



**CYBERPROAi**  
Israel

**Network Security Course for  
Cyber Defenders**

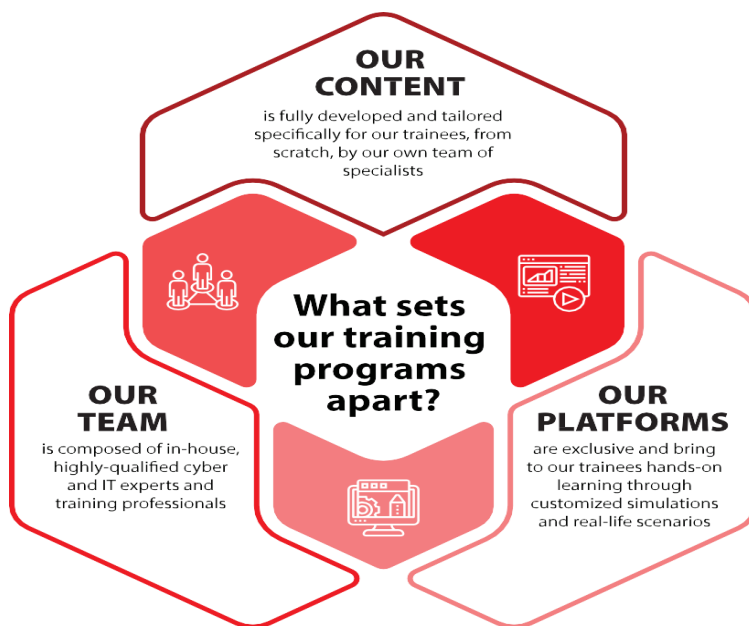
## אודות סייברפרו ישראל

סייברפרו הינה חברת הכשרות גלובלית העומדת בחזית הפיתוח של תוכניות לימוד טכנולוגיה ומוצרי הכשרה מתקדמים, אשר פותחו על-ידי מומחי תוכן מהטובים בעולם ומתעדכנים כל העת, בהתאם לצרכי התעשייה המתחדשים. תפיסת ההכשרה ממוקדת בסטודנט/ית, בדגש על למידה מעשית המשלבת טכנולוגיות מתקדמות המביאות למיצוי המירבי של הפוטנציאל ומציידות אותו/ה בידע ובמגוון כלים רלוונטיים להתחלה מיידית בתפקידים שונים בתעשייה.

סייברפרו ישראל הינה השלוחה הישראלית של זו הגלובלית ולה שני מרכזי הכשרה עיקריים, ברמת-גן וברעננה, כאשר מתקיימות הכשרות בכל רחבי הארץ, לכל חלקי האוכלוסייה ובשיתוף פעולה הדוק עם ארגונים שונים. אופן ההכשרה גמיש ומשתנה בהתאם לצרכי אוכלוסיית היעד: פרונטלי, אונליין חי, היברידי (פרונטלי-אונליין), תכנים מוקלטים ולימוד אינטראקטיבי.

## יתרונות סייברפרו

1. **הסטודנטים/ות במרכז:** חוויית למידה מעשית ופרקטית שמספקת כלים וידע מוכוון תעסוקה.
2. **הזדמנות שווה:** שיטת מיון ייחודית ומבוססת מחקר שמזהה ומכוונת את יכולות הסטודנט/ית להכשרה מקיפה.
3. **קשר לתעשייה:** יצירת קשרים עם התעשייה דרך עבודה שוטפת והתאמת ההכשרות לצרכים המשתנים בתחום.
4. **מעבדות סייברפרו:** שימוש בטכנולוגיות למידה מתקדמות וחדישות במעבדות המתקדמות ביותר.
5. **עדכון שוטף:** יותר מ-6,000 שעות הכשרה שמתעדכנות באופן תדיר בהתאם לחידושים בעולם.
6. **התאמה ללקוח:** בניית תוכניות הכשרה מותאמות לצרכים המיוחדים של כל לקוח.
7. **חברה גלובלית:** סייברפרו פועלת ברחבי העולם ומשאירה חותמת עולמית בתחום עם מומחים/ות ברמה הגבוהה ביותר.



