CYBERPROAi
Israel

Windows Malware Analysis

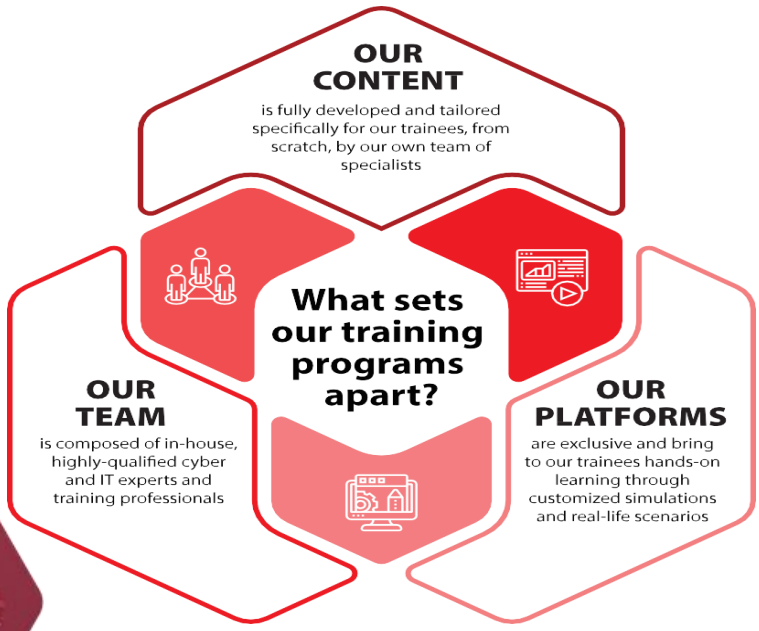
אודות סייברפרו ישראל

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 להכשרת Windows Malware Analysis

Module	Academic Hours
Foundations of Windows Forensics	
Navigating Windows File Systems	
Deep Dive into Registry Forensics	
Analyzing Windows Event Logs	
Mastery of Data Acquisition	
Windows Network Forensics	
Email and Web Artifacts Forensics	
Advanced Forensic Analysis and Correlation	
Timeline Analysis	
Effective Forensic Reporting	

Total Hours: 45

Copyright © CYBERPRO Israel | Confidential - Do not duplicate or distribute without written permission.

Module	Description
Foundations of Windows Forensics	• components of Windows operating systems relevant to forensics. • fundamental principles of digital forensics • role and functionality of primary forensic tools like Autopsy and Plaso.
Navigating Windows File Systems	• Architecture and forensic relevance of NTFS, FAT, and exFAT file systems. • Analyze file system artifacts to uncover forensic evidence. • Utilize forensic tools • Data recovery techniques
Deep Dive into Registry Forensics	• structure of the Windows Registry and identify its forensic importance. • Analyze key Registry artifacts • Demonstrate the use of forensic tools • Examine System and Application metadata • Investigate user activity through analysis of LNK files and MRU lists
Analyzing Windows Event Logs	• Windows event logs to identify security incidents and anomalies. • Correlate event log data with other forensic artifacts • Employ advanced tools for detailed log analysis, incorporating timeline techniques. • Analyze Prefetch files to understand application execution and scheduling.
Mastery of Data Acquisition	• Differentiate between static and live data acquisition methods • Execute live data acquisition techniques • Navigate and mitigate encryption challenges during data acquisition.
Windows Network Forensics	• Analyze Windows network configurations and log files • Investigate web artifacts and email data • Apply network forensic tools and techniques
Email and Web Artifacts Forensics	

Copyright © CYBERPRO Israel | Confidential - Do not duplicate or distribute without written permission.

Module	Description
Email and Web Artifacts Forensics	• Extract and analyze email artifacts • Investigate web browsing history, cookies, and cache files • Utilize specialized forensic tools • Assess the role of steganography in concealing information
Advanced Forensic Analysis and Correlation	• Implement advanced log analysis and correlation techniques • Conduct data carving operations using specialized tools • Analyze Prefetch and Thumbs.db files • Apply critical analysis to interpret complex forensic data and artifacts.
Timeline Analysis	• Differentiate between various event types and timestamp types • Apply approaches to establishing temporal proximity between events • Create detailed timelines using forensic tools • Analyze timeline data to reconstruct events • Evaluate the effectiveness of timeline analysis in digital forensics
Effective Forensic Reporting	• Construct detailed forensic reports • Communicate forensic analysis outcomes to both technical and non-technical stakeholders. • Uphold the ethical standards and legal requirements • Practice the art of clear, concise, and objective reporting in forensic investigations.

Copyright © CYBERPRO Israel | Confidential - Do not duplicate or distribute without written permission.

CYBERPROAi
Israel