TRANSFORMATION CASE STUDY

ORGANIZATION: BUILDING A MANAGED SECURITY OPERATIONS AND ENDPOINT SECURITY PLATFORM

A Security Operations Centre and endpoint protection built for Organization 's own defence and extended as a 24/7 managed security service.

Built the Organization Security Operations Centre and endpoint security capability from inception through operations, protecting Organization 's own national network while extending the same capability to enterprise and government customers as a 24/7 managed security service.

SECTOR	REGION	ENGAGEMENT	DURATION	MY ROLE
Telecommunications & Cybersecurity	**Australia; domestic & global customers**	**SOC build, endpoint & managed service**	**2016 to 2020**	**SOC & Endpoint Security Lead**

24/7 SECURITY MONITORING	**One SOC** INTERNAL DEFENCE + CUSTOMER	**Endpoint EDR** DETECT, ISOLATE, CONTAIN	**IRAP-assessed** SOVEREIGN GOVERNMENT SOC

CONTEXT & MANDATE

Rising volume and sophistication of cyber threats meant Organization had to strengthen its own defence and, at the same time, could turn that capability into an enterprise-grade managed service. The strategic insight was to use Organization 's scale, network visibility and security expertise to protect customers who could not justify building and running a comparable SOC themselves. The mandate was broader than a monitoring facility: build the capability, operationalise it to 24/7, integrate endpoint security, make the processes repeatable and onboard customers. I led the SOC and endpoint build from inception through implementation and into live operations, and led customer onboarding and endpoint provisioning. The SOC ran as "One SOC," applying the same threat intelligence, vulnerability management and threat hunting to Organization and to external customers, integrated with Organization 's Global Operations Centre and Managed Network Operations Centre.

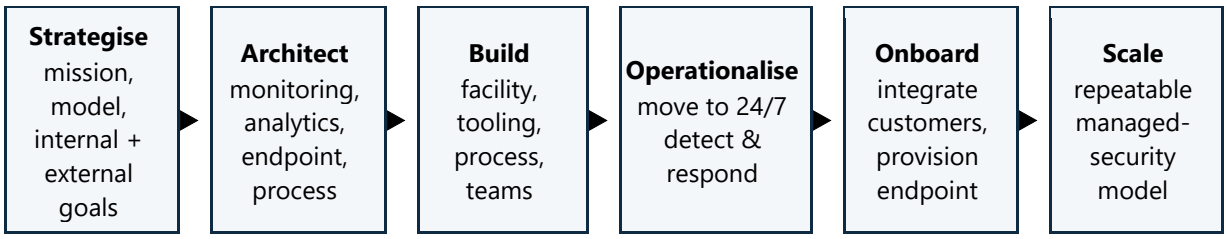
THE CHALLENGE

- **Building a SOC as an operating capability, not a tooling project:** a functioning SOC needed people, process, technology, governance, threat intelligence and incident management working as one, running continuously.
- **Protecting Organization and customers at once:** the same capability had to defend Organization 's own network and meet the controls, assurance and sovereignty demands of external enterprise and government environments.
- **Integrating endpoint into detection and response:** endpoint protection could not sit as an isolated product; the SOC needed endpoint visibility and the ability to turn a detection into immediate containment.
- **Making it a scalable service:** customer onboarding had to be repeatable, with clean technical integration and operational handover, without disturbing the core SOC operating model.

APPROACH & KEY DECISIONS

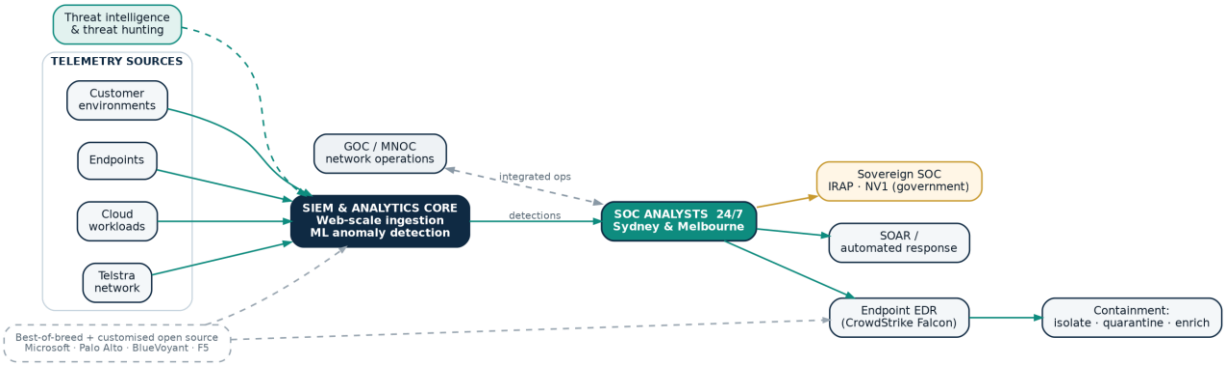
- **Design the SOC as an integrated operating model:** build around people, process, technology, governance and continuous operations, not a technology deployment.
- **Fuse internal defence with commercial service:** run one capability that protects Organization and is extended to enterprise and government customers.
- **Integrate endpoint into detection and response:** connect endpoint telemetry and containment directly into SOC monitoring and investigation.
- **Build a best-of-breed yet sovereign stack:** negotiate the vendor agreements directly and combine leading commercial tools with customised open-source technologies to avoid lock-in and meet sovereignty needs.
- **Industrialise onboarding:** turn the SOC into a repeatable managed service through a structured customer onboarding and endpoint-provisioning process.

