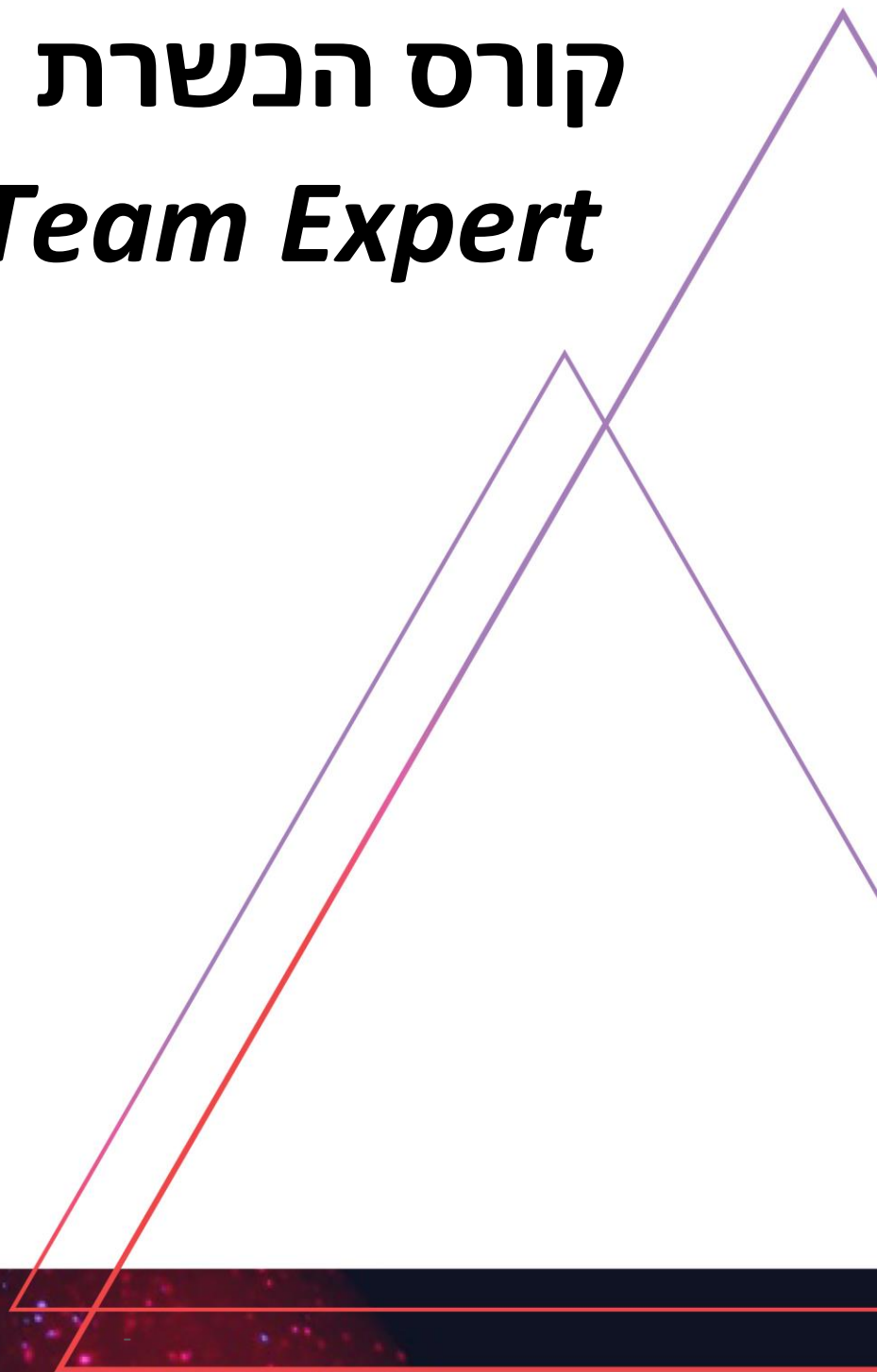


CYBERPRO  
ACADEMY

קורס הכשרת  
*Blue Team Expert*



CYBERPRO Global הינה חברה בינלאומית מובילה המספקת תוכניות הכשרה לאבטחת סייבר ואבטחת מידע, המבוססות טכנולוגיות אימון סייבר מובילות בעולם וחוויית למידה ברמה הגבוהה ביותר הקיימת כיום.

