COURSE BROCHURE

2019

TRAINING COURSE

קורס

מיישם סייבר

[CSP®]

Cyber Security Practitioner

Titans Security College

תוכן עניינים

מידע כללי 3

על הקורס

מטרת הקורס

מדוע קורס זה חיוני לכל העוסק בתחום הגנת הסייבר?

קהל יעד

תעודת גמר

שיטות הדרכה ומבנה הקורס 5

כללי

מבנה הקורס

חומר עזר

מתכונת ומשך הקורס

ערכת הלימוד שלנו

מעבדות

נושאי הלימוד 7

כללי

חלק א'

חלק ב'

חלק ג'

חלק ד'

חלק ה'

לוגיסטיקה 32

מיקום הקורס

שעות תרגול במעבדה

ספריה דיגיטלית

ספריית המכללה

תוכנית מנטור אישי

מלגות

הטבות לבוגרים שלנו

ולסיכום

אודות קבוצת טיטנס סקיוריטי 34

אודות הקבוצה

חברות בקבוצה

סגל המרצים

הטבות לבוגרים שלנו

מסלולי המשך 37

כללי

קורסים נוספים

מידע כללי

על הקורס

מכללת TS-College חיברה את המסלול הייחודי להכשרת מיישם סייבר, בהתאם לדרישות אסדרת מקצועות הסייבר של מטה הסייבר, במשרד ראש הממשלה, במטרה להכשיר את דור העתיד של מקצועני הסייבר בישראל. סגל היועצים האקדמיים בשילוב עם היועצים הבכירים שלנו בנו מסלול ייחודי הכולל ידע תיאורטי וידע מעשי בתחום הגנת הסייבר, הכולל תרגולים רבים באופן עצמאי ובכיתה, במטרה להכין את הבוגרים להשתלבות מהירה בשוק העבודה.

מטרת הקורס

מטרת הקורס הינה להקנות למשתתפי הקורס את כל הידע (התיאורטי והמעשי) שנדרש מתפקידו של מיישם סייבר, על מנת לאפשר קליטה מהירה אל שוק העבודה במשק הישראלי.

מדוע קורס זה חיוני לכל העוסק בתחום הגנת הסייבר?

- הקורס עומד באופן מלא בדרישות אסדרת מקצועות הסייבר, של מטה הסייבר במשרד ראש הממשלה.
- הקורס מכין את בוגריו באופן מלא לבחינת ההסמכה של מיישם סייבר, אשר תחול בשנת 2018.
- הקורס מכין את בוגריו לקראת קליטה מהירה לשוק העבודה במשק הישראלי.

קהל יעד

הקורס מיועד ליועצי מחשוב, מבקרי מערכות מידע, מנהלי רשתות, אנשים סיסטם, אנשי תקשורת, בוגרי תואר אקדמי בתחום מערכות מידע, בוגרי מסלולים מקצועיים (כגון CCNA®, CCNP®, MCITP®, Security+® וכדומה), בוגרי תואר אקדמי בתעשייה וניהול אשר רוצים לעשות הסבה לעולם הסייבר, ולכל הרוצה לעסוק בתחום הגנת הסייבר.

מידע כללי

תעודת גמר

לעומדים בדרישות הקורס, יהיו זכאים לקבל תעודת הסמכה של "מיישם סייבר"(CSP®), ויהיו זכאים לגשת לבחינות ההסמכה של מטה הסייבר בשנת 2019. בנוסף, בוגרי הקורס יוכלו לגשת לבחינות ההסמכה הבינלאומיות של:

- SSCP® (Systems Security Certified Practitioner) - מבית ISC2®
- A + - מבית COMPTIA®
- Security + - מבית COMPTIA®
- Network + - מבית COMPTIA®
- Cybersecurity Analyst מבית COMPTIA®

דרישות סף

- רקע בסיסי בתחום המחשוב רלוונטיות בסיסיות.
- ידע בסיסי באנגלית
- ראיון אישי עם הסגל האקדמי שלנו

הערה: למועמדים שאין להם ניסיון נדרש ולא עומדים בדרישות הקורס, תינתן אפשרות להשתתף במכינת IT של מכללת TS-College, ללא עלות נוספת (מותנה בהרשמה לקורס מיישם סייבר).

שיטות הדרכה ומבנה הקורס

כללי

קורס זה נבנה באופן ייחודי ובלעדי למכללת TS-College, במטרה להכין את בוגרי הקורס להסמכה של "מיישם סייבר", הסמכה שגובשה ע"י מטה הסייבר במשרד ראש הממשלה. קורס זה נבנה על בסיס ידע וניסיון מצטבר של למעלה מ-20 שנה של הכשרת אלפי בוגרים מכל מגזרי המשק (בארץ ובחו"ל) ע"י סגל המרצים הבכיר שלנו וידע אקדמי ומחקרי של סגל המרצים שלנו בתחומי הניהול והגנת הסייבר. הקורס מביא למשתתפיו בעיקר ידע וניסיון מעשי הן של קבוצת טייטנס סקיורטי כחברת ייעוץ מובילה בתחום אבטחת המידע והגנת הסייבר והן של סגל המרצים והמנחים בקורס, המבוסס ברובו על מנהלי אבטחת מידע ויועצים בכירים במשק הישראלי ובעולם. כל אחד מהמרצים מביא עימו ניסיון עשיר בניהול תחום אבטחת המידע והגנת הסייבר, התמודדות עם אנשים, תהליכים וטכנולוגיות בעולם הגנת הסייבר, בארגונים גדולים ומורכבים ומשתפים לקחים מהצלחות וכישלונות בפרויקטים מסוגים שונים. בנוסף לרשימת המרצים המרכזיים בקורס, שמופיעה בחוברת זו, יופיעו בפני משתתפי הקורס גם מנהלי אבטחת מידע ויועצים בכירים מהארץ ומחו"ל, אשר ישפכו אור על תפקיד מיישם סייבר מזוויות שונות, במטרה לחדד את הציפיות של הנהלת הארגון והלקוחות מדרישות התפקיד של מיישם סייבר, כישוריו, תכונותיו ואופן התנהגותו בשטח.

מבנה הקורס

הקורס נבנה בצורה ייחודית ובלעדית למכללה, ומחולק ל-5 חלקים עיקריים:

- חלק א' – הרצאות פרונטאליות
- חלק ב' – תרגול עיוני ומעשי בקבוצות
- חלק ג' – מעבדות
- חלק ד' – עבודות הגשה ופרויקט גמר
- חלק ה' – בחינת סיום (עיונית ומעשית)

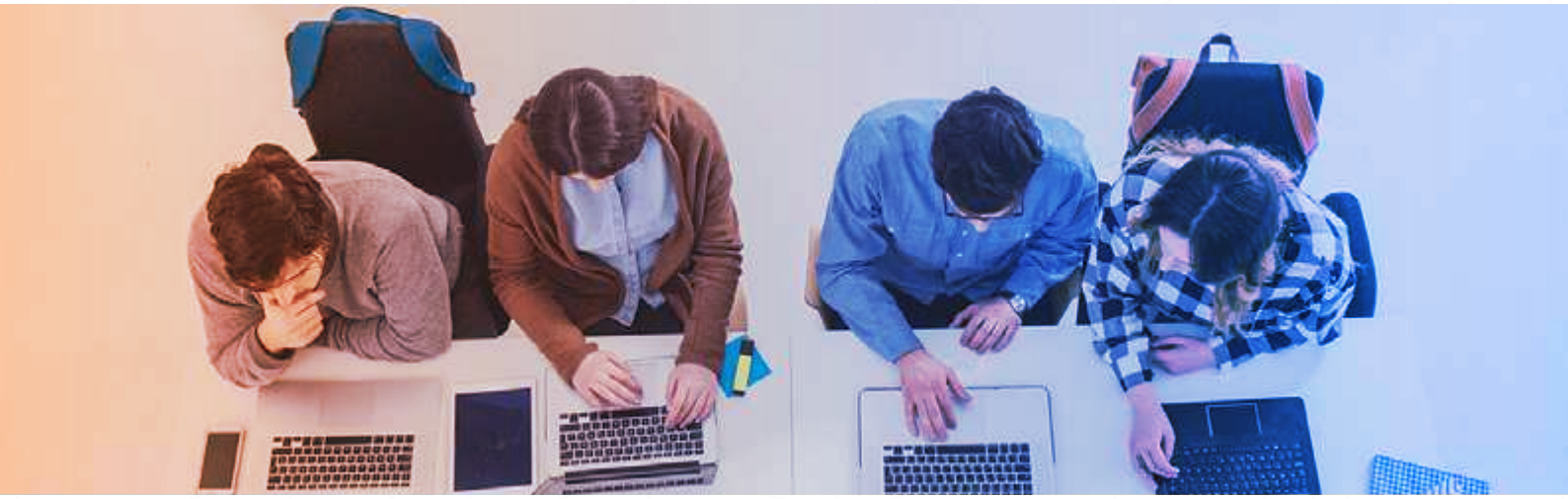
חומר עזר

כל משתתף בקורס יקבל חומר עזר רב עפ"י נושאי הלימוד בקורס, הכולל בין היתר:

- ספרי לימוד
- ספרי תרגול
- בחינות דמי
- דיסק DVD הכולל כלים ומעבדות
- מצגות דיגיטליות
- ועוד חומרים רבים

מתכונת ומשך הקורס

אורך הקורס הינו 300 שעות פרונטאליות, ועוד כ-500 שעות תרגול חופשי (מעבדות ועבודות בית). במסגרת הקורס, התלמידים ייחשפו לפרויקטים אמיתיים, ויהיו מעורבים בביצוע פרויקטים אמיתיים אצל לקוחות חברת הייעוץ המובילה TS-Consulting, לצורך צבירת ניסיון ובחינת הידע התיאורטי והמעשי שנרכש במהלך הקורס.



ערכת הלימוד שלנו

ערכת הלימוד שלנו הינה עשירה ומגוונת הן ברמת התכנים, והן ברמת האיכות והנוחות, שסגל המרצים שלנו עמל רבות על מנת להקל על תהליך הלמידה שלכם בקורס. להלן תכולת ערכת הלימוד לקורס מיישם סייבר:

- ספרי לימוד
- ספרי תרגול
- בחינות לדוגמא
- תרגולים לדוגמא
- מעבדות
- DVD הנושא כלים וחומרי לימוד רבים
- מערכת LMS ייחודית
- ועוד חומרים מקצועיים רבים

מעבדות

קורס מיישם סייבר מחבר את העולם התיאורטי עם העולם המעשי, ולכן במסגרת הקורס וגם מחוצה לו, המשתתפים יתרגלו שעות רבות בתחומים שונים ומגוונים עפ"י נושאי הלימוד בקורס.

הערה: חובה להגיע לשיעורים עם מחשב נייד. (הודעה זו מתייחסת לתלמידים אשר ביצעו הרשמה לקורס עם ערכת הלימוד הבסיסית בלבד).

