



סייבר ישראל
מערך הסייבר הלאומי

בודקי ספקים

קורס הכשרת בודקי אבטחת מידע
וסייבר לספקים
בליווי מערך הסייבר הלאומי

INT - המרכז הבינלאומי ללימודי הייטק וחדשנות

המרכז ללימודי הייטק וחדשנות הינו מוסד לימודים ותיק המוביל את שוק ההכשרה הטכנולוגית בשוק המקומי והגלובלי, הן מהצד המקצועי-מעשי והן מהצד הניהולי-עסקי.

למכללת INT מעל ל-18 שנות ניסיון שנוצרו תוך הכרה בשינויים המהירים בעולם הטכנולוגי, עדכון תמידי והכשרה מתקדמת. את הקורסים של המכללה מובילים מרצים בכירים המגיעים היישר מלב התעשייה.

המרכז ללימודי הייטק וחדשנות מהווה מרכז הדרכה מוסמך של חברות התוכנה המובילות בעולם ובמסגרת זו, מעניקה INT לבוגריה הכשרות והסמכות מוכרות מטעם ארגונים בינלאומיים.

מכללת INT היא חלק מקבוצת ההשכלה הגדולה ביותר באירופה GUS, ועל-כן נהנית המכללה מכל הידע העדכני והמגמות הבינלאומיות בשוק ההכשרות הטכנולוגיות המתקדמות בעולם.

בואו ללמוד את אחד מהמקצועות המבוקשים, המעניינים והמאתגרים בעולם!

תיאור המסלול:

היום, יותר מתמיד, ארגונים רבים ברחבי העולם עומדים בפני סיכוני סייבר משמעותיים הנובעים מחשיפה לספקים, המספקים מוצר או שירות המהווים סיכון לחוסן אבטחת המידע והסייבר של הארגון, ובהתאם הארגון נדרש להתמודד עם הסיכון. תהליך זה נקרא "הגנה על שרשרת האספקה", ולך יש הזדמנות של פעם בחיים להיות בחוד החנית של ההגנה על הארגון!

מטרת הקורס:

להכשיר בודקי ספקים כגורמי בחינה, שיישמו את תהליך הערכת הסיכונים הארגוני, ע"פ הדרישות שהוגדרו ע"י מערך הסייבר הלאומי.
מערך הסייבר הלאומי גיבש נוהל ותהליך אסדרה (רגולציה), המבוסס על מפרט בדיקות אחיד לספקים והמלצות לגבי אופן הבדיקה של המפרט.

חושבים שאתם מתאימים? זה הזמן להתקדם!

על הקורס:

תאריך פתיחת הקורס: 25/5/21

ימים ושעות: ג' + ו' | 17:00-21:00 (ג'), 09:00-13:00 (ו')

הקורס יתקיים במכללת INT בקמפוס ת"א, רח' הפלך 7, מתחם WEWORK

בחינה מועד א' - 6/7/21

בחינה מועד ב' - 13/7/21

טקס הענקת תעודות - 20/7/21

ועדת הקבלה

ועדה ראשונה - 20/4

ועדה שנייה - 4/5

ועדה שלישית - 11/5

כל הועדות יתקיימו בימי שלישי החל מהשעה 17:00

מנהל אקדמי של הקורס

עמיחי (עמי) ניסימוב

מרצה באקדמיה, יועץ ומלווה חברות מובילות בהייטק, פיננסים ותעשייה בתחומי אבטחת מידע וסייבר. בעל ניסיון עשיר של יותר מ-30 שנה במגוון תפקידים בכירים בתחומי ה-IT ובהם: סמנכ"ל מע' מידע (CIO) בחברת רב בריח, סמנכ"ל Managed Services, פיתוח וניהול לקוחות בחברות אמדוקס, ECI. בוגר תואר ראשון בהנדסה ותואר שני במנהל עסקים (MBA) שניהם מאוניברסיטת תל אביב, קורס מנהלי אבטחת מידע וסייבר (CISO) בטכניון.



