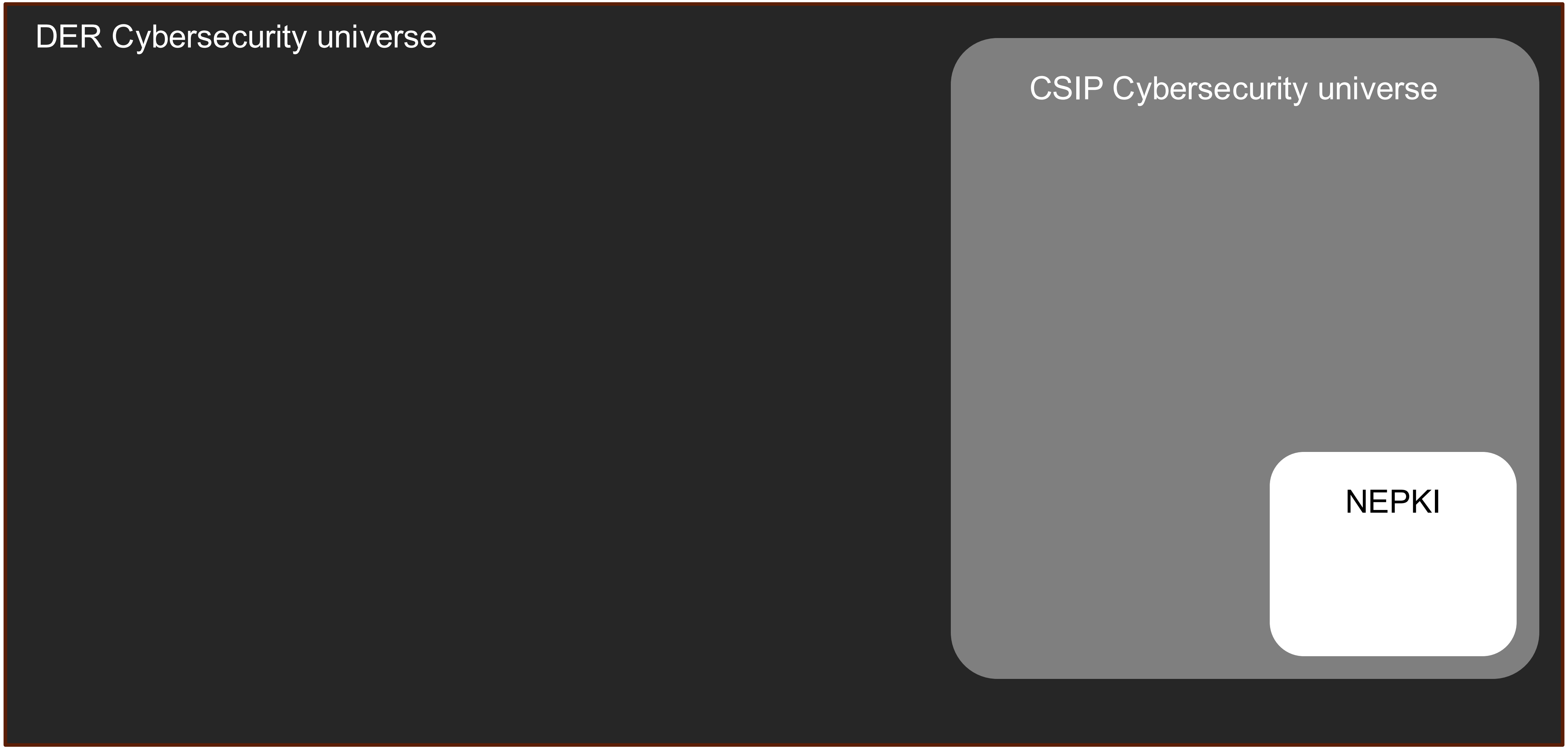
CAPA\

DER Cyber Update

CSIP Conference
October 2025

DER Cybersecurity whistlestop tour



DER Cybersecurity universe

CSIP Cybersecurity universe

NEPKI

DER Cybersecurity whistlestop tour

- How do we know if we are under attack? → CERby (ARENA)

  CERby program update

- How secure are our communications? → CAPA (ANU / ARENA)

  CSIP Aus Cybersecurity Review

- How we coordinate in an attack situation? → CERby (ARENA)

  DER cyber coordinator update

- Timing of mitgations

  One step at a time

CAPA\

How do we know if we are under attack?

