

CASE STUDY · MEDIA & BROADCAST · CENTRAL ASIA

Nation-Scale Broadcast Operations on In-Country Infrastructure

A national broadcaster in Central Asia operates Secure60 across its broadcast, IT and audience-facing systems, at high sustained ingest volumes, on Rackcorp infrastructure inside the country.

Media & broadcast

Central Asia

Log Management

SIEM

Governance

ORGANISATION

National broadcaster, critical information infrastructure

DEPLOYMENT

Sovereign SaaS, in-country (4 datacentres)

IN SCOPE

Log Management, SIEM, Governance

OPERATING MODEL

Secure60-operated, digital workers in the SOC

CURRENT SITUATION

A critical-infrastructure designation and broadcast availability requirements

The broadcaster is designated an organisation with critical information infrastructure under the country's 2021 Law on Cyber Security, and handles audience data under the Law on Personal Data Protection. Both laws set obligations that have to be demonstrated, and neither names a tool.

Broadcast systems cannot tolerate a monitoring platform that itself becomes a point of failure, and the security telemetry they generate is large and continuous. The data had to stay in the country, and the organisation did not have a security operations team to run a platform of this size.

WHAT SECURE60 DELIVERED

In-country platform operated by Secure60

Secure60 was deployed on Rackcorp infrastructure in-country, where Secure60 has four datacentres, so ingest, storage, detection and evidence all run onshore. Log Management takes the broadcast, network and IT telemetry at sustained volume; SIEM runs the managed rule library over it; Governance maps the resulting evidence to the two laws.

The operation is run by Secure60. Digital workers handle first-line triage around the clock, with Secure60 experts on escalation, so the broadcaster's own staff are not on call for the platform.

COMPONENTS IN OPERATION

01 Sovereign in-country deployment

Platform and data on Rackcorp infrastructure in the country, across four datacentres.

02 Sustained high-volume ingest

Broadcast, network and IT telemetry collected continuously at terabyte-a-day scale, with headroom for event-driven peaks.

03 Managed detection, 24/7 triage

The Secure60 rule library, with digital workers on first-line triage and experts on escalation.

04 Evidence mapped to both laws

Governance records controls and evidence against the Law on Cyber Security and the Law on Personal Data Protection.

BUSINESS IMPACT

Before and after

AREA	BEFORE SECURE60	AFTER SECURE60
Data location	Monitoring would have required data to leave the country	All telemetry and evidence resident in-country
Availability of monitoring	Single-site tooling, a point of failure in itself	Multi-datacentre deployment sized for broadcast-grade continuity
Security operations	No dedicated team; alerts unattended outside hours	24/7 triage by digital workers, experts on escalation
Time to triage	Incidents surfaced by staff, often hours later	Alerts triaged within minutes, around the clock
Regulatory evidence	Assembled on request	Maintained continuously against both laws

OUTCOMES

Results

■ Obligations evidenced

The critical-infrastructure designation brings inspection, and the evidence is maintained before it is requested.

■ Onshore by design

No telemetry or evidence is backhauled to another jurisdiction; the in-country deployment is the documented answer to the residency question.

■ Coverage without a SOC to hire

Round-the-clock detection and response without the broadcaster building a security operations team.

■ Sized for the estate

Ingest and retention sized for a nation-scale broadcaster, with retention held to the period the two laws and the broadcaster's own investigation windows require.

Critical Infrastructure With an In-Country Requirement

An architecture review covers the in-country footprint, the availability model and how the operation is staffed.

Talk to us

www.secure60.io/contact/

Start for free

30 days, every feature switched on. No credit card.

portal.secure60.io

ONE PLATFORM, ONE CONTEXT

Log Management, SIEM, Vulnerability Management, Governance, AI Security and Digital Risk Protection on one platform and one context, with the experts and digital workers to run the parts you choose.

Log Management

SIEM

Vulnerability Management

Governance

AI Security

Digital Risk Protection