Australian Government
Department of Defence
Chief Information Officer Group

Panel Discussion: Automation, continuous improvement, driving efficiency, and lessons learnt

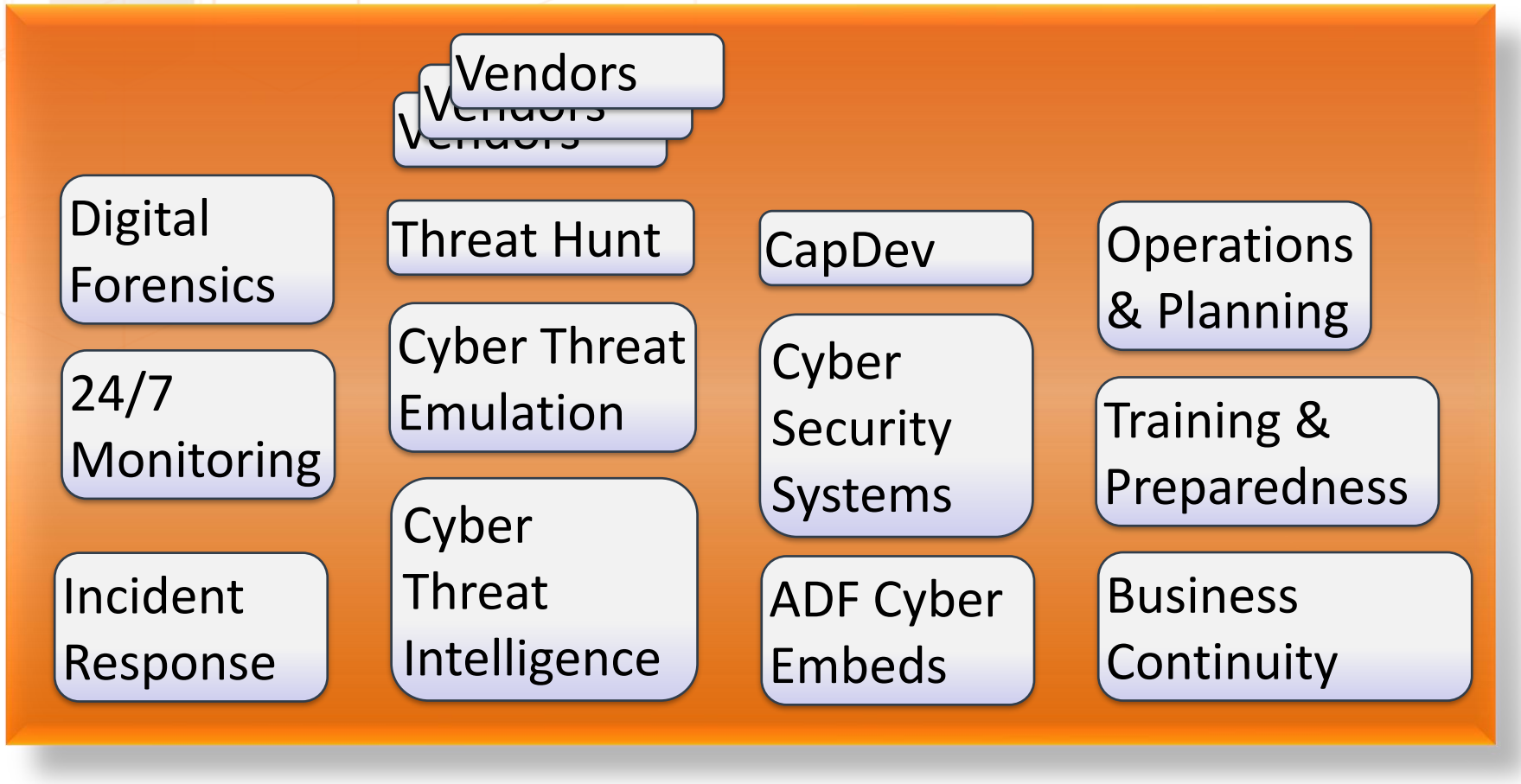
Samuel Morgan

Director Defence Security Operations Centre

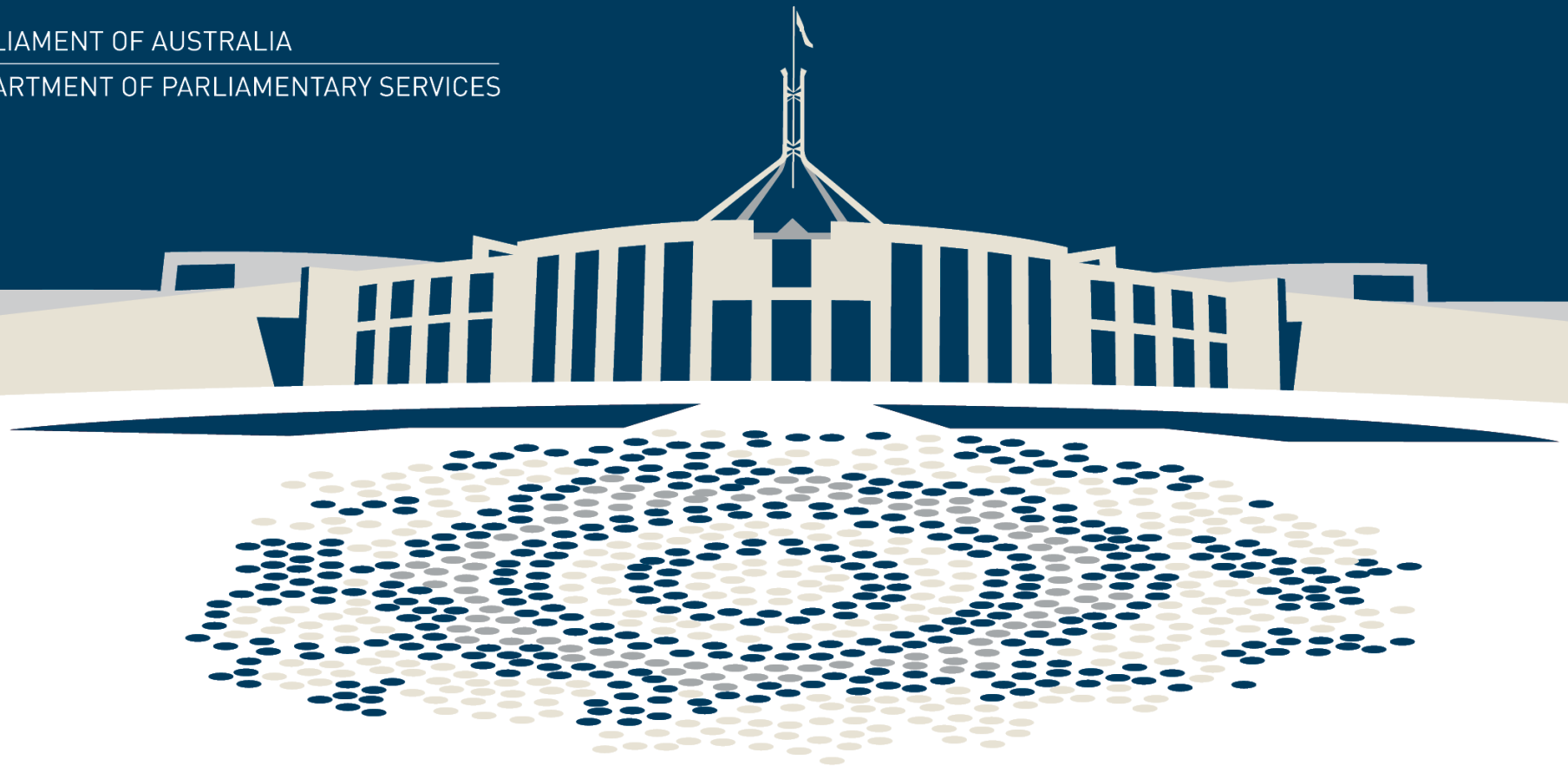
Department of Defence

Defending Australia and its National Interests
www.defence.gov.au

DSOC Functional Structure

