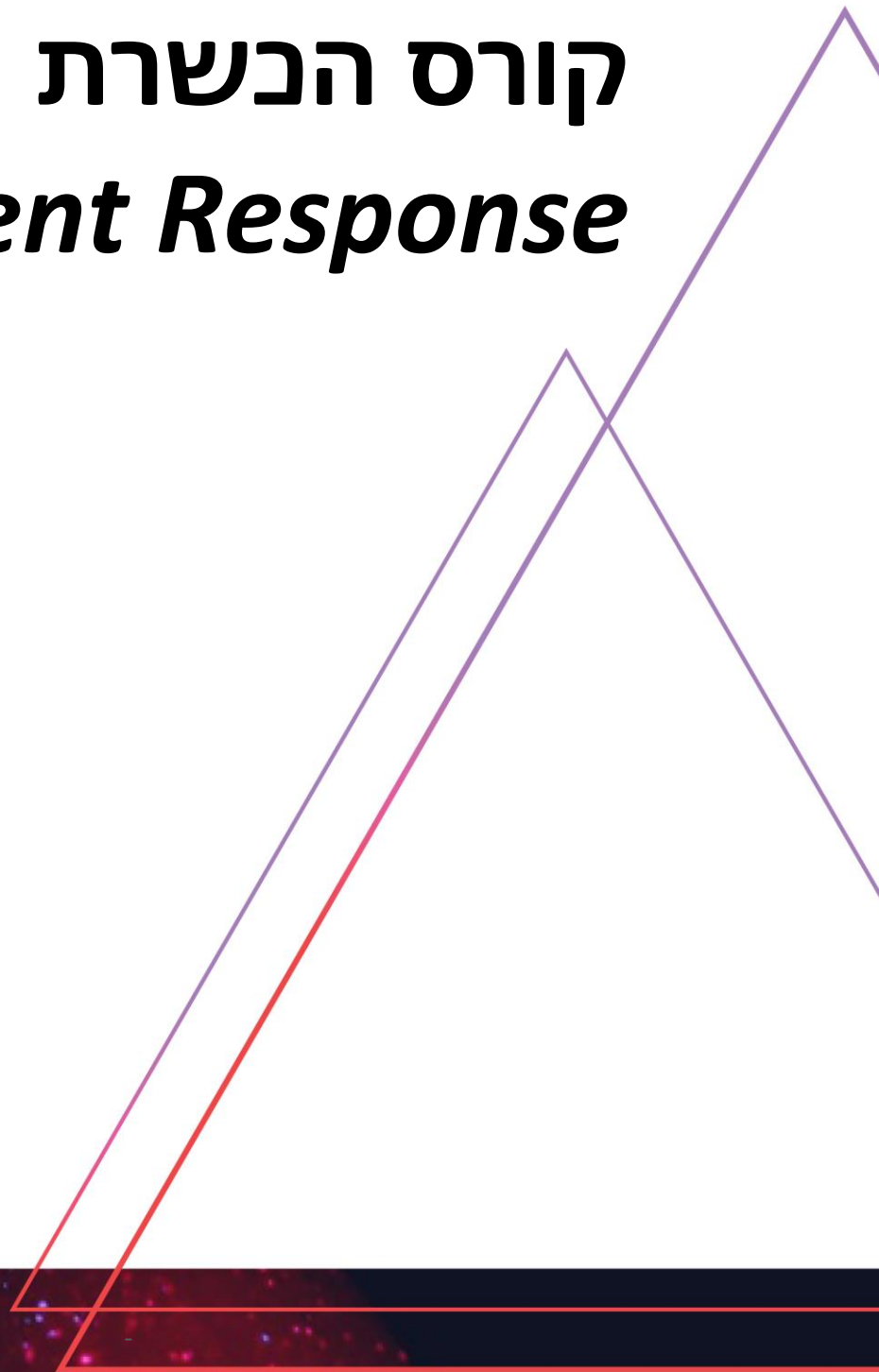


CYBERPRO
ACADEMY

קורס הבשרת
Incident Response



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 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

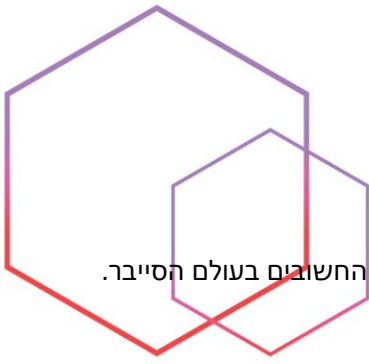


חומרי לימוד בפיתוח עצמי
הניתנים להתאמה לצרכי הלקוח



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





קורס הכשרת Incident Response

מסלול הכשרה ממוקד לתפקיד Incident Response שהינו אחד מהתפקידים החשובים בעולם הסייבר.

