matrix

THINKCYBER

JOHN BRYCE
תלמדו הייטק. זה עובד!
a matrix company

Cyber Security Red & Blue Team

מגן סייבר



המסלול היחיד שמשלב סימולטור
תקיפות עולמי, מעל 1,500 אתגרי CTF
ומבחני מעבדה מעשיים בזמן אמת.

ג'ון בריס
כולל גישה בלעדית
לפלטפורמת הסימולציה
והמעבדות החיות

770 שעות לימוד | מוכר לפיקדון | מק"ט קורס: 7736

אודות הקורס

תוכנית הלימודים מכשירה אנשי מקצוע להבין, לתקוף, להגן ולתחקר אירועי סייבר במערכות וברשתות ארגוניות מקצה לקצה.

המתודולוגיה מבוססת על גישת Holistic Defense & Threat Emulation: לומדים לעומק את ארכיטקטורת הרשת, פרוטוקולי התקשורת ווקטורי התקיפה מנקודת מבטו של התוקף ומיישמים שכבות בלימה, הקשחה וחקירה מבוססות ראיות על גבי תשתיות מקומיות ובענן.

במקום תרגילים מבודדים או למידה פסיבית, ההכשרה מתנהלת כולה כמעבדה מתמשכת ומובנית סביב סימולציות חיות ורב שכבתיות:

- מיפוי תשתיות ותקשורת רשת: פירוק וחקר חבילות תעבורה (Diving into Packets, Wireshark), שירותי רשת ופקודות מערכת בסביבות Windows ו-Linux.
- חקירה דיגיטלית ופורנזיקה: איסוף ממצאים דיגיטליים (Artifacts), ניתוח זיכרון נדיף (RAM), שחזור מידע שנפגע וחקר תעבורה חשודה במנגנוני IDS/IPS ו-DarkNet.
- Penetration Testing: איסוף מודיעין גלוי ואקטיבי (OSINT), סריקת חולשות, שימוש בכלי תקיפה מתקדמים (Metasploit), ביצוע Exploitation ושלבי Post-Exploitation בסביבות דומיין ארגוניות.
- SOC & Threat Hunting: ניהול מערכות SIEM (Splunk, ELK) וחומות אש ארגוניות (pfSense), ניתוח לוגים, מיפוי אירועים לפי מודל MITRE ATT&CK וביצוע תחקיר אירוע מבצעי.
- אוטומציה ופיתוח בסייבר: פיתוח כלי אוטומציה וסקריפטים ב-Python לטובת חקירה, סריקה ותפעול שוטף של מנגנוני אבטחה.



*הכלים הנלמדים עשויים להשתנות במהלך הקורס בהתאם להתפתחויות והמגמות העדכניות ביותר בשוק ה-AI

למה ג'ון ברייס?

- **וותק ומובילות בתעשייה:** עם למעלה מ-30 שנות ניסיון, ג'ון ברייס מהווה גורם מרכזי בהכשרת אנשי מקצוע לתעשיית ההייטק בישראל, תוך התאמה מתמדת לצרכים המשתנים של השוק ולטכנולוגיות החדשניות ביותר.
- **קשר ישיר לתעשייה:** כחלק ממטריקס, חברת שירותי הטכנולוגיה הגדולה בישראל, ג'ון ברייס מחוברת באופן ישיר לצרכים העדכניים של שוק ההייטק. חיבור זה מאפשר התאמה מתמדת של תכני הלימוד לדרישות השוק והכשרת בוגרים עם מיומנויות רלוונטיות.
- **סגל מרצים מנוסה:** המרצים בג'ון ברייס הם אנשי מקצוע מובילים בתעשייה, המשלבים ידע תיאורטי עם ניסיון מעשי, ומספקים לסטודנטים הכשרה מקיפה ומעמיקה.
- **הזדמנויות השמה:** כחלק ממטריקס, לג'ון ברייס יש גישה לרשת קשרים רחבה בתעשייה, המסייעת בהשמת בוגרים במשרות מבוקשות בהייטק. "ג'ון ברייס טאלנט" היא תוכנית הכשרה ייחודית להשמת בוגרים מצטיינים בחברות המובילות במשק.
- **שיתופי פעולה עם חברות בינלאומיות**: ג'ון ברייס היא מרכז הדרכה רשמי של חברות מובילות כמו Microsoft, AWS Cisco ועוד, מה שמאפשר לסטודנטים גישה לתכנים והסמכות בינלאומיות.

