

יסודות הגנת הסייבר

יסודות, עקרונות מנחים ונושאים עיקריים בהגנת הסייבר

תיאור הקורס

קורס זה הוא הבסיס לעולם אבטחת המידע ככלל וסייבר בפרט. הלומדים יבינו את המורכבות של נושא אבטחת המידע, יכירו את התקנים על יתרונותיהם וחסרונותיהם, את מושגי הסיכון, את ההבדלים בין הסטנדרטים המקובלים בתחום, את היבטי הגנת הפרטיות ודלף מידע, יבינו מהי אבטחה אפליקטיבית, מהי בקרת גישה, שירותי הענן וכיצד נתאושש מאסון. בסיום הקורס על הלומד להבין כיצד נושאים שונים שלמד מתממשים ואת יסודות הטיפול באבטחת מידע.

חשוב לדעת

מבנה הקורס: הקורס בנוי מ - 8 פרקים, כל פרק יכלול שעות לימוד עיוני ושעות לימוד מעשי. היקף השעות: 40 שעות אקדמיות (מתוכן 14 ש"א תרגול מעשי)

קהל יעד ודרישות קבלה:

סגל המרצים: למכללת iNT סגל מרצים ומומחי הדרכה, מהמובילים בתחום, בעלי ניסיון מעשי רב ביישום והדרכת נושאי הלימוד בתעשיית ההיי-טק הישראלית והעולמית.

זכאות לתעודת גמר מטעם מכללת iNT: תעודת גמר מטעם מכללת iNT תוענק לבוגרים

העומדים בתקנון הלימודים, בהגשת כל התרגילים והמשימות של המסלול ובעמידה בנוכחות

של 85% מהשיעורים לפחות.

תכנית לימודים

פרק 1 – מבוא לאבטחת מידע והגנת הסייבר (5 ש"א)

פרק זה מתמקד בהכרת מונחי יסוד ובניית השפה בה העוסקים בתחום מדברים, כותבים ודנים.

פרק 2 – תקני אבטחת מידע וניהול סיכונים (5 ש"א)

פרק זה עוסק בתיאור תקני האבטחה וה-Best Practices המקובלים בתחום אבטחת המידע והסייבר. נלמד מהם יסודות סקר סיכונים, סוגי סקרים, כיצד מתבצע סקר סיכונים ומה מטרותיו, הפעילויות להקטנת הסיכון, מושגים של סיכון, סיכון שיורי.

פרק 3 – בקרת גישה (5 ש"א)

פרק זה מיועד להכיר לתלמידים את נושא בקרת הגישה.

1. בחלק הראשון ילמדו הנושאים של בקרת גישה של משתמשים, תוכנות לרכיבים, מידע במערכות המחשב הארגוניות ורכיבים שונים ברשת הארגונית. כמו כן יסקרו מוצרים שונים בתחום.
2. בחלק השני ילמד התחום של מערכות ארגוניות לזיהוי ואימות משתמשים וחומרה.

פרק 4 – היבטי הגנת הפרטיות ודלף מידע (5 ש"א)

פרק זה מיועד להכרת נושא דלף המידע הארגוני, הסכנות שבו, תהליכי מניעה/ צמצום/ גילוי. בנוסף יסקרו מוצרים התומכים בהגנת המידע הארגוני מפני דלף מידע והפעולות שיש לנקוט בעת גילו.

פרק 5 – אבטחה אפליקטיבית (5 ש"א)

פרק זה בא להכיר בפני הלומד את העקרונות והמתודולוגיות הנהוגות בנושא הטמעת היבטי אבטחת מידע בתוכנה, ניהול שינויי תוכנה והיבטים של מבדקי אבטחת מידע בתוכנה. כמו כן יילמד הקשר בין איכות תוכנה לאבטחת מידע ואמינות תוכנה.

פרק 6 – מחשוב ענן, שירותי אירוח, וירטואליזציה (5 ש"א)

פרק זה בא להכיר בפני הלומד את עקרונות הענן ושירותי האירוח. מודלי IAAS, PAAS, SAAS.

פרק 7 – המשכיות עסקית (BCP/DRP) (5 ש"א)

פרק זה מיועד להכיר לתלמידים את נושא הגיבוי, השחזור והתאוששות מאסון על היבטיו וברמות השונות של גיבוי ושחזור. כמו כן יילמדו תמיכת מערכת ההפעלה ומוצרים משלימים, והיבטי אבטחת מידע.

פרק 8 – טיפול באירועי אבטחת מידע - SOC (5 ש"א)

בפרק זה נציג בפני הלומד את העקרונות של טיפול באירועי אבטחה. הבנת הסיטואציה של קיום מתקפה, שלבי המתקפה וכיצד לטפל באירוע. פרק זה מהווה אינטגרציה של הידע הנלמד במהלך הקורס.



המרכז הבינלאומי
ללימודי הייטק וחדשנות

* 6377

מתקדמים
לקריירה בהייטק



Microsoft Partner
Gold Learning



קמפוסים בפריסה ארצית:

באר שבע

רחוב האנרגיה 77
פארק ההייטק

ירושלים

רחוב יפו 34

רחובות

רחוב אופנהיימר 5
פארק המדע

תל אביב

ראול ולנברג 36
קריית עתידים