מנהלת הקורס:

נוי גרינוולד - 053-3026645

Noy.greenwald@int-college.co.il



חשוב לדעת

היקף השעות: 60 שעות אקדמיות.

קהל יעד: הקורס מיועד למנהלי אבטחת מידע בעלי ידע ברגולציה ותקינה בינלאומית בתחום אבטחת מידע, יועצים בתחום אבטחת המידע וניהול סיכונים, סייבר לחברות וארגונים, ובעלי ידע וניסיון בניתוח וניהול סיכונים.

תנאי קבלה: ניסיון מצטבר מוכח של 5 שנים לפחות בתחום הגנת הסייבר בחברות עסקיות ו/או בממשק עמך, תעודת סיום קורס באבטחת מידע/ הגנת סייבר בהיקף של 250 שעות לפחות או הסמכה לאומית/בינ"ל מוכרת (CISM, CISA, CISO, CISSP)

בנוסף תדרשו לעבור ועדת קבלה בנושאים הבאים:

- הכרת מוצרי וטכנולוגיות הגנת סייבר
- טופולוגיות רשת מאובטחות
- ידע וניסיון בניתוח וניהול סיכונים
- כושר הבעה בכתב ובע"פ
- יכולת פרזנטציה גבוהה וטיפול בהתנגדויות
- עברית - שפת אם, אנגלית - ברמה גבוהה

מתודולוגית הלמידה:

הקורס מורכב מלימוד תיאורטי של הנושאים בדגש על תרגול מעשי וסימולציות. הקורס נבנה כדי להתאים לדרישות התקופה ואם תיירש למידה מרחוק ו/או שילוב בין מפגשים בכיתה ללמידה מרחוק, נשקול להוסיף קבוצת לימוד אונליין תומכת במהלך הקורס.

זכאות לתעודת גמר מטעם מכללת iNT ומעריך הסייבר הלאומי:

תעודת גמר מטעם מכללת iNT ומעריך הסייבר הלאומי תוענק לבוגרים העומדים בכל דרישות התוכנית, לרבות נוכחות ב-100% מהשיעורים, הגשת המטלות ובסיום הקורס תתקיים בחינת הסמכה ע"י מעריך הסייבר הלאומי. מעבר בהצלחה את מבחן ההסמכה בסיום הקורס בהתאם לדרישות המסלול ועמידה בתקנון הלימודים.

הקורס נערך בליווי מעריך הסייבר הלאומי.



תכנית לימודים

פרק א' - מבוא, מדיניות ונהלים (10 ש"א)

- היכרות עם מערך הסייבר הלאומי
- שרשרת האספקה
- אסדרת ספקים - תהליך האסדרה, מודל ונוהל עבודה, רגולציה ועוד.
- ממשל תאגידי
- אחריות בעלי תפקידים בתהליך אבטחת מידע בארגון - מנהל אבטחת מידע CISO
- הערכת סיכונים בארגון - תקן ISO27001, תקנות הגנת הפרטיות, תקן GDPR, תקן PCI
- מתודולוגיות לבחינת חוסן שרשרת אספקה - Best Practice מהעולם
- תהליך ביצוע ביקורת
- מדיניות ונהלים - חשיבות הנהלים ומסמך מדיניות בארגון
- Benchmark - איומי סייבר משמעותיים בעולם"
- משאבי אנוש - תהליכי משאבי אנוש בהגנת הסייבר

פרק ב' - אבטחה פיזית, המשכיות עסקית והגנה על מידע (10 ש"א)

- מניעת גישה למערכות - מערכות הגנה פיזיות ואבטחת גישה
- המשכיות עסקית - גיבויים ושחזורי מידע, תהליך ניתוח עסקי BIA
- הגנה על מידע במנוחה ובתנועה - תקני הצפנה וטכנולוגיות נפוצות
- הגנה היקפית - מידול רשת, הכרת מערכות HIPS/IDS/IPS

פרק ג' - ניטור ובקרה (10 ש"א)

- לוגים ומערכות ניטור ובקרה
- בחינת מערכת התראה SIEM
- מלכודות דבש
- בקרת גישה
- גישה מרחוק - תהליך הבדיקה וכשלים נפוצים בגישה מרוחקת

