סייבר סקיוריטי ופורנזיקה

מנהל ההתמחות:
עו"ד רמי תמם

כמובילה עולמית בתחום הסייבר, מדינת ישראל מחזיקה בידיה ידע מתקדם וחדשני אך גם ניצבת בפני איומי סייבר מגוונים – מצד מדינות אויב, ארגונים פליליים, ארגוני טרור ויחידים. סיכוני הסייבר הפכו בשנים האחרונות לסיכון המרכזי המאיים על ארגונים מכל מגזר – פיננסי, בריאותי, ציבורי, תעשייתי ופרטי. יותר מאי פעם, ארגונים מוצאים את עצמם תחת מתקפות מתוחכמות, הכוללות גניבת מידע, מתקפות כופרה, הונאות פיננסיות וחדירות לרשתות תשתית קריטיות. מלחמות סייבר בין מדינות, לצד פשיעת סייבר מאורגנת והתקפות של האקרים ממניעים אידיאולוגיים או כלכליים, הפכו את הסביבה הדיגיטלית לשדה קרב שבו כל ארגון חייב להיות ערוך ומוכן להתמודד עם איומים דינמיים ומשתנים.

אחד האתגרים המרכזיים בניהול סיכוני סייבר הוא הפער בין עולם הניהול לעולם הסייבר. מנהלים רבים מתקשים להבין את משמעות הסיכונים הטכנולוגיים וכיצד הם משפיעים על הארגון, בעוד שמומחי סייבר מתקשים לתרגם את הידע הטכני לשפה עסקית אשר תאפשר קבלת החלטות אסטרטגיות. פער זה גורם לכך שמנהלים מתקשים להטמיע פתרונות אבטחה אפקטיביים, ומנהלי סייבר מתקשים לקבל את המשאבים והגיבוי הניהולי הנדרש; כתוצאה מכך, ארגונים נותרים פגיעים ומתקשים להתמודד עם התקפות בזמן אמת.

על מנת לגשר על פערים אלו, ההתמחות בסייבר סקיוריטי ופורנזיקה במסגרת לימודי התואר השני במנהל עסקים מציעה שני מסלולי הכשרה ייחודיים, המשלבים בין הבנה מעמיקה של ניהול משברים וסיכונים לבין ידע טכנולוגי מתקדם בזיהוי ותגובה לאיומי סייבר. ההתמחות מעניקה לסטודנטים כלים פרקטיים להתמודד עם אירועי סייבר מורכבים, תוך שילוב של גישות אסטרטגיות, טכנולוגיות ומבוססות בינה מלאכותית.

הסטודנטים בהתמחות אינם נדרשים לידע מוקדם בתחום הסייבר. במהלך הלימודים הסטודנטים בשני מסלולי ההתמחות ילמדו קורסי מבוא אינטנסיביים אשר ישלימו עבורם את הרקע הנדרש כדי לאפשר להם ללמוד יחד עם סטודנטים בעלי רקע בתחום.

ההתמחות מתאימה לאנשי כוחות הביטחון ורשויות המדינה – ביחידות טכנולוגיות וביחידות אחרות, למנהלים בחברות עסקיות, למנהלים במגזר העמותות והמלכ"רים, למנהלים בחברות ממשלתיות ומוסדות ממשלתיים, יועצים משפטיים וכל הרואה בעתידו תפקיד ניהול במקומות אלו בשנים הקרובות ומבקש לשדרג את עצמו בתחום ידע חדשני ונחוץ בכל מגזר בישראל ובעולם.