CERby Risk summary

Total risk matrix space examined = 800

- 5 threat actors
- 20 critical cyber systems
- 8 types of attack goals and failure impacts

55	Significant DER related risks identified
5	Risks categorised as VERY HIGH (9%)
15	Risks categorised as HIGH and above (36%)
21	Risks categorised as MEDIUM and above (75%)
14	Risks categorised as LOW

55 of 800 risks identified and tracked as significant

TLP:AMBER

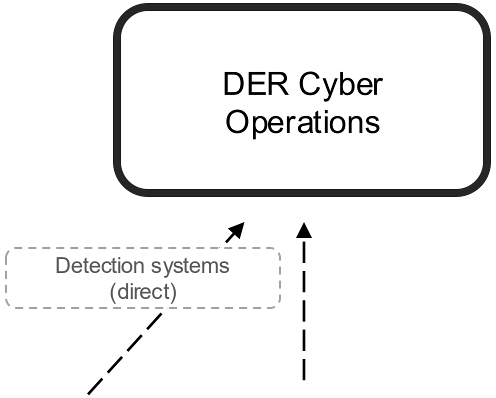
CERby Architecture for TD-IR

Two options for detection

CAPA\

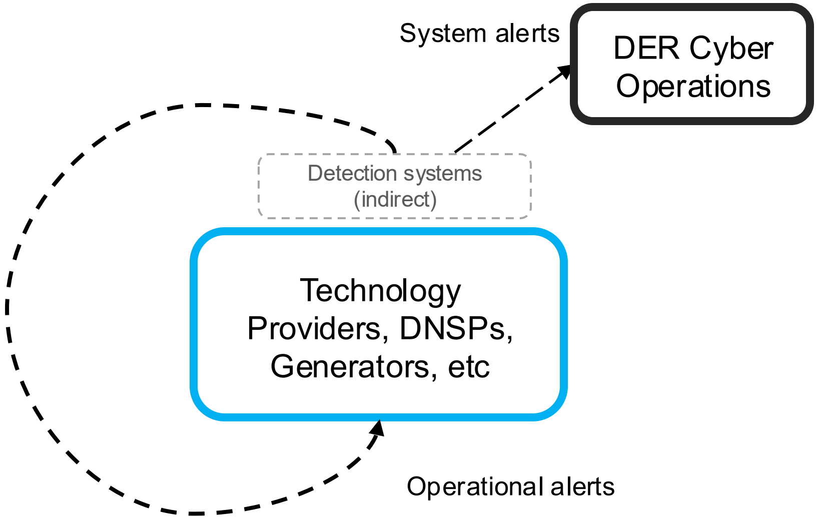
Option 1: Centralised detection

- All relevant information is collected raw form from the supply chain in quasi real=time and is subsequently stored and managed centrally.
- Detection of quasi real-time streams is carried out centrally at the system level.
- Central (or **DIRECT)** detection is suited to monitoring of external data systems, such as forecasting, telco, data centre infrastructures.
- No feedback on detections back to Operator Level systems.



