AARNet-Cybera collaborative SOC
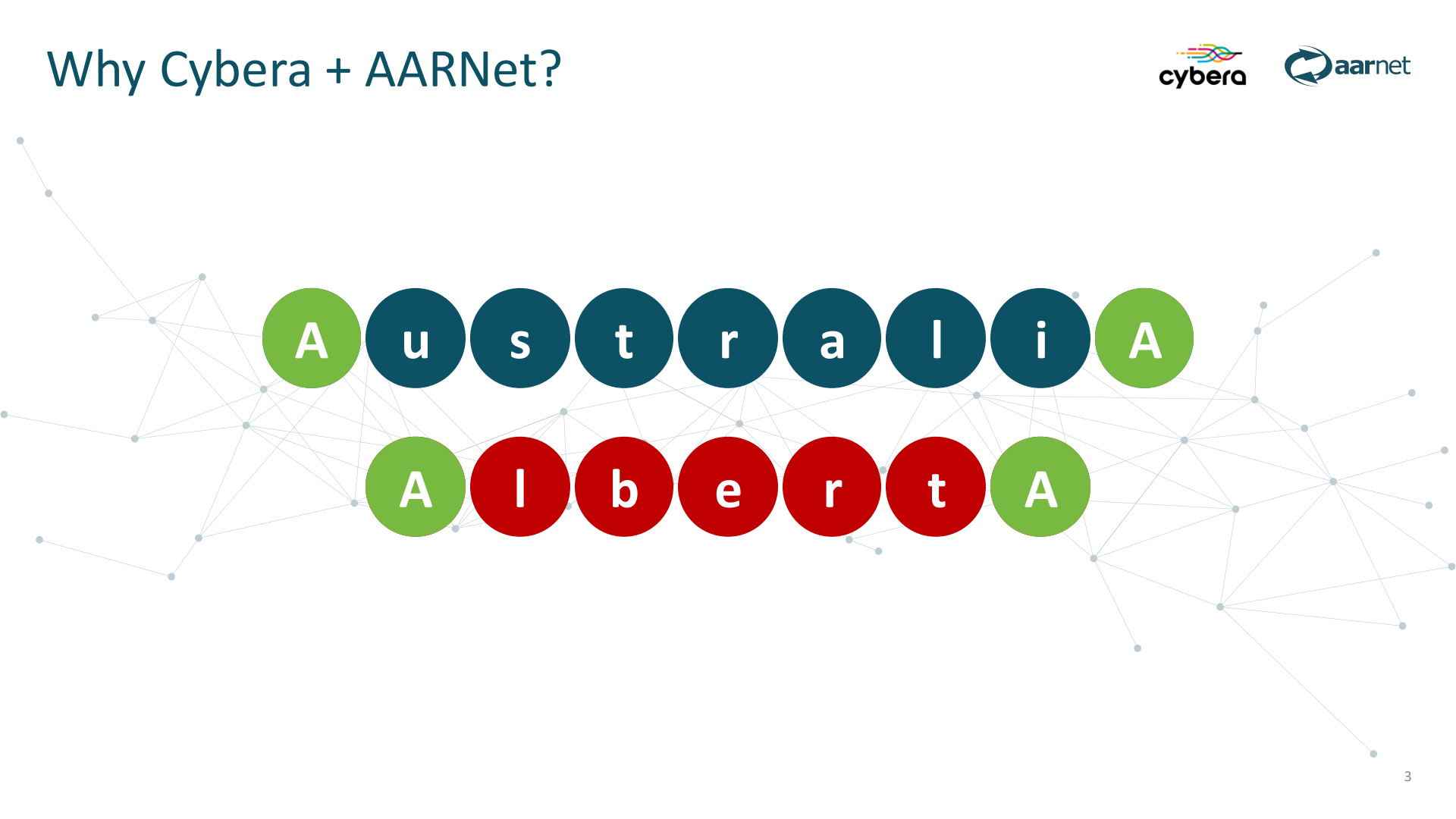
Barb Carra, President and CEO, Cybera
Chris Hancock, CEO, AARNet

TNC25, Brighton, UK
10 June 2025

How this
all started

Why Cybera + AARNet?

