



# CSRP

Cyber Security Responder & Practitioner



## אודות

סייבר סקול, מכללה בינלאומית למקצועות הסייבר, פועלת במגוון רחב של מסלולים החל מחינוך ילדים ונוער, חינוך אקדמי במוסדות המובילים, קורסי הסבה מקצועית לבוגרים עד להסמכות המתקדמות ביותר וכן, קורסי הכשרות מקצועיות לחברות וארגונים בארץ ובעולם תוך שימור על קשר הדוק עם עולם הסייבר המתפתח בשוק האזרחי והביטחוני.

ייחודה של המכללה נעוץ במקצועיות והניסיון של צוות הפיתוח הפדגוגי המורכב מאנשי הסייבר המובילים בתחום אשר חיים ונושמים את התעשייה בזמן אמת ובניסיון רב השנים של העומד בראשה, מר עומרי סגרון, ממובילי ענף הסייבר בישראל ומייסד קבוצת \*HIGHDELE.

לסגרון, ניסיון רב הן בתעשייה והן בתחום ההדרכה בארץ ובעולם והינו אחד משלושת המדריכים היחידים בארץ המוסמכים להעביר את הקורס הרשמי להסמכת CISSP - ההסמכה היוקרתית ביותר בתחום הסייבר!

\*קבוצת HIGHDELE הינה קבוצת הייטק המתמחה בתחום הסייבר ופועלת בכל רחבי העולם.  
סייבר סקול מהווה את זרוע ההדרכה של הקבוצה ומשולבת בכל אחת ממגוון פעילויותיה.

# התוכנית



קורס CSRP הינו קורס ייחודי המיועד למעוניינים בהתמחות באחד ממקצועות הליבה בתחום הסייבר- מיישם סייבר. מטרת הקורס הינה שילוב תעסוקתי של הסטודנטים בתפקיד רלוונטי בתעשייה ועל כן, תכני הקורס פותחו בקפידה תוך התחשבות וסינרגיה מלאה לדרישות המעסיקים בשוק.

## ייחוד התוכנית

התוכנית מועברת ע"י חוקרי הסייבר מהמובילים בענף בארץ ובעולם, על מנת להכין את התלמידים לשוק העבודה בתחום בצורה המיטבית ביותר. התוכנית הייחודית של Cyber School משלבת איזון בין עולם הסייבר לעולם הרשתות, אשר מהווים אבני יסוד לכל התמחות בתחום הסייבר בעתיד. התכנית כוללת הכנה להסמכות עבור סביבת לינוקס ושפת פייתון אשר מהותיים לעולם הסייבר ומתאימה גם למתעניינים במקצוע ניהול רשתות המחפשים להתבלט בדגש למעוניינים להתפתח בענף הסייבר!

## קהל יעד

קורס מיישם הגנת סייבר מיועד לבעלי זיקה טכנולוגית המעוניינים להתמקצע ולרכוש את ההסמכות המובילות בתחום הסייבר, הקורס מועבר במתכונת Zero To Hero ומיועד גם לקהל אשר מעוניין לבצע "דריסת רגל" ראשונה בענף וגם לאנשי IT המעוניינים להתמקצע. התוכנית הייחודית שלנו מאפשרת גישה לכל אחד להיכנס לעולם ההייטק ולעסוק בתחום המבוקש בעולם הסייבר.

## מה בתוכנית

מבוא לעולם הסייבר ואבטחת מידע, תקשורת נתונים, אבטחת מערכות הפעלה, אבטחת רשתות תקשורת, טכנולוגיות אבטחת מידע וסייבר, מבוא לתכנות, פיתוח מאובטח ופייתון, האקינג, תגובה לארועי סייבר.

## שעות לימוד

360 שעות | פעמיים בשבוע





**"The first step** in securing our cyber future is education, and that means everything from educating individuals to companies to the next generation of IT professionals."

**Dan Lipinski**

# אפשרויות תעסוקה

תוכנית זו לוקחת סטודנטים מכלל הרמות ומכינה אותם לעולם הסייבר החל משלבי הבסיס ועד להגשה להסמכות המובילות בתחום בדגש על הכנת הבוגרים לשוק העבודה בתחום הסייבר.

