

- ראש צוות SOC, ידע טכני רחב במערכות הגנה, יכולות בחקירת עומק, כתיבת קורלציות במערכות SPLUNK ו-XDR.
- עבודה שוטפת עם מערכות SIEM, FW, AV, SOAR, בניית Dashboards, ניהול ותחקור התראות בזמן אמת.
- הובלת פרויקטים משלב האפיון (SOW) ועד לביצוע Hands On - מערכות Splunk ES, XSOAR.
- יכולות חקירה גבוהות של אירועי סייבר, כתיבת חוקים ובניית Dashboards, דוחות מנכ"ל ומעקב אחר שינויים כמותיים.
- הבנת איומי סייבר וטכניקות פריצה, כתיבת נהלי עבודה עבור האנאליסטים, תחקור אירועים בסביבת-OT, מערכת SIEM של AZUR.

ניסיון תעסוקתי:

2019- היום ראש צוות SOC, אבטחת מידע וסייבר, מגדל, פתח תקווה

- התחלה כאנליסט סייבר בצוות ה-SOC ולאחר מכן קידום לראש צוות SOC.
- בניית קורלציות ויצירת חוקה Hands On, כתיבה והטמעה של נהלי עבודה, העברת הדרכות מקצועיות לצוות.
- הובלה של פרויקטים, עבודה שוטפת מול אינטגרטורים - ביצוע אגרגציה של החוקה אל מערכת Splunk-ES, אפיון SOW ו-Playbook's במערכת XSOAR.
- תפעול מערכות מבוססות אפליקטיביות/ענן - XDR, Xsoar, Mcafee, Fw-Check point, Secdo, cortex-Rשת OT,
- היכרות עם מערכת Sentinel של Azure. ניהול ותפעול ערוץ ה-Mail Relay - רכיבי Ironport, forcepoint.
- עבודה מול צוותי תשתיות רוחביות ותשתיות אבטחת מידע, צוותי PT צוות סייבר ורגולציה.

2018: אנליסט בצוות SOC, סטאדל, פתח תקווה

- ביצוע פורנזיקה בטיקטים ברמת Tier 1, ניתוח ההתראה מקבלתה ועד להסקת מסקנות וממצאים, עבודה על מערכת SIEM- Qradar, כתיבת דוחות ללקוחות, ביצוע עדכוני אבטחה ובדיקת חולשות חדשות - Advisory.
- תפעול מערכות מבוססות אפליקציה ושליטה מרחוק - Simplify, DDI, Arcsight, Sysaid, Secdo, Epo, Dcm, Citerix, IOC.

2017: תמיכה טכנית, טריפל סי, פתח תקווה

- נציג בקרה ותמיכה טכנית, פתרון בעיות בתחום התקשורת והאינטרנט הקווי והאלחוטי, איתור תשתיות.
- תפעול מערכות מבוססות אפליקציה, תהליכי אוטומציה בארגון, עבודה מול ממשקים.
- הקמת בסיסי נתונים, תפעול מערכות CRM, LDAP, שרתי אירוח, בקורות גישה והרשאות, מדיניות אבטחה.

2016: מנהל צוות מכירות, Eloan, הלוואות חברתיות, רמת גן

- ניהול נציגי מכירות מוקד, מעקב יומי אחר מכירות בפועל, מתן תמריצים על בסיס תוצאות.
- הדרכה מקצועית לשיחת מכירה אפקטיבית : תסריטי שיחה, טיפול בהתנגדויות, אומנות המכירה.
- הקמת בסיסי נתונים על מוצרים ולקוחות כולל תמחור במערכת CRM, ניהול סיכונים.

השכלה:

2021: תכנית לפיתוח ראשי צוותים טכנולוגיים.

2018-2017: קצין אבטחת מידע ארגוני ומומחה לוחמת סייבר, הרחבה של CISO, מכללת SELA GROUP.

2013-2010: תואר ראשון B.A בתקשורת שיווקית, דוברות יחסי ציבור ופרסום, מכללת ספיר.

2003-1997: תיכון אורט על שם צימטבאום, ערד.

** המלצות יינתנו על פי דרישה