מתנה לכל נרשם

ספר סיקור טכנולוגיות אבטחת מידע, מהדורה 2 (2017) -ספר ייחודי ובלעדי (הוצאת TS-MEDIA) שמרכז את כל טכנולוגיות אבטחת מידע והגנת הסייבר, בצורה מקצועית ומסודרת. הספר בשפה העברית, ומכיל מידע רב אודות טכנולוגיות אבטחת המידע כגון פירוולים, NAC, IPS, SIEM , DLP, ועוד.

נושאי הלימוד

כללי

הקורס מיישם סייבר נועד לספק את כל הידע התיאורטי והמעשי שנדרש לאנשים שרוצים לעסוק בתחום הגנת הסייבר. הקורס נבנה בהתאם לדרישות מטה הסייבר, עפ"י תהליך אסדרת מקצועות הסייבר בישראל, ומכין את משתתפי הקורס לעמידה בדרישות הבחינה למיישם סייבר שעתידה להיות זמינה לציבור במהלך שנת 2019. הקורס עומד בדרישות הסילבוס כפי שפורסם ע"י מטה הסייבר במשרד ראש הממשלה, ומכין את משתתפי הקורס באופן מלא לבחינות ההסמכה של מיישם סייבר. הסילבוס מתייחס ל-24 פרקים (מודולים) עיקריים, כדלהלן:

מודול	נושאי לימוד מודול עיקריים בקורס	שעות לימוד תיאורטי	שעות לימוד מעשי
1	מבוא לאבטחת מידע והגנת הסייבר	16	
2	תקני אבטחת מידע וניהול סיכונים	8	2
3	מבנה המחשב	2	
4	יסודות מערכות הפעלה	12	4
5	5 יסודות תקשורת מחשבים – חלק א' 4	4	
6	יסודות תקשורת מחשבים – חלק ב'	12	12
7	הגנת גישה בתקשורת ואינטרנט	20	10
8	בידול והפרדת רשתות תקשורת	4	4
9	היבטי אבטחת מידע בציוד תקשורת (הקשחה) ואבטחת מידע	8	8
10	הצפנה ואימות	12	4
11	בקרת גישה	10	4
12	היבטי אבטחת מידע במערכות הפעלה והקשחות שרתים	20	20
13	היבטי אבטחת מידע במסדי נתונים	8	3
14	תוכנות זדוניות וזיהוי אנומליות	12	6
15	דלף מידע	4	2
16	ניהול ורישום אירועי אבטחת מידע (Audit)	6	2
17	טיפול באירועי אבטחת מידע	6	4
18	מחשוב ענן, שירותי אירוח, וירטואליזציה	4	
19	שינוע מידע מ/אל הארגון	2	
20	ניהול המשכיות עסקית והתאוששות מאסון (DRP/BCP)	4	4
21	אבטחה אפליקטיבית	8	
22	מתודולוגיות ביצוע ניסיונות חוסן (תשתיתי ואפליקטיבי)	8	10
23	חוק ואתיקה	8	1
24	אבטחה פיזית	2	
סה"כ שעות קורס		200	100

חלק א'

הרצאות פרונטאליות

החלק הראשון מכיל את ההרצאות הפרונטאליות, בהן סגל המרצים שלנו יפרסו את כלל הידע והניסיון שלהם שנרכש במשך עשרות שנים, וינסו להעבירו בצורה אפקטיבית ויעילה למשתתפי הקורס. להלן הנושאים העיקריים שיילמדו במהלך הקורס (עפ"י דרישות הסילבוס של מטה הסייבר).

מודול 1

מבוא לאבטחת מידע והגנת הסייבר

16 שעות

כללי:

מודול זה חושף את משתתפי הקורס לעולמו הנפלא של תחום אבטחת המידע והגנת הסייבר, ומכיל התייחסות למרכיבים רבים שיחדיו מרכיבים את עולמו של מיישם הסייבר.

מטרת המודול:

מודול זה נועד לחשוף את משתתפי הקורס לעולם אבטחת המידע והגנת הסייבר, ומכיל מידע רב אודות מרכיבים רבים בעולם אבטחת המידע.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- אונטולוגיה של אבטחת המידע והגנת הסייבר: מונחים ויסודות אבטחת המידע והגנת הסייבר, איומים, קשרים בין המונחים השונים, תפיסת NIST® (מכון התקנים האמריקאי) לעולם אבטחת המידע והגנת הסייבר (כולל התייחסות למסגרות השונות שמכון התקנים האמריקאי גיבש והפיץ), תפיסת האיכות (Quality Assurance) ותקני האיכות השונים הקשורים לעולם אבטחת המידע, ואונטולוגיות אחרות.
- התייחסות לסוגי תקיפות לרבות תקיפות מחשבים ורשתות מחשוב מתוך הארגון ומרחוק, וכמו כן גם התייחסות לחדירה פיזית למתחמי וחדרי מחשב (Data Center) והטמנת ציוד האזנה.
- התייחסות להינדוס אנושי (Engineering Social), תוך ביצוע בתקיפות משולבות ע"י שימוש במייל (תקיפות פישינג ו-Phishing Spear באמצאות הדואר האלקטרוני), הפניה לאתרים נושאי תוכנה זדונית, ועוד.
- התייחסות לסוגי פגיעות במערכות מחשוב ובמידע ו\או תהליכים עסקיים קריטיים בארגון, בהתייחס למרכיבים של שלמות הנתונים, סודיות הנתונים וזמינותם.
- השלכות התמודדות ארגוניות – התייחסות למרכיבים כגון מינוי בעלי תפקידים בתחום אבטחת המידע והגנת הסייבר, הגדרת מדיניות ונהלים, הגדרת נכסי מידע ומערכות חיוניות, תהליך של ניהול סיכונים, אבטחה פיזית וסביבתית.
- התייחסות למרכיב האנושי ובדיקות מהימנות לעובדים – התייחסות לנושא הגברת המודעות בקרב העובדים לנושא אבטחת מידע והגנת הסייבר, הטמעת המודעות בתרבות הארגונית, מימוש תהליכים לדיווחים ובקרות, והכרות עם גופים לאומיים העוסקים בתחום בישראל.
- אפיון, גיבוש והטמעת מדיניות ונהלים של אבטחת מידע והגנת הסייבר, לרבות אסטרטגיה ומסגרות לניהול תחום הגנת הסייבר.
- התייחסות לאבטחת מידע בפרויקט, הטמעת היבטי אבטחת מידע במחזור החיים לפיתוח תוכנה, לרבות השלבים של הפצה לסביבת הייצור וניהול ובקרת שינויים.

מודול 2

תקני אבטחת מידע וניהול סיכונים

8 שעות

כללי:

מדובר במודול שעוסק בתיאור תקני אבטחת המידע והמלצות (Practices Best), המקובלים בתחום אבטחת המידע והגנת הסייבר. בפרק זה משתתפי הקורס ייחשפו ליסודות ביצוע סקרי סיכונים, וילמדו כיצד מתבצע סקר סיכונים ומה מטרותיו, מהם הפעילויות להקטנת הסיכון, וילמדו את משמעות המושגים של סיכון (Risk), סיכון שיורי (Risk Residual) ותאבון הסיכון (Appetite Risk).

מטרת המודול:

מודול זה נועד לחשוף את משתתפי הקורס לעולם התקנים והמסגרות שקיימות בתחום אבטחת המידע והגנת הסייבר, ביסודות ביצוע סקרי סיכונים, ותהליך ניהול סיכונים. בסיום הקורס, על הלומד להכיר את התקנים והמסגרות השונות, להבין מה הסיבה והיתרון המתקבל מקיומם, כיצד הם משפרים את ההגנה על הארגון, מהם חסרונותיהם, וההבדלים בין הסטנדרטים. כמו כן, על הלומד להכיר היטב את משמעותם של המושגים סיכון, תהליך ומטרות ביצוע סקרי סיכונים, ופעילות להקטנת סיכונים.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- הכרות עם הסטנדרטים המקובלים בעולם אבטחת המידע והגנת הסייבר, ממשפחת התקנים של 27000 כגון תקן אבטחת מידע (ISO 27001), תקן אבטחת מידע רפואי (ISO 27799), תקן סייבר (ISO 27032) תקן אבטחת מידע במחשוב ענן (27017), תקן פרטיות מידע בענן (ISO 27018), ועוד.
- סטנדרטים ותקנים בעולם ניהול והערכת סיכונים, כגון ISO 31000 (ניהול סיכונים), ISO 31010 (הערכת סיכונים), ISO 27005 (ניהול סיכונים), מסגרת NIST 53-800 (הערכת סיכונים), מסגרת NIST 30-800 (ניהול והערכת סיכונים), מסגרת NIST 37-800 (ניהול סיכונים), מסגרת OCTAVE (ניהול סיכונים), מסגרת CRAMM (ניהול סיכונים), ועוד.
- התייחסות למתודולוגיות ושיטות לביצוע סקרי סיכונים.
- התייחסות לשלבים השונים של ביצוע סקרי סיכונים.
- התייחסות ליעדים של סקרי סיכונים, כולל KRI (Key Indicators Risk).
- התייחסות לסוגי הסקרים, כגון סקר כמותי (Quantitative), איכותי (Qualitative) ו\או משולב.
- התייחסות לנושא הסקרים – אפליקציות, תשתיות, למערכות האבטחה, שילוב סקרים ועוד.

מודול 3

מבנה המחשב והכרת כל מרכיביו

2 שעות

כללי:

מדובר במודול שחושף את משתתפי הקורס במבנה המחשב ומרכיביו השונים, אשר השלכות רבות בתחום אבטחת המידע והגנת הסייבר. במודול זה, הלומד יכיר את יסודות מבנה המחשב בהיבטים של חומרה, מבנה סכמתי ותפקידי הרכיבים השונים, וגם ייחשף למתקפות ידועות על חלק מהרכיבים (דוגמא מתקפה על ה-BIOS והזיכרון). העתיד של עולם אבטחת המידע עובר משכבת האפליקציה לחומרה, ולכן ישנה חשיבות רבה שמשתתפי הקורס יכירו את מבנה המחשב ואת מרכיביו השונים. כמו כן, בתחום התחקור הדיגיטלי, הכרות טובה עם מרכיביו השונים של המחשב יכול לסייע ללומד להתמודד טוב יותר עם האתגרים של שחזור מידע.

מטרת המודול:

בסיום הקורס, הלומד אמור להכיר את רכיבי החומרה העיקריים ואת תפקידם. בנוסף, אמור הלומד להכיר מספר תקיפות ומאפייני תקיפות מול הרכיבים הרלוונטיים.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- הכרות עם חלקי המחשב השונים, כגון סוגי הזיכרון (ROM, RAM), המעבד וסוגיו (CPU), אמצעי אחסון, ומושגים נוספים כגון ALU, GPU, BIOS ועוד.
- הכרות עם UEFI (Unified Extensible Firmware Interface)
- הכרות עם תפקיד של כל רכיבי המחשב, המבנה הסכמתי של המחשב, אופי הקישור בין הרכיבי (BUS), הקישור בין כל הרכיבים ועוד.
- הכרות עם מתקפות ידועות על חלק מהרכיבים (לדוגמא מתקפה על ה-BIOS, והזיכרון).

