TOM ABAI

SECURITY RESEARCHER

Visit my llm secuirty hands-on platform @ www.llm-sec.dev

PROFESSIONAL SUMMARY

Passionate and innovative Security Researcher, specializing in AI and Supply chain security security. Proven track record of conducting cutting-edge research on vulnerabilities, open-source threats, and emerging security challenges. Skilled in analyzing complex security landscapes and collaborating across cross-functional teams to enhance product security.

REACH ME AT

Phone: 0508579043
Email: tom.abai12@gmail.com
Linkedin: https://www.linkedin.com/in/tom-abai-a4862915a/
My Articles- https://www.mend.io/author/tom-abai/

CORE COMPETENCIES

- LLM Security & Adversarial AI Research
- Vulnerability Detection and Analysis
- Owasp top 10 for llm
- Python Scripting & Security Tools
- Offensive Security (Kali Linux)
- Malware Analysis (Static & Dynamic)
- Open-Source Threat Intelligence
- Supply Chain Security

RESEARCH HIGHLIGHTS

- Created an llm security hands-on platform
- Published Supply-Chain-Threat-Hunting research report - https://www.mend.io/wp-content/media/2024/05/Essential-Guide-to-Threat-Hunting-2024-Report.pdf)
- Ongoing research into AI security vulnerabilities and mitigation strategies

ADDITIONAL SKILLS

- Programming: Python, SQL, JavaScript
- Tools: Git, Wireshark, Metasploit, Burp Suite, IDA Pro, Hugging Face, Guardrails-AI
- Languages: Fluent in English and Hebrew

MILITARY SERVICE

3 years as a fighter in NAHAL unit

INTERESTS

- Cybersecurity Research
- Capture The Flag (CTF) Competitions
- Computer Troubleshooting
- Continuous Learning in AI Technologies

PROFESSIONAL EXPERIENCE

Security Researcher | Mend.io

Nov 2022 - Present
- Research on malicious open-source packages and foundation models
- Conducted in-depth analysis of vulnerabilities in open-source projects
- Utilized AWS Bedrock models for advanced vulnerability scoring
- Wrote technical blogs documenting critical security incidents
- Analyzed malware across multiple programming languages (C++, C#, JavaScript)
- Collaborated closely with product and development teams to enhance security capabilities

Security Research Analyst | Mend.io

Aug 2021 - Nov 2022
- Investigated daily published vulnerabilities in open-source ecosystems
- Engaged with development teams to improve product security
- Identified undisclosed vulnerabilities through security advisories and bug bounty programs

Production Supervisor | Palram

Mar 2018 - Apr 2021

-Improved the plant production efficiency in 15% by creating an EXCEL app for analyzing the production process
- In charge of production orders and raw material planning

TECHNICAL SPECIALISTS TEAM LEADER | Palram

Apr 2012 - Mar 2018

- Designed and assembled complex profiles for the plastic industry
- Upgraded my department abilities and assembly time in 50% by implementing new work instructions and methodology

PROFESSIONAL CERTIFICATIONS & TRAINING

- **Practical Web Hacking | TCM Security (July 2024)**
- **Practical Bug Bounty | TCM Security (Feb 2024)**
  - Web application vulnerability assessment
  - Hands-on methodologies for security testing
- **Certified Malware Analyst Professional | MalwareAnalysis.co (Aug 2023)**
  - 40 CEU Hours | Advanced static and dynamic malware analysis
  - Reverse engineering using IDA Pro
- **Practical Ethical Hacking | TCM Security (Aug 2022)**
  - In-depth network penetration testing
  - Web application security fundamentals (OWASP Top 10)
- **Osint Fundamentals | TCM Security (Feb 2022)**

ACADEMIC BACKGROUND

Cybersecurity Diploma | Cybint & 8200 Alumni Association

Postgraduate Diploma | Apr 2021 - Present
- Foundational training in network defense, ethical hacking, digital forensics
- Threat intelligence and malware analysis

WESTERN GALIL COLLEGE

Bachelor of Arts | Oct 2017 - Jun 2020
- Academic Excellence: 91 GPA