פורטל דרושים
נשלח באמצעות www.drushim.co.il

טל סבן

נייד: +972 52 5181 349 מייל: Talsabana@gmail.com
GitHub: https://github.com/TalSaban

אודות

- מרצה ומלמדת קורסים בתחום האבטחת מידע/סייבר לאנשי תוכנה.
- ניסיון של מעל 3 שנים בתחום אבטחת המידע עם התמקדות במחקר וניתוח.
- ניסיון בניטור של מגוון רכיבי רשת ובפרט רכיבי אבטחת מידע תוך חקירת אירועים ויצירת התראות מותאמות.
- נחושה להתקדם בתחום, אחראית ובעלת מוטיבציה גבוהה!

ניסיון תעסוקתי

2019-2020
אנליסטית אירועי אבטחת מידע (SOC Analyst Tier 3)
MalamTeam
- טיפול שוטף וניהול של אירועים בזמן אמת עבור לקוחות החברה כולל דו"חות מפורטים.
- התנהלות מול הלקוח לשם חיבור מקורות מידע, קונפיגורציות רשת והתממשקות עם המערכות.
- חקירת אירועי אבטחת מידע, ניתוח מעמיק והצלבת נתונים לשם הסקת מסקנות.
- יצירת חוקים, קורלציות, התראות ודו"חות חכמים ב- McAfee SIEM \ IBM Qradar \ Symantec Endpoint Protection.
- פיתוח תוספי אוטומציות בשפת Python.
- ניטור מגוון רכיבי רשת ושרתים כמו WAF, IPS, IDS, NAC, AV, DLP, Proxy, AD וכו'.
- סיכום עדכונים ממקורות שונים כמו CERT.

2018-2019
אנליסטית אירועי אבטחת מידע (SOC Analyst Tier 2)
See Security
- עבודה שוטפת עם מערכות; McAfee SIEM/ IBM Qradar.
- חקירת נתונים המגיעים מהמערכות לשם זיהוי אירועי אבטחת מידע רלוונטיים ודיווח שלהם.
- יצירת דו"חות אוטומטיים והתראות.

השכלה

2017-2018 **מיישמת הגנת סייבר – CEH** [קורס באורך 800 שעות]
'צומת'
2016-2017 **חשבונאות ומערכות מידע**
המרכז האקדמי לב ('מכון לב'), ירושלים

שירות צבאי

2013-2015 **אנליסטית** | חיל המודיעין, יחידת 8200
- פיענוח מודיעיני ואיסוף כמויות גדולות של מידע ממקורות שונים ומתקדמים מבחינה טכנולוגית.
- מסגרת השירות כללה הובלת פרוייקטים בתוך היחידה בשילוב עבודת צוות ותכנון.
- ניהול מו"מ והתממשקות מול המחלקות והצוותים השונים.

כישורים

- שפות תכנות; Python
- שימוש בשפת SQL לצורך בניית מסדי נתונים ותשאול משדי נתונים ע"י שימוש בשאילתות מורכבות.
- ביג-דאטה; שאילתות מורכבות ומתקדמות ע"י טכנולוגיית Splunk ושימוש ב-R ו-Pandas.
- מערכות הפעלה; שירותי Windows (Servers, Domain Services), Linux (Ubuntu, Kali).
- Network Analysis; Wireshark, Security Onion, Snort.
- היכרות טובה עם AD (GPO) ו-Windows Sysintrnals.

שפות עברית - שפת אם | אנגלית - שוטף | ערבית - צרכי עבודה

המלצות יינתנו על פי בקשה.