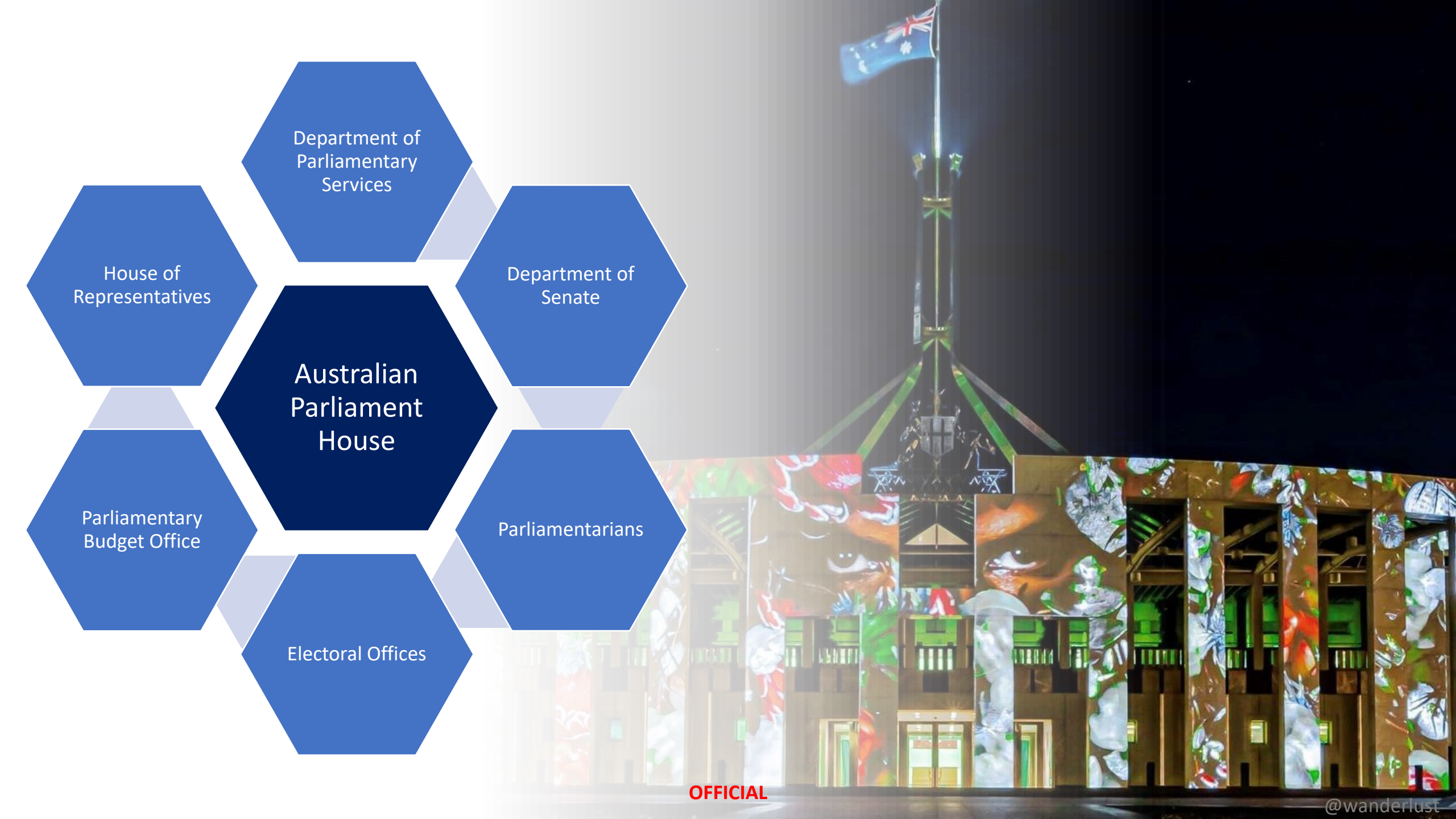


PARLIAMENT OF AUSTRALIA
DEPARTMENT OF PARLIAMENTARY SERVICES



Nadia Taggart

Director Cyber Security Operations



Parliamentary Privilege

The term parliamentary privilege refers to special legal rights and immunities which apply to each House of the Parliament, its committees and Members. These provisions are part of the law of the Commonwealth.

Parliamentary Precincts Act 1988

The precincts are under the control and management of the Presiding Officers who may, subject to any order of either House, take any action they consider necessary for the control and management of the precincts.

Capability to be Automated

Visibility

Endpoint Detection and Response
(Investigation of alerts related to endpoints or indicators coming from TI sources, can be used as Hunt tool and sometimes as primary threat detection tool on endpoints.)

