל יתר מיוחס לחולשות נפוצות או מתוקשרות לעומת חולשות פחות מוכרות.³¹

נדבר חשוב בתעדוף הוא שיוך החולשה לקבוצות תקיפה. חולשה אינה פועלת בחלל ריק אלא שמשמעותה נגזרת גם מן היריבים שעושים בה שימוש, מן הניסיון והתחכום שלהם, מן המגזרים אשר הם מכוונים אליהם ומן היעדים שהם מבקשים להשיג. לכן, אם חולשה מסוימת מזהה כחלק מארגז הכלים של קבוצת תקיפה רלוונטית לארגון, היא מקבלת משנה חשיבות. שיוך כזה הוא מלאכה טכנו־מודיעינית מורכבת הנשענת על דוחות חקירה, מזהים טכניים, דפוסי פעולה, תשתיות תקיפה ומידע שנאסף באירועים קודמים.

מכאן מתברר מקומו של המודיעין בתהליך עבודה רחב יותר, כזה שנועד לזהות, להעריך ולתעדף ברציפות נקודות תורפה ארגוניות. נקודת הפתיחה של תהליך זה אינה עוד הבנה מודיעינית של היריב, אלא יכולתו של הארגון להכיר את נכסיו הדיגיטליים, לאפיין את חולשותיו ולמפות את חשיפותיו. אולם אין פירוש הדבר שהמודיעין נדחק לשוליים; להפך, דווקא לאחר שההגנה מפנה את מבטה פנימה, נדרש המודיעין כדי להעניק למבט זה הקשר, כיוון ומשמעות. בשלב התייחסות הוא מסייע להגדיר את סביבת האיומים ואת איום הייחוס הרלוונטי, ובשלב התעדוף הוא מסייע להבחין בין חולשה טכנית לסיכון ממשי ובר־מימוש. בכך מתנסחת מחדש תרומתו: אין מדובר עוד ב"מלכת הקרב" אשר מניעה לבדה את גלגלי הפעולה באמצעות התרעה, אלא ברכיב פרשני הנמצא בתוך מערכה הגנתית מתמשכת ומחבר בין האיום החיצוני לפגיעות הפנימית של הארגון.

סיכום

המהלך שתואר במאמר זה מצביע על טרנספורמציה כפולה. הראשונה נוגעת לעולם ההגנה בסייבר עצמו: מעבר מתפיסה צרה, סטטית וטכנית של ניהול חולשות אל תפיסה רחבה, דינמית והוליסטית של ניהול חשיפה לאיומים. אם ניהול החולשות המסורתי ביקש לזהות פגמים טכניים, לדרגם ולתקנם, הרי שתפיסת ה־CTEM מציעה להבין את מצב הפגיעות של הארגון כמערכת שלמה. במובן זה, נקודת הכובד של פעולת ההגנה אינה עוד החולשה הבודדת, אלא החשיפה לאיום ממשי; לא הפגם הטכני כשלעצמו, אלא האפשרות שיהפוך, בתנאים מסוימים, לנתיב פעולה ריאלי עבור תוקף.

הטרנספורמציה השנייה קשורה למעמדו של המודיעין בתוך תפיסה זו. במסורת הביטחונית הישראלית נתפס המודיעין לא פעם כ"מלכת הקרב", או כמאמץ שבראשית דרכה של הפעולה הצבאית. אולם בעולם ההגנה הארגונית בסייבר, וביתר שאת במסגרת של ניהול חשיפה מתמשך, המודיעין אמנם משמר את חשיבותו אך משנה את מקומו. הוא חדל להיות נקודת הפתיחה הבלעדית של התהליך והופך רכיב משלים, הקשרי ו"מכוון פעולה" שתפקידו לחבר בין תמונת האיום החיצונית למצב החשיפה הפנימי של הארגון. ערכו אינו נמדד ביכולתו להתריע מפני תקיפה קרובה, אלא ביכולתו לדייק את פעולת ההגנה: לסייע בהגדרת איום הייחוס, לכוון את גבולות הבדיקה, לתעדף חולשות וחשיפות, ולוודא שמאמצי ההגנה נמצאים בהלימה לאיומים הרלוונטיים באמת.

מכאן נובעת מסקנה רחבה יותר: התפתחות ההגנה האזרחית בסייבר אינה רק סיפור טכנולוגי או ארגוני, אלא גם אתגר מושגי עבור עולם הביטחון כולו. היא מלמדת כי בעידן בו יריבים פועלים במהירות, באופרטוניזם ובמגוון רחב של נתיבי פעולה, לא די בהבנת האויב כשלעצמה. מערכת הגנה יעילה נדרשת להבין גם, ואולי בעיקר, את עצמה: היכן היא חשופה, אלו הנחות יסוד מארגנות את פעולתה, אלו תלויות הופכות אותה פגיעה, ואלו תרחישים עלולים לעשות איום חיצוני לסיכון ממשי.