Option 2: Decentralised detection

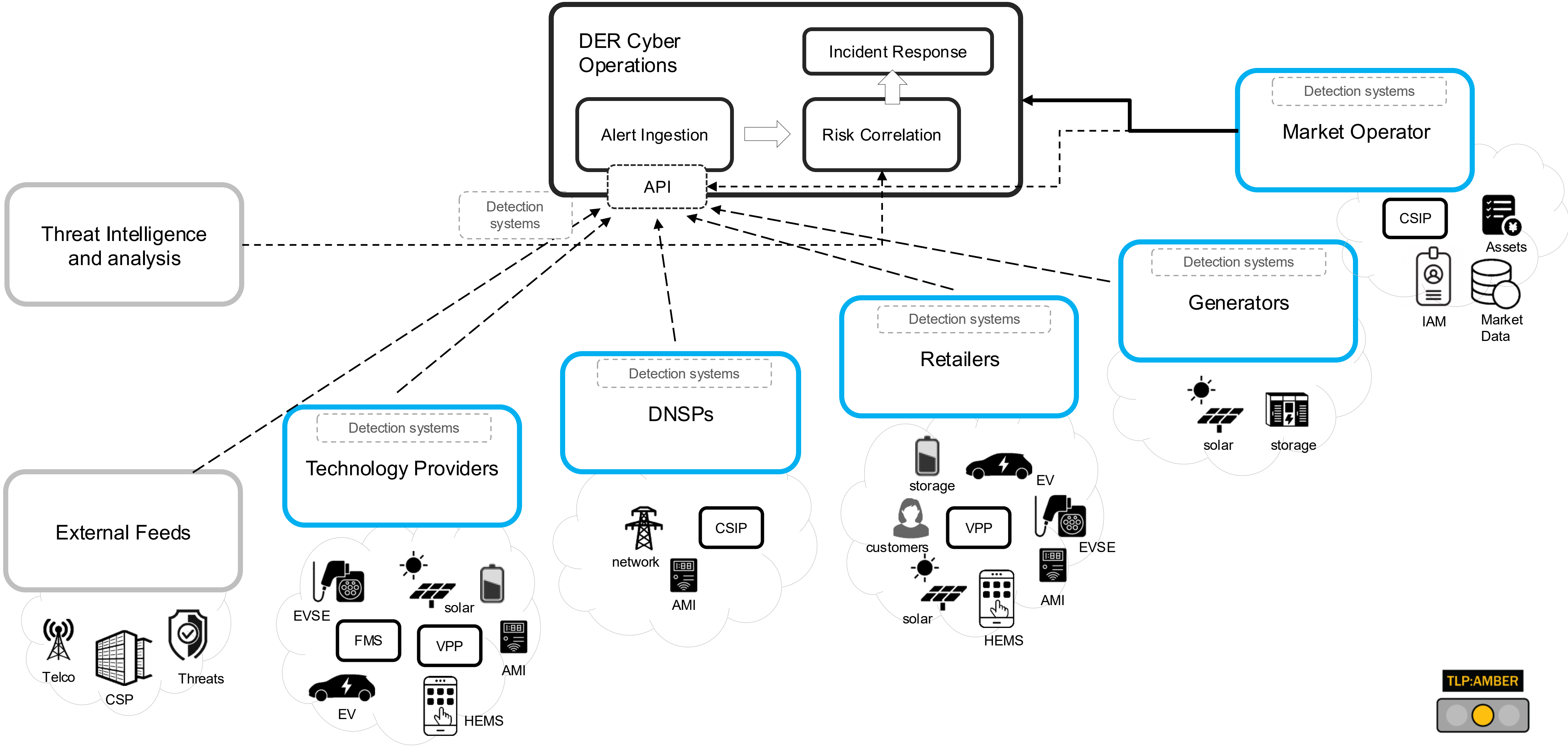
- Specific indicators are analysed and collected in quasi real-time (e.g. alerts) whilst raw form information is stored at Operator level.
- Decentralised (or **INDIRECT)** detection on quasi real-time streams is carried out at the Operator Level and signalled as System Alerts.
- Feedback from the detections can be provided back to Operator Level where required.


System alerts
DER Cyber Operations
Detection systems (indirect)
Technology Providers, DNSPs, Generators, etc
Operational alerts