קהל יעד

- חסרי רקע המעוניינים להשתלב בצוותי SOC ולהתמקצע בעולמות ההגנה כגון, פורנזיקה וחקירת אירועי סייבר

תנאי קבלה

- ראיון אישי/ ייעוץ להכוונה מקצועית
- יכולת בסיסית בעבודה מול מחשב
- היכרות עם השפה האנגלית ברמה בסיסית

תוכנית הקורס

- **370** שעות לימוד אקדמיות בכיתה
- **200~** שעות תרגול מעשי בסימולטור Cyberium ובמעבדות הבית
- **200~** שעות למידה עצמית באמצעות קורסים מקוונים של John Bryce Online Academy
- **כולל מפגשי אינטגרציה ותרגול מעשי** | שעות המוקדשות לחיבור כל הטכנולוגיות ובלימת תקיפות אמת

- חומרי לימוד הכוללים ספרי לימוד דיגיטליים מלאים לכל מודול (The Library), מצגות ותרגולים
- משימות הערכה (אתגרי CTF, מבחני מעבדה מתוזמנים, פרויקטים ומשימות בית)
- תעודת סיום רשמית ופרופיל ביצועים מאומת והכנה להסמכות ThinkCyber ו-City & Guilds

הלמידה בקורס תתקיים ב**מודל היברידי משולב**, המאפשר לכם גמישות ונוחות לצד חוויה פרונטלית משמעותית. בכל שבוע נפגש בכיתה כדי לתרגל, להתנסות ולהיות בקשר ישיר עם המרצה והכיתה ופעם נוספת נלמד מרחוק, בשיעור מקוון, שמעניק לכם את הנוחות של למידה מכל מקום.

כך תיהנו **מהשילוב האידיאלי**: גם חוויית לימודים בכיתה וגם גמישות שמתאימה לחיים שלכם.

🌙 **לימודי ערב** | פעמיים בשבוע בין השעות 17:00-21:30
או בימי ג' בשעות הערב (17:00-21:30)
ובימי ו' בשעות הבוקר (09:00-13:30)

🎉 אין לימודים בחגים ובמועדים

מה מייחד את מסלול ההכשרה בג'ון ברייס?

- מעבדות וסימולטור אמת (Cyberium Arena): מעל 80%–90% מהמסלול מועברים כ-Hands-on מול רשתות ארגוניות מלאות כבר מהיום הראשון.
- לומדים לתקוף כדי לדעת להגן | Red & Blue Team: התנסות מלאה בבדיקות חדירה (PT) ותקיפת דומיינים לצד חקירות פורנזיות עמוקות ותפעול מרכז בקרה (SOC Analyst Tier 1 & 2).
- חקר מתקפות חיות בזמן אמת | Specto: חיבור ישיר למלכודות דבש עולמיות לניתוח פריצות אמיתיות ופתרון תיקי חקירה מבצעיים (The Case Files).
- זירת אתגרים ו-CTF אינסופית: מעל 1,500 משימות Capture The Flag לאימון עצמי, עבודה בצוותים ותחרויות מול אקדמיות בעולם.
- לוחמת סייבר בעידן ה-AI: הכשרה בהתמודדות עם מתקפות מבוססות בינה מלאכותית (כולל Prompt Injection) והפעלת סוכני הגנה מתקדמים.
- פרופיל הישגים | Verified CV: תיעוד דיגיטלי מבוסס ראיות של שעות המעבדה, הציונים והתרחישים שנפתרו – להצגה בראיונות עבודה.

