INT
Institute of Innovation & Technology

CyberPro

מסלול אבטחת מידע וסייבר

בחסות

האוניברסיטה הפתוחה
מערך לימודי החוץ

Institute of Innovation & Technology

CyberPro
מסלול אבטחת מידע וסייבר

מתקפות הסייבר בארץ ובעולם הן המלחמה השקטה בעולמות העסקיים והביטחוניים, ולכן תחום הסייבר ואבטחת המידע הפך לכה מבוקש בעולם ההיי-טק.
עם השתלבותן הנרחבת של מערכות אינטרנטיות מתקדמות בארגונים נוצרה מודעות לצורך באבטחת מידע, שכן זליגת מידע, פריצות אבטחה, דרישות כופר וכדומה עלולות לגרום לנזקים עצומים לארגונים וחברות.
אבטחת מידע היא בעצם הפרקטיקה של הגנה על מחשבים, שרתים, מכשירים ניידים, מערכות אלקטרוניות, רשתות ונתונים מפני התקפות זדוניות. קורס CyberPro מבית INT הינו הקורס המקיף ביותר ללימודי אבטחת מידע וסייבר ומטרתו להכשיר את הסטודנטים להיות חלק מקהילת מומחי הסייבר הטובים ביותר. המסלול מורכב מלימוד תיאורטי של המתודולוגיות ויישומן במהלך הקורס באמצעות תרגילים, סימולציות ומעבדות המדמות עבודה יום יומית של מומחי סייבר אשר יקנו להם ניסיון אמיתי ומעשי. במהלך הקורס, תלמדו כיצד "להיכנס לראשם" של האקרים ופורצים, תתוודעו לשיטות פריצה חדשות, ותרכשו כלים המאפשרים מתן פתרונות הגנה מתקדמים לכל המערכות בארגונים עסקיים וביטחוניים. תחילה נלמדים מבוא ללימודי סייבר ונושאי אבטחת מידע, כולל יסודות, טכנולוגיה, ונושאי בסיס. בהמשך מתוודעים הלומדים לטכנולוגיות הרלבנטיות, למערכות הפעלה, לכלים, לשפות תכנות נבחרות ועוד. לאחר מכן נלמדים לעומק נושאים מרכזיים בתחום הסייבר ההגנתי וההתקפי, מתקפות סייבר והגנה מפניהן, הצפנה, פריצת סיסמאות, תוכנה זדונית ועוד.
המבנה הייחודי של הקורס מאפשר למשתתפים המגיעים ללא ידע מוקדם או רקע בתחום, לממש את ההמלצות להפחתת חדירות סייבר לארגונים של המרכז הלאומי להתמודדות עם איומי סייבר.

פרויקט גמר ברמת תעשייה

במסגרת התוכנית, תבצעו פרוייקט גמר ברמת תעשייה.
הנחיות מקצועיות יינתנו בכפוף לסטנדרטים הנדרשים מחברות, יזמים וסטרטאפים בתעשיית ההייטק.
לקראת סיום הקורס, תגישו מוצר טכנולוגי מוגמר משלב הרעיון ועד הפיתוח בפועל בחסות מרצים מנוסים שילוו את התהליך. מיזם זה יעניק לכם ניסיון מוכח בתכנון והבנה של פרוייקט, התמודדות עם אתגרים ומצבים מורכבים שעולים מן השטח.

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

למה ללמוד דווקא ב-INT?

מודל הלמידה

מתודולוגית הלמידה ב INT מבוססת על למידה אקטיבית של הסטודנט המשלבת רכישת ידע תיאורטי והתנסות Hand-On. מודל זה מקנה ללומדים יכולת חשיבה ביקורתית המאפשרת יישום מעשי של משימות מאתגרות וחשיבה מחוץ לקופסא.

חיבור לתעשייה

הלמידה בקורס מבוססת תרגילים מעשיים, מעבדות ופרויקטים המדמים את הנדרש מכם בתעשיית ההייטק. העבודה על הפרויקטים מתבצעת בקבוצות קטנות ומלווה על ידי המרצה.

מעטפת לימודית

מכללת INT מספקת לסטודנטים את המעטפת המתאימה לחווית לימודים מיטבית ופרקטית.

למידה מגוונת

רכישת הידע נעשית ע"י הרצאות תאורטיות, בשילוב פעילויות אינטראקטיביות המסייעות בהבנה ובהטמעת החומר הנלמד, תרגול וסימולציות, ובאמצעות למידה עצמאית.

סגל המרצים שלנו

INT מחזיקה בסגל מרצים מומחי הדרכה מובילים בתחומם ובפרט בתעשיית ההייטק הישראלית. המרצים בעלי ניסיון מעשי רב ביישום והדרכת נושאי הלימוד החמים והחשובים ביותר בעולם ההייטק.

