NAGARAJAN THATHASAMY

Security Engineer | Detection Engineering | Incident Response | Digital Forensics

+91 63740 99735 | nagarajan.thathasamy@gmail.com | Chennai, Tamil Nadu, India (open to relocation)

linkedin.com/in/nagarajan-t-187731213 | nagarajant37.github.io

PROFESSIONAL SUMMARY

Security engineer with **3+ years** in SOC and detection work. At Zoho Corporation I'm on the L2/L3 side of security operations, covering **40,000+ endpoints** across AWS, Azure and on-prem infrastructure. Day to day that means CrowdStrike Falcon (EDR administration, custom IOAs) and detection work in two SIEMs, Falcon LogScale and **ManageEngine Log360**: onboarding log sources, writing parsers, building correlation rules. I also handle **SpyCloud** alerts for leaked employee passwords and manage **CrowdStrike Falcon AIDR**, which watches how people use AI tools and models and flags sensitive data or prompt-injection attempts in their prompts. Other tools I work with: Cynet XDR, Forcepoint DLP, Magnet AXIOM and Cellebrite. I write my own RCAs, map cases to MITRE ATT&CK and the Cyber Kill Chain, and automate the repetitive parts of SOC work in Python. SC-200 certified.

TECHNICAL SKILLS

SIEM & Log Analysis: CrowdStrike Falcon LogScale (NG-SIEM), **ManageEngine Log360 SIEM**, IBM QRadar, FortiSIEM, Microsoft Sentinel; log-source onboarding, custom parsers, correlation and detection rules, alert triage

EDR / XDR: CrowdStrike Falcon (sensor deployment and health, policies, host groups, device/USB control, custom IOAs), Cynet XDR, Trend Micro Apex One

AI Security: CrowdStrike Falcon AIDR (AI Detection and Response) for monitoring user activity in AI tools and models, sensitive-data leak detection in prompts, prompt-injection detection and policy tuning

Credential Leak Monitoring: SpyCloud (leaked password and dark-web credential alerts, exposure triage, password resets)

Incident Response & Threat Hunting: L2/L3 triage, containment, eradication, recovery, RCA, post-incident reporting, detection tuning, threat hunting, YARA

Digital Forensics: Magnet AXIOM, Cellebrite; disk, memory and mobile acquisition and analysis; evidence preservation; timeline reconstruction

Data Loss Prevention: Forcepoint DLP (regex classifiers, endpoint policies, incident investigation, compliance monitoring)

Vulnerability Management: Nessus, Qualys, AWS Inspector; CVSS-based prioritization, CVE and vendor bulletin tracking, patch coordination

Threat Intelligence: OSINT enrichment (domains, IPs, hashes), phishing analysis, malware analysis in isolated VMs, IOC extraction

Cloud & Deception: AWS (GuardDuty, Inspector), Microsoft Azure monitoring and hardening; multi-location honeypots

Scripting & Automation: Python, Sigma, regex, entropy-based secret detection, local LLM tooling (Ollama)

Frameworks & Platforms: MITRE ATT&CK, Cyber Kill Chain, NIST CSF, CVSS; ServiceNow, ServiceDesk Plus; Windows, Linux

PROFESSIONAL EXPERIENCE

Zoho Corporation **Aug 2025 – Present**

Security Engineer – SecOps (L2/L3) *Chennai, Tamil Nadu*

- Run CrowdStrike Falcon for 40,000+ cloud and on-prem endpoints: sensor rollout and health, host groups, policies and device/USB control. I write custom IOAs and keep tuning detections to bring false positives down.
- Bring new log sources into CrowdStrike Falcon LogScale (NG-SIEM), write their parsers and build detections on top, mapped to MITRE ATT&CK and the Cyber Kill Chain.
- In **ManageEngine Log360 SIEM** I write and tune correlation and detection rules, onboard new log sources and investigate the alerts that come out of them.
- Deploy and tune **CrowdStrike Falcon AIDR** (AI Detection and Response) policies. AIDR watches user activity in AI tools and models; my focus is catching sensitive data going into prompts and spotting prompt-injection attempts.
- Handle **SpyCloud** password-leak alerts for employee accounts. If a password turns up in a breach dump or on the dark web, I verify it and get it reset before anyone can log in with it.