תוכנית הלימודים

01 | Intro to Cyber

(44 ש"א)

המודול הפותח מלמד להסתכל על ארגון בעיניים של תוקף: איתור מכשירים חשופים לאינטרנט, ממשקי ניהול פתוחים ומידע שדלף לרשת, והבנה כיצד מידע גלוי לחלוטין הופך לנקודת הכניסה הראשונה. במקביל נבנית התשתית הטכנית - תקשורת, כתובות, מערכת ההפעלה וקידוד מידע.

- Hash & Encoding: ייצוג נתונים, קידוד ופונקציות Hash.
- Networking & OSI Model: מודל השכבות, פרוטוקולים וכתובות IP.
- OSINT & Google Dorking: איסוף מודיעין גלוי על יעד, איתור מכשירים חשופים (Shodan) ומסמכים רגישים שדלפו.
- Windows & CMD Commands: ארכיטקטורת המערכת, תהליכים ושירותים, ושימוש בשורת הפקודה לתחקור התחנה.
- Intro to Linux & Text Manipulation: שליטה בטרמינל וחילוץ ממצאים.
- Scanning & Network Mapping: סריקת רשתות עם Nmap ו-Masscan, איתור שירותים חשופים וגרסאות תוכנה פגיעות.

02 | Network Research

(49.5 ש"א)

כאן מתחילה התקיפה בפועל. הסטודנטים סורקים רשתות, מאתרים את השירותים החשופים בהן ומיירטים תעבורה כדי לחלץ ממנה סיסמאות שנשלחו בטקסט גלוי. משם למתקפות אקטיביות ושבירת סיסמאות - ועד Man-in-the-Middle ויצירת סוס טרויאני ראשון. כל מתקפה נלמדת גם מצד הזיהוי והחסימה.

- Diving into Packets: יירוט תעבורה ב-Wireshark, חשיפת סיסמאות בטקסט גלוי וזיהוי חתימות תקיפה.
- Network Attacks, Password Cracking & Trojans: מתקפות ARP MITM, Brute-Force, שבירת Hash עם John the Ripper ויצירת Payload ראשון.

03 | Windows Forensics

(71.5 ש"א)

כאן חוקרים מחשב שכבר נפרץ. הסטודנטים מקבלים עמדה שהותקפה ומשחזרים את מהלך התוקף צעד אחר צעד: מה הריץ, לאילו קבצים ניגש, מה ניסה למחוק וכיצד דאג לעצמו לדרך חזרה למערכת. העבודה כוללת שחזור קבצים שנמחקו, ניתוח זיכרון חי וניתוח הנוזקה בסביבה מבודדת.

- Forensics Workstation & Data Acquisition: הקמת עמדת חקירה ודגימת מדיה.
- Carving Metadata & Steganography: שחזור קבצים שנמחקו וחשיפת מידע שהוטמן בתוך תמונות וקבצי מדיה.
- Registry, Artifacts & Windows Events: איתור מנגנוני השרידות (Persistence) שהשאיר התוקף ושחזור הפקודות שהריץ.
- Memory & Malware Analysis: ניתוח זיכרון חי (RAM) לאיתור תהליכים עוינים והזרקות קוד, וניתוח נוזקה ב-Sandbox.

תוכנית הלימודים

04 | Penetration Testing

(71.5 ש"א)

המודול ההתקפי במלואו (Red Team). הסטודנטים מבצעים בדיקת חדירות מקצה לקצה לפי סדר העבודה המקובל בתעשייה: איסוף מודיעין, סריקה ואיתור החולשה, ניצולה והשגת גישה, ומשם ביסוס אחיזה, חילוץ סיסמאות והתקדמות ליעדים נוספים - הכל על מערכות אמת במעבדה מבודדת.

