SELA

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

קצין לוחמת סייבר-מיקוד טכני

קצין אבטחת מידע ארגוני ומומחה לוחמת סייבר-מיקוד טכני

Microsoft

Autodesk Authorised Training Centre

Adobe AUTHORISED Training Centre

ISTQB International Software Testing Qualifications Board

קצין אבטחת מידע ארגוני ומומחה לוחמת סייבר-מיקוד טכני

משך הקורס 856 שעות אקדמיות (338 הרצאות ו- 518 מעבדות ופרויקטים)

למה ללמוד סייבר במכללת סלע?

>ההסמכה הטכנית המקיפה ביותר בישראל –המעוניינים לעבוד כמומחי סייבר

>הכנה גם להסמכת רשות הסייבר הלאומית וגם להסמכת ethical hacker הבין לאומית

>צוות ההדרכה הבכיר והמנוסה ביותר בישראל

>ניסיון בתחום של מעל 20 שנים

>שיטת CGS, עם ביטוח להצלחה: לא הצלחת - לא שילמת

>הכנה ומימון מבחני הסמכה בינלאומיים יוקרתיים (בכפוף לסיום מוצלח)

>אלפי בוגרים בתחום לוחמת הסייבר בישראל

>ספק מוכר של משרדי ממשלה, להדרכה וייעוץ בתחומי הסייבר

>פיקוח, הנחיה והדרכה ראשית על ידי ד"ר רוני דויטש, מומחה סייבר מהמובילים בארץ

>המסלול מתעדכן פעמיים בשנה לפחות

>המסלול מותאם להכוונת גופי תקינה, אכיפה והכוונה המובילים בישראל ובעולם בתחום

תיאור כללי

מומחה לוחמת סייבר הוא מקצוע חדש. לווחמי הסייבר ומומחי אבטחת נכסי הארגון חייבים להכיר את התשתיות והמרכיבים השונים, את שיטות הפעולה והחולשות של מערכות המחשוב בארגון. לוחם סייבר טוב, זקוק הן להבנה פסיכולוגית והן לידע טכנולוגי רחב. לכן, הסמכת הסייבר במכללת סלע מכשירה לוחמי סייבר מעולים היודעים לחשוב כתוקפים, מכירים את הסביבה והכלים בסביבת העבודה ויודעים לתכנן פתרונות יצירתיים למגוון מערכות. ההסמכה נלמדת בהתאם להנחיות הרשות הלאומית להגנת הסייבר והיא מכינה למבחן הבינלאומי היוקרתי Ethical Hacker של הארגון EC Council.

מטרות המסלול

- 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

- קציני אבטחה ובעלי רקע ביטחוני המעוניינים להתקדם לתחום אבטחת המידע.
- מועמדים בעלי יכולת ומוטיבציה רבה להצלחה.
- מועמדים בעלי רקע טכני אשר מעוניינים לבצע את הסמכת –מיישם סייבר –רשות הסייבר הלאומית
- מועמדים בעלי רקע טכני אשר מעוניינים לבצע את הסמכת –"האקר אתי" של הארגון הבינלאומי: EC Council

תנאי קבלה

- בגרות במתמטיקה ואנגלית בציון 75 ומעלה או ידע מקביל מוכח.
- מבדק ממוחשב.
- הצלחה במבוא הנמשך כחודש.

היקף הלימודים

כ- 12 חודשים

משך ההסמכה

לימודי בוקר: על פני כשנה, יום אחד בשבוע בין השעות 8:30-16:00.

לימודי ערב: על פני כשנה, שני מפגשי ערב בשבוע בין השעות 17.30-21.00.

Introductions to Cyberspace

קוד: Cintro
שנה: 1
סמסטר: 1
שעות: 40

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
16	24	1	0	3

Endpoints in the cyber environment

קוד: Cendpoints
שנה: 1
סמסטר: 1
שעות: 136

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
64	72	1	0	2

End equipment in the cyber environment

קוד: Cendequ
שנה: 1
סמסטר: 1
שעות: 80

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

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

Servers and service providers in the cyber environment

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

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
40	40	1	0	2

Communications and data communications in a cyber environment

קוד: Ccomm
שנה: 1
סמסטר: 1
שעות: 128

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
34	94	1	0	3

cyber warfare

קוד: Cwar
שנה: 1
סמסטר: 1
שעות: 160

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
56	104	1	0	2

Filtration systems and firewalls

קוד: Cfiltration
שנה: 1
סמסטר: 1
שעות: 64

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	0	2

Advanced monitoring and alert systems in the cyber world

קוד: Cadv
שנה: 1
סמסטר: 1
שעות: 64

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	0	2

cyber forensics

קוד: Cfor
שנה: 1
סמסטר: 1
שעות: 64

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
32	32	1	0	2

Data security and cyber standards

קוד: Cdata
שנה: 1
סמסטר: 1
שעות: 40

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

שעות הרצאה	שעות מעבדה	מבחנים	פרוייקטים	הגשות
16	24	1	0	2