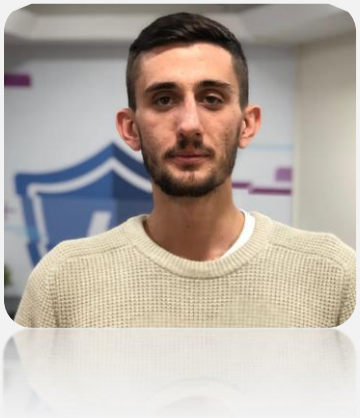
Sean Tsvik



Contact

Address:
Ramla, Israel

Phone:
+972 (0)50-7142011

Email:
seantsv@gmail.com

Languages

English –

Hebrew –

Russian –

Certifications

Offensive Security - OSCP – In Progress
EC-Council – CEHv10
Fortinet – NSE (1 & 2)
Cisco - CCNA
ICSI – CNSS
Basis Technology - Autopsy Hands On

Experience

HackerU Solutions, Israel

Head of IR & Threat Hunting – 2020 – till now

Last July, I was assigned as Head of Incident Response & Threat Hunting operations, along with the duty to lead the team.

- Creating and assigning tasks, supervising the team daily progress.
- Supervising Incident handling and documentation
- Communicating directly with the assets owners and business response plan owners during high severity incidents.
- Writing response "playbooks" for each incident or event
- Managing and assuring threat feeds are received, aggregated, reviewed, tickets and acted upon accordingly.

Additional Projects [B2B]:

- Servers & Clouds Configuration Hardening
- Risk Assessment Projects
- Threat Intelligence Reports

Cyber Security Lecturer – 2020 – till now

Lecturing in Offensive Cyber Security courses on various models, such as Cyber Infrastructure Attacks, Windows & Linux Servers Fundamentals, Web Infrastructure Attacks, Win\Linux Privilege escalation, and etc.

SOC & MSSP Deployment – 2019 – 2020

Participated in a project of building MSSP\SOC services from start.

- Deployed and configured various security products on Linux and Windows servers, such as SIEM (Qradar & ELK), Endpoint Management Server (ESET), Mail Relay(Office Security) and EDR (CrowdStrike & Carbon Black).
- Created operating procedures regarding daily operations, Incident Response, Malware Analysis, also working plans to improve the team and the services.

Cyber Security Challenges & Content Development – 2019

Developed challenges for Cywar product owned by HackerU Solution, on two main Cyber Security fields:

Offensive - Services exploitation, Win\Linux privilege escalation, Web Infrastrucare attacks [SQLi, XSS, RFI, LFI,], Basic Win\Linux Buffer Overflows.

Defensive – Memory analysis, Process Hollowing, Network traffic Investigation, Security Logs analysis from SIEM, Stenography, Fileless Malware analysis.

- Created learning materials for Cyber Security courses. The materials were used by universities around the world, and by HackerU campuses.

Motorola Solutions, Israel

Security Operational Center Analyst– 2018 – 2019 [Achieved Civilian Clearness]

- Maintained security and network assets using various products such as SIEM (Splunk), Endpoints protection, NAC (Forescout),WAF (F5), and Solarwinds.
- Administrated Windows domain servers & services such as Active Directory, Group Policy, DHCP, DNS, etc.

Israel Defense Force, Israel

Staff Sergeant Israeli Air Force "Herev-Magen" - 2015 – 2018 [Achieved Military Clearness]

- Classified

Summary

Young and highly motived Cyber Security fan, self-confident with the capability to work under presser on various projects. Good interaction with people, and working within a team. always attempting to achieve new skills and improving my knowledge. Highly experienced in building security operation programs in small companies, building and managing the SOC/MSSP while implementing advanced detection mechanisms based on known/emerging attacks, TTPs, and IOCs.