- Information Gathering: איסוף מודיעין על היעד, מאגרי סיסמאות שדלפו ומיפוי טווחי הכתובות של הארגון.
- Scanning & Identifying Vulnerabilities: סריקת רשתות ומערכות, זיהוי פגיעויות וגרסאות תוכנה פגיעות.
- Exploitation, Metasploit & Payloads: התאמת Exploit ליעד, יצירת Payloads והשגת שליטה מרחוק (Meterpreter).
- Post Exploitation, Social Engineering & WebApp: ביסוס אחיזה, חילוץ סיסמאות, הנדסה חברתית וניצול חולשות באפליקציות וווב.

05 | Network Security

(44 ש"א)

מכאן התקיפה עוברת מהמחשב הבודד אל הארגון כולו. הסטודנטים מקימים סביבת Active Directory, ממפים אותה מבפנים, מנצלים חולשה כדי להיכנס ומתקדמים בין שרתים (Lateral Movement) עד להשתלטות על הדומיין - ואז חוזרים לאותה סביבה מהצד המגן.

- Network Attacks & Traffic Capture: מתקפות על תעבורת הרשת הארגונית, וזיהוין מתוך התעבורה הנלכדת.
- Domain Setup & Domain Enumeration: הקמת Active Directory ומיפוי משתמשים, קבוצות, הרשאות ועוד.
- Domain Exploitation & Post Exploitation: ניצול חולשות דומיין, חילוץ Hash, מתקפות Pass-the-Hash ו-Lateral Movement עד להרשאות הגבוהות ביותר.
- PowerShell, Domain Security & Cryptography: שימוש ב-PowerShell לתקיפה ולחקירה, זיהוי Pass-the-Hash ביומנים והקשחת הדומיין.

06 | Python Programming

(נלמד בערכה מקוונת ללמידה עצמית)

שפת העבודה של חוקרי הסייבר. כאן הסטודנטים מפסיקים להפעיל כלים מוכנים ומתחילים לכתוב אותם בעצמם: סקריפט שמפרק לוג ענק ומאתר בו את השורה החשודה, מחולל סיסמאות לבדיקות חוסן וכלי לאיסוף מידע על המערכת.

- Python & Jupyter Basics: משתנים, מבני נתונים, פונקציות ותחביר מרכזי - הבסיס לכתיבת כלי עבודה.
- Conditionals & Loops: בניית לוגיקת החלטה ועיבוד חוזר.
- Text, Files & Log Processing: איתור הדפוס החריג בתוך כמות מידע שאי אפשר לקרוא ידנית.
- אוטומציה בסייבר: מחולל סיסמאות לבדיקות חוסן ומיכון תהליכי תחקור.

תוכנית הלימודים

07 | AI and Cyber Security

(22 ש"א)

בינה מלאכותית היא היום גם כלי עבודה וגם משטח תקיפה חדש. במודול הזה הסטודנטים בונים סוכן AI משלהם - ואז תוקפים אותו בעצמם: מזריקים לו הוראות זדוניות (Prompt Injection), עוקפים את מנגנוני ההגנה שלו ומרעילים את מאגר הידע שעליו הוא נשען.

- Intro to AI & LLM Internals: כיצד מודל שפה עובד מבפנים, הידע שנדרש כדי לתקוף אותו ולהגן עליו.
- Prompt Injection, Jailbreaks & Data Poisoning: מתקפות Prompt Injection, עקיפת מנגנוני הגנה וזיהום מאגרי ידע (Data Poisoning).
- AI for Defense & Ethics: שימוש ב-AI לאיתור אנומליות ולתגובה לאירועים.
- זיהוי ניסיונות התחזות והנדסה חברתית (Social Engineering), לצד הבנת היבטי אתיקה וגבולות השימוש המותר.

