



קורס דיגיטלי

סיובר

ואבטחת מידע

Hacker.U
by ThriveDX



קצת עלינו

HackerU היא ה'חממה' (Techcelerator) המובילה בישראל להכשרת דור העתיד של תעשיית ההייטק.

כחלק מקבוצת ThriveDX הגלובלית אנחנו מובילים את מהפכת ה-EdTech בישראל ובעולם באמצעות הכשרה מקצועית איכותית וממוקדת. תוכניות ההכשרה שלנו מועברות לעשרות אלפי סטודנטים באוניברסיטאות, גופי ממשל, צבאות ומשטרות ברחבי העולם. יותר מ-25 שנה שאנחנו מאתרים מועמדים עם פוטנציאל, מאבחנים את התחומים שמתאימים לכל אחד ואחת מהם, מלווים, מכשירים אותם מקצועית על ידי הכשרה ב-Live ולימודים מקוונים ומוצאים להם עבודה בתעשייה.



בקצרה על הקורס

קורס סייבר ואבטחת מידע של האקריו נבנה במיוחד כדי להעניק לך הכשרה מעמיקה ומעשית בתחום המרתק והמבוקש ביותר בהייטק. בקורס תלמד להגן על מערכות מידע ותקשורת מפני פריצות והתקפות, לצד פיתוח מיומנויות בתקיפת מערכות מחשוב - בדיוק כמו שמצפים בתעשייה.

הקורס משלב בין ידע תאורטי לפרקטיקה מעשית, עם סימולטור מתקדם המדמה תרחישי תקיפה והגנה אמיתיים. כל זאת בהנחיה של מומחים בעלי ניסיון מעשי והכרה עולמית בתחום הסייבר ואבטחת המידע.

במהלך הקורס תרכוש כלים ויכולות חיוניים כמו ניתוח רשתות, קריפטוגרפיה, הגנה על תשתיות קריטיות, חשיבה אנליטית ותגובה מהירה לאיומים - כך שתהיה מוכן לכל אתגר בשטח.

למי הקורס מתאים?

הקורס מיועד לכל מי שרוצה להיכנס לעולם הסייבר גם בלי רקע טכנולוגי קודם. אם אתם מחפשים קריירה עם יציבות וביטחון כלכלי – זה בדיוק המקום להתחיל.

הקורס מתאים במיוחד ל:

- אנשים שרוצים להתחיל קריירה בעולם הסייבר גם בלי ניסיון קודם.
- אנשים עם גישה טכנולוגית שרוצים להשתלב במקצוע עם אופק צמיחה.
- מי שמחפש לעשות שינוי מקצועי לתחום עם ביקוש גבוה ושכר מתגמל.
- מי שרוצה להשתלב בהייטק עם פוטנציאל שכר של 15,000-20,000 ש"ח ומעלה.

למה לבחור דווקא ב-HackerU?



ניסיון של מעל 25 שנה
בהכשרת אנשי הייטק עם אלפי בוגרים שכבר עובדים בתעשייה.



מנטורים שמגיעים מהתעשייה
כל המרצים שלנו הם אנשי מקצוע עם ניסיון מעשי – ככה אתם לומדים ממי שכבר שם.



שילוב בין תאוריה לפרקטיקה
כל שיעור בנוי כך שתבינו את התיאוריה ותתרגלו אותה מיד – כדי שתצאו עם ידע מעשי ויישומי.



תמיכה וליווי אישי
אנחנו מלווים אתכם לאורך כל הקורס וגם אחריו – עד שתמצאו את העבודה הראשונה בתחום.

מה לומדים בתוכנית ההכשרה?