מודול 4

יסודות מערכות ההפעלה

12 שעות

כללי:

מודול זה מיועד להכיר למשתתפי הקורס את יסודות מבנה מערכות ההפעלה, ארכיטקטורות שונות, ואופן הקישור בין החומרה לתוכנה.

מטרת המודול:

בסיום הקורס, הלומד אמור להכיר את רכיבי מערכת ההפעלה, הארכיטקטורה הבסיסית והיתרונות והחסרונות שבהן.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- ארכיטקטורה בסיסית של מערכות ההפעלה.
- הכרות עם הרכיבים המרכזיים (דוגמת DLL של WIN) של כל מערכת הפעלה, מבין המערכות הפעלה הבאות: VM, Android, Windows, Unix.
- כיצד מערכת ההפעלה נפרסת בזיכרון במחשב, כולל התייחסות למימוש זיכרון וירטואלי (Memory Virtual).
- אופן הקישור בין התוכנה לחומרה (לדוגמא HAL של אנדרואיד).
- מהם ההבדלים בין מערכות ההפעלה השונות.

מודול 5

יסודות תקשורת מחשבים – חלק א'

4 שעות

כללי:

מודול זה מיועד להכיר למשתתפי הקורס את יסודות תקשורת המחשבים, מדוע נדרשים שכבות בתקשורת, מהם סוגי רשתות התקשורת השונות ומהם ההבדלים ביניהן, הכרות עם ציוד תקשורת, תפקידו והשכבות בהן הוא פועל (מתוך מודל השכבות-OSI).

מטרת המודול:

בסיום הקורס, הלומד אמור לדעת את סוגי רשתות התקשורת, מה ההבדלים ביניהן, וסוגי מימוש של רשתות תקשורת אלו.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- מודל 7 השכבות (מודל OSI)
- רכיבי תקשורת – מתג (Switch), נתב (Router)
- סוגי רשתות – רשת מקומית (LAN), רשת מרחבית (WAN), רשת אלחוטית (Bluetooth, Wireless).

מודול 6

יסודות תקשורת מחשבים – חלק ב'

12 שעות

כללי:

מודול זה מתמקד בפרוטוקולי התקשורת המרכזיים, שימושם והיבטי אבטחה של כל פרוטוקול בשכבותיו השונות (של מודל OSI). בנוסף, הלומד יתבקש ללמוד את הקשרים בין הפרוטוקול לציוד התקשורת, והשכבות בהן הפרוטוקול פועל, חולשות שהתפרסמו, איומים ומתקפות, ודרכי התמודדות.

מטרת המודול:

בסיום הקורס, הלומד אמור לדעת את סוגי הפרוטוקולים השונים, לציין את תפקידם, היבטי אבטחת מידע וחולשות מרכזיות, ומי מפעיל איזה פרוטוקול. אין חובה לדעת את נבכי הפרוטוקול כפי שמופיע ב-RFC.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- תיאור הפרוטוקולים
- שימושים והיבטי אבטחה – חולשות שהתפרסמו.
- פרוטוקולים: IP/TCP, UDP, FTP, HTTP, SNTP, RIP, SIP, SNMP, ICMP, DNS, RADIUS, ARP, RARP.

מודול 7

הגנת גישה בתקשורת ואינטרנט

20 שעות

כללי:

מודול זה מתמקד במנגנוני ההגנה של רשתות המחשבים שבארגון, מוצרי אבטחת מידע, גישה מרחוק למשאבי הארגון וההגנה על דרכי גישה אלו, היבטי אבטחה בעת קישור הארגון לרשת האינטרנט, מימוש מנגנוני אבטחה ושימוש בפרוטוקולים אפליקטיביים של השכבות הגבוהות במודל (OSI 7) שכבות. כמו כן, בקורס ידונו הפרוטוקולים המרכזיים, שימושם והיבטי אבטחה של הפרוטוקולים הללו, כולל התייחסות למנגנוני אבטחה נאותים.

מטרת המודול:

בסיום הקורס, על הלומד לדעת את מנגנוני ההגנה המתאימים לכל דרך גישה למשאבי הארגון, היבטי אבטחת מידע וחולשות מרכזיות, מה הבעייתיות שבקישור הרשת הארגונית כולה ו/או חלקה לרשת האינטרנט, מימוש מנגנוני הגנה נאותים, שימוש בסוגי הפרוטוקולים השונים המשמשים לקישור אפליקטיבי, ולציין את תפקידם, היבטי אבטחת מידע וחולשות מרכזיות, ומי מפעיל איזה פרוטוקול. אין חובה לדעת את נבכי הפרוטוקול כפי שמופיע ב-RFC.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- מוצרי אבטחה והגנה ברמת הרשת (WAN/LAN), והרשתות האלחוטיות (Bluetooth, Wireless).
- גישה מרחוק למשאבי הארגון וההגנה על דרכי גישה אלו.
- טיפול בגישה באמצעות מחשבים/ מכשירים ניידים - דוגמת טלפונים חכמים וטאבלטים.
- הגדרת VLAN-ים בציוד תקשורת.
- היבטי אבטחת מידע ברשתות הארגון, בעת קישור הרשת הארגונית לאינטרנט.
- היכרות עם מוצרי אבטחת מידע שונים (פירוולים, DLP, NAC, IPS, פירוול אפליקטיבי, SIEM, EPS, וכלים נוספים).
- בניית רשת DMZ (לצורך חשיפה של שירותים שונים כגון FTP, MAIL, WEB וכו').
- תיאור הפרוטוקולים האפליקטיביים כגון HTML5, WebRTC, HTML3 וכו'.
- שימוש בפרוטוקולים אלו, והיבטי אבטחת מידע – חולשות שהתפרסמו.
- השלמה לבידול בין רשתות – נושאי הסינון תוכן (Web and Content Filtering), ושימוש באמצעי אבטחה נאותים כגון WAF (Web Application Firewall)

מודול 8

בידול והפרדת רשתות תקשורת

4 שעות

כללי:

מודול זה מתמקד במנגנונים ומוצרים שמטרתם לאפשר הפרדת רשתות בצורה מאובטחת, בין אם מדובר ברשתות פנים-ארגוניות ובין אם מדובר ברשת הארגונית כלפי העולם החיצון.

מטרת המודול:

בסיום הקורס, על הלומד לדעת את מנגנוני הבידול המתאימים עפ"י הדרישות העסקיות והתפעוליות של הארגון, מהם היתרונות והחסרונות, היבטי אבטחת מידע וחולשות מרכזיות, וכיצד יש להקשיח את רשת התקשורת מפני מתקפות מבפנים (מתוך הארגון) ומבחוץ.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- מדוע נדרש הבידול, יסודות תיאורטיים של הבידול והפרדת הרשתות.
- כיצד מבטיחים שיחד עם ההפרדה יהיה ניתן לאפשר לעובדים לממש את תפקידם בצורה יעילה ואפקטיבית (מבלי לפגוע בפרודוקטיביות שלהם).
- הכרות עם מוצרים ומנגנונים המשמשים להפרדה ובידול בין סביבות עבודה שונות (רשתות תקשורת).
- ניטור המידע העובר בין הרשתות דוגמת פירוול, שרתי פרוקסי (Proxy), שרתי Relay Mail, שרתי סינון תוכן (Filtering Content), פירוול XML לסינון תוכן בשכבת האפליקציה, מוצרי Gap Air ועוד.
- הקשחת רשת התקשורת הארגונית

מודול 9

הצפנה ואימות

12 שעות

כללי:

מודול זה מתמקד ביסודות ההצפנה ופרוטוקולי אימות נתונים. בנוסף, ילמדו משתתפי הקורס פרוטוקולי התקשרות המשמשים לאימות משתמשים ושימושם והיבטי אבטחה של כל פרוטוקול ופרוטוקול. התלמידים ילמדו גם את הקשרים בין הפרוטוקולים השונים לציוד התקשורת, והשכבות בהם הפרוטוקול פועל.

מטרת המודול:

בסיום הקורס, על הלומד לדעת את סוגי הפרוטוקולים השונים, לציין את תפקידם, להכיר את היבטי אבטחת המידע והחולשות המרכזיות, ומי מפעיל איזה פרוטוקול.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- הצפנה סימטרית ושימוש בפרוטוקולים להצפנה סימטרית (כגון AES).
- הצפנה אסימטרית ושימוש בפרוטוקולים להצפנה אסימטרית (כגון Hellman-Diffie, RSA).
- תשתית PKI
- יסודות CA (Certificate Authority), לאימות קצוות תקשורת וזיהוי משתמשים.
- פרוטוקולי תקשורת התומכים בנושא של הצפנה ואימות כגון IPSEC, SSL, TLS, SSH.

מודול 10

היבטי אבטחת מידע במערכות הפעלה והקשחת שרתים

20 שעות

כללי:

מודול זה מספק לתלמידים הכרות עם היבטי אבטחת המידע במערכות ההפעלה השונות, ומאפשר להם להכיר את העקרונות של הקשחת השרתים והשירותים השונים המטופלים במסגרת תהליכי ההקשחה.

מטרת המודול:

בסיום הקורס, על הלומד לדעת את ההיבטים המרכזיים של אבטחת המידע בכל מערכת הפעלה, להכיר את החולשות המרכזיות הקיימות בכל מערכת, להכיר מתקפות ידועות, ותהליכי הקשחה למערכות הפעלה שונות, להכיר את התהליכים השונים והשירותים הניתנים ע"י מחשב מוקשח, וכיצד ניתן לאפשר שירותים שונים על גבי מחשב מוקשח מבלי לפגוע בפרודוקטיביות של השירותים אותם הוא מספק.