08 | SOC Analyst

(55 ש"א)

המודול שמכין ישירות לתפקיד הראשון בתעשייה, ובנוי כולו סביב רדיפה אחרי תוקפים. הסטודנטים יושבים מול SIEM אמיתי (Splunk ו-ELK), מקבלים התראה, מתחקרים אותה עד למקור ומסווגים את מהלך התוקף לפי MITRE ATT&CK - ומשם לציד יזום אחר תוקף שלא הדליק אף נורה.

- Events & Log Analysis: פענוח יומני מערכת ולוגים של שרתי ווב ושל SSH, איתור ניסיונות חריגים וסינון התראות שווא.
- Firewalls, IDS & IPS: זיהוי סריקות ומתקפות מתוך לוגים של חומת אש וכתיבת חוקי זיהוי ב-Snort.
- SIEM & MITRE ATT&CK: תפעול Splunk ו-ELK, בניית חוקי זיהוי וסיווג טכניקות התקיפה לפי המסגרת הבינלאומית.
- Threat Hunting & Incident Response: מרדף יזום אחר תוקף מוסווה בעזרת Sysmon וחוקי YARA, בלימת האירוע והפקת דוח.

09 | Network Forensics

(נלמד בערכה מקוונת ללמידה עצמית)

תקיפה וחקירה בשכבת התקשורת עצמה. הסטודנטים פורצים רשתות WiFi מוצפנות במעבדה, מייצרים חבילות מידע משלהם כדי לבחון כיצד מערכות ההגנה מגיבות, חושפים תוכן של תעבורה מוצפנת שנלכדה ועוקבים אחר פעילות ב-DarkNet.
מולם - חוקי זיהוי ב-Snort שנכתבים כדי לעצור בדיוק את אלה.

- TShark & Scapy - Packet Crafting: לכידה וסינון בקנה מידה גדול וייצור חבילות מידע מותאמות לבחינת תגובת מערכות ההגנה.
- IDS & IPS in Depth - Snort & Suricata: כתיבת חוקי זיהוי למתקפות רשת וחקירת ההתראות שהם מייצרים.
- WiFi Exploitation: פריצת רשתות אלחוטיות מוצפנות במעבדה, הבנת חולשות ההצפנה ודרכי ההקשחה מולן.
- HTTPS, DarkNet & Network Hardening: חשיפת תוכן מתעבורה מוצפנת שנלכדה, מעקב אחר פעילות ב-DarkNet והקשחת ציוד תקשורת.

תוכנית הלימודים

10 | CCNA

(נלמד בערכה מקוונת ללמידה עצמית)

מודול העשרה רחב היקף המיועד להעמקת הידע התשתיולוגי בעולמות הרשתות הארגוניות ומכין ישירות לבחינת ההסמכה הבינלאומית CCNA של חברת Cisco. נלמד את עקרונות התכנון, הניתוב, המיתוג והאבטחה של רשתות ארגוניות גדולות ומבוזרות.

- Introduction to Networks – ITN: מודלי תקשורת, ארכיטקטורת רשת, פרוטוקולי Ethernet וכתובות IPv4/IPv6.
- Switching, Routing & Wireless Essentials (SRWE): הגדרת מתגים ונתבים, ניהול VLANs, מנגנוני ניתוב סטטיים ודינמיים, ואבטחת רשתות תקשורת מקומיות (LAN).
- Enterprise Networking, Security & Automation (ENSA): חיבורי WAN, מנגנוני QoS, אבטחת רשתות מבוזרות ומבוא לאוטומציה ברשתות.
- Intro to Check Point VPNs: עקרונות הקמה, הצפנה וניהול של רשתות תקשורת פרטיות מאובטחות (VPN).

סדנת קורות חיים מיתוג אישי והכנה לתעשייה

סדנה יישומית המעניקה את ארגז הכלים המדויק למעבר מוצלח של תהליכי מיון וגיוס. נלמד כיצד לבנות פרופיל מקצועי בולט, לתרגם את תיק העבודות להזדמנויות תעסוקה ולצלוח ראיונות עבודה.

