**\*\* סודיות הכרחית \*\***

**ניתן ליצור קשר בשעות הערב או להשאיר הודעה, כולל SMS, ואחזור בהקדם**

* 23 שנה בתחומי תשתיות, System, תקשורת ואבט"מ (Hands On)
* ארכיטקט מערכת: תכנון ופיקוח (יישומים מתקדמים), הגדרת סטנדרטים, כלים, תשתית ופלטפורמה
* ניהול ובניית צוות אבטחת מידע וסייבר (מומחה CISO).
* ניהול צוות מקצועי רב תחומי, ניהול פרויקטים רוחביים חוצי ארגון, ראייה מערכתית, חשיבה יזמית.

**הישגים עיקריים וציוני דרך**

* מומחיות וניסיון עשיר בתחום אבטחת המידע, סייבר ומערכות מידע
* בניית צוות אבטחת מידע וסייבר לצד אחריות על כל חדרי השרתים בארגון.
* אפיון והקמת אתרDRP .
* הטמעה בארגון של מערכות וירטואליזציה((VMware ואחסון NETAPP, HP-3par.
* אפיון / הטמעה / אחריות / תפעול / ניהול מערכת שו"ב תקשורת CA-SPETRUM ,PRTG ,SOLARWINDS Mrtg,.
* ניהול התקנה של רשת ארגונית בסביבת CISCO ו- 3, F5,HP ,COM בעלת שרידות גבוהה , נתבים ומתגים.
* ניהול DNS / DOMAIN חיצוניים ויישום CRTIFICATES.

**ניסיון תעסוקתי**

**2018 - היום: מנהל מערכות מידע (IT) אבט"מ תשתיות, טכנולוגיות. ניהול צוות של 5 אנשים.**

קבוצה, בתחומי התשתיות, התחבורה, האנרגיה, המים, התעשייה והאוטומוטיב

* ניהול וביצוע פרויקטים רוחביים: איפיון, איתור, וגיבוש פתרונות / חדשנות
* ניהול פרויקטים בתחום אבטחת מידע וסייבר מול הפיתוח וה-IT של הארגון (ועמידה ברגולציות אבטחה)
* בנית אסטרטגיה עבור מערכות המידע בארגון ובכללם אבטחת מידע.
* איפיון / איתור פתרונות טכנולוגיים מותאמי צרכים וארגון, רגולציה באבט"מ ו IT
* תכנון ובחירת פתרונות למערכות מידע ומערכות טכנולוגיות לארגון
* ידע מעמיק ברשתות תקשורת, שרתים ותחנות קצה (H/O)
* שפור תהליכים, ייעול חסכון מקסום ובקרה מול ספקים בתחום IT / אבט"מ (רכש)
* בניית תכניות עבודה שנתיות / יעוץ טכנולוגי הנחיה, כתיבת נהלים, מדיניות ותפישות אבטחת מידע והגנה בסייבר
* יכולת וניסיון בהקמת מערכות בארכיטקטורה מורכבת. עבודה HO מעמיקה עם רשתות תקשורת לרבות היכרות עם מערכות מידע.
* יכולות בחינת מוצרי אבטחת מידע וטכנולוגיות חדישות והתאמתם לארגון ע"פ צרכיו / אופיו / ותקציב.

**2004 - 2018: ראש צוות אבטחת מידע וסייבר תקשורת, System, ניהול צוות של 8 אנשים.**

ארגון ביטחוני ממשלתי – כ-5000 תחנות עבודה וכ-700 שרתים

* מעובד סיסטם התפתחתי ולמדתי, עד לתפקיד ראש צוות אבטחת מידע וסייבר תקשורת, System
* בניית והקמת צוות אבטחת מידע ותכנון אסטרטגי.
* ניהול פרויקטים מול גופי IT כגון: תשתיות, פיתוח והנדסה, ניטור מפת סיכוני אבטחת מידע וסייבר.
* כתיבת נהלים, ניתוח תהליכים וסקר סיכונים לעולם אבטחת המידע והגנת הסייבר והתשתיות.
* אפיון, בדיקת POC, והטמעה על פי צורכי הארגון .
* הכרה בתקני אבט"מ והוראות לניהול סיכוני אבט"מ וסקרי סיכונים.

