ECOM SCHOOL
המכללה למקצועות הדיגיטל וההייטק

קורס אבטחת מידע וסייבר בהתמחות מבדקי חדירה (PT)

הקורס כולל בתוכו הסמכת פייתון
והסמכת לינוקס והכנה למבחנים החיצוניים

מבנה הקורס

קורס אבטחת מידע וסייבר

בדיקת חדירה (הידועה בשם Testing Penetration או בקצרה PT) הינה תהליך מורכב המתבצע על ידי ההאקר על מנת לבדוק האם היישומים והשירותים של החברה פגיעים לליקויי אבטחה.
בדיקת חדירה הינה תהליך חשוב ביותר עבור ארגונים בארץ ובעולם ומתבצעת על ידי האקר מיומן אשר משתמש באותן השיטות בהן ישתמש ההאקר הזדוני, כדי לגלות האם הוא יכול לפגוע באפליקציות, אתרים או בתשתיות של החברה ולנצל ליקויי אבטחה על מנת לגרום לנזק. לאחר סיום הבדיקה ההאקר יספק דוח לחברה אשר יציג את כלל ליקויי האבטחה שאיתר וכמו כן פתרונות כיצד לתקן את ליקויי האבטחה האלו.
החברה יכולה לבקש מגוון רחב של בדיקות חוסן ולכן על ההאקר להיות בקיא במגוון רחב של תחומים, כגון: בדיקות חוסן ליישומי האינטרנט (האתרים והמערכות) של החברה, בדיקות חוסן לאפליקציות שמפתחת החברה הן לאנדרואיד והן לאיפון, בדיקות חוסן לתשתיות של החברה ברמה הרשתית ועוד.
עקב הידע הרב הנדרש לביצוע בדיקות חוסן והחוסר בתוכניות הכשרה מסודרות קיים מחסור רב בבודקי חוסן הן בארץ והן בעולם וכאן נכנס לתמונה קורס סייבר בדיקות חוסן ופיתוח מאובטח.
קורס בדיקות חוסן ופיתוח מאובטח הינו הקורס המקיף ביותר בתחום מבדקי החוסן המתבסס על מחקרים שביצעו מרצי הקורס תוך כדי עבודתם כבודקי חוסן / חוקרי סייבר בכירים בחברות בארץ.
במהלך הקורס המרצה יציג את הממצאים אשר מצא לאורך הקריירה שלו, ימקד את התלמיד ויפתח אצלו חשיבה יצירתית לצורך מבדקי חוסן. כך התלמיד יזכה לראות כיצד מתבצע מבדק חוסן על ידי מומחה בתחום.
במהלך הקורס התלמיד עובר התמקצעות בתחום ה- LINUX וה- PYTHON.

קהל יעד:
אנשים המגיעים ללא רקע לעולם הסייבר, המעוניינים בהסבת מקצוע עם זיקה לשינוי ופיתוח עצמי והתקדמות נרחבת בתחום.
מפתחים אשר רוצים לבצע הסבה מקצועית לתחום בדיקות החוסן עם התמקצעות בתחום הלינוקס והפייתון או להעשיר את הידע שלהם בתחום.
בודקי חוסן מתחילים שרוצים להשתפר בתחום בדיקות החוסן ולעלות מדרגה לשלב הבא.
תלמידי מדעי המחשב/ הנדסת תוכנה מאוניברסיטאות/ מכללות שרוצים לשפר את הסיכויים שלהם לעבוד בתחום מבדקי חוסן עם התמקצעות בתחום הלינוקס והפייתון.
תלמידים שעברו קורסי סייבר בעבר ועדיין מרגישים שאינם מסוגלים לעבור ראיון עבודה בתחום בדיקות חוסן עם התמקצעות בתחום ה- LINUX וה- PYTHON.
כל מי שרוצה ללמוד לבצע בדיקת חוסן מקצועית מא' ועד ת' עם התמקצעות בתחום הלינוקס והפייתון ובעל ניסיון מעשי בתחום טכנולוגי כגון ניהול רשת, DevOps ו - QA.

