

ראשי פרקים של הרצאות בנושא סיכונים ואמצעי הגנה על מערכות תעשייתיות ותשתיות חיוניות בישראל מרצה: דניאל ארנרייך	
<ul style="list-style-type: none"> • מבנה מערכתי עיקרוני עבור פתרונות שליטה ובקרה (שו"ב) • התקנים שנמצאים במערכות אלה: SIS ,IED ,PLC ,RTU ,RIO • מחשבי ניהול ברשת: HISTORIAN ,HMI ,ENG , וכו' • מבנה מודל אירגוני מחולק ל 4 שכבות ו-6 שכבות (PURDUE) • תקשורת ופרוטוקולים במערכות שו"ב ומערכת, תקשורת • מבנה מערכות DCS ,SCADA ,PLC , והשלכות על סיכוני סייבר • סיכוני בטיחות תפעוליים – לא רק תקיפות סייבר! 	מפגש 1: מבוא למערכות שליטה ובקרה
<ul style="list-style-type: none"> • סיכוני סייבר באמצעות הנדסה חברתית – Social Engineering • הסבר על תהליכי תקיפה במערכות LM Cyber Kill Chain • הסבר מפורט לגבי תהליך תקיפה על מערכת שו"ב • תקיפה על מערכות מבפנים ומבחוץ: מונחים APT /ZERO DAY • "התרומה השלילית" של התקני IIOT לסיכוני סייבר. כיצד ניתן להפחית את הסיכון? • תקיפות: GPS Spoofing ,Ransomware ,MitM ,DDoS • תחזוקה ועדכוני תוכנה של מערכות שו"ב : מה מותר ואסור ולמה? 	מפגש 2: סיכוני סייבר למערכות שו"ב
<ul style="list-style-type: none"> • התגוננות בפני תקיפות חיצוניות ופנימיות PPT TRIAD • יסודות אימות וזיהוי התקנים, מחשבים, אנשים, ומגבלות גישה • פתרונות להגנה פיזית: מפעלים, חדרי מחשבים, מחשבים אישיים, התקנים מרוחקים • הפרדה בין אזורים כאמצעי הגנה בפני תקיפות APT • אמצעי הזדהות הצפנה בין מערכות מרוחקות IPSEC וכו' • הגנה באמצעות חומת אש (FW) ומערכות אזור מפורז (DMZ) • הגנה באמצעות מערכות לזיהוי חריגים: IDS לתהליך/תקשורת 	מפגש 3: סיכוני סייבר למערכות שו"ב
<ul style="list-style-type: none"> • מגבלות לגבי התחברות מרחוק למערכות שו"ב : מה מותר ואסור לעשות ולמה...? • סקירה לגבי פתרונות של אמצעי הגנת סייבר למערכות שו"ב ספקים ישראליים • הכנות עבור התהליך של חזרה לשגרה והבטחת המשכיות עסקית • סקירה עקרונית לגבי מסמך של תורת הסייבר 1.0 – מה לומדים ממנו • סקירה עקרונית על מסמך של המשרד לאיכות הסביבה 1.1 – מה מצפה לנו • חזרה על הנושאים שנלמדו: שאלות ותשובות, חלוקת תעודות. 	מפגש 4: פתרונות ותקנים להגנת סייבר למערכות שו"ב