Time-Based Security
מודל TBS

גישה אסטרטגית למדידת אפקטיביות מערכי הגנה,

גילוי ותגובה בסייבר.

רו"ח נועם אסף, שותף,
מנהל פעילות מערכות מידע וסייבר

CISO, CISA, DPO, MBA

רוזנבלום הולצמן ושות', רו"ח
פברואר 2026

ראשי פרקים

סקירה כללית של הנושאים המרכזיים בהרצאה

- NIST Cybersecurity Framework
- מהו מודל TBS
- שכבות המיקוד
- חומות הגנה מול עולם מודרני
- מדידת אפקטיביות
- דוגמאות מהשטח
- עקרונות ליישום
- מגמות AI וקוונטים

עקרונות על:

- הסבר על שכבות ההגנה- לא "מנטליות המבצר" ובניית חומות גבוהות יותר.
- תוקפים עוקפים חומות – חדירות רבות לא מזוהות בזמן אמת.
- בחינה האם מערך האבטחה וההגנה אפקטיבי.
- מדידת זמני הגנה, גילוי ותגובה.

רעיון שנולד בשנות ה-90 (Winn Schwartau) ומאז הפך לגישה מרכזית בתחום הסייבר.

ROSENBLUM HOLTZMAN & CO. C.P.A

מסגרת אבטחת הסייבר של NIST

זיהוי (Identify)

פעילויות פונקציית הזיהוי מהוות בסיס להבנת ההקשר העסקי, הנכסים והמשאבים הקריטיים של הארגון. הן מסייעות להבטיח התאמה בין מאמצי האבטחה, אסטרטגיית ניהול הסיכונים והצרכים העסקיים.

הגנה (Protect)

פיתוח ויישום בקרות ואמצעי הגנה לאספקה מאובטחת של שירותים. כך למשל ארגון נדרש להגדיר מדיניות הגנת סייבר ואבטחת מידע, נהלים בדבר בקרת גישה למשאבים ועוד.

גילוי (Detect)

פיתוח ויישום בקרות ואמצעים לגילוי אירועי סייבר במועד התרחשותם. קטגוריות בפעילות זו יכללו: איתור דפוסים אנומליים, ניטור אבטחתי רציף של אירועים, תיעוד וניטור ועוד.

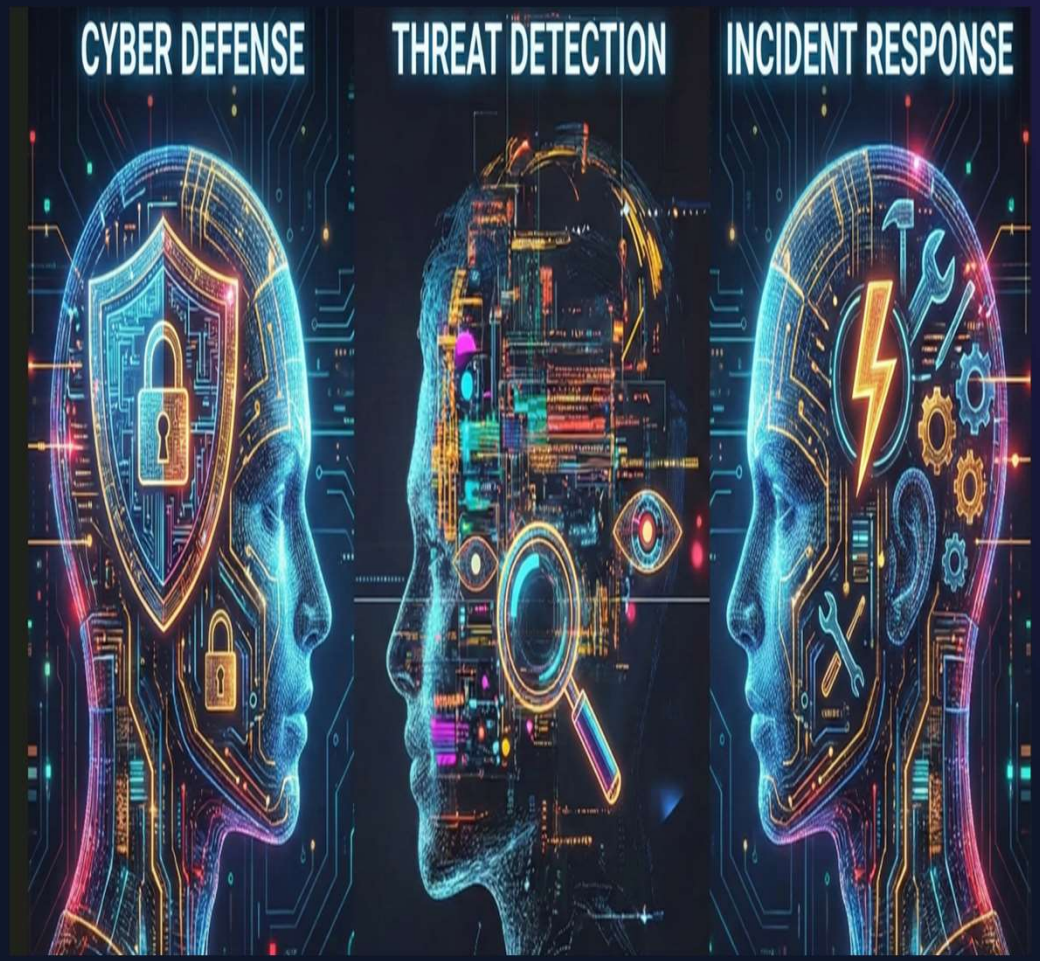
תגובה (Respond)

