רחלי בסול

soc Analyst

פרטים אישיים

053-2253005

rachelib124@gmail.com

תאריך לידה
25/10/2001

שפות

עיברית

אנגלית

תקציר

אנליסטית soc עם ניסיון עשיר בתחום אבטחת מידע מהשרות הלאומי בGOV.IL ,
תפקידי דרש ממני מיומנויות רבות כמו יוזמה, פתרון בעיות מורכבות ,עבודת צוות גבוהה, יכולת טיפול במספר משימות במקביל וצורת עבודה מסודרת ,יסודית ושיטתית. הנני אוהבת לחקור ומחפשת משרה מלאה ומאתגרת.

ניסיון תעסוקתי

soc Analyst, israel E-Goverment - gov.il, ירושלים
ספטמבר 2019 - היום

• עבודה עם טכנולוגיות וכלי אבטחת מידע -FW, WAF-Imperva
AV- SourceFire TippingPoint , IPS\IDS-CheckPoint,
TrendMicro, EDR-FireEye
• יכולת כתיבת חוקים במערכות הגנה FW, IDS / IPS
• **אחראית חקירות ואישורי אבטחת מידע בהתרעות מערכת CRM** -
- חקירת התרעות בגין גישה לip/domain זדוני או גישה מdomain\ IP
- חקירה וטיפול מעמיק בהתרעות AV של ונקיטת פעולות recovery
- חקירה מעמיקה למיילים חשודים שהתקבלו באחד ממשרדי ראש הממשלה
• **הכרות מעמיקה ועבודה עם מערכת SIEM -splunk Enterprise- Security**
- חקירה ותגובה לאירועי אבטחה
- שליטה ובקיעות במערכת החיפוש
- הכרות עם פקודות לצורך בניית חוקים וחיפוש אפקטיבי כולל Regex
- בניית החרגות לצורך טיוב החוקים ומניעת FP
• ניהול אבטחת קבצים הנכנסים לארגון ע"י שימוש במוצר OPSWAT MetaDefender
• הכרות עם שפות תכנות -Python, JAVASCRIPT
• הכרות עם מבני מערכות הפעלה windows, linux ויכולת תפעול בסביבת bash Linux
• היכרות מעמיקה עם ארכיטקטורת אבטחה ופרוטוקולי תקשורת; HTTP, SSH, DHCP, DNS, UDP, TCP, IP, ARP, Ethernet
• מנתחת דוחות אבטחה ואחראית איסוף IOCs

השכלה

קורס מגן סייבר, מכללת ג'ון בריס
נובמבר 2020 - היום

- הגנת סביבות ארגוניות ובניית ארכיטקטורת אבטחה
- התקפת סביבות סייבר וניצול חולשות
- חקירת אירועי אבטחה
- בקרה וניהול אירועי סייבר

Splunk Fundamentals
אפריל 2020 - יולי 2020

- הבנת במערכת החיפוש SPL, וביצירת דוחות
- הכרות עם שדות חיפוש חישוביים וסטטיסטים
- יצירת תגים וסוגי אירועים, באמצעות פקודות macro ויצירת פעולות workflow
- יצירה ועבודה עם DataModel, Dataset

Cisco CCNA: Cisco Certified Network Associate
ספטמבר 2019 - מרץ 2020

- יסודות הרשת - מודלים OSI ו- TCP / IP ופרוטוקולי רשת
- ניתוב טכנולוגיות LAN \WAN וארכיטקטורת רשת
- ניתוח נתוני אבטחה
- קריפטוגרפיה והגנה על נקודות קצה

תעודת בגרות מלאה , מעיינות בית רבקה -חב"ד
ספטמבר 2013 - ספטמבר 2019

- 4 יחידות מתמטיקה
- 5 יחידות כלכלה ומנהל עסקים
- 4 יחידות אנגלית

טכנולוגיות
ספטמבר 2019 - היום

- WAF-Imperva
FW-CheckPoint
IPS\IDS- SourceFire TippingPoint,
AV-TrendMicro
EDR-FireEye
SIEM- Splunk enterprise security
OPSWAT MetaDefender
CRM-Yuval System

ממליצים
ממליצים יועברו על פי דרישה