052-7201102 | [mizrahiya@gmail.com](mailto:mizrahiya@gmail.com)

שוהם

ת"ז: 303141920 | שנת לידה: 1978,ישראל

* **מנהל מרכז ל א.מ וסייבר בתעשייה האווירית , התמחות מעל ל- 15 שנים בתחום מערכות המידע והסייבר ,עבודה מול גופים אזרחים וצבאיים ניהול והכשרת עובדים לרמה מבצעית.**.
* **מנהל מרכז ל א.מ וסייבר בחברת טבע –ניהול אירועי סייבר בסביבה גלובאלית מעל ל- 80 מדינות.**
* **התמחות בניהול עובדים בסביבה הרוחבית של מערכות המידע והסייבר.**
* **ניהול וביצוע סקרי א.מ וסייבר לצורך התאמת פערי אבטחה בארגון.**
* **ראיה מערכתית ואוריינטציה עיסקית, יכולת ניתוח נתונים והסקת מסקנות, יוזמתי , יחסי בין אנוש מצוינים.**
* **רמת סיווג : צבאית – סודי ביותר / אזרחי מלמ"ב רמה 2 .**

**השכלה והסמכות:**

2018-2020 :קורסים והסמכות בנושאי ניהול, חקירות, פרוייקטים,SCADA בנושא א.מ וסייבר (במסגרת חברת טבע )

2017 :הסמכה **CCNA - Routing and Switching**

2016 **:** הסמכה **מיישם אבטחת מידע וסייבר ממוקד עבור תע"א.**

2016-2017 : קורס הסמכה מטעם מלמ"ב – **מנהל חקירה פורנזיות**.

2014 : הסמכה - נאמן ביטחון למערכות מידע.

2003-2014 : קורסים והכשרות בתעשיה האווירית ע"י מלמ"ב וגופים אחרים בנושאי-אבטחת מידע ,סייבר ,ניהול מערכות

מידע,והצפנות.

2008-2011 : תואר ראשון **(B.A ,(במגמת ניהול** אוניברסיטתבר- אילן

: 2003 הנדסת רשתות .**Microsoft MCSE**

2001-2003 : הסמכה **מנהל רשת ותומךPC** במכללת ""New Horizons

1999-2000 : הסמכה **טכנאיp.c**  ותומך רשתות תקשורת במכללת "אשרות" בחיפה.

1999 : לימודים בתחום office , פוטו-שופ , ארכיטקטורת מחשבים במכללת עמק הירדן.

1993-1996 : בגרות מלאה במגמה עיונית מסלול טכנולוגי- מכניקה הנדסית.

**ניסיון תעסוקתי:**

**2020- 2017– עובד פעיל -cyber defence center & information manager TEVA**

* **ידע ומומחיות בניהול והכשרת צוותי תגובה גלובאלים נגד אירועי סייבר ברחבי העולם.**
* **ידע מעמיק של כתיבה והבנת תרחישים מורכבים ודינמיים תוך מציאת פתרונות מתקדמים.**
* **ידע וניסיון מערכות SIEM -** **ArcSigh,Qradar,** **Resilient,Splunk ביצוע ניתוח סטטי/ דינמי.**
* **כתיבת נהלים ומטודולוגיות לכלל מערכות ההגנה,חשיבה יצירתית לתרחישים עתידיים וישומם בארגון.**
* **הגדרת תהליכים ומערכות לצורך לניטור והגנה (משלב הרכש ועד שלב עבודה בסביבית PRD)**
* **הגדרה והטמעת תהליכי SLA ואסקלציות בין צוותים בסביבות רוחביות וגלובאליות .**
* **הגדרת מערך וטכנולוגיות חדשות לאיסוף מודיעין המייצר התראות בזמן אמת תוך טיוב והחרגת.**
* **הגדרה והטמעת טכנולוגיות חדשות בעולם ה ICS – PLC -SCADA (CyberX).**
* **בחינת מוצרים וחלופות לצורך מימוש אפקטיביות תרחישים והתראות לצורך תאימות ארגונית.**
* **יכולת למידה מהירה לצורך השתלבות** **בארגון , ייצירת מערכת יחסים חזקה ומיומנויות בינאישיים.**
  1. **cyber defence center & information manager – מנהל מרכז הסייבר בתעשייה אווירית**
* **גיוס והכשרת אנליסטים לרמת תגובה בכלל מערכות השו"ב לרמה מבצעית.**
* **ניהול 15 עובדים ב**  **CDC-SOCשל תעשייה אווירית.**
* **כתיבה ואיפיון נהלים ומתודולוגיות לאירועי א.מ וסייבר.**
* **כתיבת דוחות אירועי א.מ וסייבר להנהלה בכירה .**
* **POC בתהליך הוצאת 22703 -ISO (תקן סייבר של מכון התקנים הראשון שהוצא עבור גופים בטחוניים בארץ).**
* **איפיון תהליכי מרכז הסייבר של תעש"א ומערך ההגנה הכולל הגדרת תשתית,תוכנה,רכש,גיוס עובדים,נהלים משלב הקמתו .**
* **איפיון מערכות הגנה SLA,IOC,(פיתוח פנימי).**
* **מודיעין – איסוף ועדכון מודיעין במערכות ההגנה מכלל המגזר העסקי והבטחוני .**
* **עבודה במערכת SIEM מהמתקדמות בשוק – עדכון וטיוב חוקים על בסיס טיוב המערכות בזמן אמת.**
* **עבודה עם כלל מערכות ההגנה והבקרה מהמתקדמים בשוק (יפורט בראיון העבודה במידת הצורך).**

