



**CONTEL
TECHNOLOGIES**
for Smart Manufacturing

קורס יסודות הסייבר

פרונטלי

מפגש ראשון :

מבוא:

- סקירת מהלך הקורס – מטרות ויעדים
- סקירת אירועי סייבר בעולמות התעשייתיים.
- אירועי סייבר עולמיים בתעשייה על ציר הזמן
- אירועי סייבר בתעשייה בישראל (כולל) תעשיית החומרים המסוכנים

מושגי יסוד בהגנת סייבר – חלק א'

- אבטחת מידע VS סייבר
- סייבר בעולמות IT מול סייבר בעולמות OT
- בקורות אבטחת מידע
- רבדים בהגנת סייבר, הגנה רב שכבתית
- סקירת מעגלי אבטחת המידע
- מבנה רשת ארגונית
- שרתי פרוקסי והגישה לאינטרנט
- כתובות IP ציבוריות ופרטיות
- חומת אש – עקרונות פעולה ושימושים
- חציצה (סגמנטציה)
- פרוטוקולים נפוצים בעולמות ה-IT וה-OT
- גישה מרחוק מאובטחת לארגון
- מהו VPN ומהם השימושים בו
- הזדהות : סיסמאות, הזדהות חכמה (MFA)

מושגי יסוד בהגנת סייבר – חלק ב'

- מודל הגנה בשכבות (Defence in Depth)

- התקפה ברמה אפליקטיבית : DOS , DDOS
- הגנה כנגד התקפות - מוצרי IDS , IPS
- משפחות וירוסים, עקרון הפעולה של אנטי-וירוס
- התקפת ZERO DAY
- הגנת SANDBOX
- מתקפת פישנינג (Phishing)

מושגי יסוד בהגנת סייבר - חלק ג'

- התקפת כופרה
- איומים בשכבת האפליקציה
- תקיפת Cross
- תקיפת Site Scripting ,
- Cross Site Request (XSS)
- תקיפת SQL injection
- Forgery (CSRF)
- WAF - הגנה על האפליקציה
- DAF - הגנה על בסיס הנתונים
- NAC - הגנה על חיבור התקנים זרים לרשת
- DLP - הגנה על זליגת מידע מהארגון

מפגש שני:

מושגי יסוד בהגנת סייבר - חלק ד'

- CDR - הלבנת קבצים עקרונית פעולה, דרכים
- שונות ליישום פתרון הלבנה בארגון
- דיודה חד כיוונית - Unidirectional Gateway Security
- הגנה על הבקר
- הגנה על מערכת ERP
- SIEM - SOC - עקרונות יישום

סייבר בענן

- שיקולים במעבר לענן, הבדלים בין ענן ל- ON
- PREMIS
- סוגי עננים - ציבורי, פרטי, היברידי
- סוגי שירותים בענן- laas, Paas, Saas, Daas
- הסיכונים במעבר לענן
- מזעור סיכוני סייבר במעבר לענן

שרשרת התקיפה

- מיהם התוקפים ומה מטרותיהם?
- מתודולוגיית Cyber Kill Chain
- איסוף מידע במבט התוקף
- הנדסה חברתית Social Engineering

ניהול סיכונים במפעל תעשייתי

- וקטורי התקיפה למערכות תעשייתיות
- גישות לניהול סיכונים בארגון
- זיהוי נכסים קריטיים - מתודולוגיית מיפוי נכסים בארגון
- תקן סייבר NIST CSF לניהול סיכונים

סיכונים ייחודיים במפעל עם חומרים מסוכנים

- הצגת מדריך הסייבר לתעשייה כתקן מחייב
- חישוב רמת חשיפה לתקיפת סייבר והדרכים לצמצומה
- ניהול סיכונים מלא במפעל תעשייתי הכולל
- חישוב הנזק המרבי הנגרם כתוצאה מאירוע סייבר ורמת החשיפה.
- תיאור והסבר הבקורות המומלצות להגנה במערכות תעשייתיות

הצגת ממצאי סקרי סיכונים בתעשייה

- הצגת ממצאי חשיפות סייבר מתוך פיילוט סקרי סיכונים במפעלים

חזרה והכנה למבחן סיום

- סיכום הקורס
- שאלות ותשובות על כל תכני הקורס
- מבחן מדגמי לתרגול

מבחן סיום

בנוסף: אם יאפשר הזמן ניתוח תקיפת סייבר על חברת ביטוח שירביט

- ניתוח האירוע שלב אחר שלב
- ניתוח שרשרת הכשלים אשר הביאו לאירוע
- מסקנות מהאירוע