TLP:AMBER

CERby Architecture for TD-IR

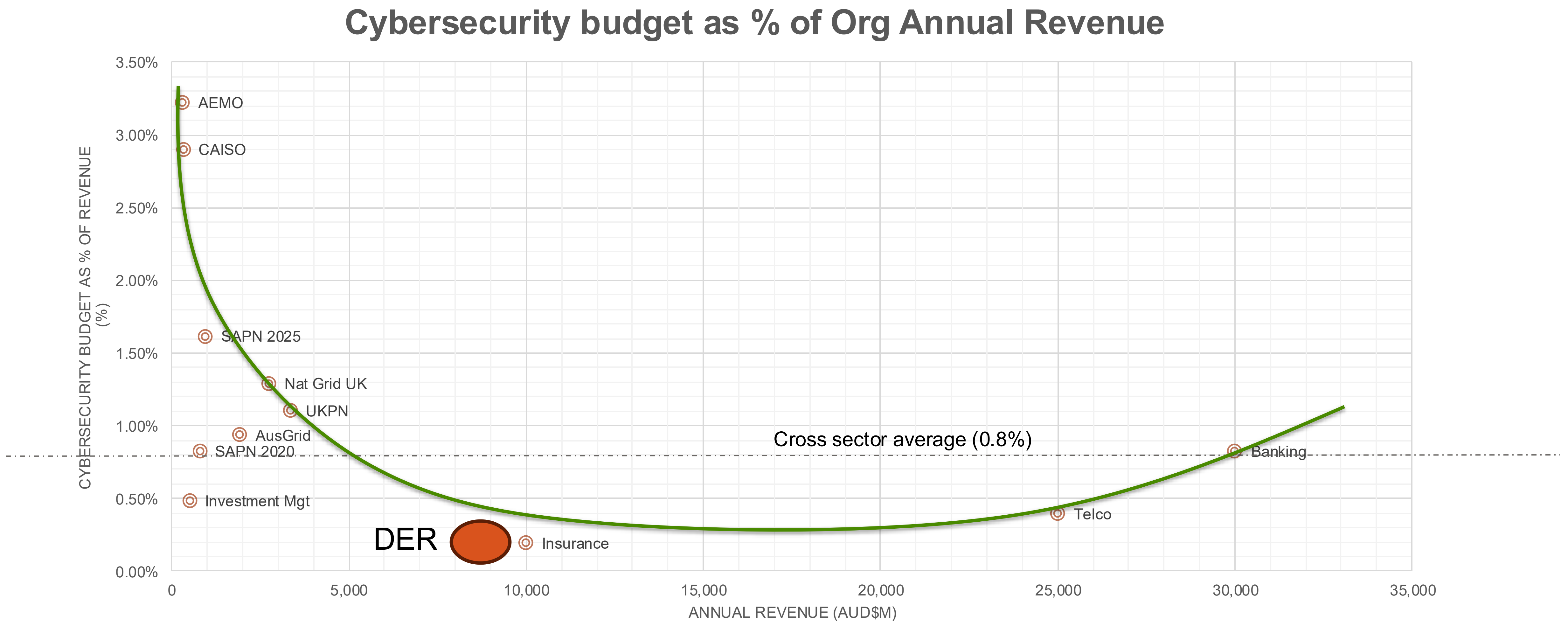
Threat Detection approach



TLP:AMBER

CERby benchmarking costs for cybersecurity

Costs for DER cyber vs other sectors



TLP:AMBER

How secure are our communications?