משך הקורס:
משך הקורס הינו 300 שעות אקדמיות המתקיימות במסגרת 60 מפגשים, פעמיים בשבוע בין השעות 17:30 ועד 21:30.

חומר עזר:
מערך דיגיטלי שמטרתו לעזור ולקדם את התלמיד, לצפייה חוזרת, במידת הצורך, ללא הגבלת זמן.
בקורס תתרגלו את כלל הנושאים על מערכת אתגרים מבוססת מחקרים אמיתיים שבוצעו על ידי המרצים של הקורס!
לרשות התלמידים מערך סרטונים דיגיטלים ללימוד אנגלית ברמה בסיסית ומתקדמת.

המכללה ליזמות, מקצועות הדיגיטל והייטק

איקום היא מיזם חברתי - קהילתי, שנוסדה במטרה לייצר שינוי תודעה בכל הקשור לשיטות לימוד, בדרכים קריאטיביות יוצאות דופן, אשר חלקן אפילו מעוגנות כפטנט עולמי!
הכיתות האורבניות, הרשת החברתית והקשר ההדוק בין המכללה לתלמידים גם לאחר סיום הקורס.
לימודי מקצועות העתיד יתנו לכם את האפשרות להשתלב בתעשיית ההייטק והדיגיטל כשכירים או עצמאיים בליווי צמוד לאורך כל הדרך.

ברשותינו רשיון השמה מטעם משרד העבודה והרווחה, כמו כן אפשרות לייעוץ עסקי, בהקמת מערך אופרטיבי ראשון באינטרנט.

מכללת איקום היא היחידה בישראל אשר נמצאת במאגר תוכניות הלימוד של משרד החינוך.

אנחנו זמינים עבורכם 24/7, ONLINE & OFFLINE, לקבלת מידע מקצועי ומהימן ממיטב אנשי המקצוע בתחום הדיגיטל וההייטק המתקדם, עם כל החידושים והעדכונים בזמן אמת ומענה חי וזמין.

אתם מוזמנים לבקר אותנו באחת מהכיתות שלנו ברחבי הארץ.
תל אביב --- נהריה --- באר שבע --- אשקלון

הרשת החברתית האקדמאית הראשונה והיחידה מסוגה בישראל
עולם שלם של קהילה שלא הכרתם!

מעל 300 שיעורים דיגיטלים מעודכנים ומתעדכנים, פרופיל אישי, צ'אט עם מדריכים, הכרות עם סטודנטים באיקום, פורומים ממוקדים, פורטל ענק ועוד.

בקורס תתרגלו את כלל הנושאים על מערכת אתגרים מבוססת מחקרים אמיתיים שבוצעו על ידי המרצים של הקורס!

תנאי סף:
הקורס הותאם לתלמידים אשר התנסו בחומר וגם תלמידים אשר מגיעים ללא רקע קודם. כל הנושאים נלמדים החל מהבסיס ועד לרמה המקצועית ביותר.
הקורס דורש אנגלית ברמה בסיסית.

בסיום הקורס:
עם סיום הקורס התלמיד ידע לבצע בדיקות חוסן בצורה הטובה והיסודית ביותר, הכוללת כתיבת דו"ח בדיקות חוסן.
תלמידים שהגישו את כל מטלות הקורס ועברו את הקורס בהצלחה עם ממוצע ציונים של 85 ומעלה, יקבלו תעודת סיום ועזרה בהשמה בתחום הסייבר ובדיקות החוסן. בנוסף הקורס מכין את התלמיד למבחני ההסמכה החיצוניים: LINUX, PYTHON.
*במידה והתלמיד רוצה לגשת למבחני הסמכה חיצוניים ניתן לגשת באופן עצמאי.