יסודות התכנות ויישומי אינטרנט

- פיתוח ושימוש בשפת Python
- סקריפטינג מתקדם ב-Bash ו-PowerShell
- יסודות פיתוח יישומי WEB ואבטחת WEB

מבוא לרשתות מחשבים

- יסודות המחשב ומערכת ההפעלה LINUX
- מבוא לרשתות והכנה לתעודת CCNA
- הבנה בסיסית באבטחת סייבר

אבטחת סייבר התקפי

- בדיקות חדירה פנימיות וחיזוניות
- עבודה עם הרשאות ב-Windows ו-Linux
- עקיפת אנטי-וירוס וניהול Active Directory
- בדיקות חדירה לאפליקציות אינטרנטיות

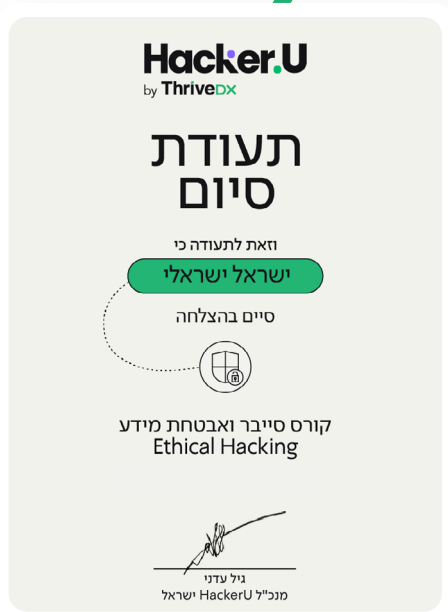
סייבר הגנתי

- היכרות עם מערכות SIEM ושירותי SOC
- עבודה עם מערכות אבטחת סייבר מתקדמות
- חקירות דיגיטליות, ניתוח זיכרון ואנליזה של מלואר
- שימוש בטכניקות אנליזה סטטית ודינמית

בקורס נשלב ידע תיאורטי עם עבודה מעשית כדי שתהיו מוכנים להתמודד עם אתגרי הסייבר של היום!

תעודת גמר

תעודת בוגר קורס סייבר ואבטחת מידע של HackerU מקבוצת ThriveDX העולמית



תכנית הלימודים המלאה

Network and Computer Fundamentals

Welcome

- Introduction
- Tools for Success
- Syllabus
- Jobs Title and salary

Introduction to Cybersecurity

- Introduction
- Laws and Regulations
- Standards and Frameworks
- Threats and Threat Actors
- The CIA Trade
- Top 10 Cyber Security Attacks

Windows Fundamentals

- Windows Operating System Overview
- User Accounts and Permissions
- File System Security (NTFS)
- Windows Services and Processes
- Windows Registry and its Security
- Windows Updates and Patch Management

VM

- Virtual Machine types
- Installation and Troubleshooting

Linux Fundamentals

- Linux Operating System Overview
- User and Group Management
- Linux File Permissions
- Linux Shell and Terminal Usage
- Linux Common Services
- Package Management

Active Directory and DC

- Introduction to Windows Server
- Installing Windows Server and Windows 10
- Creating a Domain Environment
- DNS (Domain Name System)
- DHCP (Dynamic Host Configuration Protocol)
- User and Group Management
- Organizational Units (OUs)
- Group Policy Objects (GPOs)

- Data Encapsulation
- Common Application Layer Protocols
- IP Addressing and Subnetting
- Private IP Address & NAT
- IPv6 Addressing and Types
- Introduction to Wireshark

Switching and Routing

- Installing Packet Tracer
- CISCO Switch Configuration
- Switch Security
- VLANs and Trunking
- Spanning Tree Protocol (STP)
- Routing Fundamentals
- Dynamic Routing
- ACLs for Security
- SNMP
- Network Troubleshooting

Advanced Network Technologies

- WAN Technologies
- VPNs (Virtual Private Networks)
- Wireless Technologies
- Wi-Fi Fundamentals
- WAP Fundamentals
- Wi-Fi Security

Preparation to CCNA Certification

- Introduction to CCNA
- Cisco Certification Paths
- Practice Exams and Mock Tests
- Final Exam Preparation

Network Fundamentals

- Basics of Networking Concepts
- OSI Model
- TCP/IP Model

Scripting and Web Application Fundamentals

- Functions
- Text Processing with AWK and Sed
- Error Handling and Debugging
- Advanced Scripting Techniques
- Script Automation