- Lead L2/L3 incidents from Cynet XDR and CrowdStrike Falcon EDR start to finish: triage, containment, eradication, recovery, then the RCA and post-incident report.
- Carry out forensic investigations in Magnet AXIOM and Cellebrite: disk and mobile imaging, correlating memory, disk and log artifacts, and rebuilding the attacker's timeline without compromising evidence.
- Write regex classifiers and endpoint policies in Forcepoint DLP, and look into the exfiltration and data-sharing incidents it flags.
- Designed, and still run, a honeypot network across several locations that gives us early warning of attacker activity. I also write Python tools for routine SOC chores.
- Harden AWS and Azure workloads; run Nessus scans and get findings fixed in CVSS order.

Intellect Design Arena Ltd **Jun 2023 – Aug 2025**
SOC Analyst – Security Operations Center *Chennai, Tamil Nadu*

- Worked shifts in a 24/7 SOC, clearing 1,000+ alerts a month from SIEM, EDR, antivirus, IDS, WAF, firewall and DLP feeds within SLA.
- Correlated logs across IBM QRadar, FortiSIEM and Microsoft Sentinel to find the real threats in the noise.
- Took P1–P3 incidents in ServiceNow from first ticket to closure, escalating when needed and writing RCAs with preventive fixes.
- Isolated infected hosts and removed malware with CrowdStrike Falcon and Trend Micro Apex One before it could move laterally.
- Dug into phishing emails (headers, sender domains, source IPs), checked them against OSINT and had the malicious infrastructure blocked.
- Detonated malware in isolated VMs to pull IOCs, wrote YARA rules from the results and mapped the behavior to MITRE ATT&CK for threat hunting.
- Ran 150+ Nessus and Qualys scans a month on hybrid infrastructure, automated parts of scanning and log review with Python, and hooked AWS GuardDuty and Amazon Inspector into continuous monitoring.
- Helped patch teams bring the critical-vulnerability backlog down by 40% by tracking CVEs and vendor bulletins.

PROJECTS

- **LogSec – AI-Assisted SIEM & Investigation Platform** *(Python, Sigma, YARA, Ollama):* A case-based SIEM that searches 1.6M+ events per file in under a second and combines ML with Sigma/YARA detections mapped to MITRE ATT&CK. A locally hosted LLM handles first-pass triage, attack timelines and .eml phishing analysis, so no telemetry leaves the network.
- **GIT Recon – Source-Code & Dark-Web Exposure Scanner** *(Python, GitHub API):* Searches for repositories tied to organization keywords and scans them with a custom entropy and regex engine for leaked OAuth tokens, private keys and GCP service-account keys. It has turned up 7,000+ findings, sorted by severity and confidence, with dashboards and JSON/CSV export.
- **Vuln-MS – Vulnerability Management Platform** *(Python, Nessus):* Web app for scheduling internal, external and cloud scans (150+ a month), with role-based access, trend and remediation dashboards, and its own ticketing so every finding is tracked until it's closed.
- **Honeypot Network – Multi-Location Deception Infrastructure:** Honeypots in several locations that record attacker activity and new techniques live and give early warning.

CERTIFICATIONS

- Microsoft Certified: Security Operations Analyst Associate (SC-200) – Microsoft, 2024
- Seceon Certified Professional – Seceon Inc., 2023

EDUCATION

Manipal University Jaipur **2024 – Present**
Master of Computer Applications (MCA), Computer Science

Rathinam College of Arts and Science **2020 – 2023**
B.Sc. Computer Science (Cloud Technology and Information Security)

- Coursework: Cloud Computing, Linux, Ethical Hacking.
- Presented the paper "IAC Application – Industrial Automation with Cloud Application" at ETEST-23, a national-level conference sponsored by ISTE (2023).