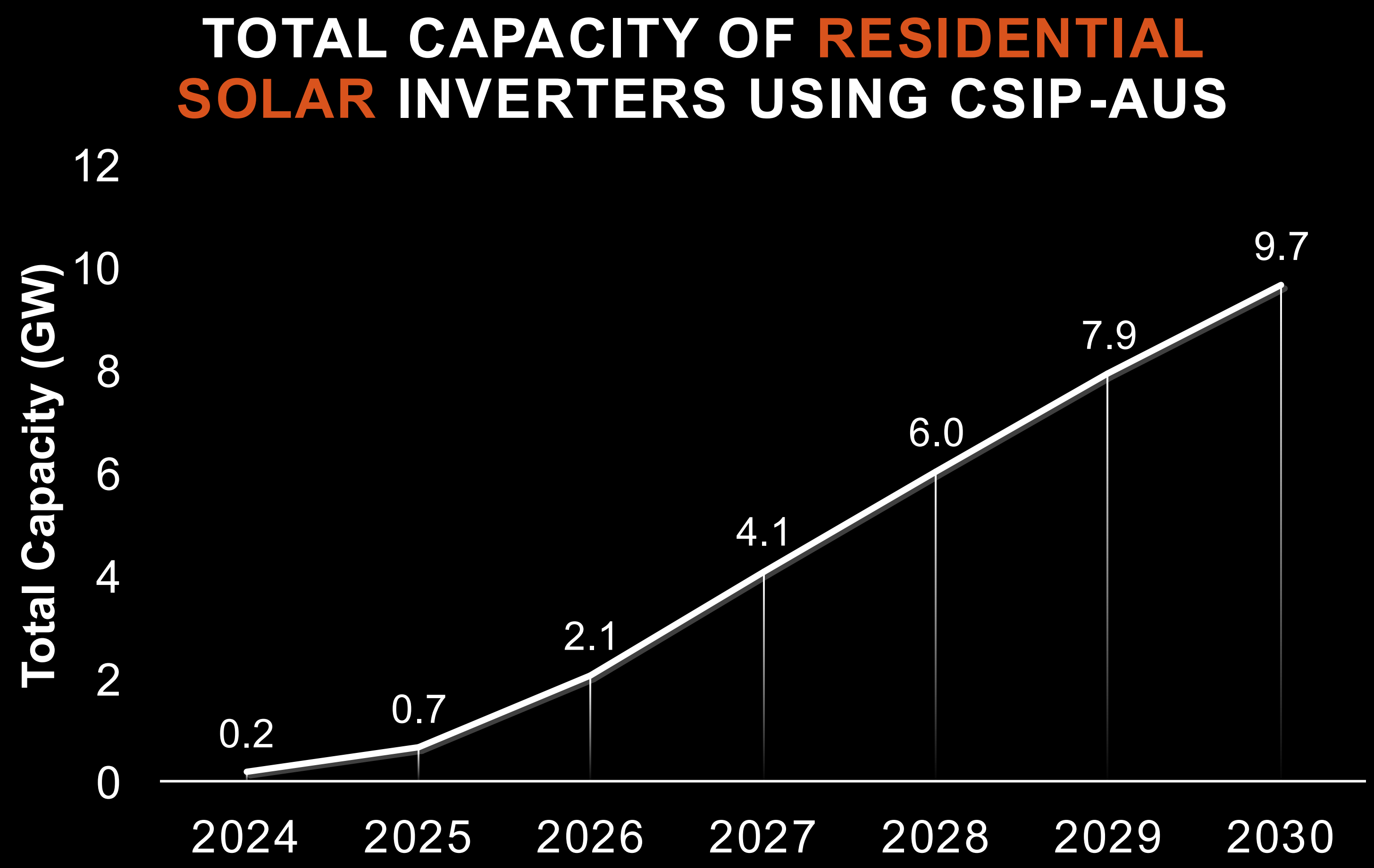
Objectives

1. Identify potential weaknesses or vulnerabilities in the CSIP-AUS standard that may affect real world usage in implementations and supporting infrastructure.

