RAMP SOC

A deep technical review of the SOC, service by service. What each service actually delivers, and where investment would change the outcome.

The question it answers

Conventional reviews stop at surface-level documentation and high-level process definitions. They establish that something exists on paper. They do not establish whether it works.

This engagement examines the design, execution and operational reality of SOC services to determine how effectively they deliver protection and value. It is not a maturity checklist.

Ten services, four axes

Ten SOC services are examined, among them monitoring, detection engineering, response, threat intelligence, threat hunting and governance. Each one is analyzed across the same four axes, so services can be compared against each other instead of each being judged on its own terms.

The engagement runs in two phases. Phase one establishes how those services are structured and executed in practice. Phase two closes the gaps it found, producing the documentation and running the sessions that make the change hold, with deliverables designed to reach Level 4 maturity.

The four axes, applied to every service

Strategy

Vision, planning and the leadership mandate behind the SOC. Weighted heavily, because in real-world defense outcomes it decides more than tooling does.

Coverage

Threat and asset coverage, and whether procedures are complete against them. The second of the two axes carrying special weight.

Integration and impact

Cross-team alignment, responsiveness and automation. Whether the services function as one capability or as adjacent teams.

Continuous improvement

Metrics, feedback loops and lessons learned, and whether any of them change what happens next time.

AT A GLANCE

SCOPE
Ten SOC services, governance included

ANALYSIS
Four axes applied to every service

STRUCTURE
Two phases: assessment, then enablement

TYPICAL DURATION
5 weeks per phase

DEPTH
Configuration-level validation, not document review

WHO THIS IS FOR

- SOCs that pass audits but cannot say which of their services actually work.
- Organizations standing up new security functions that need to be defensible from the start.
- Teams under SAMA, NCA ECC and CCC, DESC or QCB and NIA obligations, where results can be mapped to the framework.
- Leadership deciding where the next security investment should go, and needing that decision to be defendable.

How an engagement runs

01 **Kick-off and threat landscape profiling**

Sector-relevant threat actors, attack patterns and abuse scenarios are identified first, so the evaluation is anchored to what the organization will actually face.

02 **Documentation and control sampling**

Full-spectrum review of the documentation the SOC uses, alongside configuration-level validation of key controls: logging, EDR, SIEM and incident management tooling.

03 **Structured stakeholder interviews**

Deep-dive discussions with technical and functional owners to establish how each service delivers value and how it interacts with the business.

04 **Scoring and reporting**

Every service is scored on all four axes and compiled into executive and technical reports, with a prioritized capability uplift roadmap. Mapped to the applicable regulatory framework where relevant.

05 **Enablement and knowledge transfer**

Tailored documentation is developed against the findings, then explained through structured walkthroughs so service owners can apply and evolve it.

WHY ALEXSTA

- Senior hands only. The operator whose experience you are buying does the work, rather than reviewing it.
- Services are assessed as they are delivered, not as isolated domains or technologies.
- Every deliverable is walked through with the team that will own it, so the uplift outlasts the engagement.

PHASE TWO DELIVERABLES

- Incident response plan, severity model and playbooks.
- Threat hunting methodology and operational runbooks.
- SOC charter and service catalogue.
- Governance elements such as RACI matrices and control ownership.

What you receive

Threat landscape brief

A summary of the actors and scenarios relevant to your sector, which anchors every judgment made in the assessment.

Executive summary report

The findings in business terms, for the people who decide where budget goes and need the reasoning to hold up.

Full maturity assessment report

All ten services scored across the four axes, with the evidence behind each score and what it means in practice.

Capability uplift roadmap

A prioritized sequence of improvements, ordered by the difference each would make rather than by ease of implementation.

Request an engagement

The assessment is useful on its own and far more useful with the enablement phase behind it. We will tell you honestly which one your SOC needs.

contact@alexsta-cybersecurity.com
+41 76 76 44884
alexsta-cybersecurity.com