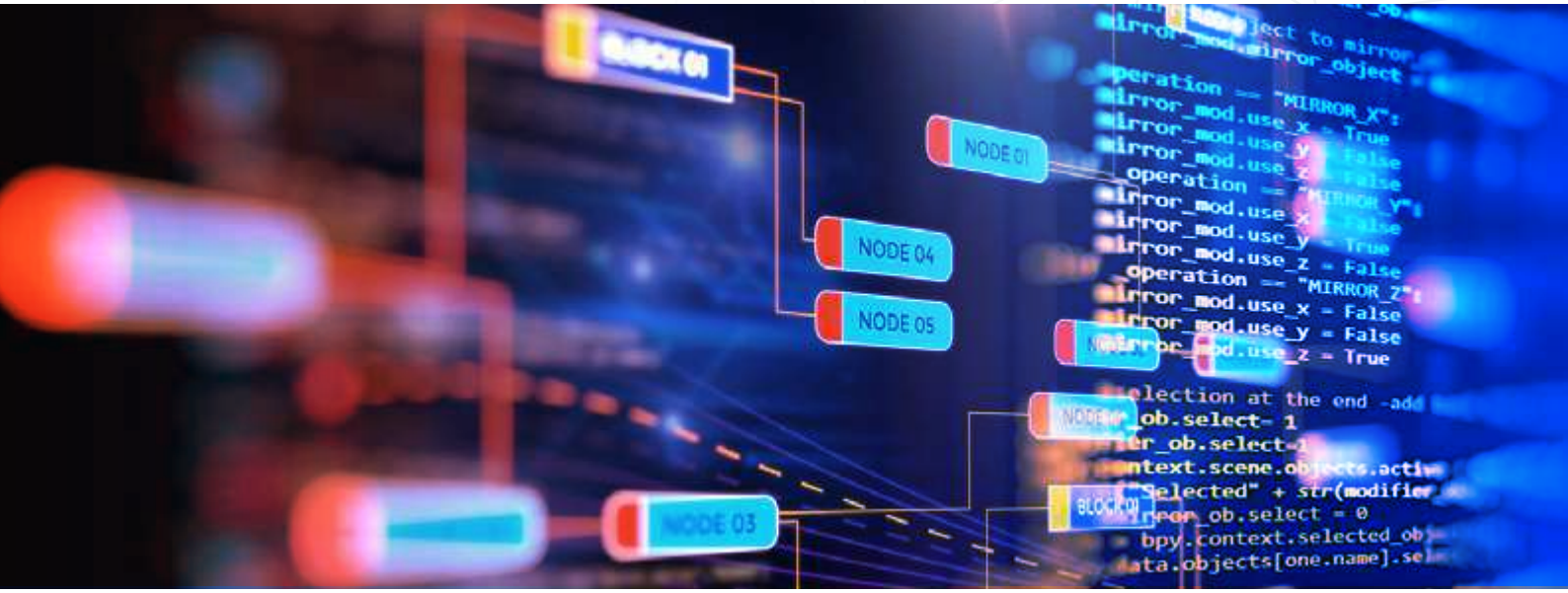
להלן הנושאים העיקריים אשר יילמדו במודול זה:

- מימוש אבטחת מידע במסגרת שירותי מערכות הפעלה הבאות: VM, ANDROID, WINDOWS, UNIX
- יסודות תהליכי זיהוי ואימות משתמשים, כגון שימוש ב-KERBEROS, מתן הרשאות ל-Objects ו-Subjects לקבצים, לקבוצות משתמשים, ועוד.
- שימוש בלוגים של מערכת ההפעלה התומכים בהיבטי אבטחת מידע.
- חלק תיאורטי של מדוע נדרש לבצע הקשחת שרתים, ומהם העקרונות של תהליך הקשחת השרתים.
- תהליך הקשחה תלוית סביבות עבודה ושירותים עסקיים\תפעוליים.
- מהם הפעולות הבסיסיות בסביבת מערכות ההפעלה השונות (VM, ANDROID, WINDOWS, UNIX).
- עדכון תוכנה, חומרה\קושחה לשרתים מוקשחים.
- בדיקת הקשחות לשרתים.
- הכרות עם מוצרים התומכים בתהליך ההקשחה.
- תיאום עם מוצרי אבטחה לצורך דיווח על זיהוי אנומליה בשרתים\מערכת הפעלה.

מודול 11

היבטי אבטחת מידע במסדי נתונים

8 שעות



כללי:

מודול זה מיועד להכיר לתלמידים את היבטי אבטחת המידע במערכות ומסדי נתונים, כולל הכרות עם חולשות, איומים ומנגנוני הגנה על מסדי הנתונים.

מטרת המודול:

בסיום הקורס, על הלומד לדעת את ההיבטים המרכזיים של אבטחת מידע במסדי נתונים כאמור לעיל, להכיר את החולשות המרכזיות הקיימות במערכת ומסדי הנתונים, את דרכי ההתמודדות עם איומים אלו, מוצרי הגנה משלימים ומתקפות ידועות.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- יסודות וסוגי מסדי נתונים: SQL, MySQL, MongoDB.
- ארכיטקטורה של בסיסי נתונים.
- היבטי אבטחת מידע כגון תהליך מתן הרשאות וניהול משתמשים.
- איתור חולשות ידועות והכרות עם מתקפות על בסיסי נתונים.
- תמיכת מערכת ההפעלה בשמירה על מסדי נתונים, תמיכת תוכנת מסד נתונים בנושאי אבטחת מידע.
- מוצרים משלימים להגנה על בסיסי נתונים.
- מערכות אחסון (Storage) והיבטי אבטחת מידע.

מודול 12

ניהול המשכיות עסקית והתאוששות מאסון (DRP/BCP)

4 שעות

כללי:

מודול זה מיועד להכיר לתלמידים את נושא הגיבוי, השחזור ותהליכי ההתאוששות מאסון על היבטיו וברמות השונות של גיבוי ושחזור. כמו כן, התלמיד ייחשף לנושאים נוספים בתחום זה, כגון תמיכת מערכת ההפעלה בנושא גיבוי ושחזור, ומוצרים משלימים. התלמידים ילמדו גם אודות מערכות אחסון (Storage), שיטות לרפליקציה של מערכות ומידע, וכמובן חולשות ודרכי התמודדות.

מטרת המודול:

בסיום הקורס, על הלומד לדעת את ההיבטים המרכזיים של נושא הגיבוי, השחזור וההתאוששות מאסון, תמיכת מערכת ההפעלה בתהליכי גיבוי ושחזור, ומוצרים משלימים.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- מתודולוגיות, מסגרות ותקנים בתחום ההמשכיות העסקית (BCP) ובהתאוששות מאסון (DRP).
- מתודולוגיות ושיטות לגיבוי ושחזור – גיבוי מלא, חלקי, שימוש בלוגים כגיבוי ועוד.
- שיטות תלויות סביבה – אתרי מחשב מפוצלים, מערכות הפעלה שונות.
- שירותי מערכות ההפעלה לגיבוי ושחזור.
- מוצרים חיצוניים משלימים לתהליכי הגיבוי.
- היבטים ארגוניים של ההתאוששות מאסון.
- היבטי אבטחת מידע של נושא הגיבוי והשחזור. לדוגמא: הרשאות יתר למשתמשים המבעים פעולות אלו, היכולת לעיין במידע שאינם מורשים לו.
- מוצרים ומערכות אחסון (Storage Systems),אופני ההגנה על המידע האגור בהן, גיבוי והתאוששות ואופני ההגנה במוצרים אלו.

מודול 13

תוכנות זדוניות וזיהוי אנומליות

12 שעות

כללי:

מודול זה מיועד להכיר לתלמידים את נושא התוכנות הזדוניות, דוגמת: וירוס מחשב, רוגלות, סוסים טרויאניים, תולעת ועוד. התלמיד ילמד להכיר את הסוגים השונים של הנוזקות (Malware), דרכי הפצה, אופני ההתמודדות, מניעה ומוצרי הגנה מפני תוכנות זדוניות. כמו כן, התלמיד ילמד גם כיצד מזהים את קיום של תוכנה זדונית, שימוש במנגנונים לזיהוי אנומליות בהתנהגות רשת ובהתנהגות המחשב, והפעולות שיש לנקוט בעת גילוי כאמור.

מטרת המודול:

בסיום הקורס, על הלומד לדעת את ההיבטים המרכזיים של נושא התוכנה הזדונית והגנת הסביבה הממוחשבת מפניהם, את דרכי ההפצה, מניעה והתמודדות, מוצרים, טיוב ותפעול שוטף של מערכות ההגנה, להכיר את נושא זיהוי אנומליות (ברשת ובתחנות הקצה), ומהו הטיפול הבסיסי בהתאם לנהלי הארגון ומוצרים תומכים בתחום זה.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- סוגים של תוכנות זדוניות (נוזקות), לדוגמא: סוס טרויאני, APT ,וכו'.
- תוכנה זדונית מוכוונת מטרה ויעד.
- שימוש בתוכנה זדונית לתקיפה, דוגמאות ודרכי הפצה.
- מוצרי אנטי-וירוס, לשרתים, מחשבים אישיים, שרתי דואר, סביבת אינטרנט ועוד.
- התקנה, טיוב, עדכון ותפעול שוטף.
- הבדלה בין מוצרים מבוססי חתימה למוצרים מבוססי התנהגות ומוצרים היברידיים (שילוב).
- מתודולוגיות להתמודדות עם תוכניות זדוניות (ע"פ NIST).
- מהי אנומליה, כיצד מזהים אנומליה ברשת, במחשבים, בטלפונים ניידים.
- טכניקות לזיהוי אנומליות – תלויות חוקים, תלויות זמן, תלויות משתמש, ובניית פרופילים לאיתור אנומליה.
- מוצרים לזיהוי אנומליות.
- תהליכים ושיטות לטיפול באירוע.
- מוצרי לזיהוי ומניעת נוזקות (IPS/IDS).
- התקנה, טיוב, תפעול שוטף ובדיקת לוגים של מערכות IPS/IDS.
- התראות שווא מול התראות אמת.
- מזעור התרעות שווא במערכות IPS (טיוב חוקים).
- זיהוי אנומליה מחייבת "הרמת דגל" והפניה לדרג בכיר.

מודול 14

בקרת גישה

10 שעות

כללי:

מודול זה מיועד להכיר לתלמידים את נושא בקרת הגישה. מודול זה מחולק לשני חלקים עיקריים. בחלק הראשון ילמדו הנושאים של בקרת גישה של משתמשים, תוכנות לרכיבים, מידע במערכות המחשוב הארגוניות, ורכיבים שונים ברשת הארגונית, כולל התייחסות למוצרים בתחום. בחלק השני של מודול זה ילמד התחום של מערכות ארגוניות לזיהוי ואימות משתמשים וחומרה.

מטרת המודול:

בסיום הקורס, על הלומד לדעת את ההיבטים המרכזיים של בקרת הגישה, תהליכים, התמודדות עם תקלות, וטיפול בחריגים, מערכות ארגוניות לזיהוי ואימות משתמשים.

להלן הנושאים העיקריים אשר יילמדו במודול זה (בחלק הראשון):

שיטות לזיהוי ואימות משתמשים, וסקירה של המנגנונים הקיימים במערכת ההפעלה לצורך זיהוי ואימות משתמשים. הכרות עם מנגנוני 2FA (2 Factor Authentication) ו\או MFA (Authentication Factor-Multi). תוכנה/חומרה נוספת לזיהוי ואימות משתמשים (דוגמת Tokens, כרטיסים חכמים, ואמצעים ביומטריים). תהליכי קישור רכיב החומרה למשתמש ספציפי, טיפול בחריגים – כגון אובדן סיסמה, הגדרת משתמש חדש במערכת, טיפול במשתמש העוזב את הארגון או מחליף תפקיד. מהי התפיסה הנכונה של שימוש ביותר מרכיב אחד לזיהוי משתמש (כדוגמא: שימוש במוצר ביומטרי לזיהוי משתמש + סיסמה).

