

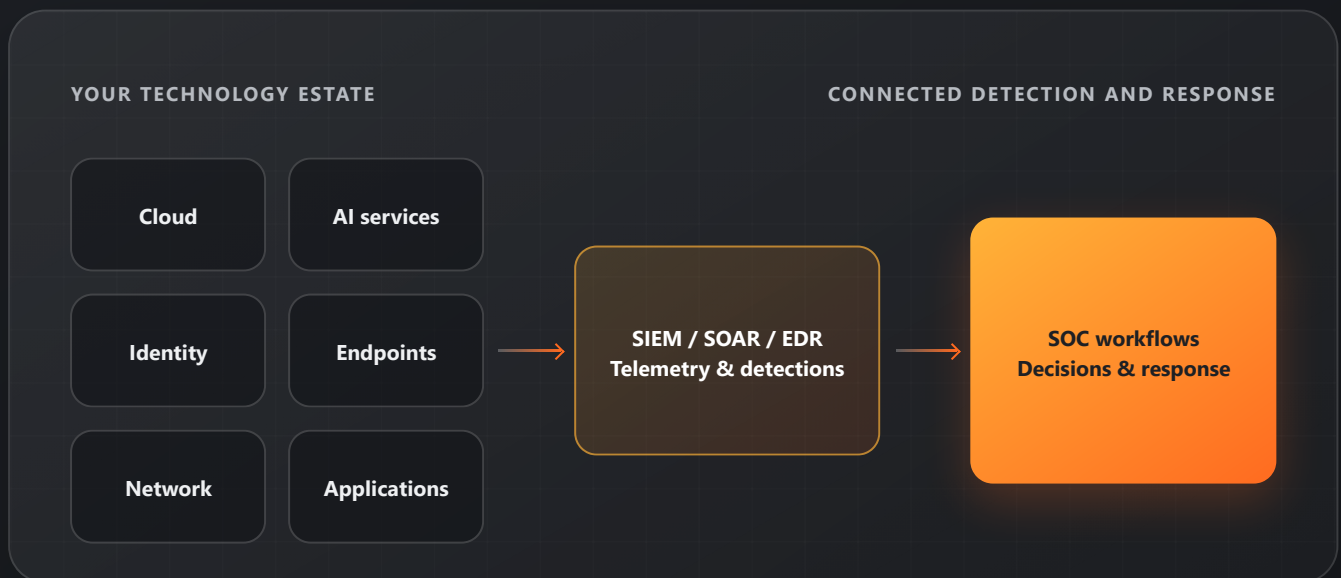
Turn your security tools into a monitoring capability you can **trust**.

Akita assesses, designs and implements monitoring across cloud, AI and infrastructure. We connect SIEM, SOAR and EDR technologies with the people and processes required to operate them effectively.

STACK ASSESSMENT

SOC READINESS

ARCHITECTURE AND ROADMAP



RECOMMENDED STARTING POINT

Monitoring capability review

Map current coverage, identify the priority gaps and agree on the next implementation steps.

Contact Akita

THREE FOCUSED ENGAGEMENTS

Start with the service that matches your current need.

The services can be delivered independently or combined into a complete monitoring improvement programme. Akita can also support implementation, tuning and handover.

01 / STACK

Detection & Response Stack

For teams that already use SIEM, SOAR and EDR but need a clear view of coverage, integration and value.

WHAT WE ASSESS AND IMPROVE

- Log-source and telemetry coverage
- Detection logic, alert quality and ownership
- Tool integrations and investigation workflow
- SOAR use cases, playbooks and automation
- Implementation, tuning and knowledge transfer

YOU RECEIVE

Coverage heatmap, risk-ranked gap backlog, integration design and sequenced remediation plan.

02 / SOC

SOC Readiness Assessment

For organizations building a SOC, changing providers or testing whether the current model is ready to operate.

WHAT WE ASSESS AND DESIGN

- People, process and technology maturity
- Roles, escalation paths and decision rights
- Incident workflows, runbooks and SLAs
- Metrics, governance and quality assurance
- Skills, staffing and service-model options

YOU RECEIVE

Maturity baseline, target operating model, RACI, runbook backlog and 90-day readiness plan.

03 / ROADMAP

Monitoring Architecture & Roadmap

For cloud, AI, application and infrastructure environments growing faster than monitoring was designed to support.

