

תוכנית מחודשת ראשי פרקים של הרצאות בנושא סיכונים ואמצעי הגנה על מערכות תעשייתיות ותשתיות חיוניות בישראל מרצה: דניאל ארנרייך, SCCE	
<ul style="list-style-type: none"> • מבנה מערכתי עיקרוני עבור פתרונות שליטה ובקרה (ש"ב) • התקנים שנמצאים במערכות אלה: SIS, IED, PLC, RTU, RIO • מחשבי ניהול ברשת: ENG, HMI, HISTORIAN, וכו' • תקשורת ופרוטוקולים ישימים למערכות ש"ב • מבנה מודל ארגוני מחולק ל 4 שכבות ו-6 שכבות (PURDUE) • תקשורת ופרוטוקולים במערכות ש"ב ומערכת IIOT • מבנה מערכות DCS, SCADA, PLC, והשלכות על סיכוני סייבר • סיכוני בטיחות תפעוליים – לא רק תקיפות סייבר! 	מפגש 1: מבוא למערכות שליטה ובקרה (OT-ICS)
<ul style="list-style-type: none"> • סיכוני סייבר באמצעות הנדסה חברתית – Social Engineering • הסבר על תהליכי תקיפה במערכות ש"ב- LM Cyber Kill Chain • הסבר מפורט לגבי תהליך תקיפה שלב-שלב על מערכת ש"ב • תקיפה על מערכות: מונחים MitM, DDoS APT /ZERO DAY, Ransomware, GPS Spoofing • • בחינה של חוסן מערכות ש"ב על ידי תהליך MITRE • הקטנת סיכוני סייבר באמצעות ניטור חולשות • הפרדה בין הרשתות במערכות ש"ב ביו ש"ב למערכת IT • תחזוקה ועדכוני תוכנה של מערכות ש"ב : מה מותר ואסור ולמה? 	מפגש 2: סיכוני סייבר למערכות ש"ב
<ul style="list-style-type: none"> • מבוא למערכות הצפנה והזדהות במערכות ש"ב • התגוננות בפני תקיפות חיצוניות ופנימיות PPT TRIAD • הגנה על מערכות בפני תקיפות פנימיות וחיצוניות • אמצעי הזדהות הצפנה בין מערכות מרוחקות IPSEC וכו' • הגנה באמצעות חומת אש (FW) ומערכות אזור מפורז (DMZ) • הגנה על מערכות SOAR, SOC, SIEM, IDS • • הגנת סייבר על בנינים ומחנות בפני איומי סייבר • הגנה על מערכות VLR, RDC, SRP, CIA ועוד 	מפגש 3: סיכוני סייבר למערכות ש"ב
<ul style="list-style-type: none"> • סקירה על אירועי סייבר במשך 10 שנים אחרונות • סקירה לגבי חולשות קיימות שלא נין להם פתרון ראוי • אתגרים להגנת סייבר לשנים הבאות • תהליכי התגוננות IR-DRP-BCP מה נכון לעשות כדי להיות מוגנים • הקפדה על תהליכי פיתוח מאובטח של פרויקטים • ניהול אבטחת סייבר לגבי שרשרת האספקה לארגון • סקירה לגב תקנים 62443, NIST, CIP-NERC, הגנת הסביבה • הדגמה של אירועם ותגובה לאירועם בתחנות כוח 	מפגש 4: פתרונות ותקנים להגנת סייבר למערכות ש"ב