מבוא

1.
- ציפיות לקורס
- עולם המחשבים כיוסעולמות תוכן ותפקידים
- מגמות צפויות לעתיד יסודות עולם המחשוב
- מבוא לחומרה
- מבוא לתוכנה

2.
- עקרונות ווירטואליזציה
- שימוש בווירטואליזציה בתעשייה
- בניית מכונות וירטואליות
- התקנת מערכת הפעלה וינדוס 10
- שימוש בווירטואליזציה באבטחת מידע
- מבוא לסייבר

LINUX

30 שיעורים מוקלטים
7 מפגשים
מעבדות תרגול
200 דקות צפייה
35 שעות אקדמיות

1. הכרות עם מערכת ההפעלה

- היסטוריית מערכות הפעלה
- מהו קוד פתוח
- סוגי מערכות לינוקס
- הכרת מערכת הפעלה KALI LINUX
- ייבוא של OVA
- עבודה בסיסית בסביבת לינוקס
- היכרות עם הטרמינל
- היכרות עם APT

2. מערכת הקבצים של LINUX

- פקודות שימושיות
- מניפולציית קלט ופלט
- חיפוש באמצעות LOCATE
- יצירת קבצי טקסט
- חשיבות קבצים ותיקיות
- עריכת קבצי טקסט
- הסתרה ומחיקה של קבצי טקסט
- צפייה בתוכן קבצי טקסט

3. משתמשים והרשאות

משתמשים והרשאות
יצירת משתמשים
סוגי משתמשים
ניהול משתמשים והרשאות
פקודת LS -l
מבנה קובץ PASSWD SHADOW

4. שירותים ותהליכי מערכת

- צפייה וניהול תהליכים
- שירותי מערכת בסיסיים
- הפקודה SERVICE
- הפעלה וכיבוי שירותי מערכת
- שירותים בסיסיים בשרתים
- איך תקשורת באה לידי ביטוי במערכת הפעלה לינוקס

5. פיתוח בסיסי בשפת BASH

- סוגי כתבנים בלינוקס
- מבוא לשפות תכנות
- ההבדל בין שפת תכנות לBASH
- הצורך בBASH
- הגדרה למונח SYNTAX
- מבוא ועקרונות של שפת BASH
- משתנים קלט ופלט

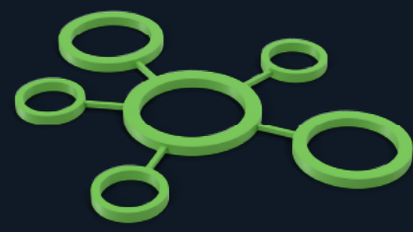
6. שכלול הפיתוח

- תנאים ולולאות
- סקריפטים בתחום התקשורת
- מבוא לאוטומציה

7. מבוא לאבטחת מידע של LINUX

- בדיקת תקשורת למכונות וירטואליות באמצעות PING
- פריצת מערכות לינוקס בצורה לוקאלית
- הגדרת מונח PE
- הבנת תהליך ה-BOOT של מערכת הפעלת LINUX
- תהליך פריצה באמצעות BRUTEFORCE
- הגנה וזיהוי באמצעות צפייה בלוגים
- מחיקת לוגים ע"י תוקף

הידעת ?
"90% מהשרתים בעולם
הינם שרתי לינוקס"



תקשורת מחשבים

30 שיעורים מוקלטים
200 דקות צפייה
4 מפגשים
20 שעות אקדמיות
מעבדות תרגול

1. היסטוריה ומודלים

- אמצעי תקשורת לאורך השנים
- תקשורת מחשבים בעידן המודרני
- הצורך בתקשורת
- הגדרות בסיסיות
- סיבנוט וניהול רשת
- מודל שבע השכבות
- מודל TCP/IP
- שירותי תקשורת, פרוטוקולים ו-פורטים

2. תהליכים ופרוטוקולים

- תהליכי ENCAPSULATIN VS. DECAPSULATION
- תהליך ROUTING
- פרוטוקולי תעבורת TCP/UDP
- פרוטוקלים אפליקטייביים רלוונטיים

3-4. ניתוח והיכרות עם קבצים

- WIRESHARK
- ניתוח תעבורה בלינוקס עם TCPDUMP
- היכרות עם קבצי PCAP
- מבוא לניתוח מתקפות סייבר
- CHALLENGE
- אופציונלי

הידעת ?

