SELA

college@sela.co.il | http://sela.co.il/college | 03-6176666

קצין אבטחת מידע ארגוני

בואו ללמוד מהמומחים המובילים, את אחד המקצועות המבוקשים ביותר. התכנים כוללים לימוד מעשי ותרגול רב, המכינים את הבוגר לעבודה בתחום הסייבר, בארגונים גדולים.

Microsoft

Autodesk Authorised Training Centre

Adobe AUTHORISED Training Centre

ISTQB International Software Testing Qualifications Board

בואו ללמוד מהמומחים המובילים, את אחד המקצועות המבוקשים ביותר. התכנים כוללים לימוד מעשי ותרגול רב, המכינים את הבוגר לעבודה בתחום הסייבר, בארגונים גדולים.

משך הקורס 1056 שעות אקדמיות (342 הרצאות ו- 714 מעבדות ופרויקטים)

תיאור כללי

מומחה לוחמת סייבר הוא מקצוע חדש בעולמנו. לשם מענה על צרכי הגנה מיוחדים של ארגונים מול מפגעים ההולכים ומשתכללים לא מספיק לשכור את שרותי איש הרשתות או אף את איש אבטחת המידע, לוחמת סייבר היא בראש ובראשונה הבנת התוקף.

ארגונים רבים מחפשים את השילוב המדובר, אך שילוב זה לא נלמד באוניברסיטה ולא במסלולי לימוד רגילים בהם לומדים או ניהול רשתות מחשב ומתמקדים בתפעול בלבד, או באבטחת מידע ומתמקדים בכלי הגנה בסביבה מאוד מצומצמת.

אם כך פתרון טוב בתחום לוחמת הסייבר הוא הבנה פסיכולוגית וטכנולוגית רחבה, ובמקביל יש להכיר היטב את יעדי התקיפה שהן תשתיות ומערכות המחשוב בארגון, אם כך, לוחם סייבר הוא אדם שיודע ומוכשר לחשוב כתוקף, מכיר את הסביבה והכלים בסביבת המותקף ויודע להשתמש בעיקר בשכלו תוך הטמעת פתרונות במגוון מערכות הארגון ביצירתיות רבה.

הפתרון המתבקש והייחודי להכשרת לוחם סייבר אם כך הוא:

הכשרה טכנולוגית בסביבות מרובות –אך לא נבירה לעומק מיותר, תוך התמקדות קבועה ועקבית בחולשות ופתרונות יצירתיים החל מהשיעור הראשון ועד האחרון, זאת תוך פיתוח יכולות מחשבה והבנה של התוקף אל מול מרכיבי הארגון המגוונים.

הכשרה כזו יכול להעביר רק מי שמומחה לוחמת סייבר עתיר ניסיון הן בשטח והן בהדרכות, זאת הסיבה ש-ד"ר רוני דויטש הוא המרצה המרכזי לאורך המסלול –כולו!

אבטחת מידע ותשתיות הארגון

תחום מערכות המידע רחב וגדול והולך ומתרחב מיום ליום. תוכנות רבות נוספות וישנות בד"כ לא נגרעות מהר ובמקביל. מי שממונה על לוחמת הסייבר ואבטחת נכסי הארגון חייב להכיר את התשתיות והמרכיבים השונים תחילה, אך חייב להכיר גם את שיטות הפעולה והחולשות הרבות מכיוונים שונים כבר בשלבי ההכשרה הראשוניים. מסגרת הכשרה זו משלבת בין הדברים תוך מבט ממוקד על צד התוקף ומספקת לחניך את הפתרונות הבאים:

הכרות עם מגוון טכנולוגיות במערכות מידע ובתשתיות.

הכרות עם חולשות בכול מרכיב ומרכיב.

הכרות עם פתרונות אבטחה בכול רכיב ורכיב.

הכרות עם פתרונות טכנולוגים שמהווים אמצעי עזר למנהל האבטחה.

קהל יעד

- אנשי אבטחה פיזית חרוצים מאוד המוכנים להתאמץ ממש על מנת להבין וליישם יכולות גם בתחום אבטחת מערכות מידע כמקצוע עיקרי או כמשלים לתפקיד הנוכחי.
- מועמדים בעלי מוטיבציה רבה להצלחה.

תנאי קבלה

ראיון אישי, מבדקים ראשוניים, מבדק על פני חודש

רקע בתחום המחשוב, הרשתות והאפליקציות

עיסוק או רקע עמוק בתחום אבטחה פיזית או ניהולו

היקף הלימודים

הלימודים כוללים 900 שעות לימוד אקדמיות, הנחלקות ל:

הרצאות בהיקף של 300 שעות אקדמיות

מעבדות ותרגול מודרך בהיקף של 600 שעות אקדמיות

פירוט משך המסלול

מסלול בוקר: על פני כשנה 1 מפגש בוקר בשבוע בין השעות 8:00-17:00.

מסלול ערב: על פני כשנה 2 מפגשי ערב בשבוע בין השעות 17:30-21:00.

CSW- introduction

קוד: CSWINT
שנה: 1
סמסטר: 1
שעות: 40

מה היא סביבת מחשוב –ומה היא סביבת סייבר ?

- תחנת קצה וציוד קצה: סקירת סוגים ומערכות
- ספק שרות (שרתים): סקירת סוגי שרתים
- תקשורת ותקשורת מחשבים: פנים ארגונית וחוץ ארגונית
- היכרות עם סביבת ה- OT וסביבת ה- ICS
- היבטי כוח אדם: נושאי תפקיד, משתמשים, מנהלים ועוד...

