המפגש התמקד בשלוש קטגוריות ההגנה המרכזיות בשוק הסייבר המודרני: **EDR, XDR ו-MDR**, תוך העמקה במתודולוגיית ה-**Zero Trust** ובחשיבותן של מערכות אוטומציה מבוססות **AI** לניהול עומס התראות 1, 2.
להלן סיכום הנושאים המרכזיים מהשיעור:

1. תפיסת ה-Zero Trust (אפס אמון)

הנחת היסוד של המודל היא שאין לסמוך על אף גורם במערכת, וכל גישה דורשת אימות בכל נקודה שדרכה המשתמש עובר 3, 4.

- **מינימום הרשאות:** צמצום הרשאות המשתמש למינימום ההכרחי לביצוע עבודתו 4, 5.
- **ניטור ורישום:** בדיקה ותיעוד של כל הפעילויות במערכת (Log) כדי לזהות ניסיונות חריגים או אסקלציה של הרשאות 6, 7.
- **מקרה בוחן - "Copy/Fail":** פגיעות יום-אפס בלינוקס המאפשרת העלאת הרשאות למשתמש Root. מערכות מבוססות Zero Trust ו-EDR מאפשרות לבודד את נקודות הקצה הנגועות ולצמצם את נזק הפריצה 5, 8.

2. פתרונות הגנה: EDR, XDR ו-MDR

המרצה חילק את הפתרונות לפי קהלי היעד והיכולות שלהם 9, 10:

- **EDR (Endpoint Detection and Response):** מתמקד בהגנה על **נקודות קצה** (מחשבים, שרתים). המערכת מבצעת ניטור רציף, זיהוי התנהגויות חשודות ומתן תגובות אוטומטיות כמו בידוד המחשב מהרשת 10, 11.
- **XDR (Extended Detection and Response):** הרחבה של ה-EDR המאחדת הגנה על הרשת, הענן, המייל ונקודות הקצה תחת **ממשק ניהול אחד**. היתרון הוא היכולת לבצע קורלציה (הצלבת מידע) בין אירועים שונים בארגון כדי לקבל תמונה מלאה על תקיפה 12, 13.
- **MDR (Managed Detection and Response):** שירות מנוהל (לרוב עבור מרכזי SOC) המספק מענה אנושי של 24/7. צוות המומחים מטפל בניתוח האיומים ובסינון ההתראות 14, 15.

3. אתגר עומס ההתראות (Alert Fatigue)

אחד האתגרים הגדולים בניהול סייבר הוא כמות המידע האדירה. ארגון של 10,000 עובדים מקבל בממוצע כ-**16,000 התראות ביום** 16.

- מערכות MDR ובוטים של AI משמשים כ"משפך" המדלל את התראות השווא (False Positives). בדוגמה שהוצגה, מתוך כ-10,000 התראות, תהליך הצמצום הותיר רק **74 התראות** שבאמת דרשו בחינה אנושית 17.

4. מיקרו-סגמנטציה (פתרון Guardicore)

המרצה הציג את שיטת המיקרו-סגמנטציה של חברת אקמאי, המאפשרת בניית חומת אש פנימית בארגון 18:

- **מודל עבודה:** התקנת סוכן (Agent) על כל יחידת קצה, המדווח למרכז שליטה (Management) דרך רכיב אגריגטור 19, 20.
- **יכולות מתקדמות:** זיהוי אנומליות גם כשהמשתמש נמצא "מחוץ לקורפורט" (Off Corporate) – המערכת מנתחת את הלוגים של התקופה בה המחשב לא היה מחובר לרשת הארגונית ברגע שהוא מתחבר מחדש 21, 22.

5. שחקנים מרכזיים בשוק

- **CrowdStrike:** פתרון Cloud Native חזק לארגוני אנטרפרייז גדולים, המאפשר שליטה על כמות אדירה של מכונות במקביל 23, 24.

- **SentinelOne:** חברה ישראלית המציעה אוטומציה מלאה בעזרת AI בתוך הסוכן 23.
- **Palo Alto (Cortex):** מספק אינטגרציה רחבה לכל המערכות בארגון תחת ממשק אחד 25, 26.
- **Microsoft Defender:** מציע עלות-תועלת גבוהה לארגונים המבוססים על סביבת Windows 27, 28.

6. בינה מלאכה (AI) וגיוס עובדים

המרצה הדגיש כי כיום המיומנות החשובה ביותר בשוק היא **Prompt Engineering** – היכולת לנסח שאילתות מדויקות לכלי AI (כמו Claude או Co-pilot) כדי לנתח לוגים, למצוא שורש של בעיות (Root Cause) ואף לבצע סימולציות של מבחני חדירה 29, 30. חברות כמו **Salesforce** מחפשות כיום ג'וניורים בעלי יכולת הפעלה של כלי AI לתפקידי מפתח 31, 32.

שיקולי הטמעה: בבחירת פתרון, יש לקחת בחשבון את העומס על המעבד והזיכרון של המכונה (CPU/Memory usage), שכן עומס יתר עלול להוביל לעיכובים (Latency) או לזליגת מידע 33, 34. בנוסף, סוג הפתרון (EDR/XDR/MDR) צריך להיות מותאם לגודל הארגון ולתקציבו 35, 36.