CYBERPRO
ISRAEL

CYBERPRO Global הינה חברה בינלאומית מובילה המספקת תוכניות הכשרה לאבטחת סייבר ואבטחת מידע, המבוססות טכנולוגיות אימון סייבר מובילות בעולם וחווית למידה ברמה הגבוהה ביותר הקיימת כיום. החברה מפתחת תוכניות הדרכת סייבר עבור גופים בינלאומיים מובילים ומפעילה מספר מרכזי לימוד ייחודיים ברחבי העולם.

CYBERPRO Israel 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 גופיי 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

זירת אימוני סייבר חדשנית וייחודית

- טובי המדריכים
- תכניות לימודים מכוונות תרגול מעשי
- טכנולוגיות חדשניות
- מעבדות מתקדמות
- פעילות בין לאומית
- **חומרי לימוד בפיתוח עצמי** הניתנים להתאמה לצרכי הלקוח

ספק מורשה משרד הביטחון

מוכר לפיקדון חיילים משוחררים

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

CYBERPRO ISRAEL | החילזון 3, רמת גן | 03-3812121 | info@cyberpro-israel.co.il | www.cyberpro-israel.co.il

CYBERPRO ISRAEL

קורס הכשרת BLUE TEAM DEFENDER (BTD)

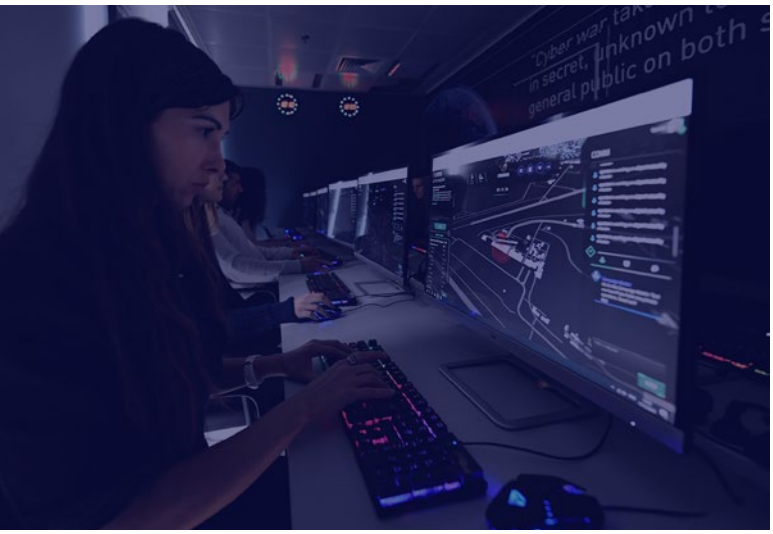
קורס הכשרת Blue Team Defender מכין את בוגריו להתמודד בהצלחה עם האיומים העדכניים ביותר שיש למערכות המידע הארגוניות כיום. הידע הנלמד בקורס מגן סייבר יסייע לך לנטר ולנתח תקשורת נתונים חשודה, לחקור נזקי פוגענים ועוד.

בהכשרה הייחודית של CYBERPRO הושם דגש על עבודה מעשית רבה שתבוצע במעבדות תרגול ובאמצעות טכנולוגיות למידה מהמתקדמות בעולם.
בסיום הקורס תוכלו להגן ולאבטח מערכות מידע, לצוד אירועי חדירה ולזהות התקפות שמתרגשות לבוא. הקורס יכשיר אתכם לתעשיית הסייבר לתפקידים כגון: Incident Responder, מפעיל SOC, אנליסט סייבר וחוקר סייבר.

תחום	Blue Team	**פורמט**	לימודי ערב פעמיים בשבוע
לימוד פרונטלי ומעבדה	**248** שעות	**מעבדות אונליין**	80 שעות
הכנה להסמכות בינלאומיות מובילות	GIAC, BTD Blue Team Defender	**מיקום**	קמפוס סייברפרו, החילזון 3, רמת גן

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



CYBERPRO ISRAEL

סילבוס

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)

Final Blue Team Challenge

- Enterprise-scale breach CTF
- Hunt and investigate "targeted" multi-vector attack
- Teams will follow SOC leads and perform ad-hoc investigations
- Teams will submit full incident reports
- Challenge walkthrough and investigative conclusions

CYBERPRO
ISRAEL

COURSES, WORKSHOPS AND TRAINING PROGRAMS

E Cyber Essentials

B Blue Team Defender

R Red Team Expert

C קורס ניהול אבטחת מידע - CISO

W Workshops

Introduction to Cyber Warfare

Anatomy of an Attack

Web Application Hacking

Network Monitoring and Detection

Windows Malware Forensics

Linux Forensics

Introduction to ASM x86 and Reverse Engineering

CISSP Bootcamp

www.cyberpro-israel.co.il | info@cyberpro-israel.co.il | 03-3812121 | החילזון 3, רמת גן | **CYBERPRO ISRAEL**