להלן הנושאים העיקריים אשר יילמדו במודול זה (בחלק השני):

- הגדרה ושימוש במערכות לניהול ובקרת זהויות – IAM (Identity and Access Management) כלל ארגוניות ואימות משתמשים והרשאותיהם במערכות השונות, כולל ניהול ההרשאות (Credentials).
- הכרות עם IDAAS- (Identity as a Service) בחיבור לענן.
- התממשקות עם DNS לניהול משתמשים כאמור.
- התראה על אירועים.
- זיהוי גישה של מכשירים ניידים מותרים (גישת ה-BYOD).
- ניהול האפליקציות והגישה אליהן – מוצרי MAM (Mobile Application Management).
- פעולות למניעת התחברות של ציוד בלתי מורשה (דוגמת מחשב נייד לרשת הארגונית).
- מוצרים וטכנולוגיות בתחום, שימוש ב-Certificate ארגוני לזיהוי ציוד תקשורת.

מודול 15

דלף מידע

4 שעות

כללי:

מודול זה מיועד להכיר לתלמידים את נושא דלף המידע הארגוני, הסכנות שבו, תהליכי מניעה / צמצום / גילוי, הכרות עם מוצרים בהגנת המידע הארגוני מפני דלף מידע, בהתנהגות רשת והתנהגות מחשב, ומהן הפעולות שיש לנקוט בעת גילוי כאמור.

מטרת המודול:

בסיום הקורס, על הלומד לדעת את ההיבטים המרכזיים של נושא דלף המידע וכיצד ניתן לפעול למניעתו / צמצומו / גילוי עובדת קיום דלף מידע.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- הגדרת המושג, מהיכן יכול לדלוף מידע, ערוצים, כיצד מזהים ניסיונות דלף מידע, אמצעים ושיטות קיימות למניעה / צמצום התופעה / וזיהוי ואיתור.
- היבטי חוק בנושא דלף מידע.
- הגנה / מניעה / צמצום של דלף מידע במסדי נתונים, מערכות אחסון (Storage).
- הגנה / מניעה / צמצום של דלף מידע בהתקנים ניידים (דוגמת טלפונים חכמים, מחשבים ניידים).
- שימוש נכון בהתקנים זיכרון נתיקים (כגון דיסק נתיק, Key on Disk).
- מוצרים וטכנולוגיות למניעה / זיהוי / גילוי – דוגמת מוצרים לסינון תוכן ו-DLP.

מודול 16

ניהול ורישום אירועי אבטחת מידע (Audit)

6 שעות

כללי:

מודול זה מיועד להכיר לתלמידים את נושא רישום וניהול אירועי אבטחת מידע על סוגיהם השונים (לדוגמא: זיהוי ממוכן של וירוס, ניסיון חדירה למערכות הארגון, ניסיון להוציא מידע אל מחוץ לארגון ע"י גורם בלתי מורשה, ועוד).

מטרת המודול:

בסיום הקורס, על הלומד לדעת את ההיבטים המרכזיים של ניהול ורישום אירועי אבטחת מידע , אופן התמודדות איתם, והלימה לנהלי התגובה לאירועים כפי שנקבעו ע"י הארגון.

להלן התרגולים, עבודות הגשה וחומרים לניהול פרויקטים במהלך הקורס:

- ניהול פרויקט להטמעת מערכת SIEM בארגון.
- ניהול פרויקט להטמעת מערכת NAC בארגון.
- הקמה וניהול של מרכז לניהול אירועי אבטחת מידע (SOC).
- כיצד ניתן להתמודד עם התראות שווא ולצמצם אותן?
- ועוד....

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- מהו תהליך הניטור, ולמה נדרש ניטור ידני וניטור אוטומטי?
- הכרות עם מרכז לניהול אירועי אבטחת המידע – SOC (Security Operation Center).
- הכרות עם מוצרים ל-SOC כגון מערכת SIEM (Security Information Event Management).
- מוצרים משלימים כגון NAC (Network Access Control).
- פריסה של מערכות אבטחה - כגון שימוש בחיישנים (Sensors), התקנה וטיוב המערכת, תהליך הגדרת חוקים בהתאם לדרישות עסקיות, תפעוליות ורגולטוריות, התמודדות עם התראות שווא (False Alarms) אל מול התראות אמת, תהליך מעקב, עדכון ותחזוקה שוטפת של המערכות הללו.
- שילוב מוצרים אלו בארגון, קביעת מסלולי דיווח (בתוך הארגון ומחוצה לו).
- אופן התייחסות למידע התרעתי המתקבל ממקורות מידע חיצוניים (כגון מודיעין סייבר), וטיפול בניסיונות חדירה מבחוץ לרשת הארגונית.
- אופן ההתייחסות למידע הרתעתי המתקבל ממקורות פנימיים, (מתוך הארגון) - המתקבל מכל מחשב וציוד המותקן בארגון ו/או הרשאי לגשת למשאבי הארגון.

מודול 17

היבטי אבטחת מידע בציוד תקשורת והקשחתו

8 שעות

כללי:

מודול זה מיועד להכיר לתלמידים את נושא הקשחת ציוד תקשורת כגון נתבים ומתגים (בסביבות התקשורת השונות).

מטרת המודול:

בסיום הקורס, על הלומד לדעת את ההיבטים המרכזיים של העקרונות והפעולות הבסיסיות בנושא מערכות ההפעלה השונות של סוגי ציוד התקשורת, וכיצד ניתן להקשיח את המערכות הללו במטרה לצמצם את שטח התקיפה.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- מדוע נדרש לבצע הקשחה לציוד התקשורת?
- מהם העקרונות לתהליך ההקשחה?
- הקשחה תלוית ציוד תקשורת (לדוגמת נתבים של CISCO לעומת נתבים של חברת JUNIPER).
- עדכון תוכנה, קושחה (Firmware) לציוד התקשורת.
- בדיקת הקשחות לציוד התקשורת.
- מוצרים תומכים בהקשחה.
- תאום עם מוצרי אבטחת מידע לדיווח אנומליות.

להלן התרגולים, עבודות הגשה וחומרים לניהול פרויקטים במהלך הקורס:

- הקשחת ציוד תקשורת (נתבים)
- הקשחת ציוד תקשורת (מתגים)
- בדיקת הקשחות (כחלק מתהליך הערכת סיכונים)
- ועוד...

מודול 18

מחשוב ענן, שירותי אירוח (Hosting), וירטואליזציה

4 שעות

כללי:

מודול זה מיועד להכיר לתלמידים את נושא העקרונות לנושאים המרכזיים בעידן של היום כגון מחשוב ענן, שירותי אירוח, ווירטואליזציה. כמו כן, התלמיד ילמד נושאים כגון קבלת דיווחים מהלוגים השונים והבנתם, היבטי חוק ורגולציות שונות, זיהוי אנומליה, ומוצרי תומכי אבטחה של המחשב האורח והמארח.

מטרת המודול:

בסיום הקורס, על הלומד לדעת את ההיבטים המרכזיים של מחשוב ענן, שירותי אירוח, וירטואליזציה, מהם החשיפות והאיומים בשימוש כל אחד מהטכנולוגיות הללו, ומהן דרכי ההתמודדות עם הסיכונים הללו.

להלן התרגולים, עבודות הגשה וחומרים לניהול פרויקטים במהלך הקורס:

- הערכת סיכונים בסביבת מחשוב ענן
- אבטחת מערכות וירטואליות
- ועוד....

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- מחשוב ענן – הכרות עם הטכנולוגיות, הסוגים והמודלים השונים של מחשוב ענן, קבלת דיווחים מהלוגים השונים והבנתם, היבטי חוק בשימוש מחשוב ענן, זיהוי אנומליה, והכרות עם מוצרים תומכים בסוגיות אבטחת מידע.
- שירותי אירוח (Hosting) – הכרות עם הטכנולוגיות, הסוגים והמודלים השונים של אירוח שרתים ומערכות, קבלת דיווחים מהלוגים השונים והבנתם, היבטי חוק בשימוש שירותי אירוח, זיהוי אנומליה, והכרות עם מוצרים תומכים בסוגיות אבטחת מידע.
- ווירטואליזציה – הכרות עם הטכנולוגיות השונות, מדוע נדרש שימוש בווירטואליזציה, מהם היתרונות והחסרונות, סביבות VM שונות, היבטי אבטחת מידע וחוק ועוד.

מודול 19

שינוע מידע מ/אל הארגון

4 שעות

כללי:

מודול זה מיועד להכיר לתלמידים את נושא העקרונות והמתודולוגיות הנהוגות בנושא של שינוע מידע מ/אל הרגון באמצעים פיזיים (דוגמת מצאי מדיה מגנטית ואופטית).

מטרת המודול:

בסיום הקורס, על הלומד לדעת את ההיבטים המרכזיים של היבטי אבטחת המידע והסיכונים הקיימים בעת שינוע מידע מ/אל הארגון והשיטות המקובלות להגן על מידע זה.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- היבטי אבטחת המידע בעת הכנסת מידע לארגון באמצעו מצאי מדיה מגנטית או אופטית.
- שינוע גיבויים
- נהלים ומתודולוגיות
- תחנות "הלבנה"
- תהליכי "השחרה".

להלן התרגולים, עבודות הגשה וחומרים לניהול פרויקטים במהלך הקורס:

- שימוש בתחנות הלבנה
- ביצוע השחרה לקבצים
- שימוש בהעברת מידע מאובטח (כגון בכספות)
- ועוד....

מודול 20

אבטחה אפליקטיבית

4 שעות

כללי:

מודול זה מיועד להכיר לתלמידים את העקרונות והמתודולוגיות הנהוגות בנושא הטמעת היבטי אבטחת מידע בתוכנה, ניהול שינויים בתוכנה והיבטים של מבדקי חוסן (אבטחת מידע) ברמת האפליקציה, ואת הקשר בין איכות תוכנה לאבטחת מידע ואמינות התוכנה.

מטרת המודול:

בסיום הקורס, על הלומד להכיר את התהליכים השונים למימוש בעת מחזור החיים של פיתוח תוכנה ושינויים בתוכנה.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- זיהוי הסיכונים העומדים בפני מערכת התוכנה / האפליקציה.
- קביעת דרישות אבטחת מידע ממערכת התוכנה / האפליקציה.
- הפעילויות השונות, מבחינת היבטי אבטחת מידע שיש לבצע בכל שלב של מחזור חיי פיתוח התוכנה / האפליקציה.
- הוספת בקרות אבטחה (Gates Control) לאיכות תוכנה ולאבטחת מידע.
- מבדקי חוסן (Testing Penetration).

להלן התרגולים, עבודות הגשה וחומרים לניהול פרויקטים במהלך הקורס:

- שילוב היבטי אבטחת מידע במחזור החיים של פיתוח תוכנה (S-SDLC).
- ביצוע סקר מערכת
- ועוד....