בוגרי התכנית יהיו זכאים לשש תעודות:

- תעודת מוסמך במנהל עסקים-MBA.
- תעודת התמחות בסייבר סקיורירטי ופורניזקה.
- ממונה הגנת הפרטיות בארגון (Data Protection Officer) DPO.
- תעודת מיישם הגנת סייבר – בהתאמה עם סילבוס הידע המומלץ לצורך הסמכה של מערך הסייבר הלאומי.
- תעודת דירקטור מומחה סייבר – הכשרה ייחודית מותאמת להנחיות בנק ישראל, רשות החברות ועוד.
- תעודת מוסמך (cyber security and forensic expert) CSFE מטעם לשכת טכנולוגיות המידע – הגוף המוביל בישראל המהווה קורת גג אחת לכל הקהילה המקצועית המגוונת העוסקת בטכנולוגיות המידע. הכשרה המאפשרת לבוגר להתמודד לתפקיד מומחה סייבר סקיוריטי ופורנזיקה בארגון. כמו כן, הבוגרים יהיו חברים בלשכת טכנולוגיות המידע במשך תקופת הלימודים ושנה מתום הלימודים בחינם, וכן, ליטול חלק בכל פעולות הלשכה.

בחזרה לתוכן העניינים

מסלולים בהתמחות

עולם הסייבר מתקיים בשני עולמות מקבילים – הטכנולוגי והרגולטורי. ההתמחות בנויה משני מסלולי לימוד המותאמים לשני קהלי יעד עיקריים והמקנים מיומנויות שונות בתחום ניהול משברי הסייבר:

מסלול IR (Incident Response) – ניהול משבר טכנולוגי

המסלול מיועד לאלו המעוניינים להתמחות בהיבטים הטכנולוגיים של הגנת הסייבר וכולל התנסות יישומית במעבדות מתקדמות. במסלול זה הסטודנטים יתנסו בחקר מתקפות סייבר, יישום פתרונות טכנולוגיים, ניתוח איומים ותגובה לאירועים בזמן אמת. מסלול זה ילמד פרונטלית בקמפוס אונו.

מסלול GRC&P (Governance Risk & Compliance) – ניהול משברים, פרטיות, ציות ורגולציה

המסלול מיועד לאלו המבקשים להתמקד בהיבטים הניהוליים והרגולטוריים. הסטודנטים יתמחו בהגנה על התאגיד ועל נושאי המשרה שבו, בהגנה על נכסי המידע של הארגון וביצירת שגרת הסייבר המונעת משברים. המסלול יכלול סימולציות מציאותיות של משברים אותם הסטודנטים ינהלו במעבדת הסייבר של הקריה. מסלול זה מתאים למנהלים, יועצים משפטיים, רואי חשבון, קובעי מדיניות ואנשי רגולציה המבקשים לרכוש כלים להבנת איומי סייבר ולתרגם אותם להחלטות עסקיות, אסטרטגיות ורגולטוריות אפקטיביות. מסלול זה ילמד בזום ויהיה זמין עבור סטודנטים משלושת הקמפוסים של הקריה.

שני המסלולים נבנו מתוך תפיסה שמנהלים צריכים לדעת "לדבר סייבר" ואנשי סייבר צריכים לדעת "לדבר ניהול". ההתמחות מאפשרת לסטודנטים לפתח מיומנויות משולבות, להבין את ההשלכות האסטרטגיות של אירועי סייבר ולבנות יכולות ניהול משברים מבוססות מידע ומודיעין מתקדם.

הקורסים הנלמדים בהתמחות* (ההתמחות כוללת 8 קורסים ופרויקט גמר):

מבוא לטכנולוגיה וסייבר: מר מוטי קארו, מר ג'קי אלטל

קורס מבוא המהווה "יישור קו" בקרב הלומדים ומספק ידע מקדים הנדרש לסטודנטים, במיוחד עבור אלו המגיעים מרקע שונה ומתחומי ידע מגוונים.

במסלול IR – קורס מבוא המספק הכרות מעמיקה עם סביבות טכנולוגיות מתקדמות ומוצרי אבטחת מידע מובילים בתעשייה.

במסלול GRC&P – קורס מבוא מספק הבנה עקרונית של טכנולוגיות אבטחת מידע ואיומי סייבר, במטרה לאפשר למנהלים לתקשר ביעילות עם צוותי אבטחה ולהבין את המשמעות העסקית של פתרונות סייבר.

הקורס מותאם לסילבוס המומלץ לצורך הסמכה בינלאומית כגון: Certified Information Systems Security Professional (CISSP) ו־Certified Ethical Hacker (CEH).

