Ido Partuk

052-8741446
Ido.Partuk@gmail.com
Even Sapir, Jerusalem
04.01.1993

Experience:

2020-Present: **Cyber security analyst at Malam team**

- Conduct proactive monitoring, investigation, and mitigation of security incidents
- Analyze security event data from the network
- create and adjust Siem correlation rules
- Perform static malware analysis on isolated virtual servers
- Recognize potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information.
- Search firewall, email, web or DNS logs to identify and mitigate intrusion attempts.
- Identifying potential threat, anomalies, and infections.
- Investigate malicious phishing emails, domains and IPs using Open Source tools and recommend proper blocking based on analysis.
- Analyze and assess security incidents and escalate to client or appropriate internal teams for additional assistance

2017-2020: **Cyber security analyst & instructor at Cyberbit**

- Conducting full investigation (windows and Linux forensics, Network forensic) with various tools Siem, FW, IPS/IDS, Sysinternals, Wireshark and NMS.
- Technical hands-on training of Cyber attack scenarios, deep understanding of attack vectors, network propagation concepts and mitigations best practice.
- Scripting language Powershell, Python, Bash, Javascript
- Extensive understanding of network protocols and behaviors.
- On site Implementation, installation and maintenance of Cyber security Products for local and international customers. Including configurations of ESXi servers, Cisco switches, VMware virtual servers, Databases and Networks.
- Performing penetration tests in order to create Cyber attack scenarios (Kali, Metasploit, SQL, PowerShell, Python, bash, Javascript, html, jQuery) and implementation in the company's products.
- Designing and migrating the company's products to Cloud infrastructure.

2016-2017: **System administrator – "Dvir communications"**

- Management and maintenance of company servers such as AD, SQL, FS, VPN and web.
- Upgrade and maintenance of Veeam backups.
- Upgrade and maintenance of Virtualization solutions – VMware vSphere.

Education:

2019-2020: penetration testing to web applications.

2016-2018: Microsoft Certified Solution Associate – MCSA.

2008-2011: high school graduate in Ort Ramot, Jerusalem.

Military service:

2011-2014: Combat engineering corps warrior and commander.

- Commander curse, commanding on 15 warriors.
- Managing tight schedules under pressure.

Languages:

Hebrew – Native

English – professional working proficiency