

מיישם סייבר

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 לתפקידכם הראשון בתחום הסייבר בתעשייה.

היתרונות שלנו

- קורס מקיף, חדשני ומעודכן הכולל את כל הטרנדים והטכנולוגיות: IOT, Big data, Blockchain
- קורס מעשי הינו מעשי כולל התנסות פרקטית עם כלים וטכנולוגיות בשימוש בתעשייה.
- הקורס היחיד בארץ המציע "האקתון" ייעודי הכולל התנסות בחמ"ל סייבר במכללה.
- הקורס מוכוון תעשייה, כולל מודל ייעודי בנושא הכנה וכניסה לעבודה בתחום הסייבר.
- הקורס מכיל את כל החומר הנדרש לקבלת הסמכות יוקרתיות בעולם הסייבר: תעודת מומחה Security+ מטעם חברת CompTIA ותעודת "האקר מוסמך" מטעם חברת EC-council

חשוב לדעת

היקף הקורס

260 שעות אקדמיות פרונטליות + 100 שעות תרגול עצמי.
מכינת סייבר ייעודית בהיקף 100 שעות אקדמיות.

אוכלוסיית יעד ודרישות קבלה

קורס סייבר חדשני ומקיף זה, מיועד למחפשים את תפקידם הראשון בעולם הסייבר בתעשייה. דרישות הסף של הקורס כוללות שנת ניסיון בניהול רשתות/ תקשורת, אנגלית ברמה טובה, ומעבר מבחן התאמה לקורס או לחילופין סיום קורס "MCSA ניהול רשתות" של מכללת INT. מועמדים אשר אינם עומדים בתנאי הקבלה לקורס ידרשו להשלים מכינת סייבר ייעודית.

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. ההרשמה לבחינות ההסמכה החיצוניות יבוצעו באופן עצמאי ע"י הסטודנטים ואינן כלולות בשכר הלימוד. בסיום הקורסים, מכללת iNT מציעה לבוגריה קורסי המשך מתקדמים הן בתחום Cyber והן כמפתחים.

- אנגלית טכנית – מושגי יסוד - הכרת השפה הטכנית וידיעת מושגים חשובים.
- מבוא להכרת המחשב האישי - למידה על חומרת המחשב האישי: מבנה המחשב, זיכרונות, דרייברים, הגדרות ברמת BIOS, פירוק והרכבת המחשב, טיפול בתקלות חומרה, טכנולוגיות מתקדמות, רכיבי לוחות אם ומעבדים.
- מערכות הפעלה - התקנה, ניהול ואיתור תקלות של מערכות הפעלה נפוצות וכלים לתחזוקתן, דיאגנוסטיקה, שחזור נתונים, ניהול מחיצות, כלי Imaging, שליטה מרחוק.
- ממשק CLI - תרגול ולמידת ממשק שורת פקודה הפועל באמצעות הקשת פקודות.
- סדנת רשתות - מושגי יסוד בתקשורת נתונים, מודל 7 (4) השכבות, תשתיות, טופולוגיות, ארכיטקטורות רשת, פרוטוקולים, הקמת תשתית לרשתות תקשורת.
- תחנת עבודה וירטואלית - הכרות עם תוכנת הווירטואליזציה Hyper-V מבית Microsoft המאפשרת הגדרה והתקנה של מכונות וירטואליות.
- WINDOWS 10 - הכרת מערכת ההפעלה החדשה מבית Microsoft ומאפייניה החדשים. ניהול, יישום ואיתור תקלות ב- Windows 10 כמערכת המותקנת ב-Client.
- עבודה עם Server 2016 – התקנה ואחסון - התקנה, שדרוג והעברה של שרתים ועומסי עבודה, פתרונות אחסון ארגוניים, מרחבי אחסון ומניעת כפילות נתונים, איזון עומסים, פריסה,
- יישומים ב- Server 2016 - IPv4, DHCP, IPv6, DNS, IPAM, גישה מרחוק, DirectAccess, VPN.
- ניהול תצורת רשת עם Server 2016 - בקרי תחום, Active Directory, AD DS, AD CS, AD FS, AD RMS, GPO.



יחידה 1: מבוא לסייבר (5 שעות)

במודל זה נלמד על אופן התפתחות עולם הסייבר, מושגי יסוד מרכזיים, נסקור מתקפות היסטוריות והשפעתן על העולם, סוגים שונים של האקרים, בנוסף לקבוצות האקרים מובילות הפועלות כיום ממניעים שונים.

בהמשך נבצע סקירה מקיפה בנושא ההיסטוריה של עולם הסייבר ונקודות ציון בהתפתחותו לאורך השנים, כולל הצצה לרשת האפלה (Darknet) והמאפיינים הייחודיים שלה תוך הכרת מושגי יסוד בעולם הסייבר – טכניים, מנהלתיים ורגולטיביים.

יחידה 2: יסודות וטכנולוגיה (100 שעות)

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 LINUX ו WINDOWS .
- 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.

יחידה 3: סייבר למתקדמים (130 שעות)

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 שירו (DOS) כולל מתקפות IOT וBOTNET.
- מתקפות אפליקטיביות, לרבות הזרקת קוד זדוניו (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.



יחידה 4: האקתון (20 שעות)

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

יחידה 5 : הכנה לתעשייה (5 שעות)

במודל זה נבצע את כל ההכנות לקראת התפקיד הראשון שלנו בתעשיית הסייבר: כתיבת קורות חיים, פרופיל LinkedIn הכנה למבחני ההסמכה, ראיונות עבודה ועוד.

- סקירה מקיפה של תעשיית הסייבר המקומית והעולמית.
- תפקידי מפתח רלוונטיים בעולם הסייבר כולל ערוצי התקדמות אישית.
- תכנון ופיתוח קריירה אישי בנושא מרכזי בעבודה בתחום הסייבר.
- מוסדות לימוד, תארים, קורסים ותעודות הסמכה בתחום הסייבר.
- סיוע והכוונה בכתיבת קורות חיים לתפקידי סייבר.
- מפגש עם מרכז ההשמה של המכללה ואיתור משרות בתעשייה.
- שיעור הכנה למבחן ההסמכה של חברת CompTIA.
- שיעור הכנה למבחן ההסמכה של חברת EC-Council/
- סיוע והכוונה בבניית פרופיל לינקדאין אישי לטובת מציאת עבודה.
- סדנת הכנה לראיונות עבודה, כולל שאלות טכניות וסימולציות.

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.



Institute of technology
& innovation

***6377**

**לוקחים את העתיד
שלך באופן אישי**



ייעוץ אישי והכוונה בכל
שלב הלימודים - וגם
לאחר סיומם.



מרכז השמה - שיחבר
אתכם אל החברות
המובילות בתעשייה.



מרצים בכירים, המגיעים
מעולם ההייטק האמיתי.



כיתות לימוד מתקדמות,
מאובזרות בטכנולוגיות
העכשוויות.

Dream . Learn . Work



Microsoft Partner
Gold Learning



תל אביב: ראול ולנברג 36, קריית עתידים | ירושלים: יפו 34, מרכז העיר
רחובות: אופנהיימר 5, פארק המדע | באר שבע: האנגריה 77 פארק ההייטק