Cyber Pro 2020

המסלול המקיף ביותר ללימודי אבטחת מידע וסייבר

תיאור המסלול

מסלול זה מחולק לשלושה שלבים:

שלב ראשון – יסודות וטכנולוגיה, בשלב זה נלמד את כל החומר הבסיסי הנדרש ללימודי הסייבר ובנוסף נלמד מגוון רחב של טכנולוגיות מתקדמות – עליהן נשען עולם הסייבר.

שלב שני – סייבר בסיסי, זהו השלב המשמעותי ביותר בקורס בו נלמד את מירב החומר ונרכוש את היכולות הייחודיות הנדרשות מאנשי סייבר בתעשייה.

שלב שלישי – סייבר מתקדם, זהו השלב המעשי ביותר אשר מהווה למעשה ממשק בין הקורס לתעשייה. בשלב זה נתנסה בפועל במגוון פרויקטים, סימולציות ותרגילים אשר יאפשרו לכם לקבל ניסיון מעשי בתחום הסייבר עוד בשלב הקורס.

חשוב לדעת

היקף המסלול: 460 שעות (360 שעות אקדמאיות פרונטאליות, 100 שעות עבודה עצמית).

קהל יעד: המסלול מיועד לחסרי רקע המעוניינים להשתלב בעולם הסייבר ותקשורת המחשבים.

מתודולוגית הלמידה: בכל אחד מהנושאים הנלמדים בקורס נתחיל בלימוד תיאורטי של החומר הנדרש, מיד לאחר הלימוד התיאורטי נבצע תרגול בסיסי מקומי ומודרך, לאחר מכן נתרגל את החומר באופן עצמאי ולבסוף נבצע משחקי מלחמה אשר יאפשרו לנו לתרגל מקצה לקצה באופן קבוצתי, לתחקר ולשפר את הפעולות שלנו. הקורס מועבר ברובו המכריע בעברית (מעט מאוד באנגלית), כל החומר מסוכם במצגות תמציתיות ואינטראקטיביות ולרוב לא נדרשים לכתוב כלל במהלך השיעור.

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

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.

Cyber Pro 2020
המסלול המקיף ביותר ללימודי אבטחת מידע וסייבר

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

תעודות הסמכה בין לאומיות: בוגרי הקורס יוכלו לגשת לשני מבחני הסמכה בין לאומיים*:

הסמכת Security+ מטעם חברת CompTIA
הסמכה בתחום הסייבר ההגנתי

הסמכת CEH מטעם חברת EC-Council
הסמכה בתחום הסייבר ההתקפי

תכנית לימודים

הקורס הינו בהיקף של 360 שעות אקדמיות ומחולק לשלושה שלבים מרכזיים, בכל שלב קיימים ארבעה מודלים (חלקים):

<u>שלב ראשון: יסודות וטכנולוגיה (150 שעות אקדמיות):</u>

- מודל האנגלית (15 שעות).
- מודל עקרונות הסייבר (15 שעות).
- מודל התקשורת וניהול הרשת (40 שעות).
- מודל הקוד (80 שעות).

<u>שלב שני: סייבר בסיסי (130 שעות אקדמיות):</u>

- מודל ההצפנה (20 שעות).
- מודל מערכות ההפעלה (20 שעות).
- מודל סייבר התקפי (45 שעות).
- מודל סייבר הגנתי (45 שעות).

<u>שלב שלישי: סייבר מתקדם (80 שעות אקדמיות):</u>

- מודל ההאקתון (25 שעות).
- מודל מבדקי החדירה (20 שעות).
- מודל המחקר (20 שעות).
- מודל התעשייה (15 שעות).

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.

Cyber Pro 2020
המסלול המקיף ביותר ללימודי אבטחת מידע וסייבר

שלב א'
יסודות וטכנולוגיה
150 ש"א

בשלב זה נלמד לעומק את כל החומר הבסיסי (יסודות) וכל התחומים הטכנולוגיים הנדרשים על מנת לעסוק בהצלחה בתחומי הסייבר השונים.

