

Shay Mordechai

Security Researcher | OS Internals & Network Specialist

❖ [052-306-4991](#) | ❖ [My E-Mail](#) | ❖ [My LinkedIn](#) | ❖ [My GitHub](#)

Summary

Security Researcher focusing on the intersection of **Low-Level Internals** and **Cloud-Native Infrastructure**. Specializing in **Browser Security (V8/JIT)** and Runtime Threat Detection. Leveraging **AI-driven methodologies** to deconstruct complex systems and build automated research workflows. Bridging the gap between raw memory manipulation and modern cloud architectures

Professional Experience

DevSecOps Intern | Israel Tax Authority | 2024 – 2025

- **Pipeline Security:** Integrated SAST/SCA (Checkmarx) into Azure DevOps CI/CD pipelines.
- **Collaboration:** Worked with SOC/SIEM teams on secure system design, code reviews, and incident handling.

Combat Soldier | Intelligence Gathering Unit, IDF

Technical Projects

End-to-End Runtime Attack Research - Architecting a full exploitation chain: Simulating **V8 JIT vulnerabilities** (Ignition/TurboFan abuse) leading to **Container Escapes**, utilizing **AI Agents** (Antigravity) for RWX memory analysis and K8s post-exploitation

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

Network Protocol & Traffic Analysis Toolset - Developed a comprehensive research portfolio including: **Custom CTF Platform:** Simulating ICMP Exfiltration and TLS Spoofing (3,400+ LoC in Python) [[GitHub](#)]. **Traffic Generator & Internals:** Built a **TLS Traffic Generator** (Scapy) [[GitHub](#)] and implemented core protocols (HTTP/DNS/SMTP) from scratch using **Raw Sockets** to analyze packet structures [[GitHub](#)]

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: V8/JIT Internals, AI Agents, K8s, eBPF, Reverse Engineering (IDA), Fuzzing, Scapy, Raw Sockets

Languages & Tools: Python, C/C++, Assembly (x86), Bash, SQL, Docker, Linux (Fedora/Kali), Git, Azure DevOps