מיישם סייבר

מגן סייבר

אנליסט סייבר

תמיכה טכנית עם התמחות בסייבר

מנהל רשתות עם התמחות בסייבר

חוקר סייבר

ארכיטקט סייבר

בודק חדירות

SOC

מנהל אבטחת מידע

\* חלק מהמשרות דורשות נסיון מעשי

# יסודות הסייבר

**80**  
שעות

אבטחת מערכות הפעלה

16 מפגשים

מערכות הפעלה מוכרות לנו כמשתמשים במחשבים אישיים, במודול זה נתעמק באבטחת המידע במערכות הפעלה, תוך הבנת המבנה והמרכיבים החשובים בשתי מערכות הפעלה המובילות בעולם:

Linux | Windows

- Windows Client
- Windows Server
- DNS
- Active Directory
- Group Policy
- DHCP - חלוקת כתובות רשת
- PowerShell
- Windows Security
- Security Policy
- הכרות עם Linux
- CLI
- הרשאות ב LINUX
- תקשורת נתונים ב LINUX
- הקשחות LINUX והגנה
- Bash Scripting

פרויקט גמר - בניית תשתיות

**35**  
שעות

מבוא לסייבר ואבטחת מידע

7 מפגשים

מודול זה כולל היכרות עם תחום הסייבר, נעבור על מושגי בסיס, נסקור רשתות תקשורת, מערכות הפעלה ונכיר כלי הגנה והתקפה בהם נתעמק בהמשך מהלך הקורס, מודול זה מהווה מעין תקציר הקורס ובסיס להבנת הנלמד בהמשך.

- היכרות עם עולם הסייבר
- יסודות התקשורת
- מערכת הפעלה WINDOWS
- מערכת הפעלה LINUX
- סייבר התקפי
- התקפות רשתיות
- סייבר הגנתי

**45**  
שעות

תקשורת נתונים

9 מפגשים

במודול זה נלמד מהי רשת וכיצד עובר המידע בה, נלמד את הכלים הדרושים לניהול וניטור רשת.

- מבוא לתקשורת נתונים
- פרוטוקולי תקשורת
- מתג והיכרות עם Cisco IOS
- VLAN
- ניתוב וכתובות IP
- Subnetting
- ניתוב דינמי
- ACL
- Troubleshooting



# תשתיות סייבר

**35**  
שעות

מבוא לתכנות  
7 מפגשים

במודול זה נלמד את הבסיס של תכנות בכללי ופייתון בפרט, ונלמד את כל הכלים הנדרשים לכתיבת קוד בסיסי לטובת כלי סייבר.

- מבוא לתכנות
- Data Types
- Loops
- מערכת קבצים
- פונקציות
- תכנות תקשורת

**35**  
שעות

אבטחת רשתות תקשורת  
7 מפגשים

במודול זה נלמד את הכלים הדרושים לצורך ניהול וניטור רשת ונתמקד בסיכונים ובשיטות ההגנה לצורך אבטחת המידע בצורה המיטבית ביותר.

- ארכיטקטורה מאובטחת
- הצפנה
- ניתוח תעבורת רשת
- Firewall
- VPN
- IPS/IDS
- מלכודות דבש (HONYPOTS)

**25**  
שעות

טכנולוגיות אבטחת מידע וסייבר  
5 מפגשים

במודול זה נסקור את האמצעים בהם יש לנקוט לצורך הגנה על רשתות ורכיבים המחוברים לרשתות (IoT), המודול כולל סקירת יחידת קצה, הגנה ותיעוד הפעילות שלהם.

- Endpoint Security
- DLP
- הגנה על מיילים
- הכרות עם SIEM
- SOAR

פרויקט גמר - הגנה

# סייבר מתקדם

45

שעות

תגובה לאירועי סייבר

9 מפגשים

מודול זה יעסוק בתיעוד ארועים והכנת תגובה עבורם, המודול כולל ניתוח נזקות ותוכנות זדוניות, חקר עמדות קצה ורשתות, מודל זה הינו מהווה את שלב סיום הקורס ואורז בתוכו הבנה עמוקה בתחום הסייבר.

- Incident Response
- Data Acquisition
- Windows Forensics
- Memory Analysis
- Linux Forensics
- Network Forensics
- Malware Analysis

פרויקט גמר התקפה והגנה

25

שעות

פיתוח מאובטח ופייתון

5 מפגשים

במודול זה נלמד את עקרונות הפיתוח המאובטח, פייתון מתקדם ונבנה כלי סריקה ותקיפת סייבר.

- עקרונות הפיתוח המאובטח
- ספריות בפייתון
- עבודה עם נתונים
- תכנות מונחה עצמים
- בניית כלי סייבר

35

שעות

האקינג

7 מפגשים

האקינג או במילים אחרות – התקפה, לאחר שהתמקדנו בכלי הגנה, במודול זה, נעסוק בפיתוח יכולות תקיפה תוך היכרות כלים נפוצים, סקירת מקרי תקיפה מוכרים, ביצוע סקר סיכונים וטיפול באיומים באופן אקטיבי.