מודול 21

מתודולוגיה ביצוע בדיקות חוסן – תשתיתי ואפליקטיבי

4 שעות

כללי:

מודול זה מיועד להכיר לתלמידים את העקרונות והמתודולוגיות הנהוגות בנושא מבדקי חוסן לתשתיות הארגון (תקשורת, אבטחת מידע, סיסטם) וגם ברמת האפליקציות (אתרי אינטרנט, יישומים פנים ארגוניים, ומערכות מחשוב אחרות).

מטרת המודול:

בסיום הקורס, על הלומד להכיר את הנושאים השונים בביצוע מבדקי חוסן תשתיתי ואפליקטיבי.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- מתודולוגיות לביצוע מבדקי חוסן תשתיתיים.
- מתודולוגיות לביצוע מבדקי חוסן אפליקטיביים.
- זיהוי חולשות פוטנציאליות במערכות מחשוב.
- זיהוי חולשות פוטנציאליות בתשתיות מחשוב.
- הכרות עם כלי תוכנה מקובלים בתחום ביצוע מבדקי חוסן (Penetration Testing).
- הכרות עם כלי תוכנה מקובלים בתחום זיהוי פגיעויות (Analysis Vulnerability).
- תהליכי דיווח הממצאים.

להלן התרגולים, עבודות הגשה וחומרים לניהול פרויקטים במהלך הקורס:

- זיהוי פגיעויות ברמת התשתיות
- זיהוי פגיעויות ברמת האפליקציה
- ביצוע מבדקי חוסן אפליקטיביים
- ביצוע מבדקי חוסן תשתיתיים
- ועוד....

מודול 22

חוק ואתיקה

8 שעות

כללי:

מודול זה בנוי משלושה חלקים עיקריים, כאשר החלק הראשון מתמקד בהכרת חוקי מדינת ישראל העוסקים בתחומי הגנת הפרטיות ומחשבים, תקינה, החלטות ממשלה ואסדרה בנושא הגנת הסייבר. החלק השני יעסוק באתיקה של העוסקים במקצוע בנושא סייבר, הגנת הפרטיות בעולם (אירופה וארה"ב). והחלק השלישי יעסוק בחוקים בינלאומיים בנושא סייבר, והגנת הפרטיות (לרבות אירופה וארה"ב).

מטרת המודול:

בסיום הקורס, על הלומד להכיר את החוקים הרלוונטיים, התקנות וההנחיות בארץ, להבין מהיכן נובעים השינויים בהנחיות השונות, להבין את המשמעויות של פעולות שאינן עולות בקנה אחד עם החוק, להבין את מחויבותו האתית למקצוע ולמקום העבודה.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- חוקי מדינת ישראל (חוק הגנת הפרטיות, חוק המחשבים, הנחיות בנק ישראל, הנחיות הבורסה לנ"ע, החלטות ממשלה ואסדרה בנושא הגנת הסייבר).
- אתיקה מקצועית
- חוקים ותקנות בינלאומיות

להלן התרגולים, עבודות הגשה וחומרים לניהול פרויקטים במהלך הקורס:

- עמידה בדרישות רגולציה אירופאית בתחום הגנת הפרטיות (GDPR).
- עמידה בדרישות SOC2
- עמידה בדרישות HIPAA
- ועוד....

מודול 23

אבטחה פיזית וסביבתית

8 שעות

כללי:

סביבת המחשוב בארגון אמורה להיות מוגנת ומאובטחת מפני חדירה פיזית, גישה ע"י גורמים בלתי מורשים, והגנה מפני אירועי קיצון (דוגמה: רעידת אדמה). מודול זה מציג בפני הלומד מתודולוגיות שונות ואמצעים להגנת אתרי המחשוב הפיזיים, בהם מצוי המידע הארגוני והמחשבים הארגוניים, לרבות סביבת העבודה של העובדים.

מטרת המודול:

בסיום הקורס, על הלומד להכיר את אמצעי האבטחה הפיזיים, מנגנוני הניטור והבקרה והאמצעים העומדים לרשות הארגון לטיפול באירועי קיצון.

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- הנחיות החוק בדבר אבטחת סביבת המחשוב.
- על מה חשוב להגן וכיצד.
- אמצעי אבטחה וניטור למניעת גישה למתקן ע"י גורמים בלתי מורשים.
- אמצעים לטיפול בפני אירועי קיצון שונים (כגון רעידת אדמה, הפסקת חשמל, שריפות, מלחמה ועוד).

להלן התרגולים, עבודות הגשה וחומרים לניהול פרויקטים במהלך הקורס:

- סקר אבטחה פיזית למרכזי מחשוב (Data Center)
- מימוש בקרות אבטחת מידע למרכזי מחשוב (Data Center)
- ועוד....

מודול 24

טיפול באירועי אבטח מידע

6 שעות

כללי:

מודול זה מציג בפני הלומד את העקרונות של טיפול באירועי אבטחת מידע, ומספק הבנה של הסיטואציות השונות של קיום מתקפות סייבר על הארגון ומערכותיו, שלבי המתקפה וכיצד לטפל באירועים אלו בצורה נאותה.

מטרת המודול:

בסיום הקורס, על הלומד להכיר ולהבין כיצד נושאים שונים שלמד במהלך הקורס, מתממשקים כעת, ויסודות הטיפול באירוע סייבר.

להלן התרגולים, עבודות הגשה וחומרים לניהול פרויקטים במהלך הקורס:

- התמודדות עם אירועי סייבר שונים (עפ"י תרחישים שונים).
- ביצוע תחקור דיגיטלי (Digital Forensics) ברמת השרת, הרשת, וטלפונים ניידים.
- ועוד....

להלן הנושאים העיקריים אשר יילמדו במודול זה:

- הכרות עם סוגי תקיפות שונות כגון מניעת שירות (Denial of Service), פישינג (Phishing) ופישינג ממוקד(Spear Phishing) ועוד.
- הבנת תהליך ביצוע התקיפה, שלבי התקיפה, (לדוגמא: התקיפה מתחילה במשלוח דואר תמים המכיל קובץ עם תוכנה זדונית).
- הבנת הנזק (Impact) הנגרם מהתקיפה.
- אמצעים העשויים לסייע לארגון לזיהוי קיומה של התקיפה.
- אמצעים העשויים לסייע בבלימת התקיפה.
- הכרות עם הנושא של התראות שווא (False Positive ו- False Negative).
- אופן הטיפול בתקיפות שהתגלו (שיטות, מתודולוגיות וכלים).
- הפעלת מנגנונים בולמים ובדיקת יעילותם.
- בדיקת נזקים.
- מימוש תהליכי תחקור דיגיטלי (Digital Forensics).
- תהליכי שחזור מידע.
- הפקת לקחים ברמות הארגוניות השונות.
- הרחבת בסיסי הידע הארגוני בתחום חקירות פשעי מחשב.
- פנייה ודיווח לרשויות החוק.

חלק ב' | תרגול תיאורטי ומעשי

החלק השני של הקורס מכיל תרגולים רבים הן בפן התיאורטי והן בפן המעשי. התרגולים מחולקים על פני כל 24 המודולים של הקורס, ומתבצעים באופן עצמאי, בקבוצות בכיתה או בבית במטרה לתרגל את החומר הנלמד, ולהמחיש למשתתפי הקורס את מהות החומר המקצועי שנלמד.

חלק ג' | מעבדות

החלק השלישי בקורס מכיל מעבדות תרגול רבות, שמתייחסות למגוון רחב של טכנולוגיות בתחום הסיסטם (כגון הקשחת מערכות הפעלה, בסיסי נתונים ועוד), תקשורת (נתבים), ופתרונות אבטחת מידע וסייבר (מערכות SIEM, פירוול, DLP, IPS, NAC ועוד). מטרת המעבדות הינה להמחיש למשתתפי הקורס את האתגרים עימם יצטרכו להתמודד בעתיד, במסגרת תפקידם בחברות. התרגולים במעבדה יתבצעו הן באופן עצמאי, והן בקבוצות (בהתאם לנושאים אותם ילמדו במהלך הקורס).

חלק ד' | עבודות הגשה ופ. גמר

בחלק הרביעי, על משתתפי הקורס להתנסות בביצוע עבודות הגשה, ובפרויקט גמר לקורס (אשר יהוו חלק מהציון הסופי של הקורס). המטרה היא לאפשר למשתתפי הקורס להתנסות באופן עצמאי בביצוע מטלות שיידרשו מהם בעתיד, במסגרת תפקידם כמיישם סייבר בארגון.

חלק ה' | בחינת ההסמכה

החלק האחרון ואחד החשובים ביותר, הינו בחינת ההסמכה. מטרת בחינת ההסמכה היא לבחון את רמת הידע וההבנה של משתתפי הקורס, הן בפן התיאורטי, והן בפן המעשי. הבחינה מחולקת לשני חלקים:

חלק ראשון – עיוני

חלק שני - מעשי

זכאות לתעודת ההסכמה

הבוגרים יהיו זכאים לתעודת ההסמכה של מיישם סייבר (CSP) בתנאי שעמדו בכל דרישות הקורס, וקיבלו ציון **מעל 70**.
להלן טבלת התפלגות האחוזים להרכבת הציון הסופי בקורס.

פעילות	משקל
השתתפות בכיתה (תרגולים)	5%
מעבדות	25%
עבודות הגשה	15%
פרויקט גמר	15%
בחינה סופית	40%
סה"כ	100%

לוגיסטיקה

מיקום הקורס

הקורס יתקיים במכללת TS-College, במשרדי החברה שבפתח תקווה. הכתובת הינה רחוב המגשימים 20, בניין B, קומה 3.
יש חניון צמוד למכללה.

שעות תרגול במעבדה

שעות התרגול במעבדה במכללה הינם כל יום כשעתיים לפני תחילת השיעור, וכשעה לאחר השיעור. לנוחיותכם, ישנה גישה מקוונת למערכת LMS של המכללה, שבה תוכלו להנות מגישה חופשית לכל חומרי הלימוד שלנו כל הזמן.

ספריה דיגיטלית

לכלל תלמידי המכללה יש גישה חופשית (באופן מקוון) לספריה הדיגיטלית של המכללה. לקבלת הרשאות גישה לספריה הדיגיטלית, ניתן ליצור קשר עם הרכז האקדמי של הקורס.

ספריית המכללה

לכלל התלמידים בקורס יש גישה חופשית לספריה של המכללה, שבה תוכלו להשאיל ספרי לימוד בתחומים שונים בתחום הגנת הסייבר.

מלגות

ניתן לקבל מלגות לימודים שונות. לצורך קבלת מידע אודות זכאות למלגה, ניתן ליצור קשר עם נציגנו בטלפון 077-5150340, או במייל info@titans2.com, נציגנו ישמחו לסייע לכם בבדיקת הזכאות, ולהנחות אתכם בתהליך זה.