Network Traffic Analysis
(Investigation of alerts & obtaining additional context about suspect activity in the network)

Vuln Assess Tools
(Identify existing vulnerabilities, Provides additional context for monitoring as well as asset inventory)

Analysis

SIEM (Used to consolidate and correlate events and logs coming form different technologies and sources, generate alerts to be investigated, or report on suspicious or priv use, provides single point to search log data and can be used for investigations and Hunt)

UEBA (Used to identify suspicious behaviours by users and other entities, used as a source of alerts, a means to refine and enrich alerts or to provide context for the SIEM)

Malware Analysis & Sandboxing
(used for investigations when suspicious software is identified in the environment)

Response

SOAR
(supports monitoring and response workflows, case management and automation, response and triage orchestration, and reporting; enables automation and prioritisation of security operations activities and report data to inform better decision making)

Threat Intelligence Platform
(facilitates collection, consolidation, refinement and sharing of CTI, increasingly incorporated into SOAR

Drivers for Automation

- Legislation & Compliance Requirements
- Processing Data
- Staff Constraints
- Asymmetric Gain

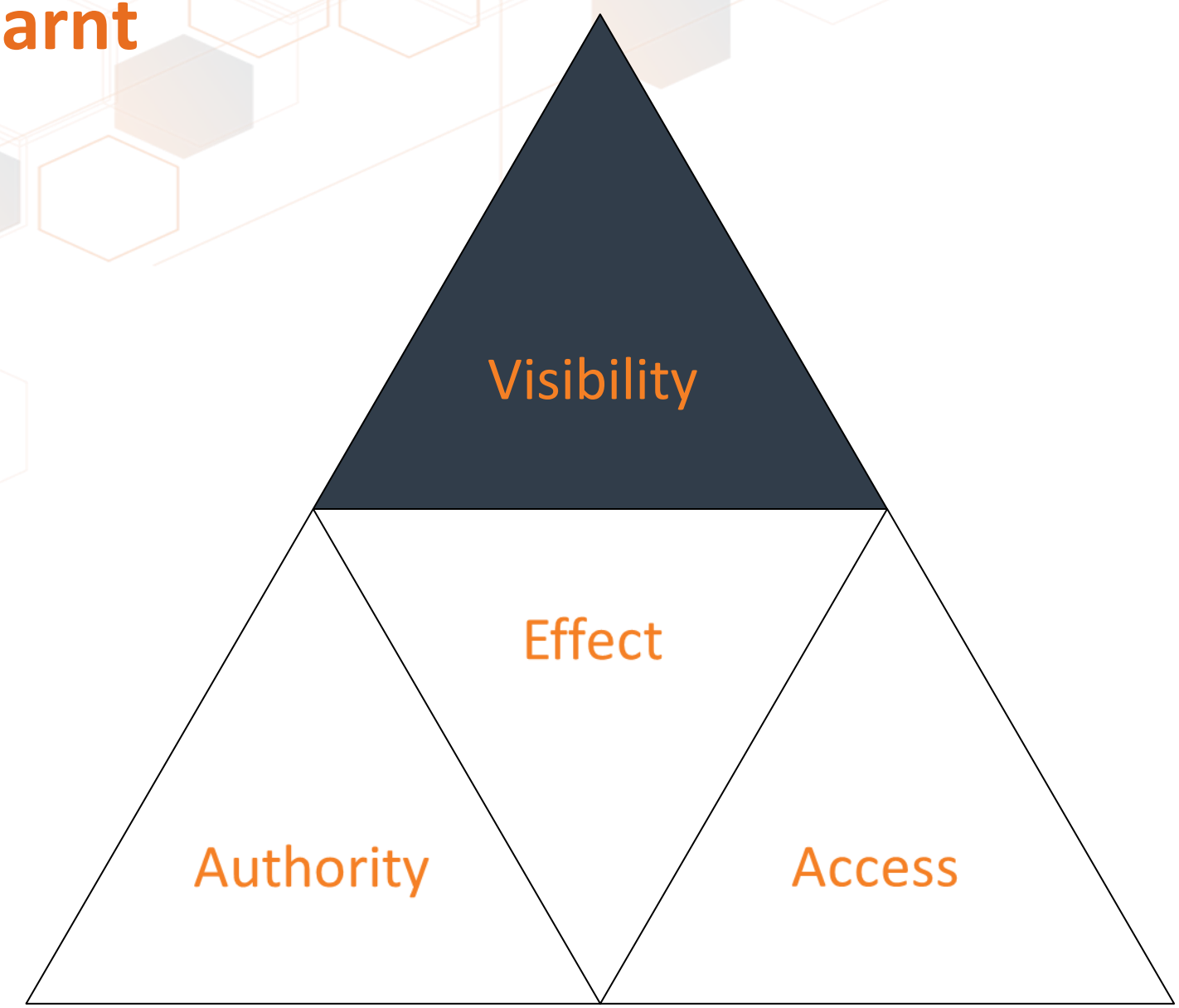
Drivers for Automation

- Legislation & Compliance Requirements
- Processing Data
- Staff Constraints
- Asymmetric Gain

