CYBERPROAi
Israel

# Linux Forensics Syllabus

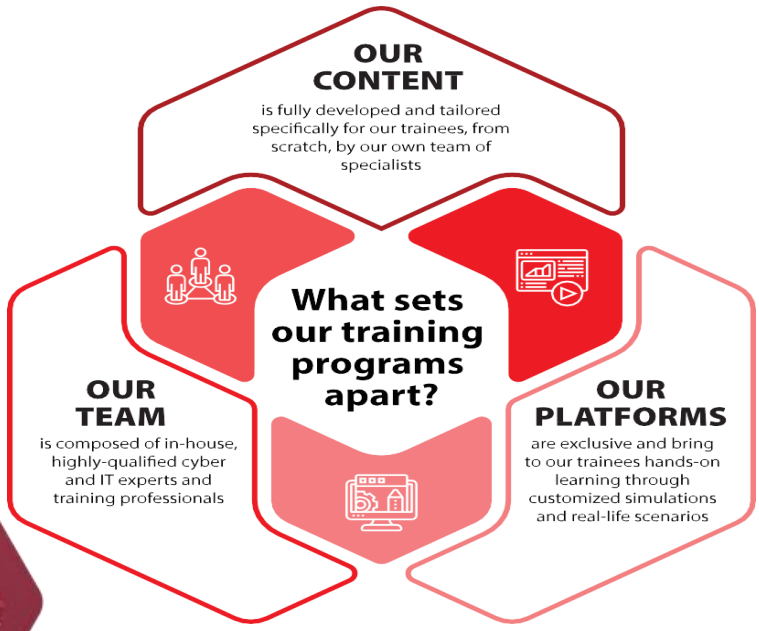
# אודות סייברפרו ישראל

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.



# Linux Forensics Syllabus סילבוס להכשרת

| Module | Academic Hours |
|---|---|
| Intro to Linux System Forensics | |
| The Linux Boot Process | |
| System Data Acquisition | |
| RAID and Remote Acquisitions | |
| Disk and Filesystem Analysis | |
| Disk and Filesystem Analysis Tools | |
| Memory Acquisition | |
| Memory Analysis | |
| Logs, Artifacts, and Timeline Analysis | |

**Total Hours: 45**

| Module | Description |
|---|---|
| **Intro to Linux System Forensics** | • Getting rolling with the Tsurugi Linux Forensics Worstation<br>• Recap of the Network Forensics Final Exam<br>• Revisiting the Value of the Blue Team<br>• Roadmap for Linux Forensics Course<br>• Continuing with Tsurugi |
| **The Linux Boot Process** | • Understanding How Things Start<br>• Understanding the Old System V init Process<br>• Understanding the New systemd Architecture |
| **System Data Acquisition** | • Understanding Collection Tools and Methods<br>• Understanding Storage Formats for Digital Evidence<br>• Determining the Best Acquisition Method<br>• Contingency Planning for Image Acquisitions |
| **RAID and Remote Acquisitions** | • Understanding RAID and the Various Levels<br>• Using Remote Acquisition Tools<br>• Perform a Remote Live Image |
| **Disk and Filesystem Analysis** | • Understanding the History of Linux Filesystems<br>• The Filesystem Abstraction Model<br>• Ext2 Structures and the Virtual Filesystem Layer (VFS)<br>• Media Analysis Concepts<br>• Carving a Partition from a Disk Image |
| **Disk and Filesystem Analysis Tools** | • Practice with Images, Creating a Filesystem, and Mounting it<br>• Exploring the Sleuth Kit (TSK)<br>• Practice with TSK Tools<br>• Test and Explore Foremost |

| Module | Description |
|---|---|
| **Memory Acquisition** | • Understanding Memory Acquisition and Forensics<br>• Factors and Concerns Involved with Memory Acquisition<br>• Historical Methods of Linux Memory Acquisition<br>• Modern Memory Acquisition with Linux<br>• Building and Using the Linux Memory Extractor (LiME)<br>• Using LiME for Remote RAM Acquisition |
| **Memory Analysis** | • Introduction to the Volatility Framework<br>• Introduction to Volatility Profiles<br>• A CFT with Volatility |
| **Logs, Artifacts, and Timeline Analysis** | • Understanding Linux Logs<br>• Getting the Lay of the Land<br>• Understanding Linux Artifacts<br>• Exploring the Unix-like Artifact Collector (UAC) |


CYBERPROAi
Israel