הטבות לבוגרים שלנו

הבוגרים שלנו נהנים מהטבות ייחודיות ובלעדיות למכללת TS-College (מבית קבוצת TITANS SECURITY), הטבות שיעזרו להם בתהליך הקליטה אל שוק העבודה במשק הישראלי והעולמי.
להלן מספר הטבות ייחודיות עבור בוגרי מכללת TS-College:

- **מקור מידע מקצועי** – גישה למקורות מידע מהארץ ומחו"ל בתחום הגנת הסייבר (כגון מאמרים מקצועיים, כתבות תחקיר, ספרות מקצועית, כנסים, השתלמויות מקצועיות ועוד).
- **הכשרה מקצועית** – במסגרת ההכשרה המקצועית במכללת TS-College, הבוגרים שלנו נחשפים למגוון רחב של הרצאות והשתלמויות מקצועיות (חלקן ללא עלות וחלקן בעלות סמלית בלבד) שמועברות ע"י מומחים ומובילי דעה מהארץ ובעולם.
- **תכנים ייחודיים** – במסגרת המפגשים המקצועיים, והחומרים שיהיו זמינים לבוגרים שלנו, הסגל האקדמי והיועצים שלנו יבצעו סינון קפדני על מקורות המידע, על מנת לספק את התכנים המקצועיים והייחודיים ביותר, ולהשמיט את התכנים השיווקיים.
- **יישומיות** – במסגרת הקורס יתבצעו סדנאות מקצועיות התלמידים ירכשו ידע תיאורטי ומעשי, במימוש ויישום מסגרות, תקנים ונהלי עבודה בתחום הגנת הסייבר. כמו כן, התלמידים ישולבו בפרויקטים חיים (אמיתיים) בחברת הייעוץ המובילה-TS-Consulting (מבית קבוצת TITANS SECURITY) לצורך צבירת ניסיון מעשי בחיים האמיתיים ויישום הידע שנצבר.
- **Networking** – במסגרת ההכשרה וגם אחריה, התלמידים שלנו יוכלו להתרברב עם צמרת תעשיית הסייבר בישראל ובעולם, ומובילי דעה מהשורה הראשונה, ולשתף ואף להעשיר את הידע בתחומים שונים.
- **חברות שנתית באיגוד העולמי לאבטחת מידע (ISSA)** – כל תלמיד במכללת TS-College יקבל כהטבה ייחודית חברות שנתית באיגוד העולמי לאבטחת מידע (ISSA), אשר תקנה לו גישה לחומרים מקצועיים, וכנסים מקצועיים בתחום אבטחת המידע והגנת הסייבר.
- **תעודות השתתפות ושימור נקודות CPE** – במסגרת החברות ב-ISSA הבוגרים שלנו יוכלו להנות מקבלת תעודות השתתפות בקורסים, סדנאות, השתלמויות ושאר פעילויות ההעשרה, אשר יהיו מוכרות לצבירת נקודות CPE (עבור ההסמכות הבינלאומיות כגון CGEIT®, CISSP®, CISM®, CISA®, CRISC®, ועוד), ואולי אף לגמול השתלמות.
- **ייחודיות** – במסגרת החברות באיגוד ISSA, תינתן הזדמנות לכל אחד להשפיע, הן באופן פרטני והן כחלק מקבוצות והוועדות השונות, בתחום הגנת הסייבר בתחומים כגון תקינה, מחקר, אקדמי ועוד.
- **תוכנית CASHBACK** – כל תלמיד אשר נרשם לקורס במכללת TS-College ייהנה מצבירת נקודות בתוכנית הייחודית של CashBack, שבה התלמיד צובר נקודות זכות למימוש קורסים עתידיים בחברה.
- **מנוי שנתי למגזין GLOBAL SECURITY** – הבוגרים שלנו יוכלו להנות מהטבה ייחודית ובלעדית למכללת TS-College, ולקבל מנוי שנתי חינם למגזין GLOBAL SECURITY העוסק בתחום הגנת הסייבר.
- **צבירת ניסיון מעשי** – עוד במהלך הקורס, התלמידים יהיו מעורבים בפרויקטים אמיתיים, אצל לקוחות החברה, בהם יוכלו לממש את הידע שנצבר במהלך הקורס ולצבור ניסיון מעשי לקראת קליטתם בשוק העבודה.
- **שירותי השמה** – כל הבוגרים שלנו יוכלו להנות משירות ייחודי ובלעדי של ייעוץ קריירה, שבו בונים לו חבילת ייעוץ ייחודיות עם מנהלת השמה ויועץ קריירה, לצורך שילובו המהיר בשוק העבודה.
- **תוכנית מנטור אישית** – כל הבוגרים שלנו יוכלו להנות במהלך השנה הראשונה בקריירה שלהם לייעוץ אישי באמצעות התוכנית הייחודית שלנו "מנטור אישי" – שבה סגל המרצים שלנו ילווה את הבוגרים בתהליך קליטתם בשוק העבודה (ייעוץ מקצועי).

אודות קבוצת טיטנס סקיוריטי

אודות הקבוצה

קובצת TITANS SECURITY נוסדה בשנת 2010, ומכילה בתוכה חמש חברות שונות, בהתמחויות שונות. הקבוצה משרתת כיום עשרות רבות של לקוחות (בארץ ובחו"ל), וביצעה מאות פרויקטים שונים בתחום אבטחת המידע, הגנת הסייבר, פרטיות, ניהול המשכיות עסקית, מחשוב ענן, ניהול סיכונים ועוד. היתרון של הקבוצה הוא בכך שתחת קורת גג אחת ניתן לקבל שירותים רבים ומגוונים, תחת אותה הנהלה , כאשר יש כתובת אחת למענה מהיר ומקצועי.

חברות בקבוצה

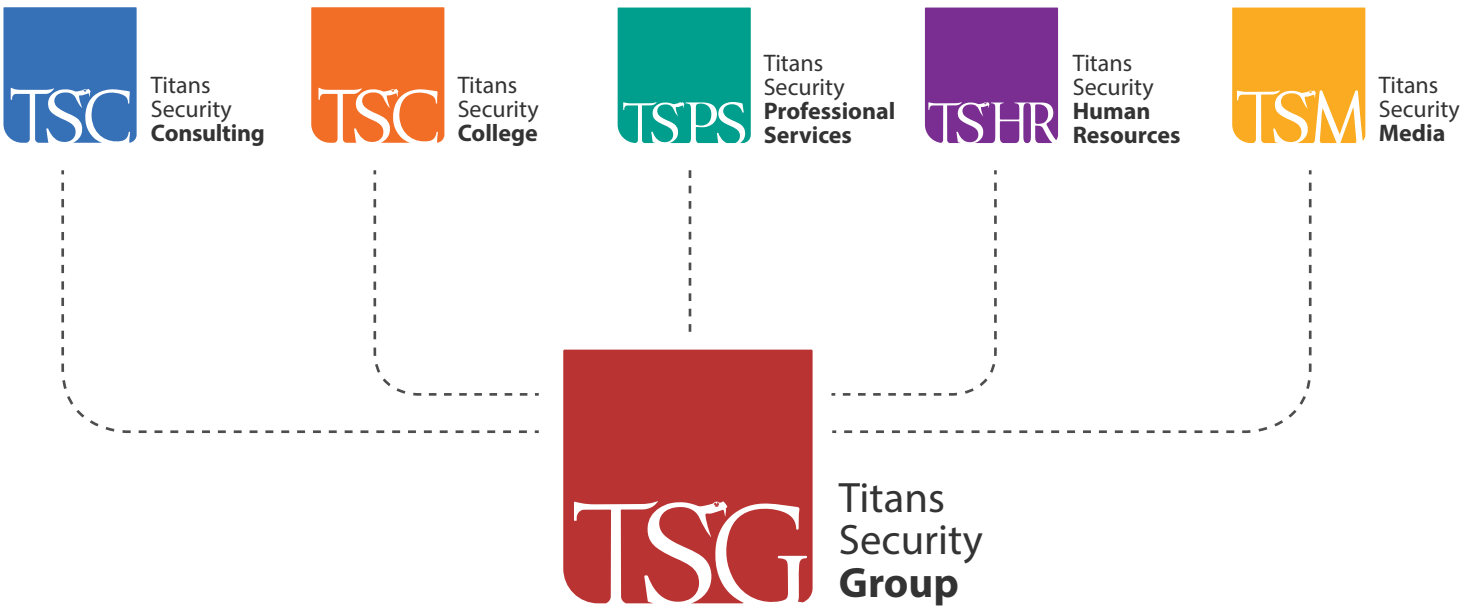
חברת TS-Consulting–מדובר בחוד החנית של הקבוצה מבחינת שירותי ייעוץ בתחום אבטחת מידע, הגנת הסייבר, פרטיות וניהול סיכונים. החברה מספקת שירותי ייעוץ לארגונים רבים בארץ ובחו"ל, וביצעה מאות פרויקטים שונים בתחום הגנת הסייבר.

מכללת TS-College – מדובר ביחידת העלית של הקבוצה מבחינת אספקת שירותי הדרכה בתחום אבטחת המידע והגנת הסייבר. המכללה מספקת כיום מגוון רחב של מסלולי הכשרה מקצועיים בתחומים שונים, כולל הכנה למסלולי הכשרה בינלאומיים. מכללת TS-College התבססה כאחת המכללות הטובות ביותר בעולם, עם אחוזי הצלחה מהגבוהים ביותר בעולם בבחינת ההסמכה הבינלאומיות, והעבירה כיום עשרות קורסים בהצלחה רבה, עם מאות בוגרים שהתברגו בצמרת התעשייה המקומית והעולמית.

TS-PROFESSIONAL SERVICES – מדובר בחטיבת השירותים המקצועיים שלנו, שמבצעת פרויקטים רבים בתחומים כגון סקרי סיכונים, ניהול סיכונים, מבדקי חוסן, ביקורות ספקים, ניהול פרויקטים בתחום אבטחת המידע והגנת הסייבר, הקשחת מערכות, אפיון וליווי להטמעת פתרונות אבטחת מידע והגנת הסייבר בארגון, ועוד.

TS-HR - מדובר ביחידת הסגולה של הקבוצה, שמספקת מגוון רחב של שירותי השמה ומיקור חוץ לקהל לקוחותינו, ללקוחות הקצה (הארגונים) והן לבוגרים שלנו. חטיבה זו מספקת קשת רחבה של שירותים כגון ייעוץ קריירה, בניית מסלול הכשרה, כתיבת וטיוב קורות חיים, הכנה לראיונות העבודה ובדיקות מהימנות ועוד.

TS-MEDIA – מדובר בחטיבה ייחודית שמספקת שירותי ייעוץ והדרכה בתחום עולם התוכן כגון הפקת קמפיין להגברת המודעות בנושא אבטחת מידע והגנת הסייבר, הכנת מערכי הדרכה פנים-ארגוניים, כנסים וסדנאות מקצועיות (בארץ ובחו"ל) ועוד.