Bash Scripting

- Introduction to Bash Scripting
- Variables and Data Types
- Control Structures

Web Application Fundamentals

- Introduction to Web Applications
- Client-Server Architecture
- HTML (Hypertext Markup Language)
- CSS (Cascading Style Sheets)
- JavaScript and the DOM (Document Object Model)
- Introduction to Front-End Frameworks (e.g., React, Angular, Vue)
- Backend Development
- Databases and Data Storage
- Web Application Architecture
- Web Requests and Responses
- PHP for Web Development
- Databases Management
- MySQL

Web Application Security

- OWASP Top 10 – Part 1
- OWASP Top 10 – Part 2
- Input Validation and Output Encoding
- Authentication and Authorization
- Web Application Firewalls (WAFs)

PowerShell Scripting

- Introduction to PowerShell Scripting
- Basic PowerShell Commands
- Variables and Data Types
- Input and Output
- Control Structures
- Functions
- Error Handling and Debugging
- Working with Files and Directories

Welcome

- Introduction
- Syllabus

Python Programming and Scripting

- Introduction to Python
- Scripting vs Programming
- Variables, Data Types, and Operators
- User Input and Conditions
- Loops
- Functions
- Data Structures
- File Handling
- Error Handling
- Modules and Libraries
- Web Communication
- Sockets
- Protocol Communication
- Debugging and Testing
- Practical Applications

Defensive Cybersecurity

Welcome

- Introduction
- Syllabus

Introduction to SIEM & SOC Service

- Security Operations Center (SOC)
- Roles and Responsibilities
- Cyber Kill Chain
- Attack Types
- MITRE Attack

Cyber Security Systems

- Security Architecture Design
- Endpoint Protection Strategies
- Network Security Devices
- Web Security
- Email Security
- Wireless Network Security

Dynamic Analysis Systems

- Behavioral Analysis
- Packet Analysis
- Analyzing Malware Behavior
- Analyzing Malware Network Behavior

SIEM Fundamentals

- Security Architecture Design
- SIEM Components and Architecture
- Building QRadar SIEM Environment
- Troubleshooting Lab Environment
- Log Collection and Aggregation
- Event Correlation and Normalization
- Creating SIEM Rules and Use Cases
- Log Analysis Fundamentals
- Log Analysis Techniques
- Alerts and Notifications

Malware Fundamentals

- Malware Types
- Hashing
- Cryptography and Encryption
- Indicators of Compromise (IOC)
- Threat Intelligence
- Threat Hunting אפקטים
- שיטות שילוב
- Clip content תרגיל

Memory Analysis

- Introduction to Memory Forensics
- Memory Analysis Techniques
- Identifying Malicious Processes
- Analyzing Network Connections
- System Investigation
- Code Investigation

Static Analysis

- Static Malware Analysis
- Understanding PE File Format
- Identifying Packed and Obfuscated Malware
- Hashing and Checksums

Incident Response

- Introduction to Incident Response
- Windows Malware Detection
- Website Defacement

Digital Investigations

- Introduction to Digital Forensics
- Digital Evidence Collection – Windows
- Digital Evidence Collection – Linux
- Forensic in Incident Response
- File Systems and Data Recovery

Offensive Cybersecurity

Linux Privilege Escalation

- Files and Users Privileges
- Information Gathering
- History Search and Transcripts
- Service Footprinting
- Automated Enumeration
- Scheduled Tasks
- Setuid Binaries and Capabilities
- Sudo Enumeration
- Passwd File Enumeration
- Automated Tasks & Permissions
- Misconfigurations

Windows Privilege Escalation

- Information Gathering
- Search for Interesting Files
- History Search and Transcripts
- Automated Enumeration
- Service Binary Hijacking
- Scheduled Tasks
- Public Exploits
- Sticky Keys
- Common Tools

Antivirus Evasion

- Known vs Unknown Threat
- AV Engines and Components
- Detection Methods
- Bypassing Antivirus Detection
- Testing for AV Evasion
- Evading AV with Thread Injection
- Automating the Process
- Obfuscation Methodology

AD Enumeration

- Manual Information Gathering
- Enumerating using PowerShell and .NET Classes
- PowerView
- SPN (Service Principal Names) Enumeration
- Enumerating Object Permissions

Lateral Movement in AD

- WMI and WinRM
- PsExec
- Pass the Hash
- Overpass the Hash
- Pass the Ticket
- Active Directory Persistence

