INT
Institute of Innovation & Technology

CyberPro

מסלול לוחם סייבר מתקדם

פריצה, הגנה ותגובה

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, ורשתות 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 לכם 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.

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.

שילוב בינה מלאכותית (AI) בתוכנית הלימודים
עתיד הלמידה כבר כאן

כחלק מהשאיפה להכשיר את הסטודנטים לעולם הטכנולוגי הדינמי של היום ושל המחר, תוכנית הלימודים כוללת שילוב מעשי וחכם של כלי בינה מלאכותית בשלבים שונים של ההכשרה. ה-AI משתלב כזרוע תומכת ללמידה, לתרגול וליישום – החל מזיהוי תקלות ברשת, דרך ניתוח לוגים ותעבורת רשת, ועד לסימולציות סייבר בזמן אמת.
כלי AI מעניקים לסטודנטים יתרון משמעותי: הם מאפשרים פתרון בעיות מהיר, חיזוי תקלות, חיזוק הבנה טכנית, ומקנים התנסות בטכנולוגיות מתקדמות שמובילות כיום את עולם הסייבר,
הרשתות והשרתים. השילוב של AI בתוכנית מדמה את דרישות התעשייה ומכין את הבוגרים לעבודה בסביבות מקצועיות שבהן נדרשים כלים חכמים, גמישות ויכולת קבלת החלטות מהירה.

השתלבות בתעשייה כבר במהלך הלימודים

הקורס בנוי באופן מדורג ומעשי, כך שכבר בסיום שלב א' – ניהול רשתות תקשורת – הסטודנטים רוכשים מיומנויות מבוקשות בשוק, המאפשרות להם להשתלב בעבודות בתחום הטכנולוגי, כגון טכנאי רשתות, תומכי IT או אנשי Help Desk.
שילוב של הכשרות רשמיות (כגון CCST Networking), תרגול Hands-On ותשתית תאורטית חזקה, מאפשר לסטודנטים לצבור ניסיון מקצועי ולהתחיל את דרכם בעולם העבודה עוד במהלך המשך הלימודים בשלבים הבאים של המסלול.

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.

מסלול רב הסמכתי להכשרה טכנולוגית מעשית

תוכנית הלימודים מכינה למגוון רחב של הסמכות מוכרות ובינלאומיות, המותאמות לצרכי התעשייה ומבוססות על סטנדרטים מקצועיים עדכניים.
השילוב בין הסמכות טכנולוגיות בתחומי רשתות, שרתים, סייבר ותכנות – מאפשר ללומדים לרכוש יתרון תחרותי בשוק העבודה, להוכיח את יכולותיהם למעסיקים ולבנות פרופיל מקצועי איכותי כבר בתחילת הדרך.
כל הסמכה מלווה בתרגול Hands-On מעשי, המדמה סביבות עבודה אמיתיות ומכין את הבוגרים להשתלבות בתעשייה באופן מידי ובטוח.

רשימת ההסמכות בתוכנית הלימודים

- **Cisco Certified Support Technician – Networking (CCST Networking)**
  הסמכה בינלאומית של חברת Cisco בתחום ניהול רשתות תקשורת.
- **Linux Essentials – LPI (Linux Professional Institute)**
  הסמכה בסיסית ומבוקשת של LPI לעבודה עם מערכות הפעלה מבוססות לינוקס.
- **PCEP™ – Certified Entry-Level Python Programmer**
  הסמכה רשמית מטעם Python Institute, המהווה בסיס לעולם התכנות, האוטומציה והסייבר.
- **Cisco Certified Support Technician – Cybersecurity (CCST Cybersecurity)**
  הסמכה בסיסית מבית Cisco בתחומי סייבר, הגנה על תחנות קצה, ניתוח חולשות ותגובה לאירועים.
- **CEH – Certified Ethical Hacker**
  הסמכה בינלאומית יוקרתית של EC-Council בתחום בדיקות חדירה, פריצה אתית והגנה ברמה מתקדמת.

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.

מעבדות וירטואליות המדמות את העולם האמיתי – אצלך בבית

התוכנית כוללת מגוון מעבדות ותרגולים מעשיים בסיבה וירטואלית מתקדמת (סימולטור), אשר נשלחת לתלמיד להתקנה אישית בביתו – כך שהוא יכול לתרגל מכל מקום ובכל זמן.
המעבדות מבוססות על סביבות מציאותיות המדמות תרחישי סייבר אמיתיים, פרצות אבטחה, תחקור אירועים, ניהול רשתות, תכנות ופריצה אתית (Ethical Hacking).
בנוסף, חלק מהתרגולים נבנים כאתגרי CTF (Capture The Flag) – תרגולים מהנים, חווייתיים ומאתגרים הפונים לאותם כלים בהם משתמשים מומחי אבטחת מידע אמיתיים.
שיטה זו מחזקת את ביטחון הלומד, מפתחת חשיבה טכנית וביקורתית, ומכינה אותו באופן מעשי לעולם העבודה.
התרגול האישי מאפשר לכל תלמיד ללמוד בקצב שלו, לחזור על משימות, ולהתמקצע דרך הידיים – לא רק מהספרים.