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

כל מה שחשוב לדעת

היקף שעות
516 שעות לימוד (396 שעות לימוד אקדמיות + 120 שעות עבודה עצמית על פרויקטים).

קהל היעד ודרישות קבלה
הקורס מתאים לסטודנטים בעלי אנגלית ברמה גבוהה ובעלי היכרות טובה עם עולם המחשב.
- נדרשת מחויבות ויכולת למידה עצמית
- יש לעבור בהצלחה מבחן פנימי של המכללה
- קיים יתרון לסטודנטים בעלי ניסיון בעבודה / לימודים בתחום

זכאות לתעודת גמר מטעם מכללת INT
תעודת גמר מטעם INT תוענק לבוגרים העומדים בתקנון הלימודים ובתנאי הקורס המשתנים מעת לעת.

דרישות מערכת לקורס
- כונן אחסון 512GB SSD
- מעבד i5 דור 8 ומעלה
- זיכרון 16GB RAM

עדיפות
- גודל מסך 14״
- מסך נוסף רחב

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

INT
Institute of Innovation & Technology

תוכנית הלימודים - שלב א'

יסודות הסייבר (130 ש"א)

Module 1	**תקשורת וניהול רשתות**	34 Hours

תקשורת מחשבים וניהול רשתות הוא תחום שכל מומחה סייבר צריך להכיר לעומק.
מגוון מתקפות סייבר מושתתות על תחומים אלה ושליטה בהם תאפשר למיישם סייבר להבין לעומק את מהות המתקפה ולמנוע אותה בזמן הקצר והאפקטיבי ביותר.

- סוגי רשתות
- מבנה כתובת הרשת
- מודל OSI
- TCP/IP
- Packet Tracer
- Network Devices
- שרתים ופרוטוקולים מיוחדים (כגון DNS, DHCP, FTP)
- Wireshark
- NAT
- ARP
- Routing, Routing Table, IP Cidr

Module 2	**תכנות + בסיסי נתונים**	60 Hours

מעצם העובדה שסייבר הינו תחום המושתת על טכנולוגיות מתקדמות, הוא מבוסס על שפות תכנות שונות שחשוב להכיר. במסגרת מודול זה, נכיר ברמה בסיסית שפות תכנות מרכזיות.

- מסדי נתונים רלציוניים ולא רלציוניים
- SQL
- העמקה בפרוטוקול HTTP
- סקירה כללית של שפות תכנות: HTML, Javascript, Python, PHP

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

Module 3	**מערכות הפעלה**	36 Hours

מרבית המטרות של האקרים מבוססות על מערכות הפעלה שונות. כדי להגן על מערכות הפעלה אלה, יש להכיר אותם לעומק. במסגרת מודול זה, נלמד על מערכות ההפעלה השונות, כיצד הן פועלות וכיצד ניתן לתקוף ולהגן עליהן.

- הקדמה למערכות הפעלה + VM
- Windows
- רכיבי המחשב המרכזיים
- מונחים חשובים הקשורים למערכות הפעלה
- Active Directory
- Domain Controller
- Remote Desktop
- Linux + פקודות נפוצות
- היכרות עם Kali Linux
- Powershell & Terminal

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

תוכנית הלימודים - שלב ב'

סייבר בסיסי (Introduction to Cyber)

(28 ש"א)

28 Hours	**עקרונות הסייבר**	Module 4
בשלב זה נלמד את העקרונות הבסיסיים בעולם אבטחת המידע והסייבר, המהווים את אבני היסוד של עולם הסייבר בתעשיית אבטחת המידע		
• הגדרות שכיחות בעולם ה Cyber וה - Security • Access Control • Physical Security • Business Continuity & Disaster Recovery • התקיפה מעיני התוקף + סוגי האקרים • הכרות עם עולם ניתוח איומים וניהול סיכונים • מיפוי נכסים והכרות עם כלי סקיוריטי מעולם ה-DAST/SAST/IAST/OSS • Risk Analysis • CIA		

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

תוכנית הלימודים - שלב ג'
סייבר מתקדם (238 ש"א)

28 Hours	**קריפטוגרפיה**	Module 5

מאז ומעולם, בני האדם עסקו בהסרת מידע רגיש באמצעות שיטות הצפנה שונות ומגוונות. בחלק זה, נלמד את עקרונות ושיטות ההצפה השונות

- היסטוריה של קריפטוגרפיה
- מיפוי נכסים – Security Policy VS Security Mechanism
- הצפנה – רקע, הצפנה סימטרית/אסימטרית, אלגוריתמי הצפנה
- ביצוע הצפנה של מידע ב-Rest
- פרוטוקולי הצפנה (SSL-TLS)
- פונקציות גיבוב (hash)
- חתימה דיגיטלית – סימטרית/א-סימטרית
- תעודה דיגיטלית ו-CA server
- שיטות הסתרת מידע (סטנוגרפיה), NFT (העשרה במידה ויש זמן – כיצד מחביאים מידע)
- NTLM, Kerberos

44 Hours	**מתקפות**	Module 6

כדי ללמוד סייבר הגנתי, עלינו להבין מה הן בכלל מתקפות סייבר.
בפרק זה נכיר מתקפות סייבר שונות כגון מתקפות רשת, פריצת סיסמאות, פישינג וכו'.