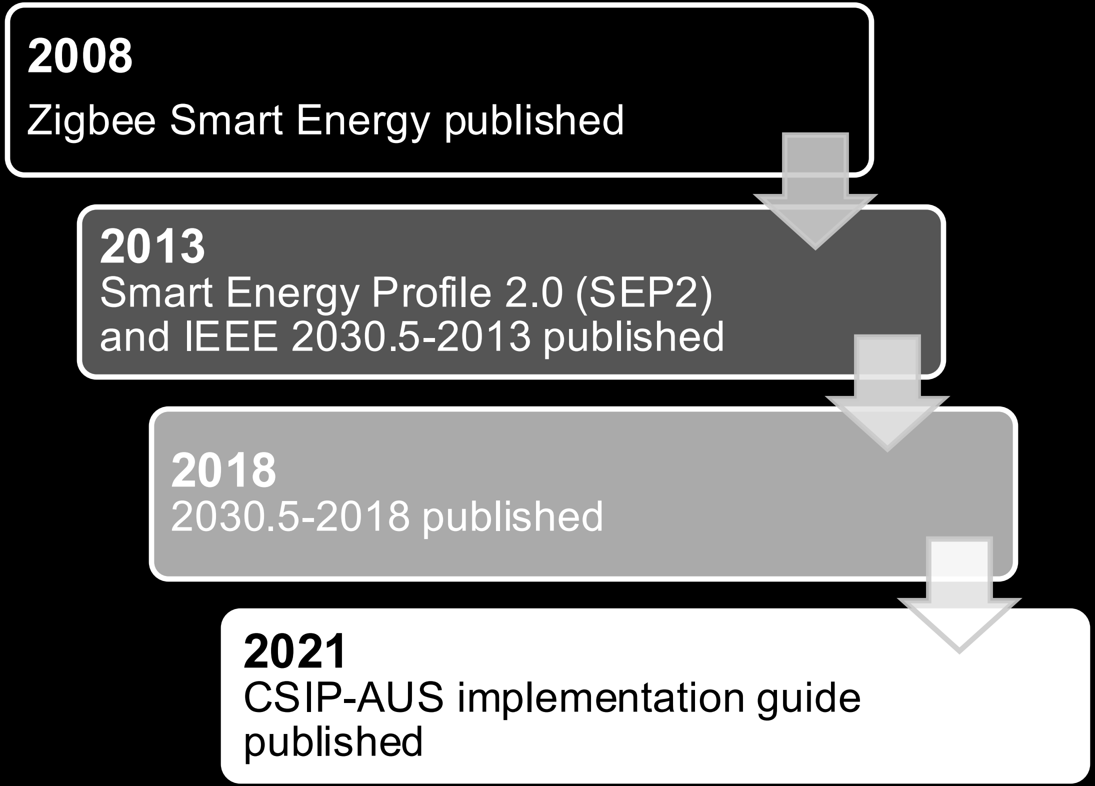
2. Provide guidance on how to mitigate those weaknesses in CSIP-AUS implementations and supporting infrastructure in the near term.

3. Provide suggestions or recommendations on how to uplift the cyber and cyber-physical security of CSIP-AUS and infrastructure over time.

Large Uptake of CSIP-AUS in Australia



History of SEP and CSIP-AUS



2008

Zigbee Smart Energy published

2013

Smart Energy Profile 2.0 (SEP2) and IEEE 2030.5-2013 published

2018

2030.5-2018 published

2021

CSIP-AUS implementation guide published

Take-outs

“CSIP-Aus is at ”startup” MVP level sophistication, for what will rapidly evolve into an industrial grade problem”