פרויקט גמר ברמת תעשייה

במסגרת התוכנית, הסטודנטים מבצעים פרויקט גמר ברמת תעשייה.
הנחיות מקצועיות יינתנו בכפוף לסטנדרטים הנדרשים מחברות, יזמים וסטרטאפים בתעשיית ההייטק.
לקראת סיום הקורס, הסטודנטים מגישים מוצר טכנולוגי מוגמר משלב הרעיון ועד הפיתוח בפועל, בחסות מרצים מנוסים שילוו את התהליך. מיזם זה מעניק ניסיון מוכח בתכנון והבנה של פרויקט, 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 Hands-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 לחוויית 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

638 שעות לימוד (370 שעות לימוד אקדמיות + 268 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 (עדיפות לדור 10)
- זיכרון 16GB RAM

עדיפות

- 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.

תוכנית הלימודים - שלב א'

ניהול רשתות תקשורת - 100 ש"א

Module 1	תקשורת וניהול רשתות	70 Hours
חלק זה מכין להסמכת: **CCST Networking (Cisco Certified Support Technician - Networking)** 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.		
יסודות הרשת		10 Hours
▪ מושגים בסיסיים: רשת, שרת, לקוח, כתובת MAC ▪ סוגי רשתות: LAN ,WAN ,WLAN ▪ פרוטוקולים ומודלים OSI ו-TCP/IP ▪ מבנה מסגרת Ethernet וכתובות MAC ▪ תקשורת בין מכשירים ברשת		
כתובות IP ותכנון רשת		10 Hours
▪ כתובות IPv4 ו-IPv6: מבנה, הקצאה, שימושים ▪ כתובות פרטיות וציבוריות ▪ Subnetting בסיסי (כולל CIDR ו-VLSM) ▪ DHCP - הקצאה דינמית ▪ ARP – מיפוי MAC ל-IP ▪ ניתוב בסיסי ו-NAT		

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.

25 Hours	ציוד רשת והגדות ראשוניות
▪ זיהוי והבנת תפקוד של נתב (Router), מתג (Switch), נקודת גישה (Wireless Access Points) ▪ הבנת CLI של Cisco IOS – ניווט, פקודות show ו-configuration ▪ Subnetting בסיסי (כולל CIDR ו-VLSM) ▪ קונפיגורציה בסיסית של מתגים ונתבים: הגדרת כתובות IP, סיסמאות גישה, Default Gateway, ניהול VLAN בסיסי ▪ הגדרת רשת ביתית/משרדית ▪ כלי בדיקה: ping, traceroute, ipconfig, show ▪ תרגול: בניית רשת קטנה עם הגדרות Cisco מלאות	
25 Hours	פתרון תקלות מעשי
▪ ניתוח תקלות פיזיות (כבלים, פורטים, קישוריות) ▪ פתרון בעיות כתובות IP, קונפליקטים, DHCP ו- DNS. ▪ פתרון תקלות אלחוטיות וניידות ▪ תרגול עבודה עם כלי בדיקה (ping, ipconfig, nslookup) ▪ פתרון תקלות מרחוק מול משתמשים ▪ ניהול תיעוד רשת בסיסי ▪ שימוש ב-AI לזיהוי תקלות רשת וניטור חכם	

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 2	ניהול שרתים של Microsoft	30 Hours
בחלק זה נלמד כיצד לנהל שרתים מבוססי Windows Server באופן מקצועי, כולל הקמה של Active Directory, ניהול משתמשים והרשאות, הגדרת שירותי רשת כמו DNS ו- DHCP וגיבוי המערכת. נעמיק בניהול מרכזי באמצעות Group Policy (GPO), ככלי חיוני לאכיפת מדיניות אבטחה, מניעת גישה לא מורשית והגנה על נתונים ומשאבים בארגון.		
הקמת שרת והגדרות בסיס		5 Hours
▪ התקנת Windows Server ▪ הגדרות רשת, שימוש ב- Server Manager, עדכונים ▪ התקנת AD		
Active directory וניהול משתמשים		10 Hours
▪ התקנת Windows Server ▪ הגדרות רשת, שימוש ב- Server Manager, עדכונים ▪ התקנת AD		
ניהול מרכזי ואבטחת מידע עם GPO		5 Hours
▪ התקנת Windows Server ▪ הגדרות רשת, שימוש ב- Server Manager, עדכונים ▪ התקנת AD		
שירותי רשת, תחזוקה ותרגול		10 Hours
▪ הגדרת DHCP, DNS ▪ גיבויים, שחזורים וניטור ביצועים ▪ ניהול RDP, חומת אש וחיבורי רשת ▪ תרגול מסכם הכולל תרחיש אבטחה מלא ▪ שילוב AI לניטור שרתים ואיתור אנומליות		