החברה מפתחת תוכניות הדרכת סייבר עבור גופים בינלאומיים מובילים ומפעילה מספר מרכזי לימוד ייחודיים ברחבי העולם.

CYBERPRO Academy הינה השלוחה הישראלית של CYBERPRO Global, אשר הוקמה על מנת לתת מענה לצורך הולך וגדל באנשי מקצוע בשוק הישראלי והרחבת שיתוף הפעולה עם חברות טכנולוגיות ישראליות המפתחות כלי סייבר מתקדמים.

ההכשרות המתקדמות והמבוקשות של CYBERPRO בתחומי תשתיות, אבטחת מידע וסייבר הינן שם דבר בעולם. הכשרות אלו פותחו על ידי מומחי סייבר מהשורה הראשונה בעולם, עבור גופי אבטחה בינלאומיים השמים דגש רב על יכולות ההדרכה הגבוהות, שיטות הלמידה המקצועיות וטכנולוגיות האימון והתרגול הייחודיות. החיבור עם גופים בינלאומיים מאפשרים לסטודנטים הלומדים אצלנו להחשף להזדמנויות תעסוקה ייחודיות בארץ ובעולם.

## CYBERANGE PRO

### סימולטור סייבר חדשני וייחודי

טובי  
המדריכים



טכנולוגיות  
חדשניות



תוכניות לימודים  
מכוונות תרגול  
מעשי



פעילות  
בין לאומית



מעבדות  
מתקדמות

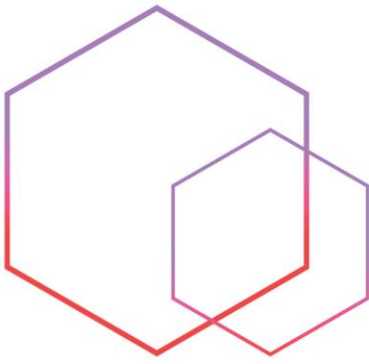


חומרי לימוד בפיתוח עצמי  
הניתנים להתאמה לצרכי הלקוח



מסלולי ההכשרה והלימוד מבוססים כולם על תרגול מעשי רב, הכנה לדרישות התעשייה והמקצוע ולכן משלבים מעבדות טכנולוגיות ותרגול באמצעות סימולטור מהמתקדמים בעולם.





# קורס הכשרת Blue Team Expert

Threat Hunting, digital Forensics & ללימודי מקיף  
Incident Response להכשרה צוותים כחולים

## היקף הקורס

היקף הקורס הינו 248 שעות אקדמאיות

## אודות הקורס

משימתו של איש אבטחת המידע הארגוני מעולם לא היתה פשוטה ובעשור האחרון היא הפכה לאתגר כמעט בלתי אפשרי; מצד אחד העליה האקספוננציאלית (מעריכית) במורכבות המערכת עליה הוא אמון ובכמות הפגיעויות המובנות בה. ומצד שני, פערי היכולת והידע אל מול התוקפים שגדלו עד כדי שספק אם ניתן יהיה לגשר עליהם אי פעם.