- שדרוג וכתיבת קורות חיים להייטק ולסוכנויות: התאמת מבנה קורות החיים לסטנדרטים הנדרשים כיום ובטכנולוגיות AI כיתרון תחרותי מובהק.
- מיתוג אישי ונוכחות ברשתות מקצועיות: אופטימיזציה של פרופיל ה-LinkedIn, בניית נטוורקינג נכון והצגת הנכסים הדיגיטליים למעסיקים ולמגייסים.
- סימולציות לראיונות עבודה (HR ומקצועי): תרגול מעשי של מענה לשאלות נפוצות, הצגת מוטיבציה אישית וטכניקות להתמודדות עם מבחני בית ומשימות מיון.
- הצגת תיק עבודות בריאיון: הצגת תהליכי החשיבה מאחורי הפרויקטים ופיצוח נכון של שיח מקצועי מול מובילי צוותים.

זכאות לתעודת סיום

על מנת להיות זכאים לקבל תעודת גמר מטעם ג'ון ברייס יש לעמוד בדרישות הבאות:

- נוכחות ב- 80% מהמפגשים לפחות
- מעבר בהצלחה משימות ו/או מבחנים פנימיים
- הגשת פרויקטים

סטודנטים שיעמדו בדרישות המפורטות, יהיו זכאים בנוסף לתעודה מטעם ג'ון ברייס הדרכה, גם לתעודת גמר מטעם משרד העבודה והרווחה עבור קורס "מגן סייבר".

הובלה מקצועית

דויד שיפמן, מנהל תחום סייבר
ג׳ון ברייס הדרכה



דוד שיפמן, מנהל תחום הסייבר ב-ThinkCyber ומומחה מוביל ומוכר באבטחת מידע ובמבצעי סייבר עם ניסיון של למעלה מ-20 שנה. דוד פיתח והתמחה בנושאים כמו מחקר סייבר, לוחמת סייבר, חקירות פורנזיות ואבטחת SCADA, ושימש כיועץ ומרצה לגורמים צבאיים, ממשלתיים ועסקיים ברחבי העולם.

דוד הוביל צוותים מקצועיים לפיתוח כלים חדשניים וליכולות מתקדמות בתחום אבטחת המידע. הוא פיתח את Cyberium Arena - פלטפורמת סימולציות מתקדמת לאימוני לוחמה בסייבר, ושימש כמאמן בכיר ליחידות מיוחדות ולגופי ביטחון חשאיים ברחבי העולם.

בג'ון ברייס, דוד מוביל את תחום הסייבר תוך שהוא שם דגש על תרגול מעשי וחשיבה מחוץ לקופסה. גישתו הייחודית מבטיחה לסטודנטים שלנו חוויית לימוד מעשירה והגעה להישגים משמעותיים בעולם האמיתי.

"תוך כמה חודשים מסיום הקורס התקבלתי לעבודה בתחום. המרצה הייתה מקצועית וקשובה, העבירה את החומר בצורה פשוטה וברורה, גם למי שאין רקע בתחום, ולאורך הקורס תמיד היה למי לפנות. גם ההכנה לראיונות העבודה עזרה לי בתהליך."

- **אריאל פולק**, מיישם SF, מטריקס

"הלימודים כללו הרבה תרגול מעשי ואתגרים שעזרו לי להתמודד עם מצבי לחץ ולהתכונן לעבודה בפועל. הקורס היה מבוסס על התנסות ותרגול. תהליך ההשמה היה מקצועי, עברתי מספר ראיונות עבודה ובסופו של דבר השתלבתי במטריקס."

- **דור עמרמי**, מיישם SF, מטריקס

"הלימודים היו עבורי חוויה טובה ומהנה כחודש וחצי אחרי שסיימתי את הקורס פנו אליי לגבי תהליך קבלה למטריקסלמי שסקרן מטבעו ואוהב לחקור ולהתמודד עם אתגרים, אני חושב שהקורס והתחום יכולים להתאים לו מאוד."

