שלומי הרצברג פתח תקווה | 050-4812250 |shrzbrg@gmail.com
ש. לידה : 1985 | ת.ז. 021522107

- 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 האיפיון (**SOW**) ועד לביצוע **Hands On**- מערכות **XSOAR**, **Splunk ES**.
- 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 כאנאליסט 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 אפליקטיבי\ענן- cortex-XDR, Xsoar, Mcafee, Fw-Check point, Secdo רשת 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: אנאליסט בצוות **SOC**, סיטאדל, 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, שרותי אירוח, בקרות 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 .

שרות צבאי: מלא, חיל חימוש (2004-2007) | קבלת אות חייל מצטיין

שפות: עברית : שפת אם | אנגלית: טובה מאוד

** המלצות יינתנו על פי דרישה