CyberPro 2025

תחום הסייבר החל להתפתח באופן מהיר מאוד. כיום, תחום הסייבר מהווה תחום מרכזי כמעט בכל מוסד, ארגון או חברה בעולם. לאור הגדילה המהירה בשוק הסייבר, נוצר מחסור גדול באנשי סייבר מקצועיים בשוק העבודה.
השילוב בין תחום מרכזי, שוק אשר גדל במהירות ומחסור גדול בעובדים מוסמכים יוצר הזדמנויות משמעותיות ביותר עבורכם, הסטודנטים ומאפשר לכם להיכנס לתחום המבוקש ביותר כיום בשוק ההייטק העולמי, להתפתח אישית ומקצועית ולהרוויח שכר מהטובים בשוק.
מכללת INT מציעה לכם את קורס הסייבר החדשני, הממוקד והאפקטיבי ביותר אשר יכין אתכם בצורה מושלמת לקריירה בתחום הסייבר.

חשוב לדעת!

היקף השעות
40 שעות אקדמיות

קהל יעד
קורס סייבר חדשני ומקיף זה, מיועד למועמדים בעלי שליטה טובה ביישומי מחשב ואנגלית ברמה גבוהה.

זכאות לתעודת גמר מטעם מכללת INT:
תעודת גמר מטעם מכללת iNT תוענק לעומדים בתקנון הלימודים, מעבר כל המבחנים בציון עובר ובעמידה בנוכחות של 85% מהשיעורים לפחות.

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 לימודים מלאה

יסודות וטכנולוגיה (10 שעות אקדמיות)

במודול זה, נכיר את כל נושאי הבסיס בתחום הסייבר, טכנולוגיות רלוונטיות, מערכות הפעלה, כלים, שפות תכנות נבחרות ועוד

1. נושאים מתקדמים בתקשורת מחשבים כולל ניטור וניתוח תעבורת רשת
2. מערכות הפעלה בדגש על Linux ו – Windows
3. הצפנה – טכנולוגיה, פרוטוקולים, שיטות וכלי הצפנה
4. יסודות פיתוח קוד בשפת Python
5. טכנולוגיית Web – כולל פיתוח בסיסי בשפת HTML
6. סייבר במובייל (סלולר) – ניהול, ניטור ובקרה
7. תקשורת אלחוטית – כולל רשתות Wifi וטכנולוגיית Bluetooth
8. טכנולוגיות מתקדמות בעולם הסייבר כמו Blockchain, IoT וכו'
9. ניהול ופיתוח מאגרי ידע כולל שפת SQL
10. ניהול סיכונים, חוקים, תקנים ורגולציה בתעשיית הסייבר

סייבר למתקדמים (25 שעות אקדמיות)

במודול זה נכיר לעומק נושאים מרכזיים בתחום הסייבר ההגנתי וההתקפי, מתקפות סייבר והגנות מפניהן, הצפנה, פריצת סיסמאות, תוכנה זדונית וכו'

1. סריקות לסוגיהן: רשתות, אתרים, מחשבים וחולשות לקראת התקפה
2. הנדסה חברתית לרבות רשתות חברתיות, מתקפות פישינג והתחזות
3. מתקפות מניעת שירות (DOS) כולל מתקפות IoT ו – BOTNET
4. מתקפות אפליקטיביות, לרבת הזרקת קוד זדוני ו XSS
5. מתקפות תקשורת אלחוטית כולל פיצוח הצפנת רשתות ו Wifi
6. מתקפות קריפטוגרפיות כולל פיצוח הצפנה של חשבונות ואתרים
7. מתקפות תוכנה זדוניות, כולל וירוסים, תולעים וסוסים טרויאנים
8. חולשות אבטחת מידע (חומרה, תוכנה ותשתיות) ואופן הניצול שלהן
9. הגנת עבטחת מידע וסייבר כולל טכנולוגיות, כלים וחברות מובילות
10. מבדקי חדירה – שלבים, כלים ואופן ביצוע כולל סימולציה מלאה

סיכום (5 שעות אקדמיות)

במסגרת מודול זה, נחשוב כמו אנשי סייבר וננסה להבין כיצד מתבצעת תקיפה והגנת סייבר על ידי שחזור מתקפות אמיתות שקרו בתעשייה, מתוך מספר אפשרויות:

1. תכנון, בנייה, ביצוע ותחקור סימולציות סייבר מרובות מתקפות
2. תרגול מתקפות סייבר ככלי מרכזי לשמירה על מוכנות ארגונית
3. עבודה מול לקוחות מותקפים, תחת לחץ, תקלות ואילוצים

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.

4. התמודדות ועבודה מול מנהלים בכירים בזמן מתקפות סייבר
5. תכנון ויישום אסטרטגיות הגנת סייבר מפני מתקפות סייבר מורכבות
6. סיכום, תיעוד, הפקת לקחים ויישומם לאחר מתקפת סייבר
7. ניהול וסנכרון אירוע סייבר מרובה משתתפים
8. תכנון והוצאה לפועל של קמפיין מתקפות מורכב ואפקטיבי
9. תקורת אסטטגית ככלי ניהול מניעת משברים בזמן מתקפת 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.

תל אביב

המרץ 2

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.