- תקפות רשת, סוגי המתקפות לפי Network layer
- מתקפת DDOS, התגוננות ברמת תשתיות ורמת האפליקציה
- דרכים לטשטש עקבות מצד התוקף
- Port Scanning
- Vulnerability Scanning
- MITM

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

- Privilege Escalation
- Reverse + Bind Shells
- פריצת סיסמאות (Password Cracking)
- Network Pivoting
- Zero Days
- Firewall + Proxy + DLP
- Metasploit
- Netcat
- The cyber kill chain
- MITRE Attack
- מתקפות Social Engineering
- Email Security
- סוגי Malwares
- Defense Types

Module 7	**סייבר הגנה והתקפה – אפליקטיבי**	32 Hours

- OWASP Top 10 web applications
- Buffer Overflow
- SQL Injection
- XSS
- CSRF
- SSDLC Process
- Csp Protection
- Session Hijacking
- Application & Database Hardening Principles
- WAF
- IDS/IPS
- Honeypots
- Burp, ZAP Tools

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

Module 8	**API Security**	16 Hours
• OWASP TOP 10 api security 2023 • REST API • Swagger • Base64, Tokens, jwt • SAML • OpenID connect, OAUTH 2.0		
Module 9	**Cloud Security**	12 Hours
• סקירת ה - Cloud Providers העיקריים בשוק: GCP, AWS, Azure • ה-Resources המשמעותיים ביותר בענן • פרצות אבטחה אפשריות בענן • IAM + Permissions • Kubernetes – Main Components + Security Principles • מוצרי אבטחת ענן		
Module 10	**התנסות מעשית בהאקינג ומבדקי חדירה**	36 Hours
במסגרת פרק זה נעסוק בתרגול מעשי של מתקפות Hacking (חדירה): סריקת רשתות, איסוף מידע אקטיבי ופסיבי, פריצת סיסמאות והשתלטות על מחשבים, שרתים ואתרים. פרק זה יאפשר לכם התנסות אמיתית בתוך מבדקי החדירה וה Hacking דבר אשר יפתח בפניכם דלת לעולם היוקרתי של סייבר התקפי.		
• סריקת רשתות • איסוף מידע אקטיבי ופסיבי • סריקת שירותים ומערכות • פריצת סיסמאות והשתלטות על מחשבים, שרתים ואתרים • Hacking and PT		

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

- Recon Tools
- OSINT
- PenTest Methodologies
- Manual and Auto Scanning
- Writing Reports

12 Hours	**טעימות קונספטים**	Module 11

בחלק זה נכיר ונעבור על תחומים מרתקים בעולם הסייבר.

- Wifi, Mobile, Blockchain, IoT, ChatGPT, Fraud
- אתגרי ה-Big Data

36 Hours	**ניהול אירועי סייבר**	Module 12

בחלק זה נלמד כיצד נראה אירוע סייבר באמצעות חשיפה למערכות ניטור ובקרה. נכיר לעומק מערכות SOC/SIEM, כלי IDS/IPS, DER ונלמד כיצד לתחקר אירועים שונים.

- SOC
- SIEM
- Logs and Monitoring
- Incident Response
- Cyber Forensics
- Malware Analysis
- Threat Hunting
- Threat Intelligence

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

Module 13	**מיומנויות והכנה לעבודה בשיתוף מרכז קריירה**	6 Hours
במסגרת הקורס הסטודנטים יעברו מספר סדנאות מטעם מרכז הקריירה של מכללת INT שמטרתן לחשוף אותם לשוק העבודה העכשווי והצרכים שלו ולסייע להם להתאים את עצמם אליו בצורה מיטבית.		
• כתיבת קורות חיים • הכנה ותחזוק פרופיל LinkedIn • כיצד עוברים בהצלחה ראיון עבודה ומבחנים טכניים וכו' • חזרות אשר יסייעו להיערך בהצלחה למבחנים חיצוניים כגון CEH Certification		
Module 14	**הכנה והגשה של פרויקט הגמר**	16 Hours

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

INT

המרכז הבינלאומי
ללימודי הייטק וחדשנות

בחסות
האוניברסיטה הפתוחה
מערך לימודי החוץ

*6377 | int-college.co.il