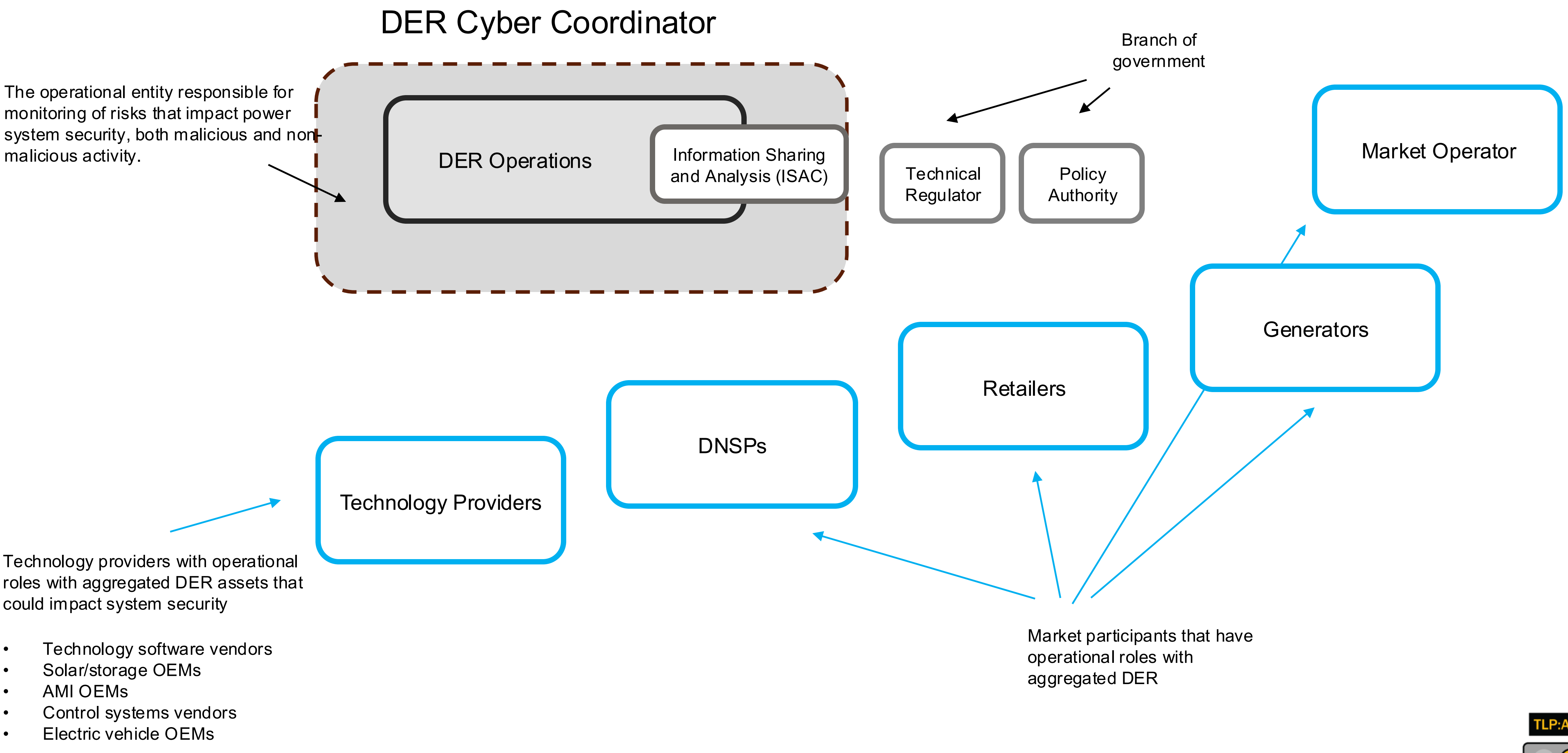
Recommended mitigations

- Introduce detections for clear protocol abuses
- NEPKI to improve PKI and reduce credential abuse
- Start on industrial grade CSIP Aus 2.0

How do we coordinate in an attack situation?

Responsible actors in DER cyber

Key Actors



The operational entity responsible for monitoring of risks that impact power system security, both malicious and non-malicious activity.

Branch of government

Technology providers with operational roles with aggregated DER assets that could impact system security

- Technology software vendors
- Solar/storage OEMs
- AMI OEMs
- Control systems vendors
- Electric vehicle OEMs

Market participants that have operational roles with aggregated DER

TLP:AMBER

CERby - The DER Cyber Coordinator Role

The DER Cyber Coordinator role has been earmarked to perform several main functions;

a) **Data**: collection of important contextual data (e.g. standing data / DER register, market info) and analytic tools to perform targeted searches for detecting anomalies & identifying threats.

b) **Intel**: collection of shared threat intel (alerts and reports) from operators in Australia on suspicious activities.

c) **Analysis**: the analysis, correlation and escalation of alert information into tracked case incidents, performed by both human security analysts and machine systems**.

These are the functions performed under the ISAC*** model in US and Europe.

d) **Coordination**: the operational case incident response coordination for incidents that pose risk to the power system.

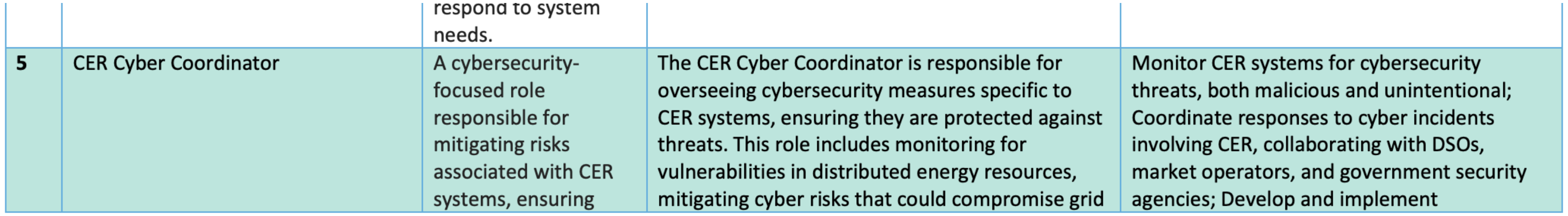
**Note that detection is assumed to be a decentralized task, done by each of the Operators of DER systems (i.e. DNSPs, Retailers, OEM, Aggregators, Metering coords)
*** Information Sharing and Analysis Centre (ISAC), which are industry specific (e.g. energy) and focus purely on cybersecurity

