

Cyber Pro

תיאור הקורס

תחום הסייבר החל להתפתח באופן מהיר מאוד. כיום, תחום הסייבר מהווה תחום מרכזי כמעט בכל מוסד, ארגון או חברה בעולם. לאור הגידול המהיר בגודל שוק הסייבר, נוצר מחסור הולך וגדל באנשי סייבר מקצועיים בשוק העבודה. השילוב בין תחום מרכזי, שוק אשר גדל במהירות ומחסור גדל בעובדים מוסמכים יוצר הזדמנות משמעותית ביותר עבורכם, הסטודנטים – ומאפשר להיכנס לתחום המבוקש ביותר כיום בשוק ההי-טק העולמי, להתפתח אישית ומקצועית ולקבל שכר מהטובים במשק.

מכללת iNT מציעה לכם את קורס הסייבר החדשני, הממוקד והאפקטיבי ביותר אשר יכין אתכם בצורה מושלמת לתחום הסייבר.

חשוב לדעת

היקף הקורס: 40 ש"א.

אוכלוסיית יעד ודרישות קבלה: קורס סייבר חדשני ומקיף זה, מיועד למועמדים בעלי לפחות שנת ניסיון בניהול רשתות תקשורת או לחילופין בוגרי קורס "MCSA ניהול רשתות" של מכללת iNT.

זכאות לתעודת גמר מטעם מכללת iNT: קבלת תעודת בוגר קורס מטעם המכללה מותנת בהשתתפות בלפחות 85% מהשיעורים ומעבר כל המבחנים בציון עובר בנוסף לעמידה בתקנון הלימודים.

סגל המרצים: למכללת iNT סגל מרצים ומומחי הדרכה, מהמובילים בתחומם, בעלי ניסיון מעשי רב ביישום והדרכת נושאי הלימוד בתעשיית ההי-טק הישראלית והעולמית.

זכאות לתעודת גמר מטעם מכללת iNT:

קבלת תעודת בוגר קורס מטעם המכללה מותנת בהשתתפות בלפחות 85% מהשיעורים ומעבר כל המבחנים בציון עובר בנוסף לעמידה בתקנון הלימודים.

יסודות וטכנולוגיה (10 שעות אקדמאיות)

במודל זה נלמד את כל נושאי הבסיס בתחום הסייבר, טכנולוגיות רלוונטיות, מערכות הפעלה, כלים, שפות תכנות נבחרות, ועוד.

- נושאים מתקדמים בתקשורת מחשבים כולל ניטור וניתוח תעבורת רשת.
- מערכות הפעלה – בדגש על WINDOWS ו-LINUX.
- הצפנה - טכנולוגיה, פרוטוקולים, שיטות וכלי הצפנה.
- יסודות פיתוח קוד בשפת פייתון (Python).
- טכנולוגיות Web - כולל פיתוח בסיסי בשפת HTML.
- סייבר במובייל (סלולרי) – ניהול, ניטור ובקרה.
- תקשורת אלחוטית – כולל רשתות WIFI וטכנולוגיית BLUETOOTH.
- טכנולוגיה מתקדמת בעולם הסייבר –IoT, Botnet, Blockchain.
- ניהול ופיתוח מאגרי ידע כולל שפת SQL.
- ניהול סיכונים, חוקים, תקנים ורגולציה בתעשיית הסייבר.

סייבר למתקדמים (25 שעות אקדמאיות)

במודל זה נלמד לעומק נושאים מרכזיים בתחום הסייבר ההגנתי וההתקפי, מתקפות סייבר והגנות מפניהן, הצפנה, פריצת סיסמאות, תוכנה זדונית ועוד.

- סריקות לסוגיהן: רשתות, אתרים, מחשבים וחולשות לקראת תקיפה.
- הנדסה חברתית לרבות רשתות חברתיות, מתקפות פשינג והתחזות.
- מתקפות מניעת שירות (DOS) כולל מתקפות IOT ו-BOTNET.
- מתקפות אפליקטיביות, לרבות הזרקת קוד זדוניות (SQL Injection) ו-XSS.
- מתקפות תקשורת אלחוטית, כולל פיצוח הצפנת רשתות – Wifi.
- מתקפות קריפטוגרפיות, כולל פיצוח הצפנה של חשבונות ואתרים.
- מתקפות תוכנה זדונית, כולל וירוסים, תולעים וסוסים טרויאנים.

- חולשות אבטחת מידע (חומרה, תוכנה, תשתיות) ואופן הניצול שלהן.
- הגנות אבטחת מידע וסייבר, כולל טכנולוגיות, כלים וחברות מובילות.
- מבדקי חדירה: שלבים, כלים ואופן ביצוע – כולל סימולציה מלאה.

מודול 4 - האקתון (5 שעות)

במודל זה נתחלק לצוות אדום (תוקפים) וצוות כחול (מגנים), שני הצוותים יתרגלו בפועל תקיפה והגנת סייבר ע"י שחזור של מתקפות אמתיות אשר קרו בתעשייה.

- תכנון, בניה, ביצוע ותחקור סימולציות סייבר מרובות מתקפות.
- צוות אדום (תוקפים), צוות כחול (מגנים) ומה שביניהם.
- תרגול מתקפות סייבר ככלי מרכזי לשמירה על מוכנות ארגונית.
- עבודה מול לקוחות מותקפים, תחת לחץ, תקלות ואילוצים נוספים.
- התמודדות ועבודה מול מנהלים בכירים בזמן מתקפות סייבר.
- תכנון ויישום אסטרטגיית הגנת סייבר מפני מתקפות סייבר מורכבות.
- סיכום, תיעוד, הפקת לקחים ויישומם לאחר מתקפת סייבר.
- ניהול וסנכרון אירוע סייבר מרובה משתתפים (SOC, NOC, ISP, MSSP).
- תכנון והוצאה לפועל של קמפיין מתקפות מורכב ואפקטיבי.
- תקשורת אסטרטגית ככלי לניהול ומניעת משברים בזמן מתקפות 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.

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.



המרכז הבינלאומי
ללימודי הייטק וחדשנות

מתקדמים | לקריירה בהייטק
* 6377

קמפוסים בפריסה ארצית:

באר שבע

רחוב האנרגיה 77
פארק ההייטק

ירושלים

רחוב יפו 34

רחובות

רחוב אופנהיימר 5
פארק המדע

תל אביב

ראול ולנברג 36
קריית עתידים

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.