SELA

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

Cyber - Security & Network

Cyber - Security Incident Response & Cyber Network

Microsoft

Autodesk Authorised Training Centre

Adobe AUTHORISED Training Centre

ISTQB International Software Testing Qualifications Board

Cyber - Security Incident Response & Cyber Network

משך הקורס 990 שעות אקדמיות (330 הרצאות ו- 660 מעבדות ופרויקטים)

להיות מקצוען סייבר

בואו ללמוד בקורס הטוב ביותר להיות איש סייבר מקצועי. זו ההזדמנות שלכם ללמוד בקורס של מכללת סלע, במסגרת קורסי ההייטק של הרשות לחדשנות. אם גם אתם שואפים להצטרף לאחד המקצועות החמים בתעשייה זו ההזדמנות שלכם. במסגרת הקורס תתחילו מאפס ותגיעו בתוך תשעה חודשים לרמה גבוהה הנדרשת כדי לעבוד בתחום. המטרה של הקורס הינה להכשיר אתכם להתחיל עבוד כאנשי סייבר טכניים המסוגלים לתת מענה לחברות וארגונים. הקורס הינו מעשי מאוד והוא כולל עשרות תרגילים ופרויקטים הממחישים את החומר הנלמד. המסגרת של לימודים בחסות הרשות לחדשנות מאפשרת לכם להיות חלק מתחום חדשני ומבוקש תוך כדי קבלת מלגת לימודים של עד 85% משכר הלימוד.

אז למה ללמוד במסלול זה?

סלע הינו מרכז ההדרכה הוותיק ביותר בארץ בתחום המחשבים (קיים משנת 90)

הכשרנו והשמנו עד היום יותר מ- 5,000 בוגרים, אחוז ההשמה של סלע הינו מהגבוהים בשוק ועומד על 77%

לסלע רשימה גדולה של ארגונים איתם היא עובדת לדוגמא צה"ל, אלישרא, רפא"ל, בנק הפועלים ,פיוניר מיקרוסופט, פייסבוק ועוד רבים רבים וטובים

שותף הדרכה של מיקרוסופט העולמית, כותבים ספרות הדרכה עבורם

תוכניות הלימוד שלנו חדשניות ומתעדכנות מול צרכי השוק

עזרה בהשמה לעבודה בסיום המסלול

תיאור כללי

ההסמת הסייבר במכללת סלע הינה המקיפה ביותר בשוק ומתחילה מאפס ומביאה את הלומדים לרמה המקצועית הגבוהה הנדרשת שחברות הייטק וארגונים בטחוניים מחפשים.

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

בתחום לוחמת הסייבר נדרשים הבנה פסיכולוגית וטכנולוגית רחבה כשבמקביל יש להכיר את יעדי התקיפה הפוטנציאליים בארגון. לכן במסלול תלמד להיות לוחם סייבר שיודע לחשוב כתוקף, שמכיר את הסביבה והכלים בסביבת המותקף ויודע להטמיע פתרונות במגוון מערכות ביצירתיות ובחכמה.

מטרות המסלול

הפתרון המתבקש והייחודי להכשרת לוחם סייבר אם כך הוא:

הכשרה טכנולוגית הנפרסת על פני פתרונות רבים, תוך מבט "על" הן מצד התוקף והן מצד המגן, 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 בהדרכה, זאת הסיבה ש-ד"ר רוני דויטש הוא המרצה המרכזי לאורך המסלול –כולו!

אבטחת מידע ותשתיות הארגון

תחום מערכות המידע הולך 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 לסטודנט את הפתרונות הבאים:

לימוד מגוון טכנולוגיות במערכות מידע ובתשתיות.

לימוד חולשות בכול מרכיב ומרכיב.

לימוד פתרונות אבטחה בכול רכיב ורכיב.

לימוד תכנון האבטחה על כלל המרכיבים.

לימוד פתרונות טכנולוגים שמהווים אמצעי עזר למנהל האבטחה.

קהל יעד

- מועמדים בעלי יכולת ומוטיבציה רבה להצלחה.
- מועמדים בעלי רקע טכני אשר מעוניינים לבצע את הסמכת –מיישם סייבר –מערך הסייבר הלאומי
- מועמדים בעלי רקע טכני אשר מעוניינים לבצע את הסמכת –"האקר אתי" - ארגון EC Council
- Ethical Hacker

תנאי קבלה

- אנגלית ברמה של 4 יחידות בגרות
- שליטה במחשב האישי, לרבות, כתיבת מסמכים, שימוש במערכות מייל ועבודה מול מנועי חיפוש
- מעבר מבחן כניסה שנועד לנבא יכולת הצלחה בקורס ובמקצוע. את המבחן ניתן לעשות מרחוק או במכללת סלע. המבחן בשיתוף חברת פילת, החברה המובילה בארץ לאבחון תעסוקתי.
- ראיון אישי

היקף הלימודים

סה"כ 990 שעות לימוד אקדמיות, הנחלקות ל:

הרצאות בהיקף של 330 שעות אקדמיות, תרגול מעשי 320, הכשרה מעשית לתעשייה (OJT) - כ 340 שעות אקדמיות

לימודי בוקר: על פני תשעה חודשים שלושה ימים בשבוע בין השעות 08.30-17.00

מבחני הסמכה

בסיום הקורס ניתן לגשת למבחן "האקר אתי" של ארגון EC Council Ethical Hacker.

שימו לב שרצוי להשקיע בהכנה עצמית נוספת, ממושכת, בדמות מענה על שאלות דוגמה כדי להצליח במבחן זה. לבוגרים יינתנו הסברים וטיפים כיצד להתכונן נכון.

