



סייבר הלכה למעשה -

יסודות הסייבר לרשתות OT, מפעלי תעשייה ומתקני תשתיות לאומיות

הקורס יתקיים בכיתת ההדרכה של קונטאל, רח' יגיע כפיים 21, פתח תקווה.

משך הקורס: שלושה ימים.

שעות הקורס 08:30-16:30.

כולל כיבוד קל לאורך היום וארוחת צהריים.

המפגש השלישי יושלב תרגול מעשי ויערך במעבדת הסייבר בב"ש (ICNL)

מטרת הקורס:

אבטחת מידע וסייבר, הפכו לנושאים החמים ביותר בתחום מערכות מידע בשנים האחרונות. ככל שמערכות המידע מתפתחות וטרנספורמציה דיגיטלית בארגונים מתפתחת, נושא אבטחת המידע והסייבר תופס נתח חשוב יותר ויותר. אנו חווים אירועים רבים בעולם הקשורים לסייבר, כגון פריצה לאתרים חברתיים וגניבת מידע פרטי, דרך התקפות על חברות כרטיסי אשראי, התקפות כופרה נגד אנשים פרטיים וכנגד ארגונים, התקפה על מערכות בחירות וניסיון לשנות תוצאות בחירות (כגון מערכות בחירות בארה"ב), ניסיונות תקיפה על משרדי ממשלה ומוסדות ממשלתיים, וכן תקיפת מוסדות פיננסים וביטוח (כגון התקיפה על חברת הביטוח "שירביט").

לאחרונה, אנו חווים יותר ויותר התקפות על התעשיות בעולם כולל על התעשייה הישראלית, תקיפות הממוקדות על מערכות בקרה תעשייתיות ורשתות תהליכים (OT - Operation Technology).

רבים ממפעלי התעשייה בישראל הוקמו לפני עשרות שנים עוד הרבה לפני עולם האינטרנט והסייבר, ומטרתם העיקרית הייתה להביא רווח כספי. בהקמתם לא נלקחו בחשבון איומי סייבר עתידיים. בזמן הקמת המפעלים הרשתות היו סריאליות וסגורות לעולם, אך בד בבד עם כניסת המהפכה התעשייתית השלישית נכנסו יותר ויותר מערכות מחשב כדי לייעל תהליכים ובכך חשפו את התעשייה לאיומי סייבר.

המהפכה התעשייתית הרביעית שנכנסה בשנים האחרונות גרמה לכניסת רכיבי IIOT (Industrial Internet of Things) אשר הגבירה עוד יותר את רמת החשיפה עקב פעילותם התקשורתית הענפה זה עם זה ועם הענן.

כיום מהווה התעשייה "הבטן הרכה" לתוקפי הסייבר, כאשר תקיפת סייבר במערכות OT - משמעותה השבתת קו ייצור, ובמקרים חמורים יותר כאשר מדובר במפעלי חומרים מסוכנים, המשמעות היא אירוע סייבר שהופך לאירוע חומרים מסוכנים ובכך מסכן חיי אדם ועלול לגרום נזק משמעותי לסביבה.

דרישות הקורס:

הקורס מיועד לאנשי IT, אנשי סייבר, מהנדסי בקרה במפעלים, מהנדסי תהליכים במפעלים, ממוני בטיחות, אחראי רעלים במפעל, אחראי סביבה במפעל, סמנכ"לים.

Cyber הלכה למעשה

3 מפגשים:

תוכנית ראשון

נושא	
1	היכרות עם עולם הסייבר התעשייתי: - סקירה של מטרות ויעדים בקורס. - הבנת הקשר בין מערכות IT למערכות OT בתעשייה. - Cyber הלכה למעשה - סקירת פרויקט לדוגמא בתחום תחנות הכח.
2	מושגי יסוד בהגנת סייבר - חלק א'
3	אבטחת מידע מול סייבר: הבדלים עקרוניים והשפעות על מערכות תעשייתיות.
4	השוואת IT ל-OT: - מאפיינים ייחודיים של מערכות OT, אתגרים וסיכונים. - חשיבות האינטגרציה עם IT בניהול סיכונים.
5	בקורות אבטחת מידע: - עקרונות ההגנה הרב-שכבתית והמבנה שלה בתעשייה. - היכרות עם מעגלי אבטחת מידע בארגונים מורכבים.
6	ארכיטקטורת רשת ארגונית: - מבנה רשתות OT טיפוסיות. - חומת אש, פרוקסי, כתובות IP (ציבוריות ופרטיות) וחציצה (סגמנטציה).
7	גישה מאובטחת מרחוק: - עקרונות תפעול VPN וחשיבותו למערכות OT. - שיטות הזדהות מתקדמות, כולל MFA, להתמודדות עם סיכוני חדירה.
8	מושגי יסוד בהגנת סייבר - חלק ב' - מודל ההגנה בשכבות (Defence in Depth): - כיצד ניתן ליישם אותו במערכות OT מורכבות. - מתקפות נפוצות על מערכות תעשייתיות: - מתקפות DOS ו-DDOS והשפעתן על רציפות תפעולית. - זיהוי וניהול איומים באמצעות מערכות IDS/IPS.
9	וירוסים ואנטי-וירוס: - סוגי וירוסים רלוונטיים למערכות OT. - פתרונות מתקדמים לזיהוי ונטרול וירוסים.
10	מתקפות ממוקדות: - תקיפות Zero Day ו-Sandbox: כיצד הן משפיעות על סביבת OT. - מתקפות ברמת האפליקציה: XSS, CSRF ו-SQL Injection.