הגנת סייבר: גב' ענת גולדיאן, מר מוטי קארו

במסלול IR – הקורס מקנה ידע במונחי סייבר, מיפוי איומים, סוגי יריבים ותקיפות, סוגי סיכונים בארגונים, פגיעויות במערכות שונות וההשלכות המעשיות שלהן.

במסלול GRC&P – הקורס יקנה ידע בנושא התקפות שונות, ההשלכות של ההתקפות והטיפול הארגוני בהן. התלמידים ילמדו ניהול שגרות סייבר, ומתודות הפעלה וממשקים עם העולם העסקי, ויכירו גופים בינלאומיים העוסקים בתחום.

הקורס נבנה בהתאמה עם סילבוס הידע המומלץ לצורך הסמכה בינלאומית כגון: Certified Information System Security Professional (CISSP) ו־Certified Ethical Hacker (CEH).

היכרות עם סביבה טכנולוגית ואבטחת ענן (Cloud Security): מר ג׳קי אלטל, עו״ד דנית ליבוביץ־שטי

במסלול IR – קורס זה מספק היכרות עם סביבות טכנולוגיות ומוצרי אבטחת מידע, תוך הקניית ידע בסיסי בהגנת סייבר על מערכות ארגוניות בענן. הדגש הוא על למידה מעשית של אבטחת סביבות ענן, כולל ניהול זהויות והרשאות גישה (IMA), הצפנת נתונים, איתור וניטור איומים, ויישום פתרונות הגנה מתקדמים בשירותי AWS, Azure ו־Google Cloud.

במסלול GRC&P – הקורס מתמקד בהבנה של סיכוני אבטחת ענן בהיבט ניהולי, כולל עמידה בדרישות הרגולציה. התלמידים יכירו תקני אבטחה שונים וילמדו את הטמעת המדיניות הארגונית לניהול סיכוני ענן. הסטודנטים יעמיקו בתקני אבטחת מידע בענן כמו ISO 27017 ו־NIST ובתקנים המקובלים בתעשייה הבינלאומית.
הקורס מותאם להסמכות בינלאומיות כגון: Certified Could Security Professional (CCSP), במטרה להקנות לכל מסלול את הכלים המתאימים לו – טכנולוגיים או ניהוליים.

סוגיות בהגנות סייבר – תקינה, הגנה והצפנה: מר הלל קוברובסקי

במסלול IR – הקורס מקנה הבנה מעמיקה של מנגנוני ההגנה בסייבר, תקנים מרכזיים, ויישום פתרונות מתקדמים לאבטחת מערכות ארגוניות. במסלול הטכנולוגי, הדגש הוא על היכרות מעשית עם מערכות אבטחה מתקדמות, כולל סגמנטציה, חומות אש, (TUM–FW/NGFW), אבטחת נקודות קצה (EDR/EPP), ניהול זהויות והרשאות (IMA), הגבת גישה (NAC, SBC) והקשחת מערכות קריטיות. הסטודנטים ילמדו על כלי מניעת חדירה ודלף מידע, לצד שיטות הגנה ברשתות תקשורת ואבטחת התקני מובייל. כמו כן, הסטודנטים יתרגלו מעבדות ייעודיות בנושאי הקורס.

במסלול GRC&P – הקורס מתמקד בחלוקת אחריות בין בעלי תפקידים במערך הסייבר הארגוני ובשיח המתמיד בין הטכנולוגי לרגולטורי. הסטודנטים ילמדו תקני הגנה מובילים, ויכירו את הכלים המקובלים לרבות כל אלו הנלמדים במסלול IR, ובהטמעת מדיניות ניהול סיכוני סייבר, לרבות אסטרטגיות התאוששות מאסון (DRP) והמשכיות עסקית. הסטודנטים יעמיקו בנושא מניעת דלף מידע, סיכונים לארגון מבפנים ומבחוץ ועוד.

הקורס מותאם להסמכות בינלאומיות: CISSP ו־CISM.

תפיסות בהגנת סייבר: מר קובי פינטו

במסלול IR – הקורס מעניק הבנה מעמיקה של אסטרטגיות הגנה, רמות סיווג מידע ותפקיד הבקרה המפצה בארגון. במסלול הטכנולוגי, הדגש הוא על יישום מעשי של מעגלי הגנה, בקרות אבטחה והקשחת מערכות בהתאם לדרישות מבצעיות.