כמו בכל מבנה היררכי, גם בקורס שלנו יסודות איתנים הם חלק חשוב ביותר – עליהם הולכים ונבנים לאורך הקורס תחומים נוספים ויכולות נוספות אשר יאפשרו לבוגרי הקורס ללמוד (ולעסוק) בהצלחה בתחומים אשר ילמדו בהמשך הקורס.

<u>מודל האנגלית (15 שעות):</u>

אנגלית בסיסית מהווה תנאי כניסה למרבית תפקידי הסייבר בתעשייה כיום, לכן אנחנו מתחילים את הקורס דווקא בלימוד נושא זה, בכדי לחשוף את הסטודנטים בשלב מוקדם ככל הניתן לשפה האנגלית הטכנית, חשיפה מוקדמת זו תאפשר לכם לחדד ולשפר את האנגלית שלכם כבר בשלב מוקדם – ולאורך כל הקורס. במודל זה נלמד מגוון רב של מושגים טכניים מעולמות הסייבר השונים לרבות מחשבים, תמיכה טכנית, ניהול רשתות, תקשורת מחשבים, תכנות וסייבר.

<u>מודל עקרונות הסייבר (15 שעות):</u>

תחום הסייבר הינו תחום רב מאוד, על מנת ללמוד אותו בהצלחה – רצוי להתחיל בעקרונות המובילים את עולם הסייבר ברמה הגלובלית. במודל זה נלמד על העקרונות המנחים את עולם הסייבר תוך התמקדות בשלושת העקרונות המובילים והם : חשאיות, שלמות וזמינות (CIA – Confidentiality, Integrity, Availability)

<u>מודל התקשורת וניהול הרשת (40 שעות):</u>

תקשורת מחשבים וניהול רשתות הינם תחומים אשר כל מומחה סייבר חייב להכיר לעומק. מגוון מתקפות והגנות סייבר מושתתות על תחומים אלו ושליטה בהם יאפשרו לאיש הסייבר להבין לעומק את מהות המתקפה ולמנוע אותה בזמן הקצר והאפטקיבי ביותר.

<u>מודל הקוד (80 שעות):</u>

סייבר, כתחום הנשען על טכנולוגיה מתקדמת, קשור בהכרח לשפות תכנות וקוד שהן אבני הבסיס לכל העולם הממוחשב כיום. במהלך המודל נלמד לעומק את שפת התכנות הפופולרית Python בנוסף על לימוד בסיסי של השפות Bash, HTML, JavaScript ו SQL. רבים נוטים לחשוש מלימוד קוד אך אל חשש ! זהו המודל בעל מספר השעות הרב ביותר בכל הקורס – זאת בכדי לאפשר לכם ללמוד את תחום זה בקצב מותאם אישית על ידי מיטב המרצים בתחום.

מבחן מסכם (2.5 ש"א)

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.

Cyber Pro 2020
המסלול המקיף ביותר ללימודי אבטחת מידע וסייבר

שלב ב'
סייבר בסיסי
130 ש"א

לאור הידע הטכנולוגי הרב אשר נלמד בשלב הקודם (שלב היסודות והטכנולוגיה), בלשב זה נתחיל ללמוד נושאים בסיסיים בתחום הסייבר. נושאים אלו הינם תחומי הסייבר אשר יאפשרו לכם להתקבל לתפקיד הראשון שלכם בתחום. שלב זה מורכב מארבעה מודלים המהווים את אבני הבסיס של עולם הסייבר בתעשייה.

