JONATHAN DAVIDASHVILLY

CYBER SECURITY ANALYST

DETAILS

PHONE
(972) 053-928-7353

EMAIL
jonathan.davidashvilly@gmail.com

NATIONALITY
American/Israeli

LINKS

LinkedIn

SKILLS

Ethical Hacking

Networking

Linux OS

Windows OS

Python

Power-Shell

Scanning

Enumeration

HOBBIES

Boxing
Drumming
Cooking

LANGUAGES

English
●●●●●

Hebrew
●●●●●

PROFILE

Ambitious cyber security analyst seeking to take on a new role in an exciting field. Previous SOC cyber security analyst in the Cyber Defense Directorate in the IDF's Northern Command Center with skills and experience. Enthusiastic, driven, curious, hardworking and a contributing team member. Currently pursuing CEH and CEH (Masters) certificates.

EMPLOYMENT HISTORY

Cyber Security Analyst , J6 & Cyber Defense Directorate, IDF

Zefat, Israel

May 2019 — Feb 2021

- Cyber analyst in IDF Northern Command Center's SOC team responsible for monitoring and analyzing IDF's northern cyber security posture on an ongoing basis.
- Administered incident response action-plan upon cyber incidents within Northern Command Center's responsibility domain by documenting all activities during an incident and provided support with status updates during the incident life cycle.
- Analyzed network activity for monitoring cyber posture using SIEM, ArcSight, McAfee EPO, Windows SysInternals, Portnox, Wireshark and general Windows network/domain tools.
- Influenced and innovated on existing processes by way of technical innovation and operational change through scripting programs in python and Power-Shell.
- Maximized SOC efficiency by automating crucial workflow patterns across multiple platforms such as Arcsight, SIEM, Excel, Outlook and Windows OS using third party python libraries.
- Mitigated attack vectors on battalion offices by enforcing security standards in software versions, networking standards, operating system configurations, physical protocols and user behavior.
- Decreased vulnerabilities and exposures through cyber investigation of local incidents by reinforcing OWASP principles across cyber infrastructure, then educating relevant personnel with enhancement reports.
- Good understanding of scanning/enumeration concepts using tools such as Nmap, Hping3, subli3ter, Sherlock, DNSRecon, Recon-ng.
- Basic experience with offensive security tools/techniques such as Metasploit, THC-Hydra, John-The-Ripper, SQLmap, SEToolkit, Yersinia, arp-spoofing and DOS.
- Basic understanding of common attack vectors across integration of OSI layers and general domain resources.
- Strong understanding of networking concepts of TCP/IP suite and protocols involved.
- Trained new recruits with cyber security work flow techniques, tactics and protocols by providing hands on personal training sessions and updating recruitment training procedures.

CERTIFICIATIONS

Cyber Security Practitioner

J6 & Cyber Defense Directorate, IDF