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 - 130 ש"א

Module 1	מערכת ההפעלה Linux	40 Hours
חלק זה מכין להסמכת: **LPI (Linux Professional Institute) Linux Essentials** בחלק זה נלמד ביצד לעבוד עם מערכת ההפעלה לינוקס ברמת משתמש ומנהל מערכת. הקורס מהווה שלב ראשון בדרך להבנת שיטות הגנה על מערכות מבוססות לינוקס וכן זיהוי חולשות וניצולן, כפי שנעשה בבדיקות חדירה (Penetration Testing).		
מבוא ללינוקס ועולם הקוד הפתוח		5 Hours
▪ הפצות נפוצות ▪ מבנה כללי של מערכת לינוקס ▪ עקרונות קוד פתוח		
שורת פקודה ופקודות בסיס		10 Hours
▪ ניווט במערכת הקבצים ▪ יצירה, העתקה, מחיקה וחיפוש קבצים ▪ הפניות, צינורות, ועזרה מובנית		
הרשאות ומערכת קבצים		10 Hours
▪ הרשאות בסיס למשתמשים וקבוצות ▪ שינוי הרשאות ובעלות ▪ מבנה ספריות במערכת		

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.

10 Hours	ניהול משתמשים ותהליכים
▪ יצירה וניהול של משתמשים ▪ ניהול קבוצות והרשאות גישה ▪ ניטור תהליכים וביצוע משימות מתוזמנות ▪ ניהול תהליכים במערכת עם כלי AI לזיהוי חריגות	
5 Hours	כתיבת סקריפטים בסיסיים
▪ יצירה וניהול של משתמשים ▪ ניהול קבוצות והרשאות גישה ▪ ניטור תהליכים וביצוע משימות מתוזמנות ▪ ניהול תהליכים במערכת עם כלי AI לזיהוי חריגות	
40 Hours	**Module 2 תכנות בשפת Python**
חלק זה מכין להסמכת: **PCEP™ - Certified Entry-Level Python Programmer** בחלק זה נלמד את יסודות שפת Python, שפה מרכזית בתחום אבטחת המידע והסייבר. נבנה הבנה תכנותית שתאפשר לכתוב סקריפטים פשוטים, לבצע אוטומציה של פעולות, ולנתח קלטים. ידע זה מהווה בסיס לפיתוח כלי אבטחה, לבדיקות חדירה (Penetration Testing), ולזיהוי חולשות במערכות.	
5 Hours	מבוא ותחביר בסיסי
▪ הדפסת נתונים ▪ קלט ▪ משתנים ▪ סוגי נתונים	

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.

7 Hours	אופרטורים ותנאים
▪ פעולות חשבון ▪ השוואות ▪ תנאים לוגיים	
6 Hours	לולאות
▪ לולאות while ו- for ▪ שימוש ב- ()range	
8 Hours	פונקציות
▪ יצירת פונקציות ▪ פרמטרים והחזרת ערכים	
8 Hours	רשימות ומחרוזות
▪ עבודה עם רשימות, מחרוזות ופעולות עליהן	
6 Hours	שימוש ב-AI לניתוח קבצי לוגים או תעבורה ברשת
▪ פרויקט: סיווג לוגים או תעבורת רשת לפי תקין/חשוד	