במסלול GRC&P – הקורס מתמקד בניבוש מדיניות אבטחת מידע, התאמתה למעגלי האבטחה השונים, והתאמת סיווגים לדרישות רגולציה וניהול בקרות אבטחה בארגונים בהתאם לנדרש בתקינה הבין לאומית.

הקורס מותאם להסמכת CISSP.

אסטרטגית סייבר ארגונית

במסלול IR: ג׳קי אלטל ומרצים אורחים

קורס R&B – Red and Blue Teaming – הקורס מתמקד בהבנת טקטיקות של תוקפים (Red Team) ובפיתוח יכולות הגנה ותגובה של צוותי אבטחה (Blue Team), תוך שימוש בסימולציות חיות המדמות תרחישי תקיפה מתקדמים. הסטודנטים יתנסו בפריצת מערכות מאובטחות, ניתוח חולשות וניסוח מתודולוגיות הגנה מותאמות לאיומים משתנים. כמו כן, יילמדו שיטות לזיהוי מתקפות בזמן אמת, תרגול תגובה מהירה וניהול אירועי סייבר בסביבה מבצעית.

במסלול GRC&P: עו״ד רמי תמם ומרצים אורחים

בקורס יתארחו אישים מובלים מהתעשייה הבינלאומית אשר יציגו זויות שונות למשבר ניהול הסייבר ובהן מו״מ, דוברות, ניהול סיכונים, מידע מודיעיני לקראת משבר ועוד, וביניהם:

- ← **עו״ד מוטי קריסטל** – מו״מ בסייבר: מומחה לניהול מו״מ, איש יחידת המו״מ המטכ״לית, ניהל עשרות מקרי מו״מ למול תוקפים בסייבר.
- ← **מר אסף ליברטי** – ניהול משבר דוברות בסייבר: מנהל משברי תקשורת בסייבר, דובר חיל האויר ודובר שב״ס לשעבר.
- ← **גב׳ ליאה צור** – ניהול סיכוני סייבר: מנהלת Riskmgmt – LT מחלוצות מנהלות הסיכונים בסייבר בישראל.
- ← **מר ליאור פישביין** – מודיעין סייבר ו״ציד איומים״ בארגונים – מנהל מודיעין הסייבר, בנק דיסקונט.
- ← **מר יריב זמר** – ראיית היריב בראי מערך הסייבר הלאומי – ר׳ אגף במערך הסייבר הלאומי.

הקורס כולל ביקורים בתעשייה בחברות שונות כגון: Cisco – Israel, Fortinet, Palo Alto, Citadel Cyber Security ועוד.

קורסים המשותפים לשני המסלולים:

ניהול משבר סייבר בארגון: עו״ד הדס בן אברהם

בעידן הנוכחי של תקיפות סייבר, ההיכרות עם סוגי התקיפות והמשמעות המשפטית של תקיפות אלו היא קריטית להמשכיות העסקית ולשרידותו של הארגון. בקורס תכירו את סוגי התקיפות הנפוצות, ותלמדו את אופן הטיפול בהן מהפן הניהולי, הטכנולוגי והמשפטי. נכיר מקרי בוחן שונים, מפי מי שניהל משברים רבים ושונים והיה שותף לניהול משברים נוספים. הקורס מותאם להסמכה בינלאומית כגון: Certified Information Security Manager (CISM). בסיום הקורס הסטודנטים ידעו לנסח ״Cyber playbook״ מקצועי – נוהל חירום לארגונים, אותו יוכלו ליישם במקום עבודתם.

שני המסלולים יתנסו בתרגילי מעבדה, כחלק מצוותי ניהול משבר, כאשר תלמידי מסלול IR יתפקדו כצוותים טכנולוגיים פורנזיים, ותלמידי מסלול GRC&P – יתפקדו כמנהלי המשבר, אנשי פרטיות, ממשל תאגידי, ניהול סיכונים ודוברות.