**2004-2013 : ראש צוות סיסטם ותקשורת (ניהול צוות של כ-10 טכנאים)**

ארגון ביטחוני ממשלתי – כ-5000 תחנות עבודה וכ-700 שרתים

* אחראי על חדרי השרתים בארגון.
* ניהול וליווי פרויקטים בדגש על תשתיות.
* אופרציות רוחביות של הארגון, כגון DRP ו BCP
* אחריות ותחזוקה כלל אירגונית לכל מערכות ההפעלה והשרתים בארגון, גיבויים ואמינות המידע.
* הטמעת מיזמי חומרה משלב תכנון, מפרט טכני עד שלב ביצוע והתקנה - החלפת שרתים, קונסולידציה של שרתים.
* ניהול תשתיות הארגון: Active directory, DNS , Certificate Auth ,DHCP ,PKI., MS Cluster , Terminal services , GPO ,File Servers ,Print servers ,Web Services
* התקנה ניהול ותפעול של מערכות WINDOWS 2000 – 2016 , LINUX
* הטמעה תחזקה והתקנה של מערכות וכלי שו"ב

**2000-2004 : ארטנט אקספרטס/ אמפא מוצרי צריכה**

מומחה פתרונות ותמיכת לקוחות במוצרים השונים.

**1994-2000 : צה"ל , שירות קבע מקצועי, דרגת רס"ר**

חיל הקשר – מפקד יחידת מחשוב בחטיבה סדירה

צל"ש מקצין תחזוקה ראשי על בניית והקמת מערכת ניהול צי רכב

**אישיות:**

ראייה רחבה, לויאלי, אוטודידקט

**שפות:**

**עברית**- שפת אם **אנגלית** –שליטה טובה מאוד בכתב ובעל פה.

**========================================================**

**הסמכות והשתלמויות מקצועיות**

* הסמכות:
* ISACA-CISM
* ISACA-CSX-F
* VCP5 5
* CCNA R&S
* NG Check Point
* השתלמויות :
  + קורס מנמרים – טכניון לימודי חוץ
  + Security:

Ciso Technion, HDE 57 – Hacker define expert , CCSK –cloud security, Advance cyber course, Projects manager.

* + Communication:

HP VIRTUAL CONNECT, CCNP Route v.2, 3com, SPECTRUM

* + System:

Veeam Backup and Restore, VCOPS, , Linux Fundamentals, NETAPP מתקדם, EVA , LIVE COMUNICATION CENTER, Right Fax, OFFICE SYSTEMS 2003, Exchange 2003, Windows 2003

* טכנאי מערכות ענ"א, בגרות מלאה מגמת מחשבים.

**ניסיון טכני**

* Security
* Firewall:
  + - Checkpoint : Management, Security module, clusters, Eventia, Blades : TP,IPS,APP Control , Mobile, DLP, Sandbox
  + Fortigate
  + Palo Alto : Panorama, Clusters
* Remote access
  + Juniper – SslVpn
* NAC
  + Portnox, MS NAP, OPEN NAC
* SEM / EVENTS
  + I wrote a system to analyze syslog messages to understand and correlates events
* SIEM
  + Mcafee Nitro
* MailRelay
  + IronPort
* End Point Security
* McAfee Enterprise sutie for end point
  + EPO,AGENT,VSE,DLP,HIPS,TIE,MAR
* PROXY
  + SQUID, McAfee Security Gateway.
* IPS/IDS
  + SNORT ,CheckPoint
* Penetration test KaliLinux , Open Vas ,Metasploit
* Communication
  + Monitoring PRTG, NXLOG, SolarWinds
  + Routers – CISCO ASR 1002 ,7200,3800,2800,2900,1800,1900
  + Switches - CISCO ,HP , 3com , Cisco 29XX , 36XX,37XX ,Hp 55XX , 7900,59XX
  + Network topology and infrastructure monitoring.
  + Communication environments: LAN WAN, APN, WIFI, Bluetooth and Internet.
  + Dynamic routing protocols: Eigrp, Ospf, BGP.
  + SNMP, SYSLOG, XFLOW, Sniffer
* System
  + Enterprise infrastructure management: Active Directory, DNS, Certificate Auth, DHCP, PKI, MS Cluster, Terminal services, GPO, File Servers, Print servers, Web Services
  + Organization-wide server maintenance.
  + Installation and management of WINDOWS 2000 - 2016 systems
  + MS updates include the POPSUM process
  + Managing Exchange Mail systems 5.5 - 2010 in DR environment
  + Operation of LINUX systems.
  + Extensive knowledge of Office systems including: VISIO, MS Project.
* Monitoring
  + mplementation and maintenance of monitoring systems
  + SPECTRUM – Implement a CA product for network management and monitoring.
  + SOLARWINDS –Implment , maintenance of network management and monitoring
  + PRTG .- Establishment of maintenance system for sampling communication equipment and saving history.
  + KIWI syslog - Setting up a system for collecting logs from communications equipment.