



# קורס יסודות הסייבר

**אונליין**

שעות לימוד	נושאים נלמדים	נושא	
<b>מפגש ראשון</b>			
1	<ul style="list-style-type: none"> <li>סקירת מהלך הקורס - מטרות ויעדים</li> <li>סקירת אירועי סייבר בעולמות התעשייתיים.</li> <li>אירועי סייבר עולמיים בתעשייה על ציר הזמן</li> <li>אירועי סייבר בתעשייה בישראל (כולל תעשיית החומרים המסוכנים)</li> </ul>	מבוא	1
1	<ul style="list-style-type: none"> <li>אבטחת מידע VS סייבר</li> <li>סייבר בעולמות IT מול סייבר בעולמות OT</li> <li>בקורות אבטחת מידע</li> <li>רבדים בהגנת סייבר, הגנה רב שכבתית</li> <li>סקירת מעגלי אבטחת המידע</li> <li>מבנה רשת ארגונית</li> </ul>	מושגי יסוד בהגנת סייבר - חלק א'	2
<b>מפגש שני</b>			
2	<ul style="list-style-type: none"> <li>שרתי פרוקסי והגישה לאינטרנט</li> <li>כתובות IP ציבוריות ופרטיות</li> <li>חומת אש - עקרונות פעולה ושימושים</li> <li>חציצה (סגמנטציה)</li> <li>פרוטוקולים נפוצים בעולמות ה-IT וה-OT</li> <li>גישה מרחוק מאובטחת לארגון</li> <li>מהו VPN ומהם השימושים בו</li> <li>הזדהות: סיסמאות, הזדהות חכמה (MFA)</li> </ul>	מושגי יסוד בהגנת סייבר - חלק א' - המשך	3
<b>מפגש שלישי</b>			
2	<ul style="list-style-type: none"> <li>מודל הגנה בשכבות (Defense in Depth)</li> <li>התקפה ברמה אפליקטיבית: DOS, DDOS</li> <li>הגנה כנגד התקפות - מוצרי IDS, IPS</li> <li>משפחות וירוסים, עקרון הפעולה של אנטי-וירוס</li> <li>התקפת ZERO DAY</li> <li>הגנת SAND BOX</li> <li>מתקפת פשינג (Phishing)</li> </ul>	מושגי יסוד בהגנת סייבר - חלק ב'	4

שעות לימוד	נושאים נלמדים	נושא	
<b>מפגש רביעי</b>			
2	התקפת כופרה	מושגי יסוד בהגנת סייבר - חלק ג'	5
	איומים בשכבת האפליקציה (תקיפת (XSS) Cross Site Scripting, תקיפת - SQL injec-tion, תקיפת (Cross Site Request Forgery (CSRF))		
	WAF - הגנה על האפליקציה		
	DAF - הגנה על בסיס הנתונים		
	NAC - הגנה על חיבור התקנים זרים לרשת		
	DLP - הגנה על זליגת מידע מהארגון		
<b>מפגש חמישי</b>			
2	CDR - הלבנת קבצים עקרונית פעולה, דרכים שונות ליישום פתרון הלבנה בארגון	מושגי יסוד בהגנת סייבר - חלק ג' - המשך	6
	Unidirectional Security Gateway - דיודה חד כיוונית		
	הגנה על הבקר		
	הגנה על מערכת ERP		
	SIEM - SOC - עקרונות יישום		
<b>מפגש שישי</b>			
2	שיקולים במעבר לענן, הבדלים בין ענן ל-ON PREMIS	סייבר בענן	7
	סוגי עננים - ציבורי, פרטי, היברידי		
	סוגי שירותים בענן- laas, Paas, Saas, Daas		
	הסיכונים במעבר לענן		
	מזעור סיכוני סייבר במעבר לענן		
<b>מפגש שביעי</b>			
1.5	מיהם התוקפים ומה מטרותיהם?	שרשרת התקיפה	8
	מתודולוגיית Cyber Kill Chain		
	איסוף מידע במבט התוקף		
	הנדסה חברתית (Social Engineering)		
0.5	וקטורי התקיפה למערכות תעשייתיות	ניהול סיכונים במפעל תעשייתי	9
	גישות לניהול סיכונים בארגון		
<b>מפגש שמיני</b>			
1.5	זיהוי נכסים קריטיים - מתודולוגיית מיפוי נכסים בארגון	ניהול סיכונים במפעל תעשייתי - המשך	10
	תקן סייבר NIST CSF לניהול סיכונים		
	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		
<b>מפגש תשיעי</b>			
0.5	הצגת ממצאי חשיפות סייבר מתוך פיילוט סקרי סיכונים במפעלים	הצגת ממצאי סקרי סיכונים בתעשייה	11
1	סיכום הקורס	חזרה והכנה למבחן סיום	12
	שאלות ותשובות על כל תכני הקורס		
	מבחן מדגמי לתרגול		
1	מבחן סיום ציון מעבר 60.	מבחן סיום	13

שעות לימוד	נושאים נלמדים	נושא	
<b>מפגש עשירי - מפגש ספקים</b>			
2	· מפגש ספקים - פתרונות סייבר לתעשייה	מפגש ספקים	14
<b>20</b>		<b>סה"כ שעות</b>	
	· ניתוח האירוע שלב אחר שלב	<b>בנוסף: אם יאפשר הזמן</b>	
	· ניתוח שרשרת הכשלים אשר הביאו לאירוע	<b>ניתוח תקיפת סייבר על חברת ביטוח שירביט</b>	
	· מסקנות מהאירוע		