Welcome

- Introduction to Penetration Testing
- Syllabus Digital Evidence Collection – Linux

External Tests

- Information gathering techniques
- OSINT Tools
- Social Engineering
- Client-Side Attacks
- Red Team Operation
- Simulated Attack

Internal Tests

- Network Scanning
- File Transfer and Compiling
- ARP and DNS Spoofing
- Encryption, Hashes and Cracking
- Password Attacks
- Mimikatz
- Pass The Hash
- NTLM Relay
- Password Manager Enumeration
- SSH Enumeration [22/TCP]
- SMTP Enumeration [25/TCP]
- SNMP Enumeration [161/UDP]
- SMB Enumeration [445/TCP]
- R Services [512, 513, 514]
- Postgres SQL Enumeration [5432/TCP]

- Introduction to Burpsuite and ZAP
- Directory / Subdomain Brute Force
- LFI & RFI
- OS Command Injection
- Directory Traversal
- Security Headers and SSL/TLS Vulnerabilities
- XSS
- SQL Injection
- CSRF & SSRF
- XXE & Broken Authentication
- SSTI
- WordPress Hacking
- API Enumeration
- General Tools

Domain Enumeration

- Enumerating Domain Shares
- Introduction to Automated Enumeration
- SharpHound
- BloodHound
- Active Directory Authentication (NTLM vs Kerberos)
- Password Attacks
- AS-REP Roasting
- Kerberoasting
- Silver Tickets

Web Application Penetration Test

- Methodology
- Fingerprinting Web Servers

יסודות מחשב ורשת

- איומים ושחקני איום
- מודל CIA (סודיות, שלמות וזמינות)
- עשרת ההתקפות הבולטות בסייבר

פתיחה

- הקדמה
- כלים להצלחה
- סילבוס
- תארי עבודה ושכר

מבוא לסייבר ואבטחת מידע

- הקדמה
- חוקים ותקנות
- תקנים ונהלים

- (DNS (Domain Name System
- DHCP (Dynamic Host Configuration Protocol
- ניהול משתמשים וקבוצות
- יחידות ארגוניות (OUs)
- אובייקטי מדיניות קבוצתית (GPO)

יסודות רשת

- חקיקות בסיסיים של מושגי רשת
- מודל OSI
- מודל TCP/IP
- עיטוף נתונים
- פרוטוקולים נפוצים בשכבת היישום
- כתובות IP ותתי-רשתות
- כתובות IP פרטיות - NAT
- כתובות IPv6 וסוגים
- Wireshark - מבוא

מתגים וניתוב רשת

- התקנת Packet Tracer
- קונפיגורציית מתגי CISCO
- אבטחת מתגים
- Trunking - VLANs
- פרוטוקול עץ מתפצל (STP)
- עקרונות ניתוב
- ניתוב דינמי
- אבטחת ACL לרשתות
- SNMP
- פתרון בעיות רשת

יסודות מערכת הפעלה Windows

- סקירה של מערכת הפעלה Windows
- ניהול חשבונות משתמשים והרשאות
- אבטחת קבצים במערכת NTFS
- שירותים ותהליכים ב-Windows
- רישום המערכת (Registry)
- עדכוני Windows וניהול טלאים

מכונות וירטואליות

- סוגי מכונות וירטואליות
- התקנה ופתרון בעיות

יסודות מערכת הפעלה Linux

- סקירה של מערכת הפעלה Linux
- ניהול משתמשים וקבוצות
- הרשאות קבצים ב-Linux
- שימוש ב-Shell וב-Terminal של Linux
- שירותים נפוצים ב-Linux
- ניהול חבילות תוכנה

Active Directory Domain וסביבות

- מבוא ל-Windows Server
- התקנת Windows Server 10-1
- יצירת דומיין

הכנה להסמכת CCNA

- מבוא ל-CCNA
- מסלולי הסמכה של Cisco
- לימודי תרגול ומבחנים מעשיים
- הכנה למבחן הסופי

טכנולוגיות רשת מתקדמות

- טכנולוגיות WAN
- VPNs (רשתות פרטיות וירטואליות)
- טכנולוגיות אלחוטיות
- יסודות Wi-Fi
- יסודות WAP
- אבטחת Wi-Fi

