CYBERPROAi
Israel

INFORMATION SECURITY & OFFENSIVE CYBER

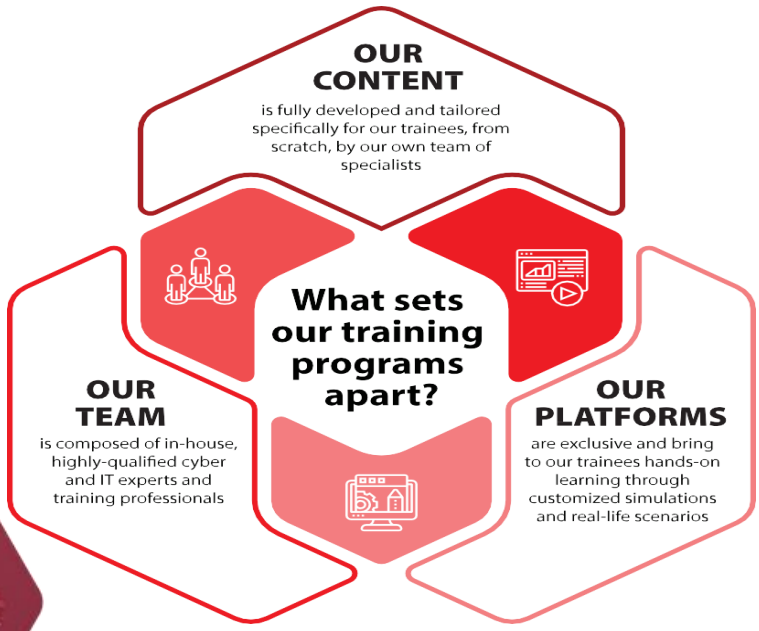
אודות סייברפרו ישראל

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.



INFORMATION SECURITY & OFFENSIVE CYBER - קורס

Module	Academic Hours
Module 1 **Networking**	100
Module 2 **Windows**	100
Module 3 **Linux**	80
Module 4 **Python**	80
Module 5 **Anatomy of an Attack**	120
Module 6 **Breach prevention**	100
Module 7 **Infrastructure PT**	120

Total Hours: 700

Module	Description	Hours
Module 1 **Networking**	• Introduction to networking • OSI and TCP/IP models – encapsulation an de-encapsulation • Layer 1 in short • Layer 2 protocols • Switch (layer 2) operation • Layer 3 protocols • Address Resolution Protocol (ARP) • Point to point delivery • Layer 4 protocols • Application protocols	100
Module 2 **Windows**	• Introduction to windows • Windows data structure • Local users and groups • NTFS permissions • Network configuration • Introduction to active directory • Install windows server 2019 • Install AD DS and DNS roles • Mange domain users and security groups • Protected security groups • Introduction to Group Policy • Introduction to AD objects • Authentication protocols in MS-domain • Introduction to Azure cloud • Introduction to PowerShell	100
Module 3 **Linux**	• Introduction to Linux • Linux terminals and shells • Linux file system structure • Working with files and folders • Important shell concepts • Basic file permissions • Managing users and groups • Special file permissions • Deep dive into text processing • Searching for files • Manage processes and signaling • Manage services (Systemd) • Package management • Networking • Bash scripting	80

Module	Description	Hours
Module 4 **Python**	• Introduction to Python • Variables and data types • Numbers • Working with strings and string formatting • Booleans and operators • User input • Advanced data structures • Logic – If, Else if, and Else statements • Loops • Reading and writing files • List and dictionary comprehensions • Functions and code reuse • Exceptions handling • Introduction to OOP • Python modules	80
Module 5 **Anatomy of an Attack**	• The cyber kill chain and MITRE • Introduction to reconnaissance (OSINT) • Active scanning • Brute force attacks • Introduction to vulnerabilities and CVEs • Remote control • Introduction to client-side attacks • Basic windows and Linux privilege escalation • Introduction to post exploitation • Introduction to lateral movement	120
Module 6 **Breach prevention**	• Vulnerability management • Firewall rules - best practice • Risk management • Security controls • Network segmentation • Network monitoring and malware detection • Security Incident and Event Management (SIEM) • Security Operation Centers (SOC) • Monitoring traffic and connections	100

Module	Description	Hours
Module 7 **Infrastructure PT**	• Advanced active scanning • Deep dive into remote control • Client-side attacks • Domain enumeration • Internal attacks • Windows privilege escalation • Windows post exploitation • Domain privilege escalation • Domain sersistence	120


CYBERPROAi
Israel