Shahar Gabay

Summary:

- Experience in SOC security field.
- Over 2 years of experience in the Mamram unit of the IDF.
- Training a team member of SOC analysts.
- A highly motivated creative thinker, an independent learner, a good team player , Finding a solution to work problems under stressful conditions.

Personal Information:

Address
39 Herzel St.
Kiryat Yam
Israel
Phone
+972-52-6600408
E-mail
Shahargb06@gmail.com
Date of birth
2000/06/11

SOC analyst Experience – Military Service

- *SOC analyst Mamram Unit* -

- Guiding and training a team of 5 SOC analysts (tiers 1) Established 2 new SOC teams at different IDF units (mainly Regional Commands) – including team design, system implementation and team qualification
- Supervision of 6 SOC teams at different IDF units.
- Endpoint forensics, based on in-house investigation
- Tools.
- Creating a manual: Defining how to respond for incidents and scenarios. Basic steps and explanations of Writing and implementing information security procedures, and cyber security system rule-sets.
- Investigation and management of cyber-security incidents.
- Performing full analysis on alerts from various cyber security systems (SIEM, HIPS, NAC, FW, and DLP).
- Finding a solution to work problems under pressure.
- Managing multiple projects at once.
- Team management as a professional figure and maintaining availability 24/7.

Cyber course – ITQ :

- A 290-hour hands-on training program includes hands-on work on the Cisco. training lab. The course included servers, networks, SOCs, and firewalls.
- Management and configuration of Windows Server 2019 servers.
- Setting up Cisco communications equipment according to CCNA v7.0.
- Studying LPI Linux Essentials.
- Cisco CyberOps Associate program studies include hands-on work with IBM QRadar.
- Establishment and setup of Checkpoint R80 firewalls.

Skills:

- Arcsight (Micro Focus) & SSIM (Symantec) – rule creation,queries & reports, case management.
- Portnox – Device management, complince setup and monitoring.
- Mcafee EPO – creating policies and rules for different Mcafee products (Dlp, HIPS, VSE), running queries&reports.

Professional Certifications:

- ArcSight Analyst & Administrator - We Ankor – 2020
- Network computing management -Bahad 7 – 2018
- CCNA & CyberOps – ITQ- 2021

Education:

SEP 2015 –JUN 2018
Rabin High School, Kiryat Yam.
Graduated with extended 5 of Psychologic.