כתיבת סקריפטים ויסודות אתרי אינטרנט

כתיבת סקריפטים ב-Bash

- מבוא לכתיבת סקריפטים ב-Bash
- משתנים וסוגי נתונים
- מבני שליטה
- פונקציות
- ניפוי שגיאות
- טכניקות מתקדמות

פתיחה

- מבוא

כתיבת סקריפטים ב-PowerShell

- מבוא לכתיבת סקריפטים ב-PowerShell
- פקודות בסיסיות של PowerShell
- עבודה עם משתנים
- מבני שליטה
- פונקציות
- ניפוי שגיאות
- עבודה עם קבצים ותיקיות
- עבודה עם שירותי רשת
- אוטומציה של סקריפטים

תכנות וכתיבת סקריפטים בפייתון

- מבוא ל-Python
- סקריפטים מול תכנות
- משתנים, סוגי נתונים ו-Operators
- קלט משתמש ותנאים
- לולאות
- פונקציות
- מבני נתונים
- טיפול בקבצים
- טיפול בשגיאות
- מודולים וספריות
- תקשורת ברשת
- Web Sockets
- תקשורת פרוטוקולים
- ניפוי שגיאות וניתוח נתונים
- יישומים מעשיים

יסודות אתרי אינטרנט

- מבוא ליישומי אינטרנט
- ארכיטקטורת Client-Server
- HTML Hypertext Markup Language
- Cascading Style Sheets - CSS

עבודה עם טקסט

- עבודה עם AWK ו-Sed
- טיפול במגבלות ותחביר בעייתי
- טכניקות כתיבת סקריפטים מתקדמות
- אוטומציה של סקריפטים

פיתוח אתרים מתקדם

- מסגרות Front-End (כגון, React, Angular, Vue)
- פיתוח Backend
- XAMPP + PHP

- ארכיטקטורות יישומי אינטרנט
- בקשות ותגובות אינטרנט
- PHP לפיתוח אתרים
- ניהול מסדי נתונים
- MySQL

כלי היד

- כלי היד
- כלי הזום
- מילוי וקו מתאר
- עיצוב הזמנה לאירוע יצירת מברשות

אבטחת אתרי אינטרנט

- OWASP Top 10 - חלק 1
- OWASP Top 10 - חלק 2
- אבטחת קליינט והגנת צד לקוח
- אימות והזדהות
- חומות אש ליישומי אינטרנט (WAFs)

סייבר הגנתי

יסודות שירות SIEM&SOC

- שירות SIEM&SOC
- תפקידים ואחריות
- Cyber Kill Chain
- MITRE Attack

פתיחה

- מבוא

ניתוח זיכרון מחשב

- מבוא לפרקטיקות זיכרון
- ניתוח תהליכים
- ניתוח חיבורי רשת
- Dumping
- חקירת מערכת

ניתוח סטטי

- ניתוח נזקות סטטי
- קבצי הרצה בווינדוס (EXE)
- Virus Total

ניתוח דינמי

- ניתוח סטטי לעומת ניתוח דינמי
- FlareVM & REMnux
- ניתוח התנהגויות מערכת
- ניתוח התנהגויות רשת

תגובה מיידית - Incident Response

- מבוא לתגובה לאירועים
- זיהוי נקודות - Windows
- השחתת אתרים

מערכות הגנת סייבר

- תכנון ארכיטקטורת אבטחה
- אסטרטגיות הגנה על נקודות קצה
- אבטחת רשת
- אבטחת אתרים
- אבטחת דוא"ל

יסודות מערכת SIEM

- (ניהול אירועים אבטחה ומידע)
- רכיבי SIEM וארכיטקטורה
- בניית סביבה של QRadar SIEM
- אינטגרציות עם WinCollect
- בניית בעיות תרגול מעבדת SIEM
- התקנה והגדרה של PFSense
- קולקטור לאיסוף אירועים
- יצירת דשבורד SIEM
- קישוריות לממשקי ניטור נתונים

יסודות קבצי נזקה

- יסוגי נזקות
- גיבוב
- קריפטוגרפיה והצפנה
- סימני זיהוי של פריצות (IOC)
- מודיעין איומים