"מספר מקומות העבודה בסייבר עומד לזנק פי 10 בעשור הקרוב."

עיתון גלובס

PYTHON

30 שיעורים מוקלטים
8 מפגשים
מעבדות תרגול
200 דקות צפייה
40 שעות אקדמיות

1. מבוא לשפת PYTHON

הגדרת והתקנת PYTHON + PYCHARM
- קלט ופלט עם השפה
- היכרות עם משתנים
- השמת משתנים וחוקיות
- אופרטורים
- עבודה עם STRING
- עבודה עם INT

2. תנאים למבני נתונים

- עבודה עם משתנים מורכבים
- היכרות עם תנאים
- טבלאות אמת

3. לולאות והסבת משתנים

- עבודה עם לולאות
- היכרות עם CASTING
- היכרות עם ניהול שגיאות

4. אפשרויות מתקדמות בשפת הPYTHON

- עבודה עם:
- קבצים
- פונקציות
- מודולים ו-IMPORT
- ספריות OS

5. תקשורת נתונים עם PYTHON

- מבוא לSOCKET וניהולו
- לקוח-שרת
- עבודה עם חבילות מידע
- בניית שרת-לקוח
- בניית סורק פורטים
- בניית SHELLCODE

6-7. פרוטוקולים ותקיפות

- עבודה עם HTTP
- היכרות עם HTTP כפרוטוקול
- ספריית REQUESTS
- בניית SCRAPPER
- בניית קוד שמתחבר אוטומטית לשרת אינטרנט ותקיפתו
- שיעור תרגול

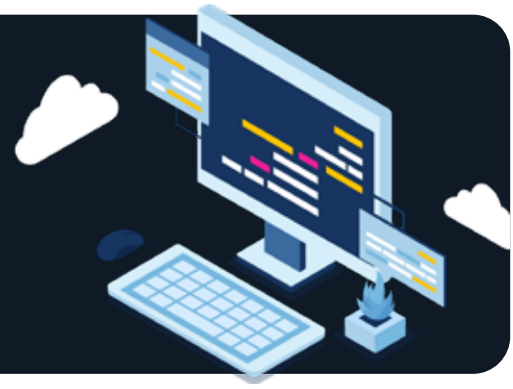
8. אבטחת מידע באמצעות PYTHON

- שליחת סמס באמצעות PYTHON
- SELENIUM ואוטומציה באמצעות PYTHON
- פיתוח FULLSTACK בסיסי באמצעות PYTHON

הידעת ?

"פייתון היא שפת התיכנות
המבוקשת ביותר בשנים האחרונות"

סייבר הגנתי



10 שיעורים מוקלטים
3 מפגשים
מעבדות תרגול

100 דקות צפייה
15 שעות אקדמיות

1. מבוא לעולם הסייבר

- מבוא לעולם הסייבר
- ההבדל בין סייבר לאבטחת מידע
- מתקפות הסייבר הראשונות
- היכרות עם מונחים בעולם האבטחת מידע ההתקי (MALWARE, RANSOMEWARE וכו)
- מבוא לסייבר הגנתי
- היכרות עם מוצרי אבטחת מידע
- היכרות עם FIREWALL
- תרגול של התקנת ראוטר מאובטח והגדרת מוצרי אבטחת מידע עליו

2. אופרציות

- היכרות עם IDS+IPS
- היכרות עם SNORT
- היכרות עם FIREWALL
- היכרות עם AV
- אופרציית NOC
- אופרציית SIEM-SOC
- היכרות עם IDS+IPS
- היכרות עם SNORT
- היכרות עם FIREWALL
- היכרות עם AV
- אופרציית NOC
- אופרציית SIEM-SOC