AustraliA

AlbertA
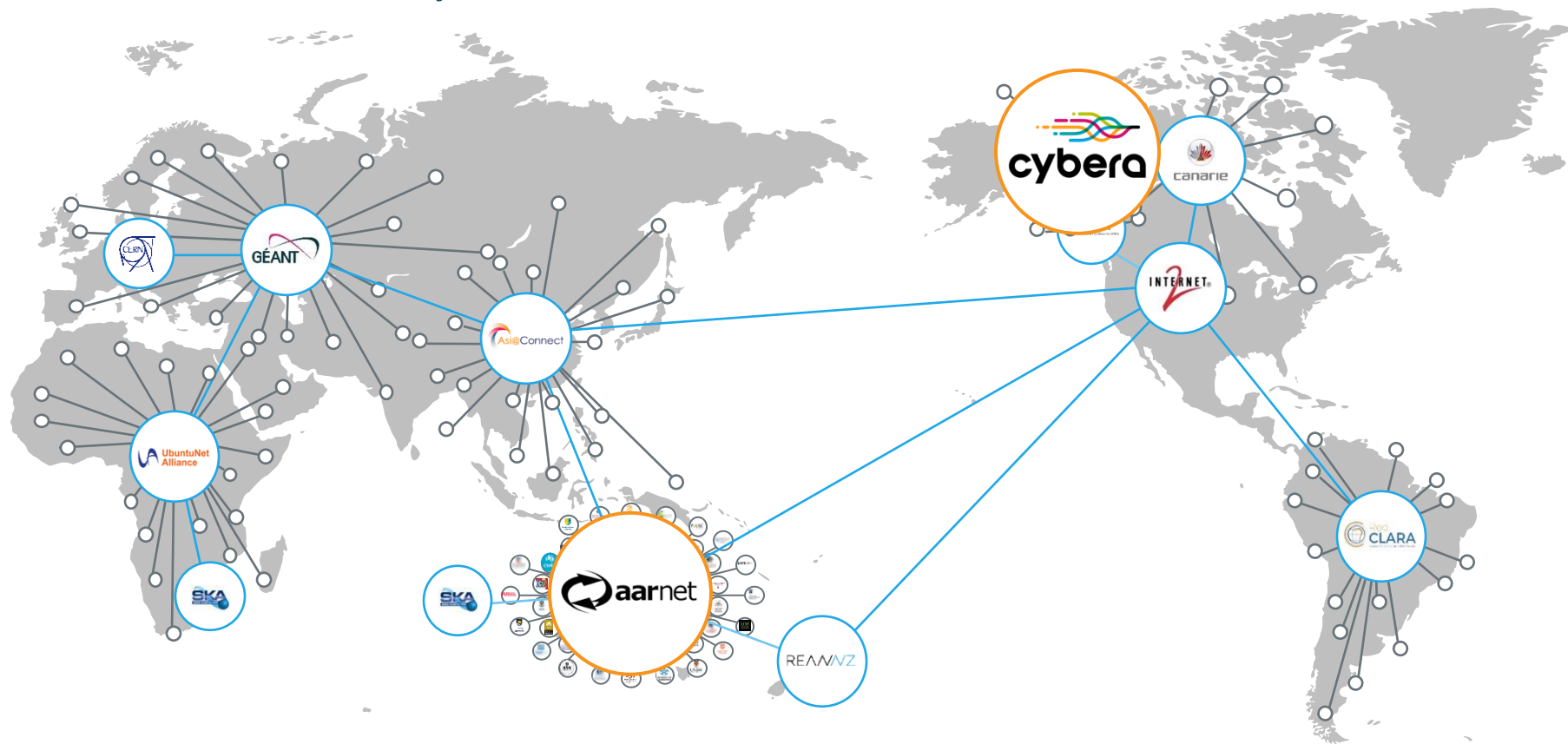
Why Cybera + AARNet?

