Assaf Morag

Director of Threat Intelligence | Cybersecurity Research
Madrid, Spain | +34 615 113 117 | assafm27@gmail.com | NIE | Spanish A2

My website

LinkedIn

PROFILE

Director-level cybersecurity researcher specializing in cloud-native threat intelligence, Linux-targeted malware, adversary infrastructure mapping, and large-scale honeypot operations. Proven executive communicator and research strategist delivering intelligence to global Fortune enterprises and driving product security evolution.

CORE CAPABILITIES

- Threat Intelligence & Adversary Tracking
- Cloud-Native Security & Kubernetes Runtime Defense
- Linux Malware Reverse Engineering (ELF, Go-based)
- High-Scale Honeypot Intelligence Systems
- AI/LLM Attack Surface Research
- Data-Driven Detection Engineering & OSINT Automation

KEY ACHIEVEMENTS

- Architected multi-region honeypot pipelines collecting ~30M artifacts/month; drove discovery of novel cloud-linked malware families.
- Published influential intelligence reports shaping Linux and cloud-native security industry standards.
- Featured by media including Dark Reading, Hacker News, and ScienceDirect for cutting-edge cloud threat insights.
- Led attacker behavior research that materially influenced product detection logic deployed at scale.

EXPERIENCE

Aqua Security | Director of Threat Intelligence | 2024 – Present

- Lead global adversary-focused research portfolio for cloud-native attacks.
- Collaborate with engineering & product security to translate insights into protections.
- Manage media & conference presence as primary research spokesperson.

Aqua Security | Security Research Team Lead | 2020 – 2023

- Managed a security R&D group delivering threat detection pipelines and attack surface discovery systems.
- Hands-on research: Kubernetes runtime abuse, cloud identity hijacking, supply-chain exploitation.
- Led extensive publication agenda including annual Cloud Native Threat Report.

BlueVoyant | Chief Cyber Threat Intelligence Analyst | 2018 – 2020

- Directed CTI strategy across 25 analysts; automated global threat telemetry ingestion.
- Provided intelligence briefings to Fortune 20 executives and national entities.

IBM Security (Trusteer) | Fraud Research TL | 2015 – 2018

- Delivered research insights powering key product detection logic for financial sector clients.
- Led bank-focused technical engagements across EU.

PUBLICATIONS & TALKS

- Lead author: Cloud Native Threat Reports (Aqua).
- Talks: RSA, TyphoonCon, KubeSec, CSIT, O'Reilly.
- Contributed: MITRE ATT&CK for Containers.
- Research cited across top-tier security and academic outlets.

EDUCATION

- M.Sc. Data Science & Business Analytics | Tel Aviv University
- B.Sc. Industrial & Management Engineering | Tel Aviv University
- B.A. Psychology, Sociology & Anthropology | Tel Aviv University | Summa Cum Laude

TECHNICAL SKILLS

- DevOps skillset.
- Linux & Linux Internals & Incident Analysis
- Python, Bash, SQL, NoSQL, Big Data
- Malware analysis (ELF, Go-based loaders, cloud payloads)
- Cloud (AWS, GCP), Containers & Orchestration (Docker/K8S)