TLP:AMBER

CER Task Force:

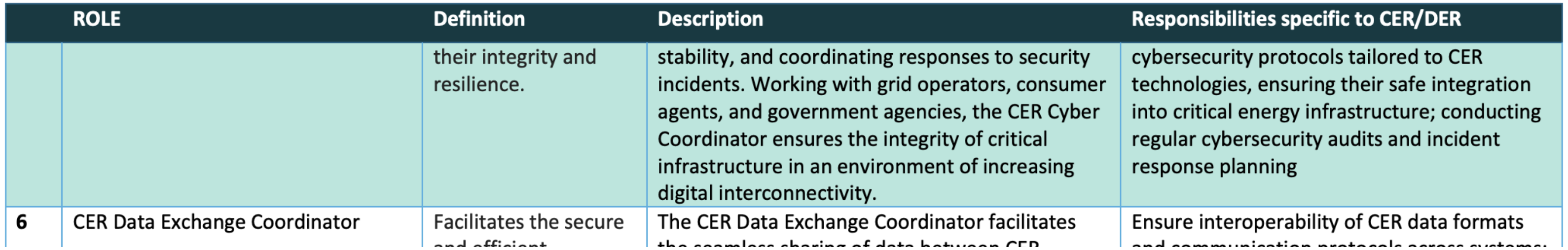
DCCEEW lead on cybersecurity streams

- Formalising role of DER Cyber coordinator (P3)
- Gaps and forward plan for wide scale cyber impacts to power systems (T5)



		respond to system needs.		
5	CER Cyber Coordinator	A cybersecurity-focused role responsible for mitigating risks associated with CER systems, ensuring	The CER Cyber Coordinator is responsible for overseeing cybersecurity measures specific to CER systems, ensuring they are protected against threats. This role includes monitoring for vulnerabilities in distributed energy resources, mitigating cyber risks that could compromise grid	Monitor CER systems for cybersecurity threats, both malicious and unintentional; Coordinate responses to cyber incidents involving CER, collaborating with DSOs, market operators, and government security agencies; Develop and implement

Consumer Energy Resources Taskforce



	ROLE	Definition	Description	Responsibilities specific to CER/DER
		their integrity and resilience.	stability, and coordinating responses to security incidents. Working with grid operators, consumer agents, and government agencies, the CER Cyber Coordinator ensures the integrity of critical infrastructure in an environment of increasing digital interconnectivity.	cybersecurity protocols tailored to CER technologies, ensuring their safe integration into critical energy infrastructure; conducting regular cybersecurity audits and incident response planning
6	CER Data Exchange Coordinator	Facilitates the secure and efficient	The CER Data Exchange Coordinator facilitates the seamless sharing of data between CER	Ensure interoperability of CER data formats and communication protocols across systems;

Timing of mitigations

SOCI obligations

If your system(s) are the control path of more than;

- 30 MW
  - risk assessment
  - Logging / basic audits
- 100 MW
  - Threat detection L0/L1
  - Basic inventory and access control
- 250 MW
  - Fleet inventory, automated access control
  - Threat sharing, threat intel
- 500 MW
  - Threat detection L3/L4
  - Infra detection & response (data centers, telco, power)

CSIP Aus 2.0

By 2030, there will be 10+ GW of generation & storage using CSIP Aus 1.x

➤ To launch a new CSIP Aus protocol by 2030, we must start in early 2026.

CAPA\

Threat intelligence, detection and response

for the electricity sector

capaintelligence.com