<u>מודל ההצפנה (20 שעות):</u>

עוד מימי קדם, בני האדם עסקו בהסתרת מידע רגיש באמצעות שיטות הצפנה שונות ומגוונות.
כיום תחום ההצפנה נשען בעיקר על שיטות ואלגוריתמים מתמטיים לטובת הנושא.
במודל זה נלמד את עקרונות ההצפנה לרבות שיטות הצפנה שונות (הצפנה סימטרית וא-סימטרית), פרוטוקולי הצפנה (TLS-SSL), פונקציות גיבוב (HASH) ושיטות הסתרת מידע (סטנוגרפיה).

<u>מודל המערכות ההפעלה (20 שעות):</u>

מרבית המטרות של האקרים בימנו (מחשבים, טלפונים סלולריים, שרתים וכו') מבוססים על מערכות הפעלה שונות, מסיבה זו בדיוק - מערכות הפעלה הפכו למטרה מרכזית לתקיפות האקרים. בכדי להיות מסוגלים להגן על מערכות הפעלה, נדרש להכיר אותן לעומק. במודל זה נלמד על סוגי מערכות ההפעלה השונות, כיצד הן פועלות וכיצד ניתן לתקוף ולהגן עליהן.

<u>מודל סייבר התקפי (45 שעות):</u>

בכדי להיות מסוגלים להגן, נדרש להכיר ולהבין תחילה את המתקפות, מסיבה זו אנו לומדים תחילה את מודל הסייבר ההתקפי ורק לאחריו את המודל ההגנתי. במודל זה נלמד ונתרגל במעבדה מתקפות סייבר שונות ומגוונות לרבות מתקפות מניעת שירות (DOS/DDOS), מתקפות רשת, מתקפות Social Engineering כגון פישינג (Phishing), מתקפות אפליקטיביות Web-Application ומתקפות Hacking מתקדמות המבוססות קוד כגון Buffer Overflow ועוד.

<u>מודל סייבר הגנתי (45 שעות):</u>

בשלב זה, לאחר שאנחנו כבר מכירים ומבינים כיצד מתקפות סייבר עובדות, נוכל להתקדם וללמוד כיצד להגן על עצמינו מפניהן. במודל זה נלמד לעומק את שיטות ההגנה המתקדמות ביותר הקיימות בשוק בנוסף לעקרונות הגנה ופתרונות הגנה מהתעשייה כגון חומת אש (Firewall), שרתי Proxy, מכשירי הגנת DDOS, הגנה כנגד פריצות IDPS והגנה על אפליקציות ואתרי אינטרנט באמצעות WAF.

מבחן מסכם (2.5 ש"א)

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.

Cyber Pro 2020
המסלול המקיף ביותר ללימודי אבטחת מידע וסייבר

שלב ג'
סייבר מתקדם
80 ש"א

בשלב זה, לאחר שכבר נכיר את מרבית החומר הבסיסי של עולם הסייבר, נוכל להתקדם וללמוד כיצד חומר זה בא לידי ביטוי באופן מתקדם בתעשיית הסייבר. שלב זה יאפשר לכם להתנסות ממקור ראשון ביישום הטכנולוגיה והידע אשר צברתם עד שלב זה, בכדי להבין ולתרגל את היכולות הנדרשות מכם כאנשי סייבר מובילים בתעשייה.

מודל ההאקתון (25 שעות):

אנשי סייבר מובילים לעולם לא מפסיקים ללמוד ולתרגל.
האקתון (הלחמה של המילים "האקינג" ו"מרתון") יאפשר לכם לתרגל באופן המציאותי ביותר מתקפות והגנות סייבר. במודל זה נתחלק לשני צוותים, צוות אדום (תוקפים) וצוות כחול (מגנים), שני הצוותים יתרגלו באופן מעשי מתקפות והגנות סייבר על בסיס מתקפות אמיתיות אשר קרו בתעשייה. כל התרגולים בשלב זה יבוצעו בחמ"ל הסייבר (SOC) אשר הוקם במכללה בכדי לאפשר לכם להתנסות בתחום הסייבר באופן הקרוב ביותר למה שקיים בתעשייה כיום.