- **תומר מנחם יעקבי**, מיישם אבטחת מידע וסייבר, מטריקס

"הקורס נתן לי את הכלים הראשונים להיכנס לעולמות אבטחת המידע ולהבין לאילו תחומים אני הכי מתחבר. היום אני מנהל אבטחת מידע בקבוצת מטריקס. אני מאוד ממליץ על ג׳ון ברייס – גם עובדים מהצוות שלי הם בוגרי ג'ון ברייס."

- **תומר קריספין**, מנהל אבטחת מידע, מטריקס

לא רק ללמוד סייבר. להתאמן על החשיבה שמאחוריו.

1 לא רק לצפות — להתמודד עם המשימה

התלמיד עובר בין שאלות ותרחישים, מנתח מידע מקצועי ומזין תשובה בעצמו. כך הלמידה הופכת מהיכרות עם מושגים לתרגול של חשיבה ופתרון בעיות.

2 תוכן מקצועי שמחבר בין עולמות הסייבר

התרגולים משלבים כתובות IP ורשתות, מודל OSI, פקודות מערכת, חיפוש מתקדם וניתוח תעבורה — בדיוק התחומים שמהם נבנית הבנה טכנית רחבה.

3 מסלול תרגול עם התקדמות גלויה לעין

ממשק תרגול מובנה, ניווט בין משימות ותצוגת אחוזי התקדמות מאפשרים לתלמיד לראות מה כבר ביצע, להמשיך במשימות ולתרגל באופן מסודר.

מה מתרגלים ב־Cyberium Arena?

INTRO TO CYBER

דוגמאות לתחומי תרגול המופיעים במערכת

01	**Numeral Systems** בינארי, עשרוני וקודי ASCII	02	**IP Addresses** כתובות פרטיות, Subnet ו־APIPA
03	**OSI Model** שכבות הרשת ותפקידי הפרוטוקולים	04	**Network Traffic** ניתוח לכידות, Wireshark ו־TCP
05	**CMD Commands** ניתוח פלט וזיהוי פקודות מערכת	06	**Google Dorks** חיפוש מתקדם ואיתור מידע ברשת
07	**Shodan + Services** איתור שירותים וחשיפה ברשת	08	**Hash & Encoding** קידוד, גיבוב וייצוג מידע

בממשק נראים גם **Interview Prep** ו־**Project**, לצד מסלול נפרד של **Linux Fundamentals**.

היתרון לתלמידי ג'ון ברייס: ידע שמתרגלים, לא רק שומעים עליו.

שילוב מערכת Cyberium Arena בחוויית הלימוד מעניק עוד דרך להפוך מושגים טכניים למשימות, לעבודה עצמאית ולהתנסות בממשק מקצועי ממוקד־תרגול.

שוק התעסוקה והשכר

לאן אפשר להתפתח בעולם הסייבר — ומהם טווחי השכר בישראל?

SOC Analyst
מסלול כניסה

ניטור התראות אבטחה, קריאת לוגים, זיהוי פעילות חשודה, תחקור ראשוני והעברת אירועים להמשך טיפול.

מיישם/ת אבטחת מידע
עם בסיס IT

הגדרות אבטחה, בקרות גישה, הקשחת מערכות ותפעול פתרונות הגנה ברשת ובתחנות הקצה.

Cyber Security Analyst
התפתחות מקצועית

תחקור אירועי אבטחה ותעבורת רשת, זיהוי איומים והמלצות לשיפור ההגנה.

חולשות ובדיקות חוסן
התמחות מתקדמת

מיפוי נכסים, איתור חולשות וביצוע בדיקות אבטחה מורשות, תיעוד ממצאים והמלצות לתיקון.

תגובה לאירועים וציד איומים (Incident Response · Threat Hunting)
לאחר צבירת ניסיון

חקירת אירועי סייבר מורכבים, ניתוח ראיות דיגיטליות, הכלת תקיפות וחיפוש יזום של פעילות עוינת.