35°C

35

-35°C

NREN community

Background: the AARNet SOC

What we do in a day

A view on a single university in one day

4.42B
Log Management

4.6M
Signals Observed

718
Investigations

54
Cases Raised

View of all logs ingested by vendor view

SOC telemetry These events populate risk scores

Alerts the SOC investigated, driven by risk scores of >90

Incidents that warrant an escalation to the customer

SOC by the numbers

115
Unique products

55.4
Billion logs per day

140TB
Average log ingestion/day

19k
Log sources onboarded

1.2M
Alarms
(12 months)

3.7k
Security cases
(12 months)

Creating a partnership

Kicking off this unique project

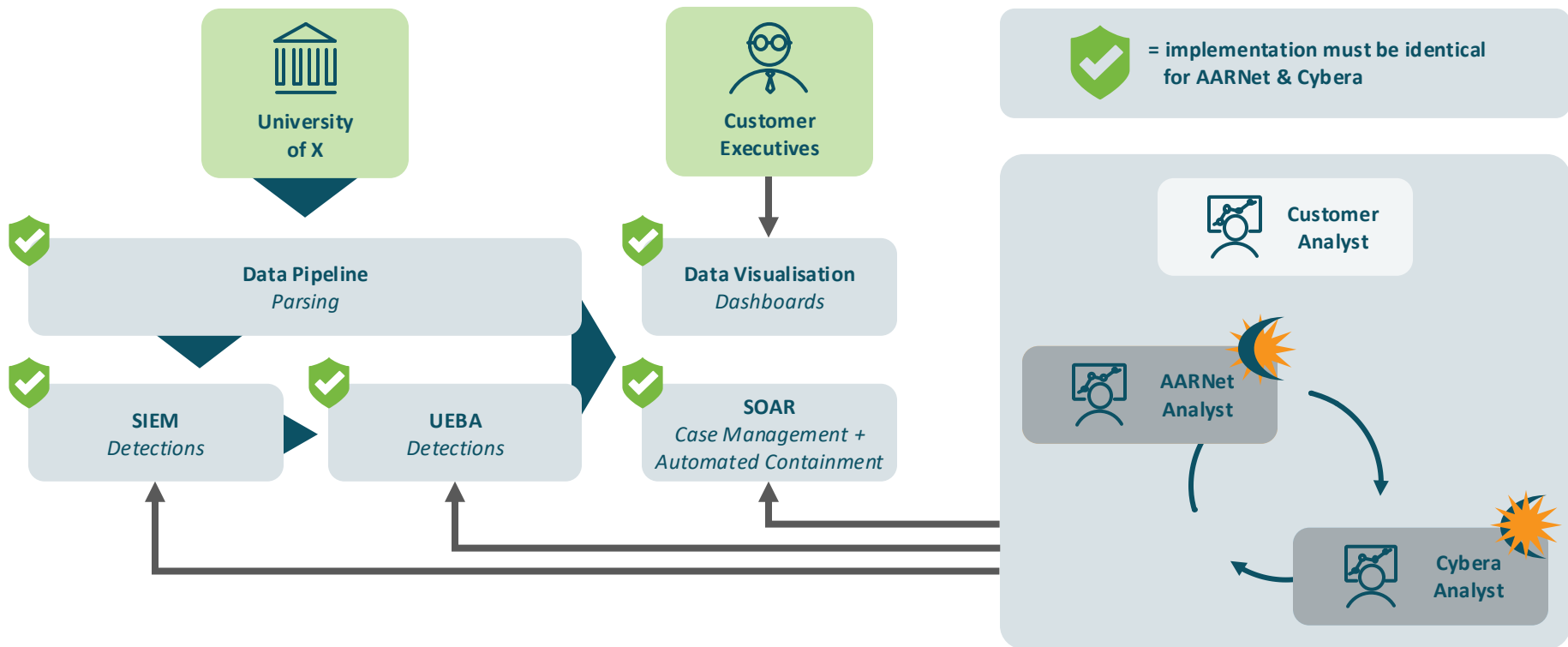Identifying the intended outcomes

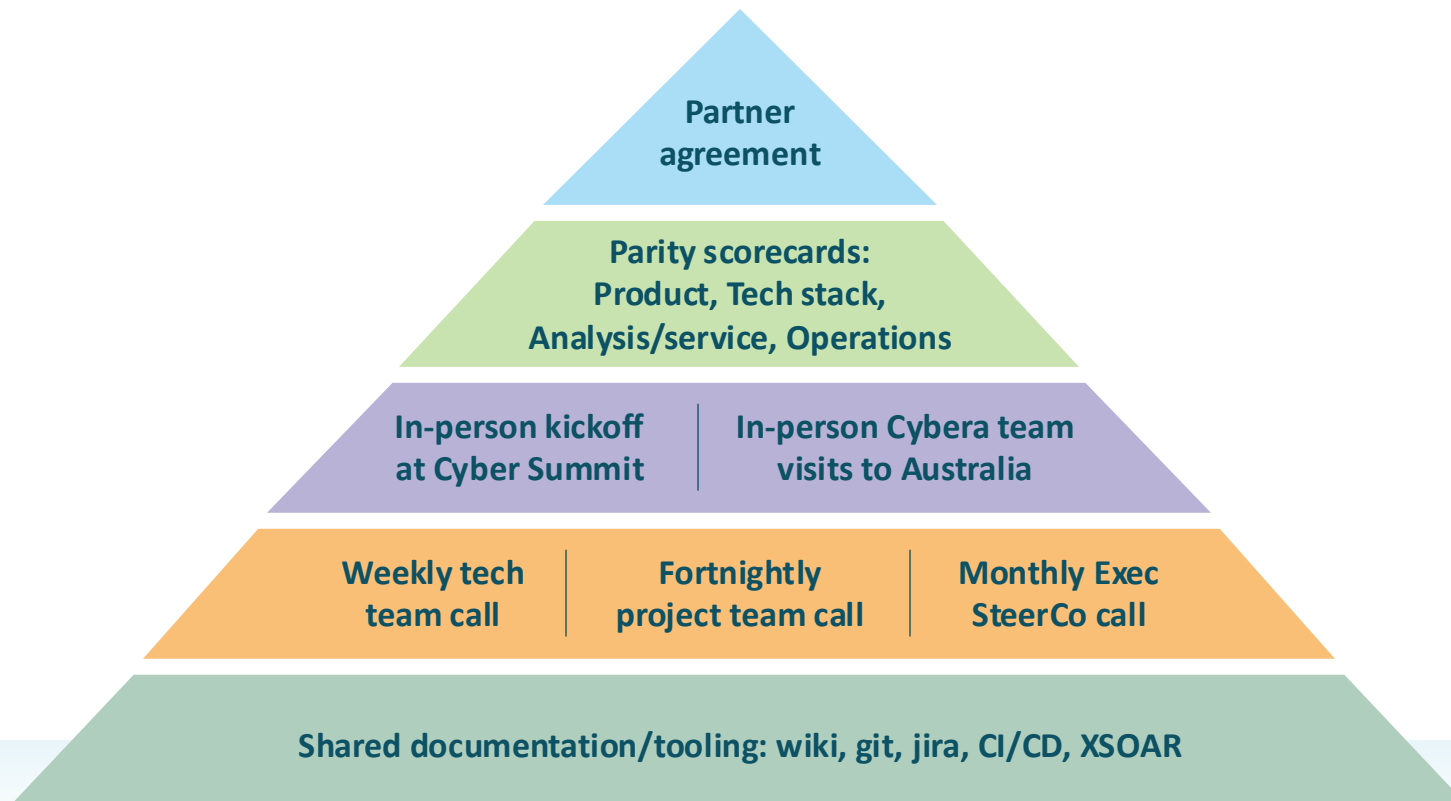**24x7 operations**

Cybera SOC sooner

Shared engineering teams

Next steps: collaborative implementation

"Functional parity" – what does this entail?

Supporting the ongoing collaboration

Partner agreement

Parity scorecards: Product, Tech stack, Analysis/service, Operations

In-person kickoff at Cyber Summit | **In-person Cybera team visits to Australia**

Weekly tech team call | **Fortnightly project team call** | **Monthly Exec SteerCo call**

Shared documentation/tooling: wiki, git, jira, CI/CD, XSOAR

Looking ahead

Successes – and challenges

Successes	Challenges
Joint 24x7 capability launched	Vendor engagement & procurement
Cybera tech stack stood up	Code sharing
Onboarding Cybera pilot customers	Case management

Looking to the future

NOW

Alignment parity scorecard

Mature governance meeting cadence

Cybera onboard pilot members

Cybera move to production

NEXT

Develop specialisations

Shared feature development

FUTURE

Add more NREN partners...

Thank You