היקף הקורס

היקף הקורס הינו 240 שעות אקדמיות.

1.1 אודות הקורס

תגובה לאירוע סייבר הינה תהליך מורכב בו ארגון מטפל בזליגת מידע או מתקפת סייבר. תהליך זה כולל גם את אופן בו הארגון מנסה לנהל את תוצאות התקיפה על מנת להכיל ולמזער את הנזק ככל שניתן. לקראת הצטרפותם למערך ההגנה הארגוני כחלק מצוותי ה CSIRT או SOC של הארגון, ילמדו משתתפי הקורס כיצד לבצע ניתוח תוכנות זדוניות וחקירות דיגיטליות על מנת לגלות את אופן פעולתה של ההתקפה על מנת לחסום ולהכיל אותה.

1.2 קהל היעד

הקורס מיועד מבקשים להיכנס לעולם מקצועות הסייבר ומעוניינים בהכשרה ממוקדת ומעשית על מנת להיות חלק מצוות ה- Incident Response של הארגון

1.3 דרישות קדם

- היכרות עם מחשבים ואינטרנט ברמת משתמש
- יכולת אנליטית טובה (חשיבה לוגית, פתרון בעיות)
- אנגלית ברמה טובה
- יכולות למידה גבוהות
- ניסיון קודם בניהול רשתות מיקרוסופט, תשתיות תקשורת ו/או כתיבת קוד – יתרון

1.4 תוכנית הקורס

- **Networking Fundamentals**
 - ◆ OSI and TCP/IP models
 - ◆ The physical layer
 - ◆ The Ethernet protocols
 - ◆ Basic switch operation
 - ◆ IPv4 addresses and VLSM
 - ◆ Address Resolution protocol
 - ◆ Point to point delivery
 - ◆ Routing protocols
 - ◆ ICMPv4
 - ◆ Introduction to IPv6
 - ◆ Application layer protocols
 - ◆ Using protocol analyzers
- **MS-Domain technologies**
 - ◆ Windows Clients
 - ◆ Windows Server
 - ◆ Install and configure Active directory
 - ◆ Create and manage Group policy
 - ◆ Remote access solutions
 - ◆ Authentication services
 - ◆ Infrastructure services
 - ◆ PowerShell

- **Linux Fundamentals**

- ◆ Introduction to Linux
- ◆ The command-line interface
- ◆ Working with files and folders
- ◆ Text processing
- ◆ Regular Expressions
- ◆ Searching for files
- ◆ Users, groups and permissions
- ◆ System administrations
- ◆ Linux networking
- ◆ Introduction to shell scripting

- **Introduction to Python**

- ◆ Hello Python
- ◆ Python variables and conditionals
- ◆ Python lists and loops
- ◆ Dictionaries and structuring data
- ◆ Manipulating strings
- ◆ Pattern Matching with regular expressions
- ◆ Function and functional writing
- ◆ Reading and writing files
- ◆ Networking with python socket
- ◆ RAW sockets with scapy module

- **Network Forensics**

- ◆ Why bother parsing network traffic?
- ◆ Parsing traffic with Linux shell
- ◆ Indexing and generating statistics
- ◆ Parsing the higher layers
- ◆ Case #1: mail harassment
- ◆ Introduction to malware and targeted attacks
- ◆ Case #2: simple exploit
- ◆ Big brother tactics
- ◆ Case#3: new perspectives

- **OS Forensics**

- ◆ Digital forensics in rapid changing space
- ◆ Disk and filesystem analysis
- ◆ Generating file system timelines
- ◆ Windows system artifacts
- ◆ Linux filesystem artifacts
- ◆ Internet related artifacts
- ◆ Server and service-related artifacts
- ◆ Super timeline all the things
- ◆ Windows and Linux memory forensics
- ◆ Hunting windows malware in memory
- ◆ Digging deeper (windows memory)

- **Windows Malware analysis**

- ◆ x86 (Dis)assembly Basics
- ◆ Working with native code
- ◆ Debuggers: GDB and WinDBG
- ◆ Linux sys calls
- ◆ WinAPI
- ◆ Analyzing PE files
- ◆ Practice Assembly
- ◆ Reversing Unknown binary with IDA

- **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)
-