



# Cyber security exercise report

## Operational Technology (OT)

Prepared by: \_\_\_\_\_

Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

## Executive summary

Our team ran a discussion-based cyber security exercise session on the reported date using the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) Exercise in a Box. This report summarises the results of this exercise and includes recommendations for our organisation to consider.

## Discussion outcomes

What we learned from running the exercise:

How our understanding of preventing this type of cyber security threat changed:

What will we look to change or implement:

## Team statements

We rated our confidence against the following statements:

### Observations from Inject 1: System design and visibility

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We have identified appropriate methods of segmentation for our network zones.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have established an attack tree that clearly outlines all possible threats to our organisation's OT systems and networks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have created a network diagram that displays the flow of data throughout our systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Observations from Inject 2: System hardening and vulnerability management

We have established a virtual environment to ensure a secure convergence between IT and OT.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have hardened the boundaries between our high-trust and low-trust network zones.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have implemented MFA to authenticate users accessing our OT systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Observations from Inject 3: Procurement

We have well-known, reputable companies and vendors selling our OT hardware and software.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The hardware and software align with our organisation's security requirements.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The newly procured hardware and software converges smoothly with our IT networks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Observations from Inject 4: Monitoring and detection

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We have an up-to-date asset register that is actively maintained.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have processes in place for monitoring, collecting and analysing logs and detecting malware.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have an isolated monitoring environment.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>