BLACK BOX

CASE STUDY
CYBERSECURITY

# Securing Australia's Defence Supply Chain with a Sovereign Managed SOC

## Overview

An Australian defence-industry participant supports platforms, systems integration and multi-tier supply-chain delivery across government and defence-prime programs. Its footprint spans manufacturing sites, project offices, mobile teams, cloud platforms and a growing supplier ecosystem, increasing the need for consistent cyber visibility across internal and third-party environments.

At the same time, the organisation was progressing a technology uplift, including a hybrid-cloud refresh, while strengthening its sovereign industrial capability position. The security model needed to support DISP expectations, Australian data-residency requirements, export-sensitive information handling and continuity of supply without forcing major changes to established technology platforms.

Black Box developed a sovereign Managed SOC design centered on Australian delivery, centralised monitoring and onshore response. The proposed model combines SIEM, managed EDR, SOAR, threat hunting, dark-web monitoring, digital forensics and incident response, with governance designed to extend security oversight into the broader defence supply chain.

## Challenges

Cybersecurity requirements extended beyond the organisation's own environment. As part of Australia's defence industrial base, the client needed visibility into risks introduced through subcontractors, suppliers and other third parties while supporting Defence Industry Security Program obligations and sensitive program data.

Data sovereignty was a central constraint. Monitoring, log processing, threat analysis and incident response needed to remain in Australia. The environment also included established technologies such as Fortinet, VMware, Veeam and Microsoft 365 that needed to be incorporated rather than replaced.

The design also had to support approximately 100 GB of log ingestion per day and scale as new suppliers and programs were added, without major re-architecture or disruption to complex, multi-party operating environments.

## AT A GLANCE

### CHALLENGES

- Distributed network of primes, subcontractors, and suppliers
- DISP compliance, export controls, and data residency
- Limited visibility into third-party and supply-chain cyber risk.
- Scalable log monitoring without major security re-architecture.

### SOLUTIONS

- Sovereign 24/7 Australian-operated managed SOC delivery.
- Centralised SIEM and managed EDR coverage.
- SOAR-enabled investigation, containment and remediation workflows.
- Onshore threat hunting, DFIR and governance.

### RESULTS

- Solution design unifies visibility across core security domains.
- Architecture supports approximately 100 GB daily log ingestion.
- Onshore operating model supports sovereignty and DISP alignment.
- Scalable design accommodates future suppliers and programs.

### BENEFITS

- Supports continuity planning for critical defence programs.
- Keeps sensitive security operations within Australia.
- Extends supply-chain risk visibility and governance.
- Protects existing technology investments through integration.

## Solutions

Black Box designed the operating model around a 24/7 Australian-operated Managed SOC, with centralised SIEM and managed EDR providing a common security view across endpoint, identity, network, cloud and operational-technology environments. The architecture also extends monitoring to access points used by subcontractors and suppliers.

SOAR capabilities were incorporated to support repeatable investigation, containment and remediation playbooks once threats are validated. The design combines these workflows with proactive threat hunting, Australian-focused threat intelligence, dark-web monitoring for compromised supplier credentials and leaked controlled data, plus onshore digital forensics and incident response.

Black Box also included monthly governance reviews, supply-chain risk insights and executive reporting. The solution was designed to integrate with the client's existing technology stack, accommodate approximately 100 GB of daily log ingestion and scale as additional programs, suppliers and security requirements are introduced.

## Results

The engagement established a sovereign security architecture and operating model designed to centralise telemetry across the client's national environment and extended supply chain. It defines consistent 24/7 monitoring, investigation and response processes, including coverage for incidents associated with third-party and supplier access.

The architecture keeps monitoring, log processing, threat analysis and incident-response functions within Australia, supporting sovereignty, DISP-alignment and export-control requirements. It also provides a structured path for integrating established security platforms rather than requiring wholesale replacement.

Capacity planning was based on approximately 100 GB of log ingestion per day, with scalability for additional suppliers and programs. The design introduces SOAR-enabled workflows intended to shorten the path from validated detection to containment while preserving onshore handling of sensitive security activities.

## Why Black Box?

Black Box combined Australian sovereign delivery requirements with managed security design, SIEM/EDR integration, SOAR, threat intelligence, DFIR and governance. The engagement addressed both the client's internal environment and its wider defence supply chain.

The Sydney-based operating model and Australian data-handling approach were designed to align security operations with Defence-industry sovereignty expectations while preserving interoperability with existing platforms.