- הכרות לסייבר התקפי
- סריקת פגיעויות
- Brute Force
- התקפות תשתיות
- Privilege Escalation
- התקפה אפליקטיבית
- SQL Injection



# תהליך הקבלה ללימודים

הדרך לקריירה בהיי טק

## צור קשר

קבע פגישת ייעוץ בחינם עם אחד מיועצי חינוך הסייבר שלנו על מנת להעריך את התאמתכם לתחום וללמוד על האפשרויות העומדות בפניכם.



## מבחן מיון

התלמידים יעברו מבחן הערכה בכדי לבחון את התאמתם לתוכנית.



## ראיון קבלה

במידה ותעברו את מבחני המיון, תוזמנו לראיון קבלה במתכונת "אחד על אחד" על מנת לדון בהמשך התוכנית, ציפיות בקריירה וכן הזדמנויות לתפקידים עתידיים.



## תכנית הלימודים

לימוד התוכנית המופעלת ע"י Cyber School אשר חרטה על דגלה 2 אבני דרך עיקריות-הן בפיתוח והן בנושא חינוך סייבר, מחקר, ושיטות עבודה מומלצות. התוכנית מספקת למידה מעשית, תוך אימון חווייתי לצד אבטחת סייבר והעברת ידע.



## עזרה בהשמה

שירותי ההשמה שלנו יספקו לתלמידים שעברו בהצלחה הדרכות לראיונות עבודה בהתאמה אישית, סיוע בהשמה והתמחות ברשת וסיוע בקבלה לעבודה בעמדת אבטחת הסייבר הראשונה שלהם.



# הסמכות

בענף הסייבר, למילה תואר אין משמעות רבה. במקום, מעסיקים מחפשים אנשים עם מיומנות וניסיון. חברות כגון מיקרוסופט, סיסקו, צ'ק פוינט ורבות אחרות מציעות אתגרי סייבר כתנאי כניסה לעבודה. על מנת לצלוח באתגרים אלו עליכם לשלוט בהסמכות המפורטות מטה. קורס CSRP מכיל הכנה לארבעת הסמכות אלו.



## Network+

הסמכה זו עוסקת בניהול רשתות, בהגדרה ואינטגרציה של רכיבי תקשורת חדשים ובתכנון של טופולוגיות רשת חדשות ותמיכה ופתרון תקלות ברשתות קיימות. כמו כן, הסמכה זו אומרת למעסיקים שהמועמד בעל ידע בטכנולוגיות רשת כולל מודל OSI ו-TCP/IP.



## LPI Linux Essentials

מערכת ההפעלה לינוקס על כל גרסתיה הרבות הוטמעה כמעט בכל תעשייה עולם. ידיעה ושליטה במערכת הפעלה הזו היא קריטית לכל מי ששואף להיכנס לענף הסייבר או לכל מקצוע טכנולוגי-מחשבי אחר. ההסמכה הזו היא הראשונה והבסיסית ביותר מבין הסמכות הלינוקס ואין לה תוקף.



## SSCP

הסמכה זו מאשרת שיש למועמד יכולות טכניות מתקדמות ואת הידע כדי ליישם, לנטר ולנהל תשתיות IT תחת הנהלים, הנחיות והתהליכים אשר הונחו ע"י מומחי אבטחת סייבר מטעם ה-ISC<sup>2</sup>.



## Security+

מטרת הסמכה זו היא להראות שהמועמד בעל ידע במושגי אבטחה, כלים ותהליכים אשר יתרמו רבות במקרה של אירוע אבטחה. כמו כן איש סייבר עם ההסמכה הזו גם יודע לחזות ולזהות פרצות אבטחה ולמגן מפניהן.

\* הקורס אינו כולל את עלות בחינות ההסמכה  
\* יתכנו שינויים בתארי ההסמכות בהתאם לגופים שמקיימים אותם

# תוכנית לימודים

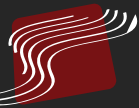
שעות	שם הקורס	נושא
35	Introduction to Cyber Security	מבוא לסייבר ואבטחת מידע
45	Computer Networking	תקשורת נתונים
80	Operating System Security	אבטחת מערכות הפעלה
35	Network Security	אבטחת רשתות תקשורת
25	Cyber Technologies	טכנולוגיות אבטחת מידע וסייבר
35	Introduction to Coding	מבוא לתכנות
25	Secure Code and Python	פיתוח מאובטח ופייתון
35	Ethical Hacking	האקינג
45	Incident Response	תגובה לאירוע סייבר
360	סה"כ	





CYBER SCHOOL

האקדמית גליל מערבי  
היחידה ללימודי חוץ ולימודי המשך



[cyber-school.co.il](http://cyber-school.co.il)



[cyber-info@wgalil.ac.il](mailto:cyber-info@wgalil.ac.il)



04-901-5103