תקינה וחקיקה בסייבר: עו״ד רמי תמם

זירת הסייבר מביאה עימה עולם שלם של חוקים, תקנות וכללי התנהגות חדשים, המחייבים מנהלים לקחת חלק פעיל בהתנהלות הסייבר של הארגון. הקורס עוסק במגוון נושאים – החל מחובות נושאי משרה, ניהול התנהלות מול תביעות, וכלה בקודקס הפלילי של דיני הסייבר. הקורס נבנה בהתאמה עם סילבוס הידע המומלץ לצורך הסמכה בינלאומית כגון: Certified Information Security Manager (CISM) ו־Certified Information Privacy Professional (CIPP). הקורס מהווה נדבך ראשון בהכשרת ה־DPO (ראו בהמשך), ובמהלכו תרכשו את הכלים הפרקטיים להבנת צרכי הארגון ונושאי המשרה בו.

הכשרת DPO (Data Protection Officer): עו"ד עלי קלדרון (קורס רשות)

בעולם בו המידע האישי הופך למטבע עובר-סוחר, כל פעולה במרחב הפיזי והווירטואלי משאירה שובל של נתונים. בקורס נבחן את הזכות לפרטיות ואת הכללים המגדירים את אופן ההגנה עליה בחוק הישראלי והבינלאומי, ונסקור את סמכויות הרגולטור והמתחים שבין אסדרה מיושנת לעולם מודרני. נדון בדליפות מידע ובמתח שבין הגנת הסייבר לאבטחת המידע, נבחן את המתח שבין הפרטיות לזכויות אחרות, ולבסוף נחקור את המגמות בהגנת הפרטיות והאם היא עוד אפשרית או נדרשת. הקריה האקדמית אונו הייתה הראשונה ללמד קורס פרטיות כחלק מההתמחות לתואר השני, וגם הראשונה להפוך את קורס ה-DPO לקורס אקדמי. הקורס מוצע כחלק מהתכנית לתלמידי ההתמחות כקורס רשות, תחת הליכי אישור והכרה של משרד המשפטים והרשות להגנת הפרטיות.

קורס דירקטורים מומחי סייבר: רו"ח אמיר שראל, עו"ד מיכל קופל ועו"ד הדס בן אברהם (קורס רשות)

עולם הדירקטוריון והפיקוח על הנהלת התאגיד בנושא ניהול סיכוני הסייבר הופך מורכב יותר. אם בעבר היה די במומחה ייעודי למשפטים וכלכלה בכל דירקטוריון, כיום נדרשים גם דירקטורים בעלי מומחיות בסייבר. בקורס נעמוד על הצורך של דירקטורים להבין בשני התחומים, גם בתחום הסייבר וגם בתחומים הקלאסיים של עבודת הדירקטוריון – על מנת לפעול באופן מושכל לקבלת החלטות עסקיות מיטביות עבור התאגיד שבו הם מכהנים. נכיר תחומים חדשים הנוגעים לעולם האחריות התאגידית, עולם ניירות הערך, העסקאות, כלי העבודה העומדים לרשות הדירקטור, חובותיו וסמכויותיו.

פרוייקט גמר:

ד"ר אורית גולדמן, עו"ד רמי תמם, מר ג'קי אלטל ועו"ד הדס בן אברהם

הסטודנטים יוכלו לבחור בין פרויקט 'טכנולוגי-פורנזי', לבין פרויקט 'מוכנות למשברים, רגולציה ופרטיות' וכן פרויקט 'עיוני-מחקרי'.

← **פרוייקט טכנולוגי-פורנזי**

הפרויקט הטכנולוגי מתחיל בסדנת פורנזיקה מקיפה, אשר במהלכה הסטודנטים יישמו את כל הידע הנלמד במהלך השנה, וישדרגו את יכולותיהם בניתוח זירות סייבר אמיתיות. הסטודנטים ינתחו סביבות שרתים ומחשבים שונות לזיהוי וקטורי תקיפה שונים, ויציעו דרכים להתמודד עם הפריצות השונות. בסוף התהליך ינסחו דו"ח פורנזי מלא לפי הסטנדרט המקובל בתעשייה. פרויקט זה יערך במעבדת הסייבר המתקדמת בקריה.

