

## SIEM SOC Analyst \ PT JUNIOR \ Cyber Integrator

ת"ז: 319036182 | נייד: 050-2211210 | מייל: [Oshritzafri@gmail.com](mailto:Oshritzafri@gmail.com) | ש. לידה: 1997, רווק

- בוגר קורס אבטחת מידע וסייבר **Cyber Ethical Hacking**, ידע בתקשורת ורשתות עד לרמת הפרוטוקולים **TCP/IP**.
- בעל ניסיון צבאי כמנהל רשתות מחשוב, אוגדה 252, חיל שריון
- ידע וניסיון מעשי בהקמה הגדרת תשתיות תקשורת ושירותי רשת מתקדמים, מיומנות כתיבת קוד ב- **Python**.
- עם מוטיבציה גבוהה ורצון עז להשתלב בתחום אבטחת מידע. אשמח להזדמנות

### השכלה:

2019 – 2020: בסיום לימודים – קורס אבטחת מידע, מכללת "האקר-יו", ת"א. היקף הקורס כ- 540 שעות.

### התנסות מעשית במהלך הלימודים:

- ניסיון **Hand on SIEM SOC Alerts** - חקירת לוגים ויצירת במערכת **Splunk**.
- **Virtualization** – עבודה עם סביבות וירטואליות הכולל הגדרות רשת שונות.
- הגדרת מערכות **IPS/IDS** וכתיבת חוקים לזיהוי מתקפות תשתית ורשת.
- **Infrastructure Attacks** – ביצוע תקיפות תשתית ומעקף של מערכות הגנה להשגת **Shell** על מחשב מרוחק.
- בדיקות חדירה לאתרים – החל מהסריקה הראשונית ועד לכתיבת דוח ה- **PT**.
- **Mobile Reverse Engineering** – חקירת אפליקציות **Android** ב- **Smali** ו- **Java**.
- **Malware Analysis & Reverse Engineering**.

2009 – 2015: בגרות מלאה במגמת אלקטרוניקה ותקשורת, תיכון מרחבים.

### ניסיון תעסוקתי:

2016 – 2018: שירות סדיר חיל תקשוב שחרור בדרגת סמ"ר

מנהל רשתות מחשוב, אוגדה 252 (2016 - 2018)

- אחראי לתקינות, זמינות ובקרת מערכות מחשוב וצידוד קצה של כ-150 יחידות קצה וכ-300 משתמשים.
- בקרה והטמעה של מערכות מיקרוסופט (**AD, Exchange, XP, W7, Office**).
- אחראיות צידוד תקשורת וחומרה וטיפול בתקלות (**Cisco, HP, Lexmark**).
- טיפול בשרתים, רשתות, אבטחת מידע ותקשורת; הקמה, התקנה, שדרוג, הטמעה ותחזוקה שוטפים.
- אבטחת משתמשים ונקודות קצה, עבודה עם תוכנת אנטי וירוס: **McAfee**.

05.01.2021: שכיר בחברת "בזק-אונליין" במשרת **Help-Desk**

- רפרנט על 2 מוקדים טלפונים המונים עשרות נציגים, כולל אחמשיה ועמדות מנהלים
- אחראי לתקינות זמינות ובקרת מערכות מחשוב וטלפוניה, כ-400 יחידות קצה וכ-800 משתמשים.
- עבודה באופן שוטף עם **AD, Portnox, CME, CrowdStrike, FortiNet, XORCOM**,

### כלים וטכנולוגיות:

- שרתים: **IBM, HP, Dell, Windows Server 2016**
- מערכות הפעלה: **Windows 10, Debian, Ubuntu**
- יישומים: **Active Directory, Exchange**
- שפות פיתוח: **HTML, JavaScript, Python**
- וירטואליזציה: **VMWare, VirtualBox**
- תקשורת: **Switches, Routers, Firewalls, TCP/IP**
- רשתות גלובליות: **LAN / WAN**

### שפות:

עברית – שפת אם, אנגלית – טובה

המלצות יוגשו לפי דרישה.