

Facilitator Runsheet

[Exercise Name]

**Prepared by**

**Sun Chaser Cyber**

Purpose and use: You can use this document to help prepare the tabletop exercise and the injects, and think about further context around each inject. This document is then intended to be a resource for the exercise facilitator/s, to assist them with running the tabletop on the day of the exercise. It details the real-time run sheet for the day, and provides prompts to encourage and facilitate participant discussion.

# Exercise Summary

## High level scenario

[Fill in the high-level scenario and organisational context here]

## Aim

[Insert exercise aim]

## Objectives

[Insert exercise objectives]

## Attendees

|  |  |  |
| --- | --- | --- |
| Role | Name | Position |
| Facilitator |  |  |
| Participant |  |  |
| Participant |  |  |
| Participant |  |  |
| Participant |  |  |
| Participant |  |  |
| Participant |  |  |
| Participant |  |  |
| Participant |  |  |
| Observer |  |  |
| Observer |  |  |

## Details

* **Date**:
* **Time**:
* **Location**:

# Detailed timeline

Example filled below:

* 9:00: Welcome to session
	+ Acknowledgement of country
	+ Housekeeping – toilets and emergency exits
	+ Explain purpose of tabletop, how it will be conducted and timeframes
	+ Any pre-exercise questions from participants
* 9:40: Exercise starts, as per table below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Real time | Inject | Facilitator questions | Other info that may or may not be shared with participants | Expected participant response |
| 9:40 | 3pm Saturday – [xxx team] receives an alert from [alert service] about [service] | * Would anybody receive this alert on the weekend?
* Is there somebody assigned on call?
* Would anything be actioned on the weekend, or would you wait until business hours?
* Do you have processes to follow? If so, what do they look like?
 | * [Service] is aware of the security issue
 | * On-call to investigate alert
 |
| 9:50 | 8pm Saturday – An adversary appears to have gained unauthorised access to [compromised service] | * What steps would you take to isolate this incident?
* Who would be required in order to do this?
* Do you have a playbook to follow?
* Would you escalate this incident / advise any more senior stakeholders yet?
* Who are you communicating with?
* Have you set up a War Room? What does this look like (in-person, online)?
 | * [Adversary]
* [Motive]
 | * Set up virtual War Room
* Engage with [team]
 |
|  |  |  |  |  |
|  |  |  |  |  |

# References / resources

[Additional page for references / resources if required]