לאחר אירועי 7 באוקטובר קשה להימנע מן התהייה אם גם המערכת הביטחונית והצבאית נדרשת לתמורה דומה. כישלון ההתרעה באותו היום לא היה רק כשל מודיעיני, אלא גם חשף את הסכנה הכרוכה בהסתמכות יתרה על מתן התרעה ובתפיסתה כמקור לפעולת ההגנה. הוא גם המחיש את חוסר הבקיאיות של ארגוני המודיעין במערכות ההגנה (החל בגדר הגבול וכלה במערכות התצפית והניטור) ואת הסתייגותם משילוב מערכות אלה בתהליכים המודיעיניים. כך שבסופו של דבר, המחלל הבהיר כי נוסף

31 יש גם ביקורת על כך שמסתמכים יותר מדי על ה־EPSS כמודל חיזוי: מחקר אשר בחן חולשות שנוצלו ב-2023-24, הראה כי שימוש בסף EPSS של 0.1 (הסתברות של 10% לניצול) תפס רק 25.3% מהחולשות שנוצלו בפועל - כלומר כ-75% מהחולשות שנוצלו קיבלו ציון EPSS נמוכים מ-10%.
VULN CHECK KNOWN EXPLOITED VULNERABILITIES REPORT - SUMMER 2024

על הקושי להבין את כוונות חמאס הייתה גם בעיה עמוקה יותר: היעדר תפיסה הוליסטית ושיטתית לניהול פגיעויותיו של הצד הישראלי לנוכח האיומים החיצוניים שהלכו והתגבשו סביבו.

אין פירוש הדבר שאפשר להעתיק בפשטות את תפיסת ה־CTEM מן הסייבר הארגוני אל שדה הביטחון הלאומי. ארגון עסקי אינו מדינה, חולשת תוכנה אינה פרצה בגדר, ונתיב תקיפה דיגיטלי אינו זהה לנתיב חדירה של כוח צבאי. אולם ההיגיון המארגן עשוי להיות רלוונטי: נדרש מעבר מן השאלה "מה האויב מתכוון לעשות?" לשאלה משלימה (ולעיתים מקדימה): "באלו תנאים אנו בעצמנו חשופים לפגיעה?". שאלה זו אינה מחליפה את המודיעין ואינה מפחיתה מחשיבותו; היא מחייבת להציבו בתוך מסגרת רחבה יותר של ניהול פגיעות מתמשך.

רשימת מקורות

- אייזן, גלעד (2025), "ההתרעה הבסיסית - מבחנו העליון של המודיעין", המכון לחקר המתודולוגיה של המודיעין.
- Ainslie, Scott, Thompson, Dean, Maynard, Sean B., and Ahmad, Atif, (2023) Cyber-threat intelligence for security decision-making :A review and research agenda for practice , "Computers & Security.
- Alharbi, Abdulrahman ,et al , (2025) .A Systematic Review of Cyber Threat Intelligence :The Evolution, Challenges and Future Directions ,Sensors.
- Frank ,Lars ,and colleagues , (2024) The Whole of Cyber Defense :Syncing Practice and Theory, Information & Management.
- Gartner , (2025) Strategic Roadmap for Continuous Threat Exposure Management ,Gartner.
- Hodgson ,Quentin E ., Lilly ,Bilyana ,Moore ,Alyson ,and Ma ,Len , (2020) RAND's Scalable Warning and Resilience Model) SWARM : (Enhancing Cyber Warning and Resilience ,RAND Corporation.
- Healey ,J . (2013) .A Fierce Domain :Conflict in Cyber Space .2012–1986 ,Cyber Conflict Studies Association.
- Husák ,Martin ,et al , (2019) .Survey of Attack Projection ,Prediction ,and Forecasting in Cyber Security ,IEEE Communications Surveys & Tutorials.
- Libicki ,Martin C , (2009) .Cyberdeterrence and Cyberwar ,RAND Corporation.
- Lilly ,Bilyana ,Ablon ,Lillian ,Hodgson ,Quentin E .,and Moore ,Alyson , (2019) Applying Indications and Warning Frameworks to Cyber Incidents ,NATO CCDCOE
- Mandiant (2010), "M-Trends: The Advanced Persistent Threat"
- Mohammed, Marwa Q., and Al-author(s) (2026), A Comprehensive Review of Predictive Vulnerability Prioritization Using AI, International Journal of Computer Engineering and Applied Emerging Technologies.
- Munk, Tine. Cyber Intelligence: Thinking About Cyber Security With An Intelligence Mindset. 2022.

Oosthoek, Kris, and Doerr, Christian (2021), "Cyber Threat Intelligence: A Product Without a Process?", International Journal of Intelligence and CounterIntelligence.

Proctor, Jonathan D. (2024), The Warning Renaissance, National Intelligence University

Riedl, Stephanie, and Runge, Lena (2025), Cyber Threats and Crisis Early Warning, Universität der Bundeswehr München / CISS Working Paper Series.

Romanosky, Sasha, Edwards, Benjamin, and Roytman, Michael (2021), "Exploit Prediction Scoring System", Digital Threats: Research and Practice.

Schlette, Daniel, Böhm, Franz, Caselli, Marco, and Pernul, Günther (2021), "Measuring and Visualizing Cyber Threat Intelligence Quality", International Journal of Information Security.

Tenable (2025), Exposure Management Education Center: Continuous Threat Exposure Management Resources, Tenable.

Tounsi, Wiem, and Rais, Helmi (2018), "A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks", Computers & Security.

Verizon (2025), 2025 Data Breach Investigations Report, Verizon.

Welte, Todd M. (2025), Pulling the Thread: A Campaign Approach to Mission Thread Defense of Force Projection, The Cyber Defense Review.

Willard, G. N. (2015), Understanding the Co-Evolution of Cyber Defenses and Attacks to Achieve Enhanced Cybersecurity, Journal of Information Warfare.