תכנית לימודים

פרק ד' - עמדות קצה ושרתים (6 ש"א)

- התראת זיהוי פגיעויות ואנומליה
- פרוטוקולים לא בטוחים, אנטי וירוס ועדכוני תוכנה

פרק ה' - ניהול אירוע סייבר (4 ש"א)

- ניהול אירוע סייבר - מדיניות טיפול באירוע
- טיפול בהתנגדויות לביקורות

פרק ו' - מעגל הביקורת השלם (10 ש"א)

- אסדרת ספקים כחלק מאסדרת שירותים
- ניגוד עניינים ואתיקה מקצועית
- תהליך ביצוע ביקורת
- היבטים משפטיים בעת ביצוע ביקורת
- בניית תיק ספק

פרק ז' - ענן ופיתוח מאובטח (4 ש"א)

- הגנה על מידע בענן ועל ספקי שירותים מנוהלים XAAS
- פתרונות הגנה נפוצים בשירותי ענן
- תהליך פיתוח מאובטח

פרק ח' - תרגולים וסימולציות (6 ש"א)

- סימולציה מלאה לביצוע סקר/ ביקורת



מפגש 1 + מפגש 2

תחום	נושא השיעור	הנושאים הנלמדים	שעות לימוד אקדמיות
מפגש 1 - יום ג' 25/5/2021 - 17:00-21:00			
כללי 17:00-17:45	פתיחה (יינתן ע"י מערך הסייבר)	היכרות, יעדי הקורס	1
הפסקה			
מבוא	מערך הסייבר (יינתן ע"י מערך הסייבר)	מערך הסייבר הלאומי, ייעודו ותרומתו הקמתו למשק, תהליך אסדרת התפקיד שרשרת אספקה	1
אסדרה 18:00-19:30	מהי אסדרה בכלל ואסדרת ספקים בפרט (יינתן ע"י מערך הסייבר)	תהליך האסדרה, מודל ונוהל עבודה מול ועדת ההתעדה, רגולציה ועוד	1
הפסקה			
מעגל הביקורת השלם 19:45-21:00	תהליך ביצוע ביקורת	<ul style="list-style-type: none"> הכנת תשתית נורמטיבית ביצוע הביקורת הסקת מסקנות כתיבת דו"ח ביקורת לזיהוי ואימות משתמשים וחומרה 	2
מפגש 2 - יום ו' 28/5/2021 - 09:00-13:00			
ממשל תאגידי 19:45-21:00	אחריות בעלי תפקידים בתהליך אבטחת מידע בארגון	הגדרת תפקיד מנהל אבטחת מידע (CISO) תפקיד זה ממלא על ידי מנהל מערכות מידע, איש מחשוב פנימי או חיצוני, קב"ט או גורם אחר. אחריות הנהלה ודירקטוריון.	1
הפסקה			
מדיניות ונהלים	מדיניות ונהלים	<ul style="list-style-type: none"> חשיבות נהלים ומסמך מדיניות בארגון דגשים לביצוע ביקורת על נהלים בחינת אופן יישומם של הנהלים בפועל 	1
משאבי אנוש 10:00-10:45	תהליכי משאבי אנוש בהגנה בסייבר	<ul style="list-style-type: none"> בניית מענה ארגוני בתחום הדרכות והכשרות לעובדי הארגון בניית תוכנית מודעות לעובדי הספק הדרכות מותאמות קהל יעד תהליכי קליטה וניוד עובדים ודגשים לגבי עובדים חיצוניים וספקים של הספק 	1
הפסקה			
ממשל תאגידי 11:00-11:45	הערכת סיכונים בארגון	<ul style="list-style-type: none"> תהליך הערכת סיכונים בארגון הגדרות המענה לליקויים עמידה בתקן ISO27001 תקני פרטיות עמידה בדרישות תקנות GDPR עמידה בתקן PCI קיום תהליך להערכת נכסים קריטיים 	1
הפסקה			
12:00-12:45	מרצה אורח		1
שיחת סיכום שבועית ומשוב - 12:45-13:00			