פיתוח ויישום תוכניות ונהלים להתמודדות עם אירועים שהתגלו. קטגוריות בפעילות זו יכללו: ניהול אירועים ודיווח, תכנון תגובה, אמצעי ניתוח ותחקור אירוע (פורנזיקה), דיווח אירועים, יח"צ, מו"מ ועוד.

התאוששות (Recover)

פיתוח ויישום פעילות ואמצעים אשר יבטיחו שרידות, צמצום נזק ויכולת התאוששות של שירותים שנפגעו כתוצאה מאירוע סייבר. קטגוריות בפעילות זו יכללו: תכנון תהליכי התאוששות, גיבויים ושחזורים, מיפוי תהלכים עסקיים (BIA), תוכנית המשכיות עסקית (BCP), אתר חירום (DR) ועוד.

ROSENBLUM HOLTZMAN & CO. C.P.A



המיקוד של מודל TBS

כיצד לבקר ולבחון האם קיים מערך אבטחה אפקטיבי ?

ההרצאה תתמקד ב-3 המרכיבים הקריטיים מתוך ה- 5 של NIST:

- הגנה (Protection)
- גילוי (Detection)
- תגובה (Response)

RH ROSENBLUM HOLTZMAN & CO. C.P.A

מי זה Protect ?

מה המטרה האמיתית בלהגן?

הגנה...? אבטחה...? לצמצם
סיכון...? למנוע...?

RH ROSENBLUM HOLTZMAN & CO. C.P.A

לעכב!

המטרה היא לקנות זמן.

ROSENBLUM HOLTZMAN & CO. C.P.A

Time-Based Security

$$P > D + R$$

אם התוקף מצליח לפעול מהר יותר מזמן הגילוי והתגובה של הארגון –הארגון לא מאובטח.

Protection (P)

למרות השקעה בבניית חומות –מערכות מאובטחות נפרצות בהצלחה.

ההגנה לבדה אינה מספיקה.

Detection (D)

חדירות רבות לא מזוהות כלל. תוקפים פועלים בארגון מבלי שאף גורם שם לב.

Response (R)

אי אפשר להגיב למה שלא מזהים.

ללא זיהוי, זמן התגובה הוא אינסופי.

מה נחשב "אירוע אבטחה חמור?"

תיעוד אירועי אבטחה

בעל מאגר מידע אחראי לתיעוד כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה.

רמת אבטחה בינונית

אירוע שנעשה בו שימוש **בחלק מהותי** מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע לגבי חלק מהותי מן המאגר

רמת אבטחה גבוהה

אירוע שנעשה בו שימוש במידע מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע.

ROSENBLUM HOLTZMAN & CO. C.P.A

מי מחליט מהי "האמת המוחלטת?"

- הרשות להגנת הפרטיות
- המשטרה
- מערך הסייבר
- הארגון (CISO/DPO)
- היועץ המשפטי
- המנכ"ל
- חברת הביטוח

האם האמת היא אבסולוטית ? ההחלטה מתי "חשש "הופך ל"אירוע "היא מורכבת.

ROSENBLUM HOLTZMAN & CO. C.P.A

REAL WORLD IMPLEMENTATION

לא "האם" ולא "מתי"

אירועים/ חששות קורים לכולם . השאלה היא איך מתייחסים אליהם.

תרחישים נפוצים

פישינג : עובד לחץ על לינק וה- EDR חסם. אירוע או חשש?

FW: זיהה חריגות בנפח תעבורה או כניסה מחו"ל - אירוע או חשש?

waf: זיהוי תווים אסורים חשש/ אירוע?