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
16	24	1	0	3

CWS-End stations

קוד: CWSEnd
שנה: 1
סמסטר: 1
שעות: 136

עמדות קצה

- עמדת קצה נייחת (מערכות windows 7\8\10)
- מחשב נייד (מערכות ייעודיות לניידים)
- מחשב כף יד (מערכות גוגל אנדרואיד)
- טלפון סלולארי (מערכות גוגל אנדרואיד)

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
64	72	1	1	2

קוד:	CWSTer
שנה:	1
סמסטר:	1
שעות:	80

CWS- Terminal equipment

נקודות קצה וציוד נוסף

- מדפסת (רשתי)
- מכונת צילום
- פקס
- מצלמת אבטחה
- ועוד...

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
16	64	1	1	0

קוד:	CWSSer
שנה:	1
סמסטר:	1
שעות:	80

CWS- Servers

שרתים ונותני שרות מרכזיים

סביבת LINUX servers and 2008\2012\ LINUX applications

\

Microsoft 2008\2012

- קבצים (סביבת LINUX \Microsoft 2008\2012)
- הדפסה (סביבת LINUX \Microsoft 2008\2012)
- אינטראנט (סביבת LINUX \Microsoft 2008\2012)
- מערכת 2008\2012\ LINUX ACTIVE DIRECTORY\LDAP + מייל (מערכת LINUX\ EXCHANGE)

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
40	40	1	1	2

Database Technologies

קוד: DBtech
שנה: 1
סמסטר: 1
שעות: 48

בסיס נתונים

- בסיס נתונים (בסיס נתונים SQL \ LINUX מבית Microsoft)

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
4	44	1	1	1

CWS- Communication

קוד: CWSComm
שנה: 1
סמסטר: 1
שעות: 80

תקשורת נתונים, סביבת LINUX servers \2012\2008 Microsoft

וברמת

CISCO CCNA

- תשתית פאסיבית
- תשתית אקטיבית
- רכזות ומתגים
- נתבים
- גשרים
- ציוד אלחוטי

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
30	50	1	1	2

קוד:	CWSWar
שנה:	1
סמסטר:	1
שעות:	80

CWS- Warfare

לוחמת סייבר

- מה המשמעות של לוחמת סייבר
- ניתוח אירועים משמעותיים בעולם הסייבר
- רשתות בקרה תעשייתיות ICS מגוונות והקשר לעולם הסייבר
- הכרות עם מגוון כלי תקיפה

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
32	48	1	1	1

קוד:	CWSADV
שנה:	1
סמסטר:	1
שעות:	80

CWS- ADV- Warfare

לוחמת סייבר מתקדם

- שימוש בכלי הערכה וניהול סיכונים
- מדיניות אבטחת מידע
- מרכיבי מערכת הגנה בסייבר (בסיסי)
- כלים טכניים מתקדמים להערכת חולשות סייבר (pen test)
- בניית כלי תקיפה מתקדמים בסביבה מגוונת תוך שימוש בכלי הטעיה

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
24	56	1	1	2

קוד:	CWSFW
שנה:	1
סמסטר:	1
שעות:	64

CWS- FW

חומות אש (CP

,

LINUX

)

- פתרונות של חומות אש בסביבת קוד פתוח
- פתרונות של חומות אש בסביבה בתשלום
- שיטות ניתוח, תקיפה, חבלה והטעיה אל מול חומות אש
- אמצעים לזיהוי אירועים חריגים בחומות האש ותגובה אליהם

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
32	32	1	1	2

קוד:	CWSIDS
שנה:	1
סמסטר:	1
שעות:	64

CWS- IDS

IDPS

מערכות ניטור והתראה בסביבה מתקדמת בעולם הסייבר

- סקירת מערכות ניטור והתראה (SIEM-SIM\SOC-IDS-IPS)
- יישום מערכות ניטור והתראה בסביבת IT, OT, ICS
- שיטות תקיפת של מערכות אלו
- פתרונות לכידה, הטעיה ואיסוף ראיות
- כיצד "למשוך" את התוקף הזדוני
- כיצד לזהות אותו ואת היכולות שלו ומטרותיו

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
32	32	1	1	1

CWS- Forensic

קוד: CWSFo
שנה: 1
סמסטר: 1
שעות: 64

אמצעי חקירה (פורנזיקה) בעולם הסייבר

- מה היא חקירת מחשב?
- אמצעים לחקירת מחשב
- ניתוח סטאטי ודינאמי בסביבות מגוונות
- ניתוח וחקירה של אירועי רשת
- ניתוח וחקירה של מגוון אירועים פליליים

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
32	32	1	1	1

CWS- Standards

קוד: CWSSt
שנה: 1
סמסטר: 1
שעות: 40

תקני אבטחת מידע בעולם הסייבר

רקע, יתרונות, חסרונות והיבטים שונים

- תקן המפקח על הבנקים, הביטוח
- תקנים חיצוניים ISO 17XXX, 27XXX
- באזל 2 ובאזל 3
- ISA
- PCI
- ועוד...
- היבטי יישום, הטמעה, בקרה, עלויות ומשמעויות אבטחה

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
16	24	1	0	0

CWS-Final Project, Thesis

קוד:	CWSFinalPr
שנה:	1
סמסטר:	1
שעות:	200

פרויקט סיום

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
4	196	0	1	0