3. SIEM & LOGS

- התקנת מערכת SIEM
- היכרות עם לוגים
- היכרות עם העברת לוגים ממקום למקום (FORWARDER)

האקינג ובדיקות חוסן תשתיתי

50 שיעורים מוקלטים
450 דקות צפייה
10 מפגשים
50 שעות אקדמיות
מעבדות תרגול

1. איסוף מידע אפליקטיבי&פאסיבי

- חיפוש מידע על ידי google hacking
- איסוף ואיתור כתובות מיילים
- איסוף מידע פאסיבי על ידי open source
- DNS ENUMERATION
- תקשורת מול שרתי DNS
- מחקר אוטומטי מול שרתי DNS
- FORWARD LOOKUP BRUTE FORCE DNS
- REVERSE LOOKUP BRUTE FORCE DNS

2. סריקות פורטים

- לחיצת יד משולשת ותקשורת TCP
- סריקות בפרוטוקול UDP
- טעויות נפוצות בסריקות פורטים
- סריקות פורטים על ידי NMAP
- סריקות מתקדמות NMAP NSE
- סריקות עקיפת Firewalls ומוצרי הגנה
- זיהוי מערכות הפעלה
- מחקר service enumeration שירותים וחקר פגיעויות

3. METASPLOIT ואקספלויטים

- הכרות עם Metasploit
- המודלים השונים בתוך Metasploit
- Payloads
- Auxiliaries
- Exploits
- תקיפת FTP עם חולשת RCE
- הזרקת Shellcode
- מעבר בין תהליכים לאחר הזרקת הקוד.
- שיטות למעקף חומות אש (firewalls)
- שליטה Meterpreter
- Process Backdoor
- Advance Meterpeter
- Keylogging
- פונקציות download/upload
- SMTP Enumeration
- העלאות קבצים
- העברת קבצים באמצעות פייתון
- העברת קבצים בWindows על ידי Powershell
- העברת קבצים בין Windows ל Linux על ידי FTP
- העברת קבצים על ידי שרת באמצעות SMB
- שיטות נוספות למעבר קבצים

4. AV & SHELL

- עקיפת AV
- איך AV עובד
- מהי אובפוסקציה
- מהו VIRUS TOTAL
- יצירת SHELL שעוקף אנטי וירוס
- לקיחת קוד SHELL בפייתון ולהמיר אותו לEXE

5. Pishing

- Pishing
- מהי הנדסה חברתית
- באילו תחומים ניתן לבצע הנדסה חברתית
- הקמת אתר PHISHING
- הוספת אמינות לאתר פישינג
- קניית דומיין
- בנייה עצמית
- חתימה עם CERTIFICATE

6. האצלת סמכויות ב-WINDOWS

- UAC Bypass-user interaction
- UAC Bypass WITOUT USER INTERACTION
- PE SUGGESTER
- PATCH ENUMERATION
- UNQUOTED PATH
- INSECURE SERVICE

7-8. האצלת סמכויות ב-Linux

- BASICS ENUMERATIONS
- KERNEL EXPLOITS
- SUID EXPLOITATION
- SUDO ABUSE
- WORD WRITEABLE
- CORNTAB PE
- SENSITIVE FILES
- HTTP METHODS

9. סיסמאות

- מנגנון הזדהות RESPONSE CHALLENGE
- גיבוב LM/NTLM
- SAM AND PASSWORD FLOW
- שליפת סיסמאות Minikatz
- שליפת סיסמאות WCE
- Minikatz using powershell
- Hash extraction samdump
- Hash extraction secretdump
- SecretDump remoting
- Password cracking hashcat / john
- Pass the hash
- Responder introduction to LLMNR
- Responder capture NTLMv2

10. מערכות ארגוניות & פרוטוקול KERBEROS

- היכרות עם מערכות ארגוניות ועם פרוטוקול KERBEROS כולל התקפות מוכרות

האקינג ובדיקות חוסן לאתרים

70 שיעורים מוקלטים
10 מפגשים
מעבדות תרגול
550 דקות צפייה
50 שעות אקדמיות

1. בניית סביבת מעבדות

- מבוא ל HTML5.
- הכרת השפה ומבנה התגים.
- טפסים ותגים חיוניים למבדקי חוסן.
- עיצוב בסיסי.
- עיצוב לפי,Id,Tag,Class.
- עיצוב מתקדם ויכולות למבדקי חוסן.