WHAT WE MAP AND CREATE

- Critical services, threats and monitoring needs
- Cloud, AI, identity, application and infrastructure signals
- Target-state monitoring architecture
- Data onboarding, ownership and dependencies
- Phased implementation and validation approach

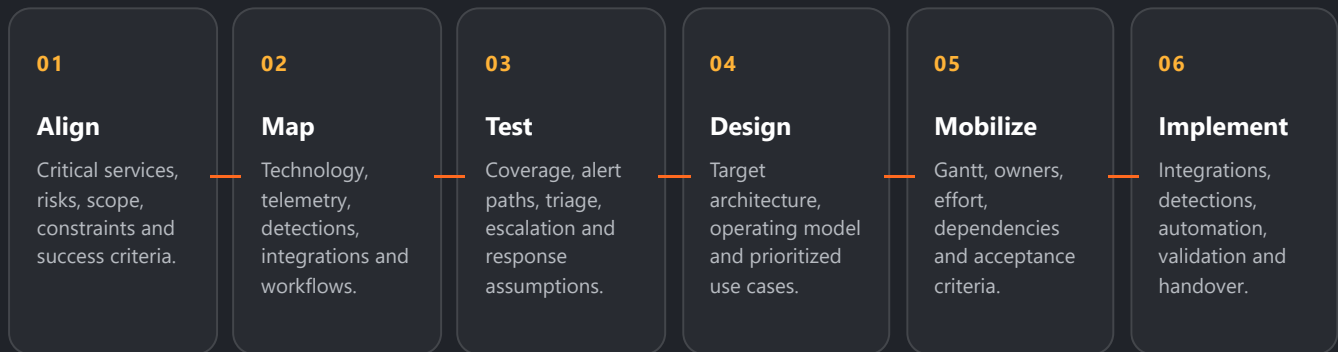
YOU RECEIVE

Target architecture, implementation Gantt, work packages, owners, dependencies and acceptance criteria.

FROM ASSESSMENT TO IMPLEMENTATION

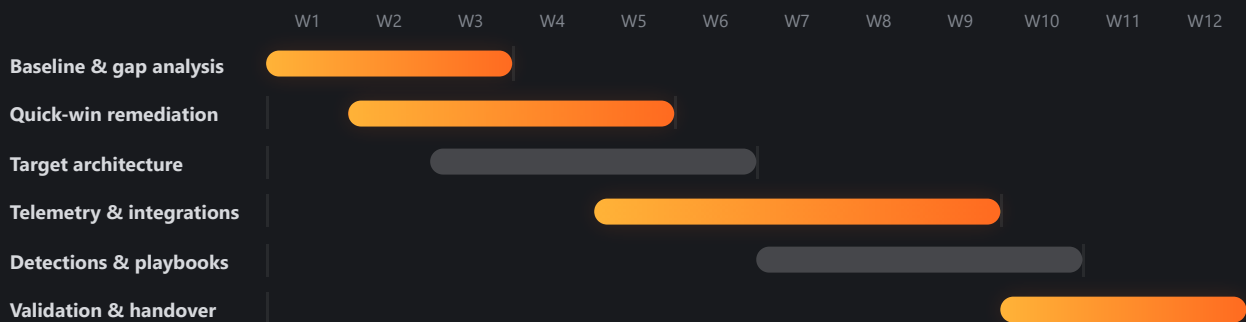
Move from identified gaps to scheduled work.

We map critical business services to telemetry, detections, workflows and accountable owners. The design is then converted into work packages with clear scope, ownership and timing.



Illustrative 12-week roadmap

Exact sequence is tailored after discovery



Illustrative only. Scope, duration and workstreams depend on environment size, access, technology choices and implementation ownership.

Architecture pack

Current state, target state and integration decisions.

Operating pack

Ownership, workflows, measures and governance.

Delivery pack

Prioritized backlog, Gantt, dependencies and acceptance tests.

ENGAGEMENT OUTCOMES

Turn monitoring technology into an accountable business capability.

**Visibility you can explain**

A defensible view of what is monitored, where coverage is weak and why remediation is prioritized.

**A roadmap leadership can fund**

Sequenced work packages with owners, effort, dependencies and measurable acceptance criteria.

**Consistent detection and response**

Clear alert ownership, triage decisions, escalation paths and automation opportunities.

**Less wasted technology investment**

Existing capabilities are integrated and tuned before another product is introduced.

**Evidence for governance and assurance**

Documented architecture, controls, decisions, responsibilities and improvement tracking.

Every engagement is designed to answer:

What can we see today, what matters most, and what must happen next?

Current-state coverage **KNOWN**

Critical blind spots **PRIORITIZED**

Target architecture **DESIGNED**

People and process changes **ASSIGNED**

Implementation sequence **SCHEDULED**

Success criteria **MEASURABLE**

Designed for: CISOs, CTOs, Heads of Security, SOC leaders, cloud/platform owners and risk stakeholders.

Make your monitoring stack operational.

Share your current architecture, audit findings, SOC plan or plans for cloud and AI expansion. We will identify the priority gaps and define an implementation plan.

Schedule a monitoring review