**סילבוס מוצע Network Security Course for Cyber Defenders**

Module	Academic Hours
Module 1 <b>Introduction</b>	
Module 2 <b>Network Hardening</b>	
Module 3 <b>Wireless Network Security</b>	
Module 4 <b>Network Monitoring and Logging</b>	
Module 5 <b>Incident Response</b>	
Module 6 <b>Cloud Network Security</b>	
Module 7 <b>Cryptography in Network Security</b>	
Module 8 <b>Automation and Scripting for Network Security</b>	
Module 9 <b>Emerging Trends and Technologies</b>	
Module 10 <b>Practical Labs and Exercises</b>	

**Total Academic Hours :40**

Module	Description	Hours
<b>Module 1</b> <b>Secure Network Design</b>	<ul style="list-style-type: none"> <li>Zero Trust Architecture</li> <li>DMZ configuration and use cases</li> <li>VPNs and secure remote access solutions</li> <li>Redundancy and failover strategies</li> </ul>	
<b>Module 2</b> <b>Network Hardening</b>	<ul style="list-style-type: none"> <li>Secure configuration of routers, switches, and firewalls</li> <li>Disabling unused services and ports</li> <li>MAC address filtering and port security</li> <li>Defense against common attacks (DDoS, ARP spoofing, etc.)</li> </ul>	
<b>Module 3</b> <b>Wireless Network Security</b>	<ul style="list-style-type: none"> <li>Securing Wi-Fi access points and routers</li> <li>WPA3 and other modern wireless protocols</li> <li>Detecting and mitigating rogue access points</li> <li>Wireless penetration testing techniques</li> <li>Wireless signal jamming and its detection</li> </ul>	
<b>Module 4</b> <b>Network Monitoring and Logging</b>	<ul style="list-style-type: none"> <li>Log aggregation and analysis</li> <li>Detecting lateral movement within a network</li> </ul>	
<b>Module 5</b> <b>Incident Response</b>	<ul style="list-style-type: none"> <li>Network-based incident detection and response</li> <li>Containing and mitigating network breaches</li> <li>Forensic investigation of network traffic</li> <li>Post-incident analysis and reporting</li> </ul>	

Module	Description	Hours
<b>Module 6</b> <b>Cloud Network Security</b>	<ul style="list-style-type: none"> <li>• Securing hybrid and multi-cloud networks</li> <li>• Cloud-native firewalls and monitoring solutions</li> <li>• Shared responsibility model in cloud security</li> <li>• Secure API communication</li> </ul>	
<b>Module 7</b> <b>Cryptography in Network Security</b>	<ul style="list-style-type: none"> <li>• Understanding SSL/TLS encryption</li> <li>• Configuring HTTPS on servers and clients</li> <li>• VPN encryption protocols (IPSec, OpenVPN)</li> <li>• Certificates and PKI (Public Key Infrastructure)</li> </ul>	
<b>Module 8</b> <b>Automation and Scripting for Network Security</b>	<ul style="list-style-type: none"> <li>• Writing scripts for network monitoring (Python, PowerShell)</li> <li>• Automating log analysis and alerting</li> <li>• Integration with tools like Ansible for network management</li> </ul>	
<b>Module 9</b> <b>Compliance and Policy</b>	<ul style="list-style-type: none"> <li>• Network security standards (NIST, ISO 27001, etc.)</li> <li>• Regulatory compliance (GDPR, HIPAA, etc.)</li> <li>• Writing and enforcing network security policies</li> </ul>	
<b>Module 10</b> <b>Emerging Trends and Technologies</b>	<ul style="list-style-type: none"> <li>• Post-incident analysis and reportingAI and ML in network security</li> <li>• Securing IoT devices in networks</li> <li>• Quantum cryptography and its impact on network security</li> <li>• Next-generation firewalls (NGFW)</li> </ul>	
<b>Module 11</b> <b>Practical Labs and Exercises</b>	<ul style="list-style-type: none"> <li>• Setting up a secure VPN tunnel</li> <li>• Configuring firewalls with advanced rules</li> <li>• Responding to a simulated DDoS attack</li> <li>• Simulating network congestion and its resolution</li> </ul>	





CYBERPROAi  
Israel