TRANSFORMATION APPROACH



SOLUTION DESIGN

Telemetry from the Organization network, customer environments, endpoints and cloud feeds a SIEM and analytics core, enriched by threat intelligence and threat hunting; SOC analysts drive automated response and endpoint containment, a Sovereign SOC serves government, and the platform integrates with network operations.



OUTCOMES & BUSINESS VALUE

The programme gave Organization security as both an internal defensive capability and a commercial managed service. For Organization, it centralised monitoring and response and strengthened protection of the critical network infrastructure that underpins its customers. For customers, it delivered 24/7 monitoring, threat detection and intelligence, and endpoint response without the cost of building an equivalent in-house SOC, positioned as an at-scale service more affordable than a self-built alternative. Because it runs at carrier scale, the SOC could serve organisations from mid-sized business through to whole-of-government, and later provided the security layer that was integrated into Organization 's broader managed propositions, including the Microsoft 365 and Calling for Office 365 platform.

HICCUPS, AND HOW THEY WERE OVERCOME

- **Alert volume and false positives:** web-scale event streams risk drowning analysts; addressed with machine-learning anomaly detection, tuning and threat-intelligence enrichment so analysts focused on real threats.
- **Containment without business disruption:** aggressive isolation can break legitimate work; resolved with graded response playbooks (isolate, quarantine, remove) governed by SOC analysts rather than blanket automation.
- **Multi-vendor integration:** a best-of-breed toolset risks fragmentation; resolved by centralising telemetry into a common SIEM and analytics core with orchestration across the vendor and open-source ecosystem.
- **Repeatable onboarding at scale:** each customer environment differs; resolved by industrialising assess, integrate, provision and handover into a standard onboarding lifecycle.

TECHNOLOGY TRANSFORMATION

Security Operations

- 24/7 monitoring from high-security facilities in Sydney and Melbourne (ASIO T4 standard)
- Web-scale security-event ingestion and near-real-time analysis
- Machine-learning anomaly detection, threat intelligence and threat hunting
- Incident investigation, and security orchestration and automated response

Endpoint Security

- Endpoint Detection and Response integrated into SOC operations (CrowdStrike Falcon as primary EDR)
- Continuous endpoint visibility, including fileless and zero-day coverage
- Immediate containment from the SOC: host isolation, malware quarantine and removal
- Real-time indicator extraction and enrichment

Security ecosystem: a best-of-breed multi-vendor platform, with the commercial agreements negotiated directly (CrowdStrike, Microsoft Defender for Endpoint and Sentinel, Palo Alto Networks Prisma Access and SecureEdge, BlueVoyant and F5), combined with customised

open-source technologies to avoid lock-in. A Sovereign SOC for government is IRAP-assessed, with data residency and NV1-cleared personnel.

CUSTOMER & SERVICE TRANSFORMATION

The decisive step was converting an internal security capability into a repeatable commercial service. I led customer onboarding and endpoint provisioning, connecting customer environments into the SOC operating model and establishing the operational handover for ongoing monitoring and response.

Service lifecycle: assess ▸ integrate ▸ provision ▸ monitor ▸ detect ▸ respond ▸ improve, designed to support customers from mid-sized business and government agencies through to enterprise and whole-of-government.

STAKEHOLDER & C-SUITE GOVERNANCE

The transformation required coordination across cybersecurity, network operations, technology, service operations, product, engineering, customer teams and external technology partners. The central leadership challenge was aligning security strategy with operational reality and commercial service economics, so that capability translated into a reliable customer service with repeatable onboarding and response. Integration with the Global Operations Centre and Managed Network Operations Centre tied security monitoring to network operations.

WHAT THIS ENGAGEMENT DEMONSTRATES

End-to-end cybersecurity transformation leadership, from defining and building a SOC through technology integration, operationalisation, endpoint security, managed-service design and customer onboarding. It shows the ability to convert security strategy and complex technology into an operational, scalable and commercially viable enterprise service, balancing security effectiveness, customer outcomes, operational resilience and service economics.