קורות חיים- קיריל קולשוב

- **בוגר תואר ראשון**
- **מוסמך קורס באבטחת מידע ולוחמת סייבר.**
- **בעל קשרים בין אישיים מעולים, ראיה טכנית רחבה, יכולת עבודה תחת לחץ תוך תיעדוף משימות, יכולת עבודה בצוות ובעל נכונות לעבודה קשה.**

פרטים אישיים:
סיווג ביטחוני: רמה 2 בתוקף
כתובת: יגאל אלון 40, הרצליה
טלפון: 054-7908755
כתובת מייל: kuleshov7186@gmail.com

השכלה:
2016-2017– קורס קצין אבטחת מידע ומומחה לוחמת סייבר במכללת סלע (CWS& CISO)- לימוד תשתיות מחשוב ואבטחת מידע.
2009-2012 – תואר ראשון באוניברסיטת בר אילן במסלול "ניצבים", מקצוע ראשי קרימינולוגיה.
2001-2005- כ"ג יורדי הסירה, בית הספר לקציני ים בעכו. בגרות מלאה במגמת מכטרוניקה.

ניסיון תעסוקתי:

2019- עד היום : מנהל SOC באחת מחברות הביטוח הגדולות בארץ. במסגרת התפקיד נדרש ניהול של צוות SOC מקומי, אינטגרטורים וצוות SOC נוסף (הנותן גיבוי מעבר לשעות פעילות החברה). כמו כן, בניית נהלים, מתודולוגיות עבודה ובקרה על מידע רגיש של החברה. כחלק מיישום הבקרה יש למפות שלבים קריטיים ורגישים של מערכות מידע שונות בחברה וליצור בקרות ובקרות מפצות בכדי למנוע הונאות בכספי הלקוחות, דלף או גניבת מידע רגיש של החברה. בנוסף לעבודה השוטפת, גייסתי שלושה מתוך ארבעה אנשי צוות (בקר, מומחה טכני ואנליסט) וניהלתי מספר POC's מול חברות שונות.

שירות מילואים פעיל במשרד ראש הממשלה – במסגרת השירות נדרשת הערכת חשיבות הנכס מבחינת אבטחת מידע, פגישה עם גורמי חוץ וביצוע בקרות על תשתית בה נשמר המידע הרגיש אצל גורמי החוץ.

2018-2019: ראש צוות SOC בחברת ADAMA LTD. במסגרת התפקיד נדרש ניהול צוות אנליסטים, כתיבת מתודולוגיית עבודה, נהלי IRT, ניהול והגדרת מערכת ה-SIEM (כולל חיבור רכיבים ופרסור), הובלת פרויקט הקמה וחיבור מערכת ה-SIEM לכלל הסניפים בעולם (מעל 50 מדינות ברחבי העולם). פרט לניהול הצוות וכחלק מהתפקיד יש לתעדף משימות ולייעץ לאנליסטים בביצוע חקירות נרחבות יותר תוך שימוש בכלים דוגמת Checkpoint, EPO , Mcafee Forensics ועוד.

2017-2018 : אנליסט SOC בכיר בחברת 2Bsecure. במסגרת התפקיד נדרש פיקוח ובקרה על אירועי אבטחת המידע השונים של הלקוחות השונים בביצוע חקירה פרואקטיבית על תעבורת תקשורת הלקוחות. תחקור האירועים נעשה בעזרת מערכת RSA Security Analytics ,IBM QRadar, ו- WAF של Reblaize. בתום הליך החקירה נדרשה הגשת חוות דעת ללקוחות כולל ממצאים, מסקנות והמלצות לביצוע.

2016-2017 : NOC בחברת AMDOCS - במסגרת התפקיד נדרש פיקוח ובקרה על כללי שרתי לינוקס ו- Windows (עשרות אלפי שרתים ברחבי העולם) עם מערכות שו"ב, גיבוי ושחזור שרתים, עבודה מול בסיסי נתונים, ניהול ותפעול תקלות שונות תוך Drill Down וניטור של מערכות התקשורת השונות.

2016 : Help Desk בחברת כלל ביטוח- במסגרת התפקיד נדרש מתן פתרונות טכניים לעובדי החברה ולגורמים חיצוניים העובדים עם החברה (מעל 10 אלפי משתמשים).

2013-2016 : מז"פ- חוקר זירת עבירה במשטרת ישראל- במסגרת התפקיד נדרש ניתוח מידע בזירה, הפרדה בין עיקר וטפל ויצירת תמונה של התרחשות בזירה לבית המשפט.

2009-2013 : משרד ראש הממשלה- במהלך התקופה ביצעתי מספר תפקידים שבמסגרתם נדרש ניהול של בקרת כניסה והרשאות, ניהול פגישות עם גופי מודיעין עמיתים, טיפול בחומר מסווג ואבטחתו ועבודה על חומר מודיעיני מסווג ביותר כאנליסט מודיעין.

שירות צבאי: 2005-2008 : שירות כלוחם ביחמ"מ- בגדוד 869 במודיעין שדה.

שפות: רוסית- שפת אם. עברית- ברמת שפת אם. אנגלית- ברמה גבוהה מאוד.