סגל המרצים

סגל המרצים שלנו מורכב מבכירים בתעשייה בארץ ובעולם, ביניהם מנהלי אבטחת מידע, חוקרים בתחום אבטחת המידע והגנת הסייבר, יועצים בכירים, ועוד. להלן חלק מסגל המרצים שלנו בקורס:

מר דני אברמוביץ

מנכ"ל קבוצת
TITANS SECURITY

דני הינו מנכ"ל קבוצת TITANS SECURITY, ומשמש כנשיא של האיגוד העולמי לאבטחת מידע ISSA (הצ'אפטר הישראלי), ויו"ר ה-SIG סייבר בלשכת טכנולוגיות המידע. בנוסף, דני מנהל את תחום אבטחת המידע עבור כמה ארגונים בינלאומיים. דני בעל ניסיון רב, של מעל 20 שנה בתחום אבטחת המידע והגנת הסייבר, מרצה בעל שם עולמי, ומחבר ספרים רבים בתחום אבטחת המידע, תקינה ורגולציה ותחום הגנת הסייבר.

מר קובי לכנר

CISO של חברת WIX

קובי הינו אחד מהבכירים בתעשיית הסייבר המקומית, עם למעלה מ-20 שנה בתחום. קובי כיום מנהל את תחום אבטחת המידע בחברת WIX, ושימוש בעבר כמנהל אבטחת המידע בחברת PLAYTECH העולמית, ויועץ בכיר במספר חברות ייעוץ מובילות.

מר איתן סטמרי

Security Architect
בחברת WIX

איתן הינו אחד מהבכירים בתעשיית הסייבר המקומית, עם למעלה מ-20 שנה בתחום ה-Application Security. איתן משמש כיום כ-Security Architect בחברת WIX, ושימוש בעבר כיועץ בכיר במספר חברות ייעוץ מובילות.

סגל המרצים

מר עומרי נוימן
COO בחברת BUGSEC

עומרי הינו אחד מהבכירים בתעשיית הסייבר המקומית, עם ניסיון רב בתחום אבטחת המידע והגנת הסייבר. עומרי משמש כיום כ-COO (סמנכ"ל טכנולוגיות) בחברת GUBGSEC, ושימוש בעבר כארכיטקט אבטחת מידע בבנק הפועלים, ויועץ בכיר במספר חברות ייעוץ מובילות.

מר דניאל ציציק
CISO של חברת WALKME

דניאל הינו ה-CISO של חברת WALKME, ובעל ניסיון עשיר וידע עצום הן בפן הטכנולוגי והן בפן הניהולי. דניאל היה בעברו חוקר בכיר בתחום אבטחת המידע, בחברת SECUREWAVE, והרצה על הבמות הגדולות ביותר בעולם כגון RSA , FIRST, BLACKHAT, DEFCON ועוד.

מר אריק וולובסקי
מהנדס בכיר בחברת FORCEPOINT

אריק וולובסקי, משמש כיום כמהנדס בכיר בחברת FORCEPOINT (לשעבר מהנדס בכיר בחברת WEBSENSE אשר נרכשה ע"י חברת FORCEPOINT), בעל ניסיון וידע בתחום אבטחת המידע והגנת הסייבר, הן בפן הטכנולוגי והן בפן הניהולי. אריק ניהל בעבר את תחום אבטחת המידע בחברת פלאפון, ולפני זה עבד כיועץ בכיר במספר חברות ייעוץ ואינטגרציה.

מסלולי המשך

כללי

בעידן הסייבר, שבו האיומים הולכים ומשתנים מדי יום, הן ברמת התחכום והן במידת הנזק שעלולים לגרום לארגונים ו\או למידע שמאוחסן במערכות המחשוב שלהם, כל העוסקים בתחום הגנת הסייבר, לרבות מיישמי סייבר, מוצאים את עצמם במרדף אין סופי אחר שיפור רמת הידע והיכולות בהתמודדות עם אירועי הסייבר השונים.
לנוחיותכם, פירטנו לכם קורסים נוספים שיכולים לסייע לכם בהמשך הקריירה בתחום הגנת הסייבר. לכל שאלה, סגל היועצים האקדמי שלנו ישמחו לשבת אתכם, וביחד לבנות לכם מסלול פיתוח אישי, לקראת קריירה מאובטחת ומובטחת בעולם הסייבר.

קורסים נוספים

- **קורס CSIH®**
  Cyber Security Incident Handler
  קורס ייחודי עבור מפעילים במרכז לניהול אירועי אבטחת מידע (SOC). הקורס הינו קורס בן 40 שעות, ומשלב בתוכו ידע עיוני ומעשי בתחום ניהול ותגובה לאירועי אבטחת מידע.
- **קורס CSIM®**
  Cyber Security Incident Manager
  קורס ייחודי עבור מנהלי SOC. הקורס הינו קורס בן 24 שעות (3 ימים), והוא משלב בתוכו ידע עיוני ומעשי אודות ניהול ותפעול שוטף של מרכז SOC.
- **קורס CFI®**
  Certified Forensics Investigator
  קורס ייחודי עבור מפעילים ואנליסטים במרכז לניהול אירועי אבטחת מידע (SOC). הקורס הינו קורס בן 40 שעות, ומשלב בתוכו ידע עיוני ומעשי בתחום ניהול ותגובה לאירועי אבטחת מידע, כולל תחקור דיגיטלי (Forensics Digital).
- **קורס CFA®**
  Certified Forensics Analyst
  קורס ייחודי עבור מפעילים, אנליסטים, וצוותי תגובה ותחקור דיגיטלי במרכז לניהול אירועי אבטחת מידע (SOC). הקורס הינו קורס בן 40 שעות, ומשלב בתוכו ידע עיוני ומעשי בתחום תחקור דיגיטלי.
- **קורס CFS®**
  Certified Forensics Specialist
  קורס ייחודי עבור מפעילים, אנליסטים, וצוותי תגובה ותחקור דיגיטלי במרכז לניהול אירועי אבטחת מידע (SOC). הקורס הינו קורס בן 40 שעות, ומשלב בתוכו ידע עיוני ומעשי בתחום תחקור דיגיטלי. קורס זה הינו המשך של קורס CFA®.
- **קורס CFE®**
  Certified Forensics Expert
  קורס ייחודי עבור מפעילים, אנליסטים, וצוותי תגובה ותחקור דיגיטלי במרכז לניהול אירועי אבטחת מידע (SOC). הקורס הינו קורס בן 40 שעות, ומשלב בתוכו ידע עיוני ומעשי בתחום תחקור דיגיטלי. קורס זה הינו המשך של מסלולי ההכשרה CFA® ו-CFS®.
- **קורס CMFA®**
  Certified Mobile Forensics Analyst
  קורס ייחודי עבור מפעילים, אנליסטים, וצוותי תגובה ותחקור דיגיטלי במרכז לניהול אירועי אבטחת מידע (SOC). הקורס הינו קורס בן 16 שעות, ומשלב בתוכו ידע עיוני ומעשי בתחום תחקור דיגיטלי במובייל.
- **קורס CMFS®**
  Certified Mobile Forensics Specialist
  קורס ייחודי עבור מפעילים, אנליסטים, וצוותי תגובה ותחקור דיגיטלי במרכז לניהול אירועי אבטחת מידע (SOC). הקורס הינו קורס בן 16 שעות, ומשלב בתוכו ידע עיוני ומעשי בתחום תחקור דיגיטלי במובייל. קורס זה הינו המשך של הקורס CMFA®.

מסלולי המשך

- **קורס CMFE®**
Certified Mobile Forensics Expert
קורס ייחודי עבור מפעילים, אנליסטים, וצוותי תגובה ותחקור דיגיטלי במרכז לניהול אירועי אבטחת מידע (SOC). הקורס הינו קורס בן 16 שעות, ומשלב בתוכו ידע עיוני ומעשי בתחום תחקור דיגיטלי במובייל. קורס זה הינו המשך של הקורס CMFA® ו-CMFS®

- **קורס CISO**
Certified Chief Information Security Officer
מסלול ייחודי של הכשרת מנהלי אבטחת מידע המסלול עורך כ-200 שעות, והוא משלב בתוכו ידע תיאורטי ומעשי בתחום ניהול אבטחת המידע והגנת הסייבר. הקורס מיועד אנשים הרוצים להתקדם לתחום ניהול אבטחת המידע בארגון.

- **קורס CISSP®**
Certified Information Systems Security Professional
ההסמכה המובילה ביותר בעולם בתחום אבטחת המידע. הקורס עורך כ-56 שעות, והוא מכין את משתתפיו לבחינת ההסמכה הבינלאומית של CISSP מבית ISC2.

- **קורס CISM®**
Certified Information Security Manager
ההסמכה המובילה ביותר בעולם בתחום אבטחת המידע. הקורס עורך כ-40 שעות, והוא מכין את משתתפיו לבחינת ההסמכה הבינלאומית של CISM® מבית ISACA.

- **קורס CRO®**
Chief Risk Officer
מסלול ייחודי של הכשרת מנהלי אבטחת מידע. המסלול עורך כ-100 שעות, והוא משלב בתוכו ידע תיאורטי ומעשי בתחום ניהול והערכת סיכונים. הקורס מיועד אנשים הרוצים להתקדם לתחום ניהול סיכונים, והוא מכין גם להסמכה הבינלאומית CRISC®,מבית ISACA.

- **קורס CRISC®**
Certified Risk and Information Systems Control
ההסמכה המובילה ביותר בעולם בתחום ניהול סיכונים. הקורס עורך כ-40 שעות, והוא מכין את משתתפיו לבחינת ההסמכה הבינלאומית של CRISC מבית ISACA.

- **קורס CISA®**
Certified Information Systems Auditor
ההסמכה המובילה ביותר בעולם בתחום הביקורת מערכות מידע. הקורס עורך כ-56 שעות לקורס הקצר, ו-200 שעות לקורס המורחב, והוא מכין את משתתפיו לבחינת ההסמכה הבינלאומית של CISA, מבית ISACA.

למידע נוסף אודות הקורסים, מסלולי ההכשרה שלנו ולימודי ההמשך, ניתן לפנות בכל עת ליועצי הקריירה שלנו או ליועצים האקדמיים. לפגישת ייעוץ חינם (ללא כל התחייבות) ניתן ליצור איתנו קשר בטלפון 077-5150340, או במייל: info@titans2.com

ולסיכום

אני רוצה לברך אותך באופן אישי על בחירתך בקורס מיישם סייבר של מכללת TS- College מבית קבוצת TITANS SECURITY. אני בטוח שביחד עם נחישותך להצליח בקורס, סגל המרצים והצוות האקדמי שלנו יעשו הכל על מנת לספק לך חוויה אישית נפלאה ומיוחדת, ולסייע לך בהמשך הדרך לקליטה מהירה בשוק העבודה בתחום ההיי-טק בארץ ובעולם. אני מברך אתכם על תחילתה של דרך ארוכה, ומלאת אתגרים, ומאחל הצלחה גדולה ופורחת לכולנו!

בברכה,
דני אברמוביץ
מנכ"ל קבוצת טיטנס סקיורטי
והרכז האקדמי של הקורס