**דור אבגנים** **ירושלים | 050-7573326 | doravganim@gmail.com**

* **ידע מעמיק וניסיון עשיר בתחום אבטחת המידע וסייבר, היכרות עם מגוון מערכות ותהליכים בארגונים ממשלתיים ופרטיים**
* **תפעול, תחזוקה וטיפול במגוון תקלות בכלי אבטחת מידע לצד הובלת פרויקטים להטמעת מערכות בסביבה פיסית ווירטואלית**
* **ניסיון בתחקור וניהול אירועי אבטחה, היכרות עם סוגי מתקפות ופתרונות אבטחה, עבודה עם מערכת SIEM**
* **הכרות עם כלים ומע' אבטחה, אנגלית ברמת שפת אם, ניהול והנעת צוות עובדים, תקשורת מול לקוחות, וגופים פנים וחוץ ארגוניים**

**ניסיון תעסוקתי:**

2018 – כיום: **מיישם אבטחת מידע, צוות אבטחת מידע תשתיתי, משרד הבריאות**

* **התקנה, תפעול ותחזוקת כלי אבטחת המידע** - עבודה בצוות, בנית תוכניות עבודה, הקמת פרויקטים
* **עדכון, גיבוי, אחסון, טיפול במגוון תקלות במערכות:**

**Checkpoint FW, Palo Alto (IPS, IDS, URL Filtering, WF) , FireEye (NX, EX), NAC**

**RSA (SIEM, OPT) , Qradar (SIEM), CyberArk IBV, ODI**

* **ניהול אירועי סייבר מקצה לקצה** (זיהוי, תגובה, תחקור, ניהול וכו').
* **ניהול חדר כספות ושירותי הלבנה מקומית ובענן** (AZURE).
* **תמיכה במנהלי אבטחת המידע** בבתי החולים ועשרות ארגונים בכל מגזר הבריאות (15,000 משתמשים):

 ליווי אירועי אבטחת מידע (Tier 3), תפעול מערכות מתממשקות, הטמעת פתרונות לתהליכים המשתנים.

2018-2016: **מנהל צוות SOC , משרד האוצר**

* **הקמה מן היסוד של מרכז בקרת אבטחת מידע הפועל 24/7**; גיוס אנליסטים, פיקוח על התקנת המערכות,

בנית נהלים ושגרות עבודה לכל תרחיש ואירוע. (מנגנוני בקרה ונהלי תגובה).

* **ניהול צוות אנליסטים**, קליטה והכשרה, חלוקת משימות ומעקב אחר הביצועים ומתן מענה לדילמות מקצועיות.
* **העברת הדרכות שוטפות וטיוב הידע המקצועי**, חשיפה לחידושים וטרנדים בעולם אבטחת המידע.
* **ניהול ובקרת אירועים,** איסוף, עיבוד וניטור נתונים ומידע מהתראות וממגוון מערכות המידע
* **הובלת מגוון פרויקטי ליבה** משלב תכנון, ליווי תהליך ההקמה ועד לשלב ההטמעה בקרב המשתמשים.
* **הובלת פרויקט מורכב להטמעת מערכת SIEM,** לרבות איפיון וכתיבת חוקים לאופטימיזציה וטיוב ההתראות.
* **עבודה עם כלים וטכנולוגיות ניטור**, ידע מעמיק בתחום חולשות ופגיעויות אבטחה פומביות.

2016-2015: **אנליסט אבטחת מידע וסייבר, חברת טראסטנט בע"מ**

* **מתן שירות אבטחת מידע וסייבר למגוון חברות**, עבודה בצוות INCIDENT RESPONSE במרכז SOC.
* **תחקור מידע המתקבל ממערכות מנוטרות**, איסוף נתונים, זיהוי פעילויות חריגות, ניתוח אירועים
* **הכנת דוחות יומיים, שבועיים וחודשיים** ביניהם דוחות פרואקטיביים ודוחות אירוע.
* **עבודה מול מערכות** **(Firewall, IPS, IDS, Proxy, Anti-Virus, SIEM, DLP),**

**שרות צבאי:**

2015-2012: **אנליסט אבטחת מידע בצוות SOC , ממר"ם**

* **תחקור אירועים**, איסוף, עיבוד וניתוח נתונים ומידע מהתראות וממגוון מערכות המידע מסווגות ומערכת **SIEM**.
* **ליווי האירועים**, הנחית קציני הסייבר ביחידות לדרכי התמודדות ומעקב אחר התפתחויות.

**סגן קצין סייבר פיקודי, פיקוד מרכז**

* **אחריות ומתן מענה מקצועי** בתחום אבטחת המידע בפיקוד וביחידותיו.
* **ניהול ותחקור אירועי סייבר ברמת השטח**, ממשק שוטף מול גוף הסייבר המטכלי והצוותים הכפופים.
* **טיוב הידע המקצועי של יחידות השטח**, העברת הדרכות ואימון בנושאי סייבר ואבטחת מידע.

**השכלה:**

2015: לימודי תעודה, **קורס מנהלי רשתות ומיישמי אבטחת מידע**, **CCNA CCSA,** מכללת שיא סקיוריטי

2012-2011: לימודי תעודה, **קורס מנהלי תשתיות ואבטחת מידע, MCITP MCSA MCTS MCSE,** מכללת גון ברייס

2011-2007 בגרות מלאה, תיכון קדמה, ירושלים

**שפות:** עברית – שפת אם, אנגלית – ברמת שפת אם ***\*המלצות יינתנו עפ"י דרישה***