**מרון מהדב**

פתח תקווה | ש.לידה 1997

[meronmm@gmail.com](mailto:meronmm@gmail.com)| 054-4891903

* אנליסט סייבר בכיר בעל ניסיון והתמחות במערכות ענן ובמערכות תפעוליות(OT)
* ניסיון בניתוח חקירת וניהול אירועי סייבר.
* ניסיון הטמעה, ניהול ותחזוקה של מערכות SIME שונות אצל לקוחות בקנה מידה גדול
* בעל הסמכת – Azure Administrator Associate, AWS Cloud Practitioner, IBM Qradar fundamental
* AWS Certified Security – Specialty, Cybersecurity Fundamentals Certificate .

**השכלה:**

* 2018: קורס "מיישם הגנה בסייבר"(CSP)-מוסמך הרשות הלאומית להגנת סייבר
* 2015-2012: בגרות טכנולוגית מלאה, מגמה מקצועית הנדסת תוכנה ופיזיקה, תיכון מקצועי "עמל ב".
* 2012-2015: תעודות בגרות חברתית 2011:תעודת מדריך מטעם משרד החינוך

**כלים טכנולוגים:**

* שפות תכנות: C#, ,BASH, PYTHON,POWERSHELL
* מערכות הפעלה
  + LINUX: KALI, UBUNTU, CentOS
  + :Windows Windows 10, Windows Server
* מערכות אבטחה וניטור: QRadar , AlienVault , ArcSight, DataDog
* מוצרי EDR: CISCO AMP, carbon black, CrowdStrike
* פרוטוקולי תקשורת: כגון- DNS,HTTP,SNMP. IP,SSH,SMTP ,UDP/ .Syslog,TCP
* הבנת איומי סייבר וטכניקות פריצה לעומק: כגוון- DOS,BRUTE FORCE,PHISHING Ransomware.
* אנטי וירוס וFW: Zscaler, McAfee,TrendMicro ,
* שירותי ענן:AWS , AZURE , IBM CLOUD,GCP

**ניסיון תעסוקתי:**

2020: אנליסט סייבר בכיר:

* ביצוע סקרי סיכונים ומענה על חוזים ומכרזים ברמה מקצועית
* התמעת מערכות אבטחת מידע שונות אצל לקוחות
* פיתוח אינטגרציה בין מוצרי אבטחה שונים- שימוש בAPI וכתבית אוטומציות לתהלכים אלו
* עבודה מול גופים רגולטורים בארץ ובעולם (משרד האנרגיה,המכון לסייבר לאומי,תיקני PCI,ISO12007)
* עבודה מול תשתיות מדינה קריטיות- חיבור המערכות לSOC המדיני, ביצוע שידרוגים במערכות רגישות חיות

2019:SOC\NOC Analyst Tier 1

* כתיבת דוחות על מתקפות סייבר חקירתם וישום הגנות רלוונטיות.
* פיתוח כלי אוטומיזיציה שונים בפיתון בעולם הענן.
* עבודה יומיומית עם שרתי לינוקס.
* פיתוח כלי אינטגרציה אבטחתיים בעולמות הענן.

2011-2016: מדריך בניה והטסת טיסנים ב"קלוב תעופה פ"ת"

* ניהול צוות המדריכים
* הדרכה והעברת ידע מורכב

**שירות צבאי:**

2016-2019: לוחם במערך הרקטי, חיל התותחנים (שחרור דרגת סמל ראשון)

* עבודה בצוות בתנאי לחץ מסביב לשעון
* מעבר קורס "מיישם הגנה בסייבר"(CSP) הראשון בצבא בהצטיינות.

**שפות:** עברית-שפת אם | אנגלית-רמה טובה מאוד