קוד:	Cintro
שנה:	1
סמסטר:	1
שעות:	40

Introductions to Cyberspace

מבואות לתחומי הסייבר

מבוא לאבטחת מידע והגנת הסייבר | תחנת קצה וציוד קצה | סקירת סוגי מערכות | 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

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
20	20	1	0	3

קוד:	Cendpoints
שנה:	1
סמסטר:	1
שעות:	130

Endpoints in the cyber environment

עמדות קצה בסביבת הסייבר

עמדת קצה נייחת | סביבתWindows Linux | פתרונות למערכות ניידות פתרונות למחשבי כף יד | פתרונות לסביבה סלולארית | יסודות מערכות הפעלה | מחשוב ענן בהיבט הלקוח | שירותי אירוח | וירטואליזציה | היבטי אבטחת מידע במערכות הפעלה והקשחת תחנות | הצפנה ואימות | בקרת גישה

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
40	90	1	1	2

קוד:	Cendequ
שנה:	1
סמסטר:	1
שעות:	90

End equipment in the cyber environment

ציוד קצה בסביבת הסייבר

מדפסת (רשתי) | מכונת צילום | פקס | מצלמות אבטחה | אבטחה פיזית | ציוד האזנה ומעקב

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
30	60	1	1	1

קוד:	Cservers
שנה:	1
סמסטר:	1
שעות:	80

Servers and service providers in the cyber environment

שרתים וספקי שרות מרכזיים בסביבת הסייבר

שרתי קבצים ואחסנה | פתרונות הדפסה | פתרונות לאינטראנט ואינטרנט | מערכות זיהוי | אישור מסוג LDAP | מערכות לשירותי E-MAIL ושיתופיות | בסיסי נתונים | BIG - DATA

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
20	60	1	1	2

קוד:	Ccomm
שנה:	1
סמסטר:	1
שעות:	90

Communications and data communications in a cyber environment

תקשורת בסביבת הסייבר

מבוא לתקשורת | תקשורת קווית, אלחוטית, סיבים | תשתית פאסיבית | תשתית אקטיבית | מבנה השכבות | מערך כתובות ה-IP | מתגים, נתבים, גשרים, נתבים אלחוטיים | תקיפה והגנה | שילוב תקשורת בסביבת הסייבר

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
30	60	1	1	3

קוד:	Cwar
שנה:	1
סמסטר:	2
שעות:	130

cyber warfare

לוחמת סייבר

המשמעות של לוחמת סייבר | ניתוח אירועים משמעותיים בעולם הסייבר | רשתות בקרה תעשייתיות ICS והקשר לעולם הסייבר | הכרות עם מגוון כלי תקיפה | 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 תוך שימוש בכלי הטעיה

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
50	80	1	1	2

Filtration systems and firewalls

קוד: Cfiltration
שנה: 1
סמסטר: 2
שעות: 70

מערכות סינון חומות אש

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
30	40	1	1	2

Advanced monitoring and alert systems in the cyber world

קוד: Cadv
שנה: 1
סמסטר: 2
שעות: 70

מערכות ניטור והתראה בסביבה מתקדמת בעולם הסייבר

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
20	50	1	1	2

cyber forensics

קוד: Cfor
שנה: 1
סמסטר: 2
שעות: 70

אמצעי חקירה (פורנזיקה) בעולם הסייבר

מה היא חקירה (Forensic science) בסביבה ממוחשבת? | אמצעים לחקירת מחשב, ציוד קצה, תקשורת ועוד' | ניתוח סטאטי ודינאמי בסביבות מגוונות | ניתוח וחקירה של אירועי רשת | ניתוח וחקירה של מגוון אירועים פליליים

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
20	50	1	1	2

Data security and cyber standards

קוד: Cdata
שנה: 1
סמסטר: 2
שעות: 40

תקני אבטחת מידע וסייבר

והכנה לפרויקט גמר

בניה של סביבת סייבר | לרבות שרתים | שירותי הגנה | סינון | חקירה | לכידה. שימוש בכלי תקיפה להפקת דוחות | שימוש בכלי ניטור על מנת לזהות תקיפה | דימוי מצבים מקביל לסקר סיכונים | שימוש בתקני אבטחה | בניית דוח פגיעות ב- 3 רמות עומק שונות | בהתאם לארגונים שונים | תיקון חולשות אלו תוך שימוש בכלים ללא תשלום | כלים בתשלום | שילובים יצירתיים

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
40	0	0	0	0

Curriculum Vitae

קוד: CV
שנה: 1
סמסטר: 2
שעות: 20

כתיבת קו"ח, הכנה לראיונות עבודה, הכוונה וליווי אישי

הכנת קורות חיים | מעבר על משרות מתאימות בשוק העבודה | היכרות עם אתרי עבודה מובילים | משלוח ראשוני של קורות חיים | הכנה לראיונות עבודה | סימולציות ראיונות עבודה | טיפים למקומות ספציפיים

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
10	10	0	0	0

Final Project: Design + WPF

קוד: FinalProj
שנה: 1
סמסטר: 2
שעות: 160

פרויקט גמר

בניה של סביבת סייבר | לרבות שרתים | שירותי הגנה | סינון | חקירה | לכידה. שימוש בכלי תקיפה להפקת דוחות | שימוש בכלי ניטור על מנת לזהות תקיפה | דימוי מצבים מקביל לסקר סיכונים | שימוש בתקני אבטחה | בניית דוח פגיעות ב- 3 רמות עומק שונות | בהתאם לארגונים שונים | תיקון חולשות אלו תוך שימוש בכלים ללא תשלום | כלים בתשלום | שילובים יצירתיים

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
20	140	0	1	0