

ETHAN C. HOUGHTON

Cybersecurity Platform Engineer

South Africa (UTC+2) | Australian citizen | Open to fully remote roles | +27 64 030 2731

ethan.c@houghton.ocks | linkedin.com/in/ethan-c-houghton

PROFESSIONAL SUMMARY

Self-taught, I went from a support desk to co-running the search and log platform behind a security operations team: 220 nodes, about 2 PB, 200k events a second. I've delivered 15+ client deployments, cut routine diagnosis from 45 minutes to 2, and I'm sitting my CKA in December 2026.

CORE SKILLS

Observability and Search: Elastic Stack, OpenSearch (ISM/ILM, hot/warm/cold tiering), Grafana, Zabbix

Data Pipelines: Logstash, Filebeat, Kafka, RabbitMQ

Configuration Management: Puppet (custom module authorship)

Scripting and Automation: Python, Bash, PowerShell

Containers: Docker (Compose, private registry), Kubernetes (CKA in progress)

Linux and Virtualisation: Ubuntu, Debian, Proxmox, VMware, Hyper-V

Version Control and CI: Git, GitLab, GitHub Actions

Practices: DevOps, Incident response, Root cause analysis, Change management

PROFESSIONAL EXPERIENCE

Nclose (Integrity360), managed detection and response provider

September 2023 to present

SysOps Engineer (Platform & Observability)

Acquired by Integrity360 in January 2025

Search and log platform

- Co-run 5+ Elastic and OpenSearch clusters (220 nodes, about 2 PB, hot, warm and cold tiers), including the SIEM that ingests an average 200k events per second.
- Cut routine OpenSearch diagnosis from 45 minutes to 2 with Python tooling, and added capacity forecasting so the team plans ahead instead of firefighting.
- Ended manual index deletion on 12 compliance clusters by applying an updated ISM retention policy to existing indices.
- Resolved Elastic, OpenSearch and Logstash performance issues for 10+ clients.
- Monitor 300+ hosts with Zabbix and Grafana dashboards I built.

Pipelines and automation

- Turned noisy cloud security alerts into usable SIEM events with an Orca Security ingestion pipeline in Python, deployed via Puppet to three clients and now the standard for new deployments.
- Manage 350+ hardened Linux nodes as code with Puppet, plus 70+ VMs on Proxmox.
- Operate the ingest layer: Logstash, Filebeat, RabbitMQ and Kafka; extended the Puppet module that monitors Logstash pipeline health.
- Run Docker in production: multi-stage builds, custom networking, a private registry, Compose and Swarm.
- Migrated a financial asset manager's log collectors across three offices from Ubuntu to Debian without reconfiguring a single log source, using self-reverting IP swap scripts.

Client delivery and incident response

- Delivered 15+ client deployments, configuring collectors and pipelines remotely inside each client's environment, for international and national enterprises and government in consumer finance, higher education, oil and gas, retail and hospitality.
- Restored log visibility in a major healthcare security incident by making raw Windows event logs searchable, saving the client millions; recognised by the CEO.
- Write root cause analyses, CAB submissions and runbooks; mentor colleagues on Linux and platform tooling.

Afrihost

April 2021 to August 2023

WhatsApp Support Consultant | Johannesburg

- Consistently ranked in the top 15 of ~150 consultants.
- Built a Python triage tool adopted by ~10 consultants.
- Mentored junior consultants and wrote onboarding material.

CERTIFICATIONS

- **Certified Kubernetes Administrator (CKA):** exam scheduled 15 December 2026

EDUCATION

National Senior Certificate | Jeppe High School for Boys, Johannesburg

2020