2. Javascript

- מבוא ל-Javascript.
- עבודה עם משתנים וסוגי משתנים.
- תנאים.
- לולאות.
- פונקציות.

3. PHP

- ניהול משתמש באמצעות COOKIE
- בתוספת היכרות עם התקפה מעניינת של INSECURE DESERIALIZATION
- מבוא ל-7PHP.
- עבודה עם משתנים וסוגי משתנים.
- תנאים.
- לולאות.
- פונקציות.
- סרליזציה.
- עבודה עם פרוטוקול HTTP הכולל COOKIES/POST/GET.
- ניהול משתמש באמצעות COOKIE
- בתוספת היכרות עם התקפה של INSECURE DESERIALIZATION

4. MYSQL

- מבוא ל-MYSQL.
- יצירת מסד נתונים.
- יצירת טבלאות.
- יצירת עמודות והגדרת הנתונים.
- ביצוע פעולות על הנתונים.

5. ניתוח קוד ואיתור ליקויי

- שיטת החשיבה לאיתור ליקויי אבטחה.
- חקירת מקרה : FACEBOOK MESSENGER.
- הקמת סביבת מחקר ליישומי אינטרנט.
- DEVELOPER CHROME TOOLS רמה בסיסית.
- DEVELOPER CHROME TOOLS רמה מתקד־מת.
- עבודה בסיסית עם BURPSUITE.
- עבודה מתקדמת עם BURPSUITE.

6-9. סוגי הגנות והתקפות

- OWASP TOP 10
- וניתוח מתקפות שונות
- XSS
- היכרות עם מנגנוני הגנה כמו: SOP, CORS, CSP
- SSRF
- CSRF
- LFI/RFI שמובילים לRCE
- BROKEN ACCESS CONTORL
- JWT
- SENSITIVE DATA EXPOSURE
- BROKEN AUTHENTICATION
- COMMAND INJECTION
- XXE
- SQLINJECTION

10. דוח PT

- כתיבת דוח PT + דמו שהמרצה מראה איך תוקפים אתר

הידעת ?

"מספר מקומות העבודה בסייבר עומד לזנק פי 10 בעשור הקרוב."

עיתון גלובס

האקינג לאפליקציות אנדרואיד

40 שיעורים מוקלטים
6 מפגשים
מעבדות תרגול

300 דקות צפייה
30 שעות אקדמיות

1. מבוא להאקינג אפליקציות וניתוח אפליקציות NATIVE

- מבוא לפיתוח אפליקציות אנדרואיד.
- היכרות עם מערכת ההפעלה אנדרואיד.
- היכרות עם סוגי אפליקציות:
- WEB APP
- HYBRID APP
- NATIVE APP
- הגדרת סביבת מחקר ופיתוח Android Studio.
- Genymotion.
- מבנה של אפליקציה Web App.
- ניתוח אפליקציית Native.
- מבנה של אפליקציית Native.
- Android Building Blocks.
- Manifest File.
- Activity.
- Views.
- Fragments.
- Intent.
- Content Provider.
- Service.
- Broadcast Receiver.

2-3. ליקויי אבטחה בפיתוח

- Android App Sandbox.
- תהליכים בעולם האנדרואיד.
- קבצים ונתיבים File Structure.
- Working with adb.
- Importer platform usage.
- Exposed Application Interfaces.
- LogCat.
- Working with Drozer.

4-5. ליקויי אבטחה בתקשורת נתונים ואחסון

- Insecure Data Storage.
- Attacking Shared Preferences.
- Attacking SQLite Database.
- Attacking data on sdcard.
- Insecure communication.
- Sniffing Android Traffic with Wireshark.
- Using Burp Suite.
- HTTPS and Burp Suite.
- Bypass SSL Pinning.