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	אבטחת מידע	50 Hours
חלק זה מכין להסמכת: **CCST Cybersecurity – (Cisco Certified Support Technician - Cybersecurity)** בחלק זה נלמד את עקרונות הסייבר המעשיים, כולל זיהוי איומים, ניתוח חולשות, דרכי תקיפה נפוצות ואמצעי הגנה בסיסיים, תוך תרגול תגובה ראשונית לאירועים. נבין כיצד מתבצעות תקיפות ברשתות, באפליקציות ובמכשירים וכיצד ניתן לעצור אותן בעזרת כלים ותהליכים פשוטים.		
מבוא לסייבר ואיומים נפוצים		10 Hours
▪ עקרונות אבטחת מידע (CIA) ▪ סוגי איומים: פישינג, נוזקות, הנדסה חברתית ▪ תפקידי אבטחת מידע בארגון (SOC, Analyst)		
תקיפות וחולשות		10 Hours
▪ חולשות באתרים, תוכנה ורשתות ▪ תקיפות נפוצות: SQL Injection, MITM, Brute Force ▪ תקיפות על מכשירים ניידים ורשתות אלחוטיות		
הגנת תחנות קצה ומערכות		10 Hours
▪ אנטי-וירוס, אנטי-malware, חומת אש מקומית ▪ עדכונים, הרשאות והרשאות משתמש ▪ תיעוד פעילות חשודה, כלים פשוטים (Event Viewer, Task Manager)		
אבטחת רשת בסיסית		10 Hours
▪ הגדרת אבטחה בנתבים (WPA2/WPA3) ▪ בקרת גישה, זיהוי תעבורה חריגה ▪ תפקיד ה- Firewall		

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.

10 Hours	תגובה לאירועי אבטחה
▪ שלבים בתגובה: זיהוי, הכלה, שחזור ▪ עבודה מול משתמשים ו-Help Desk ▪ תיעוד ראשוני של אירוע ▪ סימולציות בסיסיות: מה עושים כשיש חשד לפריצה? ▪ שימוש ב- AI בזיהוי מתקפות בזמן אמת (EDR/XDR)	

תוכנית הלימודים - שלב ג'

התמחות מעשית בסייבר ו-PenTesting – 140 ש"א

חלק זה מכין להסמכת: **Certified Ethical Hacker (CEH)**
מטעם EC-Council (International Council of E-Commerce Consultants)
בחלק זה נלמד כיצד ליישם בפועל את עקרונות הסייבר ההגנתי וההתקפי ברמה תעשייתית.
נתמקד בטכניקות תקיפה מתקדמות, שימוש בכלים מקצועיים, הגנה על אפליקציות וענן, ניתוח תקריות, וכתיבת דו"חות מקצועיים.
נבצע סימולציות מעשיות, נבנה תרחישי חדירה ונתרגל תחקור בזמן אמת.
בסיום החלק יוגש פרויקט גמר מלא ויוקנו כלים מעשיים לקראת הסמכת CEH ולשילוב בתעשייה
כ- PenTester או SOC Analyst.

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 1	**מתקפות מתקדמות וכלי פריצה**	**30 Hours**
▪ Privilege Escalation (Windows/Linux) ▪ Reverse Shell, Bind Shell ▪ שימוש ב- Metasploit Framework ▪ שימוש ב-Netcat, Powershell, Bash ▪ טשטוש עקבות ו- Anti-Forensics		
Module 2	**אבטחת אפליקציות ו-Web Hacking**	**20 Hours**
▪ OWASP Top 10 - SQLi, XSS, CSRF, IDOR, SSRF ▪ שימוש מעשי ב- Burp Suite, ZAP Proxy ▪ Session Hijacking ▪ Application Hardening		
Module 3	**אבטחת ענן ו-WiFi**	**15 Hours**
▪ פרצות נפוצות ב- AWS, Azure, GCP ▪ ניהול IAM, הרשאות, bucket misconfiguration ▪ פריצת WiFi - WPA2/WPA3 עם aircrack-ng ▪ Rogue AP, Evil Twin Attack		
Module 4	**כלי סריקה, איסוף מידע ו-OSINT**	**20 Hours**
▪ map, Nessus, OpenVAS ▪ theHarvester, Maltego, Shodan ▪ DNS enum, WHOIS, Metadata analysis ▪ טכניקות Google Dorking		

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 5	קריפטוגרפיה מתקדמת	15 Hours
▪ Hashing, Encryption (RSA, AES) ▪ SSL/TLS, PKI, CA Server ▪ Kerberos, NTLM ▪ Steganography בסיסית		
Module 6	**SIEM, forensics ותגובה לאירועים**	**20 Hours**
▪ מבוא ל- SOC: תפקידים, מערכות ניטור ▪ זיהוי מתקפות ב- logs (Windows/Linux) ▪ Incident Response: זיהוי, הכלה, שחזור ▪ Malware Analysis בסיסי ▪ שימוש בכלים: Sysmon, Wazuh ▪ יישומי AI באיתור מתקפות ומלכודות דיגיטליות (Honeytokens)		
Module 7	**דו"חות, סימולציות ופרויקט גמר**	**20 Hours**
▪ כתיבת דוחות PenTest לפי תקן CVSS ▪ ניתוח סיכון ודיווח ללקוח ▪ תכנון והצגת פרויקט גמר (תרחיש חדירה או מיזם אבטחה) ▪ פרזנטציה מול מדריך מקצועי		

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

*6377 | int-college.co.il