

Amit Adler

Threat Detection Engineer

amit.adler12@gmail.com | [Linkedin](#) | [0522442013](#) | [Github](#)

SUMMARY

Cybersecurity professional with hands-on experience in advanced threat detection, behavioral investigation, and automation-driven response. Proven ability to design high-fidelity detection logic, develop custom research tools, and lead investigations across enterprise environments. Passionate about uncovering hidden threats through anomaly detection, log correlation, and proactive tool development.

TECHNICAL SKILLS

- **Security Tools:** Splunk, Splunk SOAR, OSQuery, BigFix, SCCM, McAfee EPO, SmartConsole
- **Scripting & Programming:** Python, PowerShell, C#, C, Bash, SQL/SPL
- **Network & Domain Security:** CheckPoint Firewall, Active Directory, Network Security, Domain Security, Network Protocols, Wireshark, Anomaly Detection
- **Operating Systems:** Windows, Linux

PROFESSIONAL EXPERIENCE

Detection Engineer, Israeli Military Intelligence Aug 2022 - Apr 2025

- **Threat Detection:** Designed and fine-tuned sophisticated SPL detection logic to identify complex attack patterns, significantly reducing false positives and increasing detection velocity.
- **Security Research:** Led in-depth incident investigations, focused on uncovering hidden threats through multi-source log analysis, anomaly detection, and behavioral pattern recognition resulting in an enhanced defense capabilities.
- **Automation & Response:** Led the implementation of Splunk SOAR, Developing and maintaining automated playbooks to streamline response workflows and boost efficiency.
- **Scripting & Automation:** Developed custom Python and PowerShell scripts for analyzing large-scale security telemetry, uncovering behavioral patterns and hidden anomalies. Built automated enrichment pipelines to accelerate IOC identification and enhance attribution accuracy.

EDUCATION

Splunk	Jan 2025
Investigating Incidents With Splunk SOAR	
IDF - BHD 7	Aug 2022 - Dec 2022
Cyber Security Analyst	
Introduction To Cyber Security	
Pre-Army Leadership Academy	Sep 2021 - Jun 2022
Mechinat 'Beit Yisrael'	
NESS Technologies	Apr 2017 - Apr 2019
CTM-ED - Certification Technology Management	