

SOC BUILDING CAPABILITY • NATIONAL & DEFENCE

Most national SOCs fail quietly, long before the first real incident finds them.

A national or defence Security Operations Centre usually gets built the same way: procure a SIEM, hire a handful of analysts, cut a ribbon. Eighteen months later something happens at 2am on a Saturday, and whoever is on shift does not have the authority to escalate it to the person who does.



The Real Exposure.

A national or defence Security Operations Centre usually gets built the same way: procure a SIEM, hire a handful of analysts, cut a ribbon. Eighteen months later something happens at 2am on a Saturday, and whoever is on shift does not have the authority to escalate it to the person who does.

Signing the policy is the easy part. Running a SOC that actually catches something at 3am, with an analyst who knows exactly who to call, is the part most build programmes underestimate.

That gap is rarely a technology gap. It shows up as a roster that cannot survive two people resigning, an escalation path nobody has tested, and a playbook written for a threat model that no longer matches the organisation.

01 · THE LINE ITEM THAT NEVER MAKES THE BUDGET

A SOC is people before it is technology

4-5

analysts needed to staff a single genuinely 24/7 SOC position, once leave, training and attrition are accounted for.

A well-worn rule of thumb in security workforce planning — and routinely left out of budgets built around hardware and licences rather than people.

A SOC is not the room, the screens or the licence. It is a rested analyst, a tested playbook, and a clear answer to who gets called at 3am. Most build programmes get the first part right and never quite finish the third.

- **Rosters that survive resignations**
Shift design built around real leave, training and attrition.
- **Escalation paths that have been tested**
Mapped to your command structure before go-live, not during an incident.
- **Playbooks that match the threat model**
Reviewed as the organisation and its exposure change.

02 · THE BUILD

Our Process. —

The four phases we run every SOC build through, in order. Each one closes off before the next begins, so capability is proven rather than assumed.

01

Design

Threat landscape, facility, monitoring architecture and tooling decided against your actual risk and budget — before anything is procured.

02

Build

Monitoring stack stood up, detection use cases written, analysts recruited and tiered against a roster that reflects reality.

03

Operate

Playbooks and escalation paths tested under load, so the first real incident is not also the first rehearsal.

04

Mature

Independent assurance and performance measurement, feeding detection, staffing and design decisions back into the programme.

What We Do.

We design and build monitoring and response capability for defence, government and critical infrastructure operators, covering the people and the process as closely as the technology.

Defence forces, ports, utilities and other national infrastructure operators are under growing pressure — often backed by government or donor funding — to stand up their own capability rather than outsourcing it entirely.

We help organisations build that capability properly the first time, because a SOC that fails quietly is worse than no SOC at all: it creates the appearance of coverage without the substance of it.

03 · CAPABILITY

People and process, as closely as the technology —



SOC design and build

Facility, monitoring architecture and tooling selected against your actual threat landscape and budget — not a vendor's default stack.



Staffing models and shift design

Analyst tiering and genuine 24/7 rostering built around the reality of leave, training and attrition — not an org chart on a slide.



Detection use cases and playbooks

Escalation paths mapped to your command structure and tested before go-live, rather than discovered during the first real incident.



Independent SOC assurance

Performance measurement by a team that did not build the SOC, so the grading of it is worth something.

SOC BUILDING CAPABILITY · NATIONAL & DEFENCE

**A Security Operations Centre
is not a room full of monitors.
It is a rested analyst, a tested
playbook, and a clear answer
to who gets called at 3am.**

DISystems – cybersecurity and GRC advisory across South Africa, the SADC region and internationally, in partnership with **Cyberantix™**

CONTACT US AT:
tsepang@disystems.co.za
to setup a time for more details.