מפגש 3 + מפגש 4

תחום	נושא השיעור	הנושאים הנלמדים	שעות לימוד אקדמיות
מפגש 3 - יום ג' 1/6/2021 - 17:00-21:00			
אבטחה פיזית 11:00-11:45	מניעת גישה - מערכות מתח נמוך	מערכות אבטחת גישה - הגנה על מתחמים רגישים, מצלמות, טלוויזיה במעגל סגור- טמ"ס, הזדהות ביומטרית, כרטיס מגנטי. מערכות הגנה פיזיות - הגנה בפני פגיעה פיזית (שטפון, שריפה, פריצה פיזית, הפסקת חשמל) מערכות גריסה ומערכות הטיפול במדיה מגנטית.	1
הפסקה			
אבטחה פיזית 18:00-18:45	מניעת גישה - מערכות מתח נמוך	• אבטחה פיזית מתוך תורת ההגנה • בקורות ודגשים בבדיקות ספקים - אבטחה פיזית	1
הפסקה			
19:00-19:45	מרצה אורח		1
הפסקה			
רציפות תפקודית / המשכיות עסקית 20:00-21:00	גיבויים ושיחזור מידע	• מושגי יסוד בהמשכיות עסקית • אבחנה בגודל הארגון וסוגי השירות הניתן • ביצוע תהליך ניתוח עסקי BIA • תהליך ביצוע גיבוי (ענן, מדיה מגנטית, שרתי בארגון ומרוחקים, גיבוי ידני/אוטומטי) • יעילות ומועילות הגיבוי	2
מפגש 4 - יום ו' 4/6/2021 - 09:00-13:00			
הגנה על מידע 09:00-09:45	הגנה על מידע במנוחה ומידע בתנועה	• הגנה על מידע במנוחה • הגנה על מידע בתנועה • ערוצי העברת מידע, כספות • רמות הצפנה שונות • ביעור מידע	1
הפסקה			
הגנה היקפית 09:00-09:45	תהליך בדיקה עבור סוגיות הגנה היקפית	• ביצוע מידול רשת באמצעות מערכות ייעודיות • התקני אבטחת רשת: Firewall, WAF, Proxy, MDM, BYOD, SSL VPN, NAC • תהליכי הלבנה, הקשחה • הכרת מערכות HIPS/IPS/IDS ובחינת מיקומן ברשת	1
הפסקה			
11:00-11:45	אירוע Target		1
הפסקה			
12:15-13:00	תרגול שבועי מסכם בקבוצות לבקורות שנלמדו בקורס עד כה		1

מפגש 5 + מפגש 6

תחום	נושא השיעור	הנושאים הנלמדים	שעות לימוד אקדמיות
מפגש 5 - יום ג' 8/6/2021 - 17:00-21:00			
גישה מרחוק 09:00-09:45	תהליך הבדיקה עבור סוגיות בדיקה מרחוק	<ul style="list-style-type: none"> מערכות תקשורת מוצפנת ו-F/W נהלי התקשרות מרחוק מול הלקוח ניצול ממשקי חיבור מרחוק לצרכי הזלגת מידע גישה מרחוקת של ספקים באמצעות טכנולוגיות נפוצות כשלים נפוצים בגישה מרחוקת 	2
הפסקה			
ניטור ובקרה 18:00-19:45	לוגים ומערכות ניטור ובקרה	<ul style="list-style-type: none"> הכרת לוגים במערכות אבטחה AV, FW מערכות תיעוד ושמירת לוגים טכנולוגיות ניטור משמעות מימוש האיום על שרתי הספק בחינת מערכות התראה SIEM קיום חוקים פריסת מלכודות דבש דגשים לפריסתן ברשת, שיטות, איתור תקיפות והכלה באמצעות מלכודות דבש הכרת כלים לסריקת רשת ואיתור פגיעויות 	2
הפסקה			
מניעת דלף מידע 20:00-20:45	מניעת דלף מידע	<ul style="list-style-type: none"> מדיניות מניעת דלף מידע מיפוי מידע מיפוי ערוצי דלף אפשריים 	1
מפגש 6 - יום ו' 11/6/2021 - 09:00-13:00			
בקרת גישה 09:00-09:45	ניטור בקרות גישה	<ul style="list-style-type: none"> מדיניות ניטור בקרות גישה, לציוד תקשורת, תיקיות וקבצים, בסיסי נתונים ומערכות מידע מדיניות הזדהות, הזדהות חזקה, חד ערכית בחינה של אופן הניטור היכן וכיצד מתקבלות התראות האם קיימת חסימת אירועים? 	1
הפסקה			
בקרת גישה 10:00-10:45	ניטור בקרות גישה	<ul style="list-style-type: none"> בחינת מדיניות משתמשים והרשאות צפייה במערכת ה-AD לכמות החברים בקבוצת ה - Domain Admin מידור הרשאות עובדים כלי מניעת גישה IDM מדיניות קליטת עובד וסיום העסקה האם גישה מרחוק מחייבת הזדהות חזקה MFA? 	1
הפסקה			
11:00-11:45	תרגול שבועי מסכם בקבוצות לבקרות שנלמדו בקורס השבוע		1
הפסקה			
12:00-12:45	מרצה אורח		1
שיחת סיכום שבועית ומשוב			