Login Failure : 6 ניסיונות כושלים חשש/ אירוע?

דוגמא

ה-EDR של הארגון זיהה פעילות חשודה בעמדת מחשב של עובד.

התרחיש :עובד נפל בהונאת דיוג.

אבטחה (P) איזה אמצעי אבטחה קיימים לעכב? סינון מיילים, מודעות, עדכוני תוכנה, סיגמנטציה.

גילוי (D) האם יש EDR/MDR? האם מישהו ראה את ההתראה? כמה זמן לקח?

תגובה (R) כמה זמן לקח לצוות לקבל את המידע ולבודד את התחנה? סריקת תחנה?

עקרונות ליישום

ארגונים ללא MDR / SIEMSOC יעיל –לא "נמצאים באירוע" כלל.

שאלות מפתח

האם מערך ה- SIEMSOC פנימי או חיצוני?

מי מאייש בסופי שבוע וחגים?

האם זה רק מוקד הודעות או שיש יכולת תגובה?

האם יש הרשאות ביצוע או רק צפייה?

מי סוגר טיקטים? האם יש פרוטוקול טיפול למשל: ניתוק מיידי?

מ"מנטליות המבצר" למודל ה- TBS: שינוי פרדיגמה

הגישה המסורתית

- בניית חומות הגנה גבוהות.
- הסתמכות על מניעה בלבד.
- תחושת ביטחון מזוייפת.

גישת המודל (TBS)

- התמקדות בפער הזמן (P > D + R)
- ההגנה נועדה "לקנות זמן".
- חיזוק גילוי ותגובה במקום עוד חומות.
- השקעה מושכלת בהגנה - קבלת החלטות מבוססת מספרים, לא תחושות.
- אבטחה דינמית ולא סטטית.

ROSENBLUM HOLTZMAN & CO. C.P.A

כיצד מודדים שיפור?

תגובה (RESPONSE)

- כמה זמן לוקח עד שמבוצעת פעולה אפקטיבית לעצירת התקיפה.
- כמה זמן לוקח לצוות להגיע לעמדה, לפתוח מערכת ולבצע פעולה.
- אחוז האירועים שנענים אוטומטית (ב-SOAR או חוקים מתוכנתים).
- משך הזמן בין "אירוע זוהה" לבין האירוע הגיע לדרג בעל סמכות החלטה.

גילוי (DETECTION)

- הזמן הממוצע מהרגע שהתקיפה מתחילה ועד שהמערכת מגלה אותה.
- אחוז מערכות/שירותים המוגנים על-ידי ניטור בזמן אמת.
- כמה אירועי תקיפה לא זוהו כלל?
- כמה התנהגויות חריגות תורגמו לאירוע אמיתי?

הגנה (PROTECTION)

- הערכה מבוססת בדיקות PT לזמן שנדרש לתוקף לעבור את שכבת ההגנה.
- משך הזמן שמערכת נמצאת פרוצה בגלל פאצ' שלא הוטמע.
- אחוז המערכות שההגנה עליהן מוגדרת לא נכון (לפי סריקה אוטומטית).

פרוטוקלים מובנים

חובה להגדיר מראש

1. אילו אירועים מזוהים?
2. מה המשמעות שלהם?
3. מה הפעולה הנדרשת?
4. תוך כמה זמן הפעולה חייבת לקרות?
5. מי מוסמך לבצע אותה? (למשל: סמכות CISO להפיל שירות).
6. מה האלטרנטיבות במקרה שהתגובה כשלה?

אחרת

- בלבול
- עיכובים
- הסלמה
- לחץ והחלטות שגויות

אוטומציה היא המפתח

עדיפות לתגובה אוטומטית ומהירה (אוטומציה) על פני תגובה ידנית איטית.

מנהל אבטחת מידע נדרש לסמכות פעולה מיידית - יש לו סמכות למשל "להפיל" שירות.

ROSENBLUM HOLTZMAN & CO. C.P.A

FUTURE STRATEGY

מגמות לעתיד

מחשוב קוונטי

איום על יסודות הקריפטוגרפיה הנוכחית.

AI

מאיץ תקיפה והגנה כאחד - מגדיר מחדש את הזירה.

מהירות חומרה

כל פעולה הופכת למיידית, ומקצרת את זמן הזיהוי והתגובה הנדרש.

Zero-Trust

ריבוי איומים מחייב גישת Zero-Trust Everywhere.

בהצלחה !

בשינוי התפיסה ובשיפור המתמיד

לכל שאלה: נועם אסף

noam@rhcpa.co.il

רוזנבלום הולצמן ושות'

RH ROSENBLUM HOLTZMAN & CO. C.P.A