**IT MANAGER 2003-2015 - מנהל מחשוב ואבטחת מידע**

* **מנהל רשתות ואבטחת מידע בתעשיה האווירית (תעשיות גולן) .**
* **התמחות בניהול צוותי עובדים וקבלת החלטות בזמן אמת ומתן מענה להמשכיות עסקית.**
* **הקמה ותחזוקה של מערכות המחשוב ומערכות המידע חומרה\תוכנה, שרתים,נתבים,מרכזיות .ip**
* **הצפנת נתונים מול סביבה רוחבית תוך שימת דגש על תקנים ורגולציות בתחום אבטחת מידע והסייבר.**
* **הקמה ומיפויי רשתות תקשורת בתשתית של סיבים אופטיים, נחושת,RF.**
* **מטמיע מערכות POC בפרוייקט הטמעת מערכות בסביבה הרוחבית SAP-ERP .**
* **POC בפרוייקט הקונסולידציה שבמערך הסייבר ומערכות המידע .**
* **אחראי על רכש המחשוב וציוד הקצה, תמחור הזמנות ורכוש קבוע.**
* **אחראי על וועדות מחשוב ויישום תוכניות אב רב-שנתיות,**
* **אחראי על תוכנית DRP (תוכנית התאוששות מאסון),איפיון מערכות בשעת חירום .**
* **מנהל חוות שרתים –הפצה,גיבוי,מדפסות,A.D, פרוטוקולי- sql, TCP/IP, HTTP, SSL, HTML, XML,Java, DNS,**
* **מגדיר אסטרטגיות, מדיניות באבטחת המידע והסייבר ומתן מענה להמשכיות עסקית.**
* **ניסיון עם מערכת שו"ב (SIEM) , device control, control guard ואחרים.**

2007- 2003 : **פתיחת עסק וניהולו**

● **תחזוקת מחשבים ורשתות תקשורת שיחזורי מידע -"חקירת מחשבים".**

● **תחזוקת מערכות מידע מול מוסדות ציבוריים ומוסדות של משרד הביטחון.**

1. **אחזקת רשת מחשבים במכללת y2k" טכנולוגיות"** ,

* סיוע ואחזקת רשת מחשבים במהלך השעורים במכללה.

2000 **מנהל מעבדת מחשבים**

● ניהול ואחזקה מעבדת מחשבים בחנות "קלאסיק חשמל מחשבים טבריה".

● עבודה שוטפת עם תוכנה וחומרה מהמתקדמות ביותר.

● התקנת מחשבים שרתים וציוד קצה.

● תיקון בעיות מחשוב וציוד תקשורת עד בית הלקוח/העסק.

**שפות:** עברית – שפת אם | אנגלית- ברמה טובה מאוד.

**שרות צבאי:**

1996-1999 – שרות צבאי מלא באוגדת שריון.

* טירונות בביסל"ח.
* מילוי תפקידים אחראיים ובכירים.
* ארגון וניהול כולל.
* תאום וקישור ליחידות.
* יישום והפעלת נהלים בשטח.
* מציאת פתרונות לבעיות טכניות.
* שחרור בדרגת סמ"ר, כיום דרגת רס"ל ומשמש כמומחה סייבר בחטיבה.