מפגש 7 + מפגש 8

שעות לימוד אקדמיות	הנושאים הנלמדים	נושא השיעור	תחום
מפגש 7 - יום ג' 15/6/2021 - 17:00-21:00			
1	מרצה אורח - מר זהר בן דוד - מערך הסייבר	הרצאה בנושא טיפול בהתנגדויות	טיפול בהתנגדויות לביקורת 17:00-17:45
הפסקה			
1	סימולציות מפגש מבקר - מבוקר זהר בן דוד - מערך הסייבר	סדנת סימולציה טיפול בהתנגדויות	טיפול בהתנגדויות לביקורת 18:00-19:30
הפסקה			
2	<ul style="list-style-type: none"> • נוהל הגנה על תחנות קצה • בחינת שרת הניהול של מערכת ה-EDR • בדיקת כמות ההתראות והאירועים לבחינת רמת • הטיפול והתראות השווא • היבטי זיהוי פגיעויות • אנומליה ותחקור • תהליך בדיקת חדירות ברמת תשתית 	התראות זיהוי פגיעויות ואנומליה	עמדות קצה ושרתים 19:45-21:00
מפגש 8 - יום ו' 18/6/2021 - 09:00-13:00			
1	תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר		היערכות וניהול מצבי משבר 09:00-09:45
הפסקה			
1	מרצה אורח		10:00-10:45
הפסקה			
2	<ul style="list-style-type: none"> • מדיניות טיפול באירוע סייבר • ניתוח אירוע מקצה לקצה תוך ניתוח מקרי בוחן (ניתוח טיפול באירועים לדוגמה) • דיווח לבעלי עניין כגון לקוחות/מערך הסייבר/רגולטור • בהתאם לעניין והצורך • אבחנה בין ארגון גדול לקטן 	מדיניות טיפול באירוע סייבר	11:00-11:45
הפסקה			
1	Case Study - תרגול שבועי מסכם בקבוצות לבקורות שנלמדו בקורס עד כה		12:00-12:45
שיחת סיכום שבועית ומשוב			