סייבר התקפי

- מיפוי פעילויות באמצעות כלים אוטומטיים
- חיפוש קבצים בינאריים של שירותים
- משימות מתוזמנות
- פעילויות ציבוריות
- Sticky Keys

הסלמת הרשאות גישה בסביבת Linux

- הרשאות קבצים ומשתמשים
- איסוף מידע
- חיפוש היסטוריה
- מיפוי שירותים
- ניצול פעילויות אוטומטי
- ניצול פקודת Setuid
- ניצול פעילויות ב-Sudo

מיפוי קובץ סיסמאות

- פעילויות ציבוריות
- אוטומציה של משימות
- הרשאות עגונות

פתיחה

- פתיחה
- הקדמה ל-Offensive Security

בדיקות חוסן חיצוניות

- הקדמה לבדוק חוסן חיצוני
- טכניקות איסוף מידע
- איסוף מידע פסיבי
- איסוף מידע אקטיבי
- OSINT
- הנדסה חברתית

בדיקות חוסן פנימיות

- סריקת רשת
- העברת קבצים
- DNS Spoofing - ARP
- הצפנה, גיבוב ופיצוח
- ניצול חולשות סיסמאות
- Mimikatz
- Pass The Hash
- NTLM Relay

הסלמת הרשאות גישה בסביבת Windows

- איסוף מידע
- חיפוש קבצים מעניינים
- חיפוש היסטוריה

הסלמת הרשאות גישה בסביבת Windows

- מתודולוגיה
- ניתוח שרתי אינטרנט
- הקדמה ל-Burpsuite ו-ZAP
- מציאת תיקיות ותתי דומיין באתרי אינטרנט
- LFI & RFI
- הדבקת פקודות OS
- מעבר בבניית ספריות
- כותרות אבטחה ופגיעויות SSL/TLS
- XSS
- הדבקת SQL
- CSRF & SSRF
- XXE & Broken Authentication
- SSTI
- פריצה ל-WordPress
- ניצול פגיעויות ב-API
- כלים כלליים

בדיקת חוסן בסביבת AD

- איסוף מידע ידני
- מיפוי באמצעות PowerShell
- NET Classes
- PowerView
- מיפוי שמות Principal של שירות (SPN)
- מיפוי הרשאות אובייקט
- מיפוי שרישת אירועים
- ניצול חולשות בכבלים אוטומטיים
- מציאת פעילויות
- SharpHound
- BloodHound
- אימות משתמשים ב-NTLM (Active Directory כ Kerberos)
- AS-REP Roasting
- Kerberoasting
- Silver Tickets

אמנת ה'חממה'

ההצלחה שלכם היא ההצלחה שלנו. אנחנו בטוחים שבעבודה משותפת נוכל להביא אתכם לעבודה הראשונה שלכם בהייטק. אנחנו כאן כדי ללוות, לתמוך ולהעניק לכל אחד ואחת מכם את הידע, הכלים והקישורים הנדרשים כדי להצליח בתחום שבחרתם. אצלנו תקבלו הזדמנות שווה ואמיתית, אם יש לכם את הרצון והמוטיבציה, לנו יש את הכלים לשלב אתכם בתעשייה.

ההתחייבות שלנו: להפוך חלום למציאות ולקחת אתכם יד ביד עד לעבודה הראשונה שלכם בהייטק.

ההתחייבות שלכם: להגיע עם נכונות לתת 100% מעצמכם ולהיות מחויבים לתהליך. את השאר תשאירו לנו.

האינטרנט שלנו ברור: ההצלחה שלכם היא ההצלחה שלנו.



רשימה חלקית של החברות שבוחרות בנו ובבוגרים שלנו

CYREBRO



MOONACTIVE

papaya global



Aman



abra



HiBob

zap group

one Taldor

CLEAR GATE
CYBER SECURITY & RESEARCH

teva

DataScope



salesforce

PassportCard

amd docs

LEOS
MEDIA & INTERACTIVE group

Playtika

רמת ישראל

CodeOasis

solar edge

YOUNG
DIGITAL AGENCY FOR THE NEW GENERATIONהתעשייה
האווירית IAI