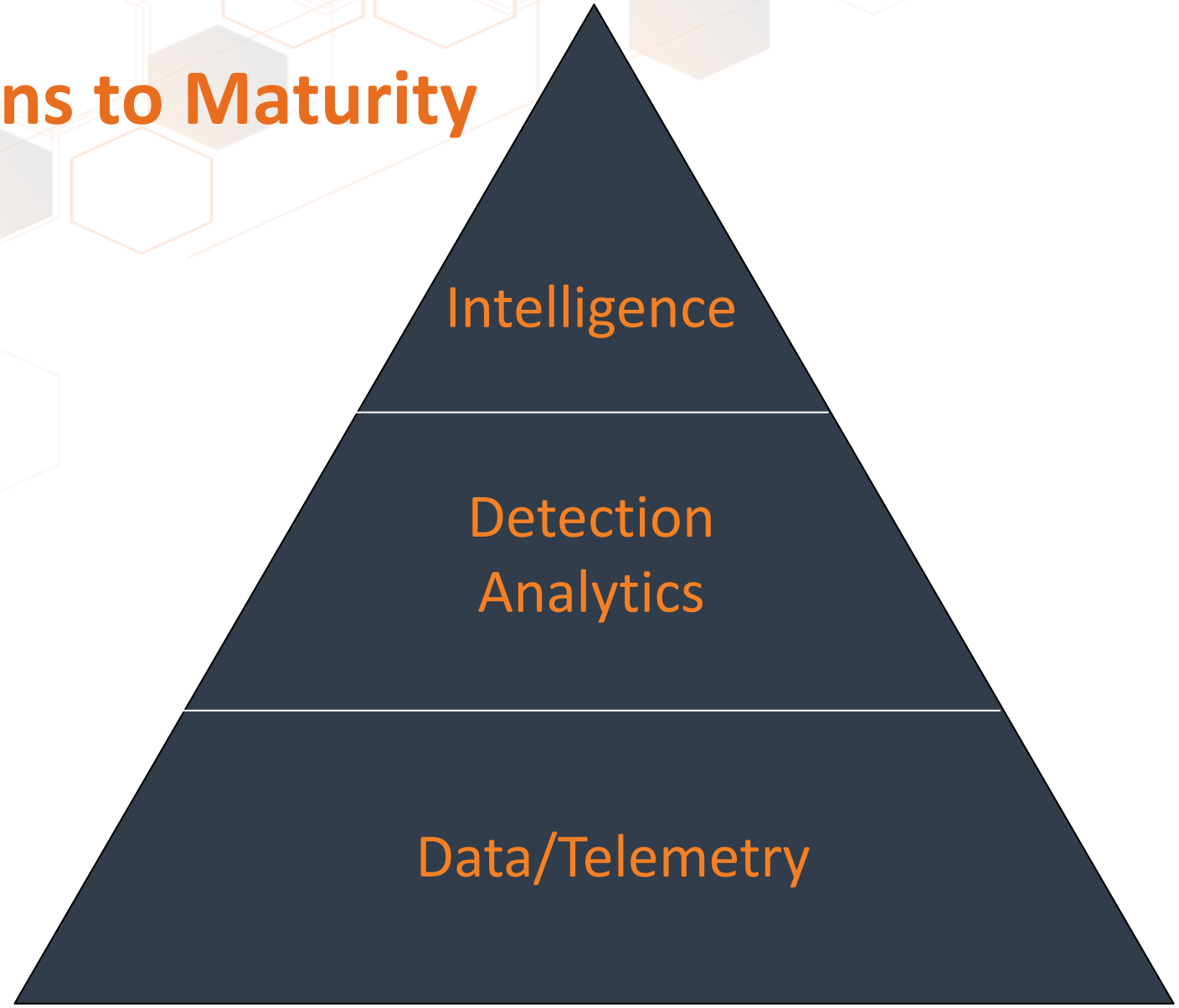
How are we getting there?

How are we measuring our success?

Lessons Learnt



Visibility: Foundations to Maturity



THANK YOU

Defending Australia and its National Interests
www.defence.gov.au