מפגש 9 + מפגש 10

תחום	נושא השיעור	הנושאים הנלמדים	שעות לימוד אקדמיות
מפגש 9 - יום ג' 22/6/2021 - 17:00-21:00			
אסדרה 17:00-17:45	אסדרת ספקים (ייתן ע"י מערך הסייבר)	<ul style="list-style-type: none"> אסדרת ספקים כחלק מאסדרת שירותים סוגי ספקים (A-C) רישום במאגר מערך הסייבר ביצוע ביקורות מטעם המערך נטילת תעודה ניגוד עניינים ואתיקה מקצועית 	1
הפסקה			
שאלון ספקים 1.3 18:00-18:45	הבהרות על שאלון 1.3 (ייתן ע"י יובל שגב ממערך הסייבר)	היכרות עם יובל שגב, שאלות והבהרות בנושא שאלון 1.3	1
הפסקה			
פיתוח מאובטח 19:00-19:45	תהליך פיתוח מאובטח	<ul style="list-style-type: none"> ביצוע תהליך פיתוח מאובטח בחינת כלי צד ג' לפיתוח קוד מאובטח דרישות ההגנה מאנשי QA 	1
הפסקה			
פיתוח מאובטח 20:00-20:45	מרצה אורח		1
מפגש 10 - יום ו' 25/6/2021 - 09:00-13:00			
פיתוח מאובטח 09:00-10:45	תהליך פיתוח מאובטח - המשיך	<ul style="list-style-type: none"> ביצוע תהליך פיתוח מאובטח בחינת כלי צד ג' לפיתוח קוד מאובטח OWASP Top 10 דרישות ההגנה מאנשי QA 	1
הפסקה			
פיתוח מאובטח 10:00-10:45	תהליך פיתוח מאובטח - המשיך	<ul style="list-style-type: none"> פיתוח מאובטח - תורת ההגנה 1.0 פיתוח מאובטח - שאלון ספקים 1.3 	1
הפסקה			
11:00-11:45	מרצה אורח		1
הפסקה			
תרגול 12:00-12:45	Case Study - תרגול שבועי מסכם בקבוצות לכל הבקורות שנלמדו בקורס עד כה		1
שיחת סיכום שבועית ומשוב			

מפגש 11 + מפגש 12

תחום	נושא השיעור	הנושאים הנלמדים	שעות לימוד אקדמיות
מפגש 11 - יום ג' 29/6/2021 - 17:00-21:00			
ענן 17:00-17:45	הגנה על מידע בענן ועל ספקי שירותים מנוהלים (XAAS)	<ul style="list-style-type: none"> פתרונות הגנה נפוצים בשרותי ענן תקני סביבת ענן (CSA, SOC2) הגנה על סביבת המידע באמצעות DDoS Protection פתרונות בדיקת קלט 	1
הפסקה			
ענן 18:00-19:45	הגנה על מידע בענן ועל ספקי שירותים מנוהלים (XAAS)	<ul style="list-style-type: none"> הגדרות תצורה נכונות וסוגיית Misconfigurations הפרדת ומידור המידע בענן הבנת הסיכון אליו נחשף הלקוח כתוצאה מהתלות בספק שירות הענן 	1
הפסקה			
תרגול 20:00-21:00	תרגול ביצוע סקר / ביקורת	Case Study	1
מפגש 12 - יום ו' 2/7/2021 - 09:00-13:00			
Hosting 09:00-09:45	שרתי אירוח Hosting	<ul style="list-style-type: none"> שירות אחסון אתרי אינטרנט סוגי השירותים הפרדוקס 	1
הפסקה			
היבטים משפטיים בעת ביצוע מבדק 10:00-10:45	היבטים משפטיים ומגבלות חוקיות בעת ביצוע מבדק	<ul style="list-style-type: none"> תקנים ורגולציה באבטחת סייבר בינ"ל ובישראל נב"ת 362/363 רגולציה, סטנדרטים ותקנים עבור אנשים פרטיות 	1
הפסקה			
חזרה 11:00-11:45	הכנה למבחן	חזרה על החומר	1
הפסקה			
תרגול 12:00-12:45	הכנה למבחן	Case Study + Kahoot!	1
שיחת סיכום	סיכום קורס	סיכום ומשוב לקורס בהשתתפות מרצים ומשתלמים, בסיס לקורס הבא	



המרכז הבינלאומי
ללימודי הייטק וחדשנות

* 6377

מתקדמים
לקריירה בהייטק



Microsoft Partner
Gold Learning



קמפוסים בפריסה ארצית:

באר שבע
רחוב האנרגיה 77
פארק ההייטק

ירושלים
רחוב יפו 34

תל אביב
הפלך 7