מסלול זה מכשיר את התלמיד לתפקיד המגן הארגוני (איש צוות כחול) ברמה שתאפשר לו להתמודד בהצלחה עם האיומים המודרניים על מערכות המידע הארגוניות; לצורך זה הוא ילמד את תהליך התקיפה באופן מעשי, יכיר בצורה עמוקה את שלל פתרונות ההגנה המקובלים בתעשייה, ילמד "להסניף", לנטר ולנתח תקשורת נתונים, לבצע חקירות של פוגענים על גבי מערכות הפעלה מבוססות Windows ו-Linux, לאסוף, לסדר ולצוד אירועי מערכת מכל הארגון כדי לזהות IoC's (אינדיקטורים לתקיפה) ולחקור אותם תוך כדי תנועה ובתוך מגבלות של זמן ומידע.

המסלול יועבר תוך מתן דגש על עבודה מעשית, כך שמרבית הזמן יוקדש למעבדות ותרגול. בסוף הקורס יתמודדו החניכים עם אתגר חקירה של אירוע אמיתי מורכב ש"התפרק" על גבי מערכת מידע ארגונית גדולה.

## קהל היעד

הקורס מיועד לצוותים כחולים, לאנליסטים ובקרי SOC, חוקרי אבטחה, חוקרים פורנזיים, מומחי IT ותשתיות, בוגרי מסלול Cyber Essentials וצוותי Incident Response המעוניינים לרכוש ידע מעשי בתחום.

## דרישות קדם

- היכרות טובה עם מערכות הפעלה מבוססות Windows
- היכרות עם מערכות הפעלה מבוססות Linux
- היכרות עם טכניקות לוחמת סייבר
- היכרות עם פרוטוקולי תקשורת TCP/IP
- היכרות עם קוד - יתרון



- **Anatomy of an attack**

- ◆ Attack lifecycle and the Cyber Kill Chain
- ◆ Information Gathering
- ◆ Vulnerability Assessment
- ◆ Server-side Attacks
- ◆ Client-Side Attacks
- ◆ Web Application Hacking
- ◆ Windows Privilege Escalation
- ◆ Lateral Movement
- ◆ Persistence and Backdooring

- **Enterprise Defenses**

- ◆ Enterprise information systems as a battleground
- ◆ Start with inventory
- ◆ Vulnerability assessment and path management
- ◆ Network segmentation, segregation and separation
- ◆ Deep visibility at the endpoint
- ◆ Managing privileged accounts and hosts
- ◆ Anti-malware defenses
- ◆ Windows client configuration and hardening
- ◆ Linux server and service configuration and hardening
- ◆ Backup and forensic readiness

---

- **Network Monitoring and Detection**

- ◆ Networking 101
- ◆ Parsing traffic with network shell
- ◆ Indexing and generating statistics
- ◆ Parsing the higher layers
- ◆ case#1: mail harassment
- ◆ Introduction to malware and targeted attacks
- ◆ case#2: browser exploit
- ◆ sniffers, sensors, taps and protocol analyzers
- ◆ case#3: malware in pcap
- ◆ IDS/IPS, monitoring and network security analytics

- **Windows Malware Forensics**

- ◆ Digital forensics in rapid changing space
- ◆ Disk and fs analysis
- ◆ Generating fs timelines
- ◆ Windows system artifacts
- ◆ Internet related artifacts
- ◆ Super timeline all the things
- ◆ Memory forensics
- ◆ Digging deeper into Windows memory
- ◆ Windows forensic challenge

---

- **Linux Forensics**

- ◆ Disk and filesystem analysis
- ◆ Generating fs timelines
- ◆ Linux filesystem artifacts
- ◆ Server and service-related artifacts
- ◆ Super timeline all the things
- ◆ Linux memory forensics
- ◆ Linux forensic challenge

- **Threat Hunting with SIEM**

- ◆ State of the SOC/SIEM
  - ◆ Log collection, normalization and aggregation
  - ◆ SIEM Architectures
  - ◆ Profiling windows endpoints
  - ◆ Profiling Linux endpoints
  - ◆ Profiling infrastructure services
  - ◆ Profiling application services
  - ◆ Generating baselines, thresholds and detection rules
  - ◆ Hunting indicators of compromise (IoC's)
-