6. ניתוח ושינוי קוד אפליקציה סטטי ודינאמי

- Client Code Quality.
- Google Maps Case Study.
- Pro Guard.
- Code Tempering.
- Frida and Dynamic Instrumentation.
- שינויי קוד המקור באפליקציה Repackaging.

נושאי הקורס

שעות אקדמיות (ש"א) בחלוקה לתשעה מודולים
מודל 1 - מבוא 10 ש"א
מודול 2 - לינוקס 35 ש"א
מודול 3 - תקשורת מחשבים 20 ש"א
מודול 4 - פייטון 40 ש"א
מודול 5 - סייבר הגנתי 15 ש"א
מודול 6 - האקינג ובדיקות חוסן תשתיתי 50 ש"א
מודול 7 - האקינג ובדיקות חוסן לאתרים 50
מודול 8 - האקינג לאפליקציות אנדרואיד 30
מודול 9 - התמקצעות מעשית עם המרצה 50 ש"א
סה"כ שעות 300

*3952

info@ecomschool.co.il

ecom school

ecom school

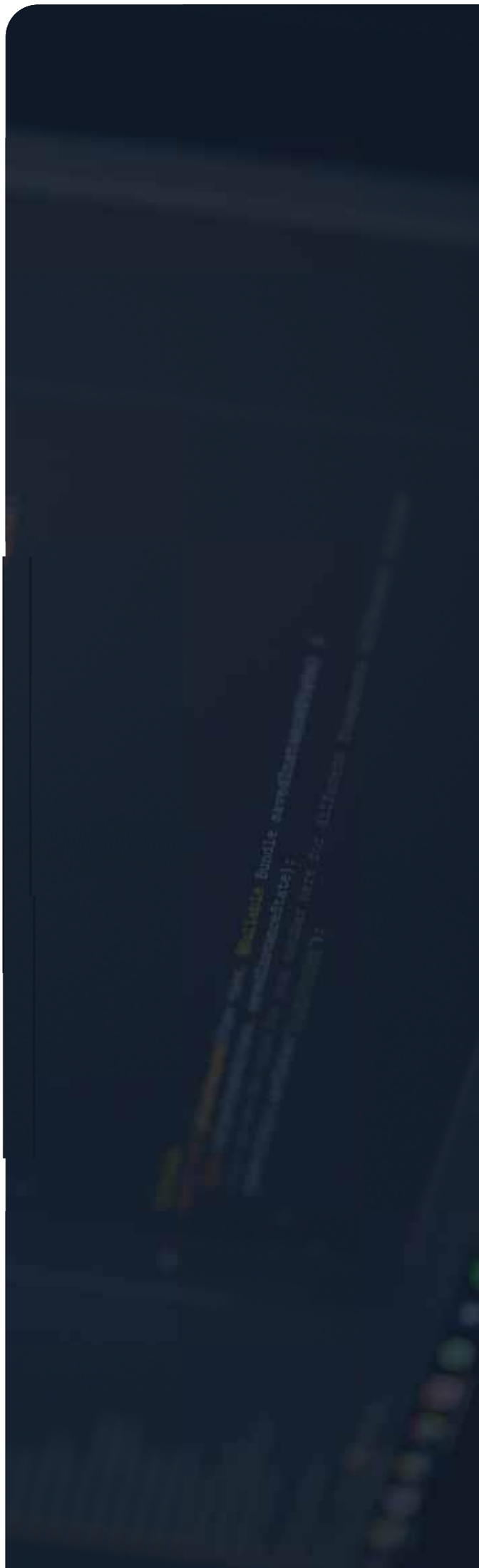
053-556-5617

SCAN ME

נהריה
הגעתון 31

רמת החייל
ראול ולנברג 24

TLV
אברבנאל 74

אשקלון
בת גלים 1

באר שבע
רמב"ם 4