

Cyber Threats Intelligence

אנשי מקצוע בתחום אבטחת הסייבר צריכים להבין את האיומים, התוקפים ולהיות בעלי הבנה ברורה איך תוקפים מנסים לנצל נקודות תורפה. הקורס מספק מבט היכן קיימות נקודות תורפה בתוכנה, בענן ובמשטחי תקיפה אחרים. נחקר כיצד לסווג איומים, לעבוד עם הפגיעויות ולהשתמש במתודולוגיות הערכה נפוצות. הקורס יצלול גם להבנת איומים נגד IoT, מערכות הפעלה בזמן אמת וסביבות מבוססות ענן. הקורס יכסה את שיטות העבודה המומלצות לאבטחת סייבר בצורה שקל להטמיע בעולם האמיתי.

חשוב לדעת!

היקף השעות:

40 שעות אקדמיות

קהל יעד ודרישות קבלה:

הקורס מתאים לאנשי אבטחת מידע או סטודנטים המעוניינים להכיר את עולם אבטחת המידע ויש להם ידע בסיסי בתקשורת מחשבים ובאנגלית.

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 הקורס ובעמידה בנוכחות של 85% מהשיעורים לפחות.

תכנית לימודים

- החשיבות של Threat Intelligence
- שימוש ב- Threat Intelligence כדי לתמוך באבטחת הארגון
- ניהול Vulnerability
- שימוש בכלים נפוצים להערכת פגיעות וניתוח הפלט
- איומים ופגיעויות הקשורות לטכנולוגיות SCADA, SOC, APT, IoT, Mobile
- איומים הקשורים לענן
- הטמעת בקרות לצמצום שטח התקיפה
- הטמעת בקרות לצמצום פגיעויות בתוכנה
- ניתוח יומנים



המרכז הבינלאומי
ללימודי הייטק וחדשנות

₪6377

מתקדמים
לקריירה בהייטק

תל אביב
המרץ 2

המכללה שומרת לעצמה את הזכות לערוך מעת לעת, לפי שיקול דעתה, שינויים בתכנית הלימודים, היקף שעות הלימוד, סגל המדריכים וכד', ולא יראו בכל מידע המפורט בדפי מידע של המכללה כהתחייבות כלשהי מצד המכללה.