Cyber הלכה למעשה

3 מפגשים:

נושא		
מפגש ראשון	11	מושגי יסוד בהגנת סייבר - חלק ג' • מתקפות מתקדמות: - כופרה והשפעתה על מערכות OT קריטיות. - מתקפות ברמת האפליקציה: XSS, CSRF ו-SQL Injection. • מערכות הגנה ייעודיות: - WAF: הגנה על אפליקציות תעשייתיות. - NAC: מניעת חיבור התקנים זרים למערכות קריטיות. - DLP: מניעת דליפות מידע מארגונים. - ועוד • חקירת אירועי סייבר בתעשייה: - ניתוח אירועי סייבר משמעותיים בעולמות תעשייתיים, כולל תאריכי מפתח ולקחים שנלמדו. - דיון באירועי סייבר בישראל עם דגש על תעשיות עם חומרים מסוכנים.

נושא		
מפגש שני	1	מושגי יסוד בהגנת סייבר - חלק ד' • טכנולוגיות הגנה מתקדמות: - CDR: הלבנת קבצים בעולמות OT, עקרונות פעולה ושיטות יישום. - שער חד-כיווני (Unidirectional Gateway): יישומים בתעשייה עם חומרים מסוכנים. - הגנה על בקרי PLC ומערכות ERP קריטיות. • מערכות SIEM ו-SOC: - עקרונות ניטור, ניהול ותחקור אירועי סייבר. - דוגמאות מעשיות ליישום בתעשייה.
	2	סייבר בענן • מעבר לענן בארגונים תעשייתיים: - שיקולים בתכנון המעבר לענן, הבדלים בין ON-PREMISE לענן ציבורי, פרטי והיברידי. - שירותים בענן (IaaS, PaaS, SaaS, DaaS) והשפעתם על מערכות OT. • סיכוני סייבר בענן: - ניתוח סיכונים ודרכים למזעורם במערכות OT המשולבות בענן.



Cyber הלכה למעשה

3 מפגשים:

נושא		זמן מפגש
שרשרת התקיפה - פרופיל התוקפים: - סוגי תוקפים (מדינות, האקרים, מתחרים) ומטרותיהם. - מתודולוגיית Cyber Kill Chain: שלבי התקיפה ואמצעי מניעה. - הנדסה חברתית: - כיצד תוקפים מנצלים חולשות אנושיות כדי לחדור למערכות תעשייתיות.	3	
ניהול סיכונים במפעל תעשייתי - וקטורי תקיפה במערכות OT: - נקודות חולשה נפוצות וכיצד ניתן להגן עליהן. - ניהול סיכונים שיטתי: - זיהוי נכסים קריטיים ומתודולוגיית מיפוי נכסים. - הטמעת תקן NIST CSF בניהול סיכוני סייבר. - סיכונים בתעשיות עם חומרים מסוכנים: - הבנת תקנים מחייבים, חישוב רמת חשיפה והפחתת סיכונים.	4	
הצגת ממצאים - ניתוח תוצאות מסקרי פיילוט בתעשייה. - דוגמאות לממצאים ואמצעי שיפור.	5	
מבחן סיום בנוסף: ניתוח אירוע מתקפת סייבר - ניתוח שלבי התקיפה, הכשלים והמסקנות. - לקחים רלוונטיים להגנת מערכות OT.	10	

נושא		זמן מפגש
הצגת האקוסיסטם בבאר שבע ומעבדת ICNL	1	
תרגול חולשה בשרשרת האספקה	2	
History manipulation	3	
Man in the middle	4	
תרגול LLM	5	