Yoav Yehudai

Security Researcher

Haifa, Israel 054-2043697 doubley612@gmail.com

SKILLS

Blue Team, TTP Research, Threat Hunting, Scripting (Python, PowerShell), Software Development (C#), Neo4J DB, Computer Networks, Windows Internals, Threat and Network Protocols Analysis

EXPERIENCE

Novartis, Tel Aviv- *Defensive Cyber Security Researcher* (Nov 2017 - PRESENT)

- Design and implement new capabilities for the Security Operations Center.
- Assess current detections and implement new ones according to MITRE TTPs research.
- Develop internal custom tools to identify and reduce attack surface.
- Produce detailed technical reports and metrics for management and stakeholders.
- Evaluate the company's security posture regularly and compose risk analysis papers.
- Lead "hunting expeditions" using threat intelligence to detect threat actors in the network.
- Work closely with Offensive Security Researchers to mitigate security gaps by leading purple team investigations.
- Evaluate and integrate new security products in the environment.

Check Point, Tel Aviv - *Security Analyst* (Aug 2015 - Oct 2017)

- Research of malwares' network traffic and develop protections.
- Web applications' analysis using Wireshark, data analysis using SQL.
- Content management of the Anti-Bot blade, including urgent releases of 0-day protections.
- Facilitate the weekly release cycle in coordination with the Anti-Bot release manager.
- Python scripting - development of integration and automation tools.

EDUCATION

Technion, Haifa - *B.Sc. in Math & Computer science* (Oct 2012 - Feb 2017)

MILITARY SERVICE

Head of Program, Academy Of Combat Physical Training (Oct 2007 - Nov 2011)

VOLUNTEERING

CISV Organization - Leader of kids' delegations (ages 11-15) to international summer camps (Aug 2014 - PRESENT)