Shay Mordechai

Security Researcher | OS Internals & Network Specialist

❖ **052-306-4991** | ❖ **My E-Mail** | ❖ **My LinkedIn** | ❖ **My GitHub**

Summary

Security Researcher specializing in **Network Protocols** and **Anomaly Detection**. Expert in building automated research tools, bridging low-level packet manipulation with high-volume data analysis. Combines theoretical networking foundations with hands-on experience in Python, SQL, and Cloud Security

Professional Experience

DevSecOps Intern | Israel Tax Authority | 2024 - 2025

- **Defense in Depth & AppSec**: Orchestrated a multi-layered security strategy across the SDLC. Conducted Threat Modeling (Design), integrated **SAST/SCA** pipelines (Build), and enforced **JSON**/XML schema hardening *on IBM DataPower (Runtime). Collaboration:* Partnered with SOC/SIEM teams on secure system design, code reviews, and incident response procedures.

Combat Soldier | Intelligence Gathering Unit, IDF

Technical Projects

Real-Time Anomaly Detection System ("Project Sniper")

- **Architecture & Logic:** Architected a high-performance **ETL Pipeline** (Python/SQL) for financial time-series data. Developed a heuristic engine to identify **behavioral anomalies** (e.g., "Whale" accumulation) and separate signal from noise
- **Security Correlation:** Applied **Threat Hunting methodologies** to financial markets, simulating SIEM/XDR logic to detect manipulation patterns and volatility spikes

Network Protocol & Traffic Analysis Toolset

- **Traffic Generator:** [GitHub] Built a **TLS Traffic Generator** using **Scapy** and [GitHub] implemented core protocols (HTTP/DNS/SMTP) from scratch using **Raw Sockets** for deep packet inspection
- **Custom CTF Platform:** [GitHub] Developed a Python-based platform (3,400+ LoC) simulating **MITM attacks** on Certificate Authorities (CA), designing scenarios for CSR interception using **Burp Suite**

AI-Augmented Vulnerability Research | *Responsible Disclosure in Progress* - Orchestrated an AI-driven fuzzing workflow identifying **3 zero-day vulnerabilities** (Memory Corruption) in the SBCL compiler

Education

B.Sc. Computer Science | Jerusalem College of Technology | ***2021-2025*** | GPA: 89
Relevant coursework: Network Analysis (97)**,** Reverse Engineering (93), Information Security (90)

Technical Skills

Core Skills: Anomaly Detection, Data Analysis, Network Analysis (L2-L7), Threat Hunting, Research Automation
Languages: Python (**Pandas, SQL**), C/C++, Assembly (x86), Bash
Tools & Infra: Burp Suite, Wireshark, Scapy, Docker, Linux (Fedora/Kali), Azure DevOps