BENNY GINGIHASHVILI

SOC Analyst | Incident Response | Threat Hunting | Security Engineering

gingi2603@gmail.com • Holon, Israel • bennygingi.tech • linkedin.com/in/benny-gingihasvili • github.com/BennyGingi

PROFESSIONAL SUMMARY

SOC analyst with hands-on enterprise experience in incident response, threat hunting, and endpoint and identity investigations. Daily operator of CrowdStrike Falcon, Hunters SIEM, Microsoft Defender, Palo Alto Panorama and Entra ID, mapping adversary behaviour to MITRE ATT&CK across the full incident lifecycle. Also a full-stack developer — sole builder of an internal IOC enrichment platform adopted into daily analyst workflow, plus several shipped side projects. Seeking a DevSecOps or Security Engineering role.

EXPERIENCE

SOC Analyst (Tier 1) — Mobileye (Intel)

Jun 2025 – Aug 2026

Jerusalem, Israel · Enterprise Security Operations Center

- Investigated and triaged security alerts across CrowdStrike Falcon (EDR/XDR), Hunters SIEM and Microsoft Defender, prioritising critical incidents for rapid containment and escalation.
- Performed process tree analysis on defence-evasion detections, tracing execution chains against command-line arguments, file paths and hash reputation to classify true positives and escalate through structured incident reports.
- Hunted across identity, network and endpoint telemetry; surfaced a credential-harvesting phishing campaign, drove containment with the email security team, and briefed leadership post-incident.
- Contained phishing and malware incidents end to end, mapping adversary behaviour to MITRE ATT&CK and owning case lifecycle through closure.
- Detected identity-based attacks in Entra ID sign-in and audit logs — impossible travel, OAuth consent abuse, suspicious MFA activity — correlating with endpoint and firewall telemetry to assess lateral movement.
- Designed, built and deployed two internal tools into the team's production triage workflow as sole developer.

SOC Portal — *IOC enrichment & investigation platform · sole developer*

- Built an internal analyst tool that consolidated investigation steps previously spread across separate vendor consoles into a single workflow, reducing time to verdict per alert.
- Integrated eight threat-intelligence sources (VirusTotal, AbuseIPDB, AlienVault OTX, URLScan, Hybrid Analysis, GreyNoise, URLhaus, OpenPhish) behind one interface, plus bidirectional SIEM API integration pulling alert context directly into the enrichment view.
- Delivered analyst feedback scoring, tiered authentication and an admin panel; owned the full stack and production operations end to end (Next.js, Node.js, PostgreSQL).

Phish-IT — *automated phishing analysis module · sole developer*

- URL and domain extraction, brand-impersonation detection, screenshot capture and multi-source verdict scoring; tuned against live analyst feedback and deployed into the triage workflow.

SentinelForge — *detection engineering prototype*

- Auto-scores alert severity and generates draft Sigma rule templates from observed telemetry patterns.

SELECTED PERSONAL PROJECTS

- **FoodCritic** — full-stack restaurant discovery and review platform. Next.js 14, TypeScript, Supabase, PostgreSQL, Leaflet.js. Real-time social feed, referral and reward system, 45 end-to-end tests passing. *Live.*
- **GHOSTEYE Suite** — Python OSINT and recon toolkit: passive reconnaissance, a SOC command centre with phishing analyser, and supporting tooling.
- **ANTIGRAVITY.SYS** — Android bank-transaction analyser using Gemini AI and the Salt Edge API, built with Capacitor over Next.js.
- **Rati Tours** — multilingual tourism platform (English, Hebrew RTL, Russian) with booking integration and dynamic pricing. *Live.*

TECHNICAL SKILLS

Detection & SIEM	Hunters SIEM, CrowdStrike Falcon (EDR/XDR), Microsoft Defender, Palo Alto Panorama, Cisco IronPort ESA, QRadar, log correlation, alert tuning
Incident Response	Alert triage, containment, process tree analysis, MITRE ATT&CK mapping, Windows security event analysis, escalation, case lifecycle management, post-incident reporting
Threat Intelligence	Threat hunting, IOC analysis and enrichment, VirusTotal, AbuseIPDB, AlienVault OTX, URLScan, Hybrid Analysis, GreyNoise, URLhaus, OpenPhish
Identity Security	Entra ID / Azure AD sign-in and audit logs, OAuth 2.0, SAML, Kerberos, MFA bypass detection, impossible travel, credential theft and lateral movement analysis
Engineering	Python, PowerShell, Bash, SQL, REST APIs, JSON / webhooks, Next.js, React, TypeScript, Node.js, PostgreSQL, Supabase, Tailwind, Docker, Git / GitLab CI, Vercel

CERTIFICATIONS, TRAINING & SERVICE

TryHackMe — SOC Level 1 Path
115+ rooms completed · Top 3% globally

Wiz Kubernetes Security CTF
7 / 7 flags captured

Military Service — IDF
Israel Air Force, Air Defense Division

Languages
Hebrew (native) · Georgian (native) · Russian (fluent) · English (professional)