← **פרוייקט מוכנות למשברים, רגולציה ופרטיות**

הפרויקט המעשי יבוצע בשיתוף עם ארגונים בארץ, ויתן ערך לאותם ארגונים על ידי הענקת כלים ממשיים אשר ישדרגו את יכולות ההגנה שלהם. הסטודנטים יעבדו בצוותים במודל המעשי לפיו עובדים צוותי סייבר בעולם. העבודה תתנהל מול ארגונים שונים ויעבירו בהם תהליך מוכנות סייבר מלא, המתמקד בשגרות העבודה ובגורם האנושי כפקטור המשמעותי ביותר במוכנות הסייבר. לבסוף הסטודנטים יגישו לארגון דו"ח מוכנות, הכולל ניתוח המצב הקיים, מסקנות והמלצות. פרוייקט זה הוא חלק מהתרומה לקהילה ונעשה למול ארגוני מגזר שלישי וארגוני התנדבות

← **פרוייקט עיוני מחקרי – בתחומי רגולציה, ציות, פרטיות וניהול משברים בסייבר**

הסטודנטים יחקרו סוגיה בנושאים שונים הקשורים לסייבר, ויגישו עבודה מקיפה בנושא בקבוצות. המחקרים ייערכו בליווי מנהלי המסלול ובליווי ראשת המכון לחקר סיכוני הסייבר של הקריה. סטודנטים מצטיינים יוכלו לבחור בביצוע מחקר בצוותי המחקר של מכון המחקר לסיכוני סייבר כבר בשלבים מוקדמים בתואר. המכון לחקר סיכוני סייבר הינו מוסד מחקר מוביל המתמחה בניתוח, הערכה וניהול של סיכונים בתחום הסייבר. המכון מפרסם ניירות עמדה מקיפים המספקים תובנות, המלצות ומדיניות לארגונים וקובעי מדיניות בנוגע להתמודדות עם איומי סייבר מתפתחים.

מסלולי קריירה:

בוגרי התואר יוכלו לעסוק בשורה של תפקידים ומקצועות בניהול מערכות סייבר ואסטרטגית סייבר ארגונית – בחברות עסקיות וממשלתיות, במשרדי ממשלה ובהם משרד ראש הממשלה ומשרד הביטחון, צה"ל – ביחידות השונות, לרבות יחידות מודיעין ותקשוב, משרד ראש הממשלה, המשרד לביטחון הפנים ויחידות העילית של המשטרה, בתאגידים עירוניים, ברשויות שונות, כמבקרי פנים ברשויות, במשרדי רו"ח מובילים, במשרדי עורכי דין ועוד.

Graduates tell...

כבוגרת תואר ראשון במשפטים בקריה האקדמית אונו, שמחתי מאד לשוב ללימודים בקריה. אני ממליצה בחום על התואר השני במנהל עסקים, בהתמחות בסייבר! מדובר במסלול מדהים וייחודי, מותאם לבעלי קריירה, מעשיר ומאפשר חשיפה למגוון תחומים בעולמות הסייבר, גם למי שהגיע ללא כל ידע טכנולוגי מוקדם. מרגישה שנפתח בפניי עולם חדש ומרתק!
זכיתי להכיר מרצים מדהימים, זמינים, קשובים ואכפתיים להצלחת הסטודנטים, שחשוב להם שנפיק את המיטב מהלימודים.

אביבה דוד, עו"ד

מנהלת מחלקה לביטוחי אחריות מקצועית וביטוחים נלווים לבעלי מקצועות חופשיים

התואר השני במנהל עסקים והתמחות בסייבר סקיוריטי ופורנזיקה בקריה האקדמית אונו חיבר את בשבילי את עולמות העסקים, החוק והטכנולוגיה בצורה משמעותית ויצק המון תוכן לעבודה שלי. ממליצה מאוד על תואר מרתק ומקדם עם מרצים שהם אנשי תעשייה מובילים בתחומם!

יסמין חמי

Global Partners Director
LayerX Security