מודל מבדקי החדירה (20 שעות):

מודל זה, רובו ככולו יעסוק בתרגול מעשי של מתקפות "האקינג" (חדירה). החל מסריקת רשתות, איסוף מידע אקטיבי ופאסיבי, סריקת שירותים ומערכות, פריצת סיסמאות והשתלטות על מחשבים, שרתים ואתרים. מודל זה יאפשר לכם תרגול אמיתי ומקיף בתחום מבדקי החדירה וה- Hacking – דבר אשר יפתח בפניכם דלתות לעולם היוקרתי של סייבר התקפי.

מודל המחקר (20 שעות):

למרות שתחום מחקר הסייבר נחשב לתחום בכיר אשר מגיעים אליו לרוב לאחר שנות ניסיון רבות בתחום הסייבר, אנחנו מעוניינים להכיר לכם את עולם זה כבר בשלב הקורס. יכולת מחקר בתחום הסייבר היא יכולת אשר תהפוך אתכם מאנשי סייבר טובים למצוינים ותאפשר לכם יכולת לימוד עצמית של טכנולוגיות ומתקפות חדשות – מה שיבטיח את הרלוונטיות שלכם בשוק לאורך זמן.

מודל התעשיה (15 שעות):

למצוא את התפקיד הראשון שלכם בתחום הסייבר זהו תהליך מאתגר ואנחנו מבינים זאת. בכדי להקל עליכם ולהגדיל את הסיכויים שלכם להתקבל לחברות מובילות בנינו עבורכם את מודל התעשייה. במודל זה נעסוק אך ורק ב"איך מוצאים עבודה", החל בכתיבת קורות חיים, יצירת פרופיל LinkedIn, כיצד עוברים בהצלחה ראיון עבודה ומבחנים טכניים וכו'. במודל זה נסייע לכם בנוסף להיערך בהצלחה לבחינות ההסמכה שלכם באמצעות חזרות וסימולציות.

מבחן מסכם (2.5 ש"א)

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.

נושאים מרכזיים

יסודות וטכנולוגיה	• Cloud • Network protocols • Switch • Router • WireShark • TCPDump • Forensics • Python • SQL • Bash • HTML • JavaScript • Scripts	• Anonymous • Armada collective • Lizard squad • Availability • Script kiddies • White hat hacker • Black hat hacker • Gray hat hacker • Cloud • Confidentiality • Dark net • Hacktivism • Integrity
סייבר בסיסי	• Regulation • Vulnerabilities & Exploits • Buffer overflow • Firewall • WAF • IDPS • Anti-DDOS • False positive • False negative • Honeypot • NAT • DLP • SIEM	• Encryption • SSL-TLS • Hash • Steganography • OS • Windows OS • Linux OS • Kali linux OS • Cyber attack • DOS/DDOS attack • Social engineering • Phishing • Web application attack
סייבר מתקדם	• Metasploit • Password cracking • Bind shell • Reverse shell • Netcat • MITM • Wifi cracking • Crunch • CV writing • LinkedIn • Work interview • Security+ certification • CEH certification	• SOC • NOC • Hackathon • Penetration testing • Hacking • Scanning • Fuzzing • Reconnaissance • Cyber kill chain • Exploitation • Privilege escalation • Backdoor • Risk assessment

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

מתקדמים
לקריירה בהייטק

6377*

Cisco Networking Academy

Microsoft Partner
Gold Learning

GLOBAL UNIVERSITY SYSTEMS · ibat COLLEGE DUBLIN · HIGHQ מכינים אותך לעולם האמיתי · ARDEN UNIVERSITY · The University of Law · London School of Business & Finance · HTK · TORONTO SCHOOL OF MANAGEMENT

קמפוסים בפריסה ארצית:

תל אביב	רחובות	ירושלים	באר שבע
ראול ולנברג 36 קריית עתידים	רחוב אופנהיימר 5 פארק המדע	רחוב יפו 34	רחוב האנרגיה 77 פארק ההייטק