המפגש ה-11 של הקורס התמקד בטכנולוגיות ההגנה המתקדמות **EDR, XDR ו-MDR**, תוך העמקה במודל ה-**Zero Trust**, ניהול עומס התראות ושילוב בינה מלאכותית (AI) במערכי ההגנה 1, 2.
להלן סיכום הנושאים המרכזיים מהשיעור:

1. מודל ה-Zero Trust (אפס אמון)

הנחת היסוד של המודל היא שאין לסמוך על אף גורם, פנימי או חיצוני, וכל גישה דורשת אימות בכל נקודה 3, 4.

- **מינימום הרשאות:** צמצום הגישה של המשתמש רק למה שנדרש לו לביצוע עבודתו 4, 5.
- **ניטור ורישום רציף:** תיעוד כל הפעילויות ברשת כדי לזהות ניסיונות אסקלציה (העלאת הרשאות) או חריגות 6, 7.
- **מקרה בוחן - "Copy/Fail":** פגיעות יום אפס (Zero Day) בלינוקס המאפשרת להגיע למשתמש Root דרך פקודה פשוטה. מערכות מבוססות Zero Trust ו-EDR מאפשרות לבודד נקודות קצה נגועות ולמנוע את התפשטות הפריצה 5, 8.

2. פתרונות הגנה: EDR, XDR ו-MDR

המרצה סיווג את ההגנות המודרניות לפי שלוש קטגוריות עיקריות 9, 10:

- **EDR (Endpoint Detection and Response):** מתמקד ב**נקודות קצה** (מחשבים, שרתים). המערכת מזהה התנהגות חשודה, מאפשרת חקירה ומספקת 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 לזהות קורלציות (הקשרים) בין אירועים שונים בארגון 12, 13.
- **MDR (Managed Detection and Response):** שירות מנוהל המספק מענה אנושי של 24/7. צוות המומחים מסנן את אלפי ההתראות ומטפל רק באירועים קריטיים 14, 15.

3. אתגר עומס ההתראות וניהול SOC

אחד האתגרים הגדולים בניהול סייבר הוא **"Alert Fatigue"** (עומס התראות). ארגון של 10,000 עובדים מקבל בממוצע כ-**16,000 התראות ביום** 16, 17.

- מערכות ה-MDR וה-AI מסננות את ה-"False Positives" (התראות שווא) ומצמצמות אלפי התראות לעשרות בודדות שבאמת דורשות ניתוח אנושי 18.

4. מיקרו-סגמנטציה (פתרון Guardicore)

המרצה הציג את שיטת המיקרו-סגמנטציה של חברת אקמאי (גארדיקור), המאפשרת לבנות חומת אש פנימית בתוך הארגון 19:

- **תהליך:** מיפוי כלל הנכסים (Visibility), בניית מדיניות אבטחה (Policies) ובידוד אפליקציות או שרתים נגועים (Segmentation) 19, 20.
- **סוכנים (Agents):** התקנת סוכן על כל יחידת קצה (בכל מערכת הפעלה) המדווח לאגרגטור ומשם למוח המרכזי של המערכת 21, 22.
- **יכולות מתקדמות:** זיהוי אנומליות גם כשהמשתמש "מחוץ לקורפורט" (Off Corporate) – המערכת מנתחת לוגים מתקופת הניתוק ברגע שהמחשב מתחבר שוב לארגון 23, 24.

5. שחקנים מרכזיים בשוק והתאמה לארגון

- **CrowdStrike:** מובילה בעולמות ה-Cloud Native, מתאימה לאנטרפרייזים ענקיים בזכות יכולת שליטה במאות אלפי מכונות 25, 26.

- **SentinelOne:** חברה ישראלית המציעה אוטומציה מלאה בעזרת AI בתוך הסוכן 25.
- **Microsoft Defender:** אינטגרציה מובנית וחזקה בעולמות הווינדוס עם עלות-תועלת גבוהה 27, 28.

התאמה לפי גודל ארגון 29, 30:

- **ארגון קטן:** אנטיווירוס ומערכות EDR בסיסיות.
- **ארגון בינוני (SMB):** מערכות EDR כחובה ולעיתים שירות MDR.
- **ארגון Enterprise:** מערכות XDR לניהול אחוד של כלל כלי האבטחה.

6. בינה מלאכותית (AI) בעולם הסייבר

המרצה הדגיש כי כיום חלק משמעותי מגיוס עובדים לסייבר מתבסס על היכולת להשתמש בכלי AI (כמו Claude, Co-pilot) 31, 32.

- **Prompt Engineering:** היכולת לנסח שאילתות מדויקות היא קריטית לקבלת תוצרים איכותיים בביצוע משימות כמו ניתוח לוגים, זיהוי שורש בעיה (Root Cause) ואפילו סימולציות של מבחני חדירה (Penetration Testing) 31, 33.

בסוף השיעור ציין המרצה כי המפגש הבא יעסוק ב**מרכזי SOC**, מבנה חשיבותם והשינויים שהם עוברים 34.