Shmuel Hayun

Agam Kineret 8
Netanya

0545312253
Shonhay@gmail.com

Experience

BlueVoyant / L1 Operations
November 2019 - April 2020, Tel Aviv

Whitelisting/Blacklisting items after researching them, analysing over 200 financial organisations' traffic, files and various other potential risk vectors.

Splunk, Demisto, Carbon Black, Alien Vault, CrowdStrike.

BDO / SOC analyst
June 2018 - April 2019, Tel Aviv

Includes sending regular hunting reports correlating latest indicators of compromise for over 50 clients as well as communicating with them on a regular basis.

Kibana, Demisto, Splunk, Arcsight.

Cynet / Analyst
February 2017 - April 2018, Rishon Le'Zion

Part of a six man team operating and maintaining Cynet 360 EDR, updating the database with new malicious signatures as well as forensic research into new malware and customer/technical service.

Sysinternals.

FeeX / Pension Analyst
April 2016 - January 2017, Herzliya

Analysing US pension plans to optimize growth against fees, heavy utilization of SQL queries.

MySQL.

Education

John Bryce / Cyber Defender
March 2017 - February 2018, Tel Aviv

Certificate of approximately 420 hours of study including forensics, organisational security, pen-testing with Kali, risks and mitigation, vulnerabilities and exploits, data recovery, server deployment and maintenance, in-depth networking, Linux with Regex usage and basic operation of AD and other cloud based providers.