טבלת שכר בסייבר בישראל

נתוני שוק 2026 | שכר חודשי ברוטו

כמה אפשר להרוויח?

דוגמאות לפי תפקיד וותק

אנליסט/ית SOC בתחילת הדרך (0–2 שנים)	₪11,000 – ₪16,000
אנליסט/ית אבטחת מידע (3–5 שנות ניסיון)	₪20,000 – ₪30,000
מומחה/ית תגובה לאירועים (6–10 שנות ניסיון)	₪35,000 – ₪40,000

חשוב לדעת: אלו דוגמאות לתפקידים שונים, ולא מסלול שכר מובטח. השכר בפועל תלוי בניסיון, במעסיק, בתחום ההתמחות ובתוספות כגון משמרות. אורך הפס מייצג את קצה הטווח העליון, עד 40,000 ₪.

מתחילים בבסיס מקצועי. מתקדמים להתמחות.

היכרות עם רשתות, מערכות הפעלה וניתוח מידע תומכת בכניסה לעולם ההגנה. ככל שצוברים ניסיון מעשי, אפשר להתפתח לחקירת אירועים, ניתוח איומים ובדיקות חוסן.

הקשרים שלנו, הגשרים שלכם

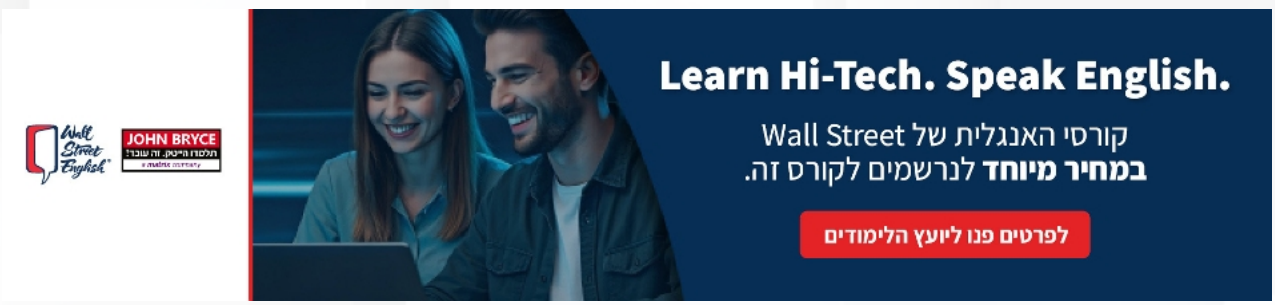
שלב חיפוש העבודה הינו שלב קריטי בתהליך הסבה מקצועית ומציאת עבודה ולכן הקמנו את מחלקת השמת בוגרים המסייעת לבוגרי הקורסים להשתלב בשוק העבודה ללא עלות!

המחלקה מציעה לסטודנטים סדנאות מקצועיות, מענה לשאלות, ייעוץ והכוונה בדרך למציאת עבודה. כחלק מהפעילות, נערכות אחת לשלושה חודשים, סדנאות כתיבה נכונה של קורות חיים והכנה אפקטיבית לראיונות עבודה.

מחלקת ההשמה מאפשרת לבוגרים להיחשף ישירות בפני מעסיקים פוטנציאליים שהינם שותפים עסקיים של ג'ון ברייס הדרכה, המחפשים בין בוגרי הקורסים מועמדים לתפקידים מקצועיים ומגוונים בחברות המובילות בענף ההייטק. המחלקה המיוחדת מנהלת מאגר קורות חיים ממוחשב הבנוי על פי מסלולי לימוד, כך שכל תלמיד הוא למעשה מועמד פוטנציאלי להצעות עבודה ומשרות שמתקבלות במכללה.

נשמח ללוות גם אותך!

לפרטים נוספים | jobjb@johnbryce.co.il



בין החברות בהן תמצאו את הבוגרים שלנו













































































*6460
www.johnbryce.co.il
עקבו אחרינו