DATA 61 CSIRO

2nd Data61/DST Group Cyber Summer School

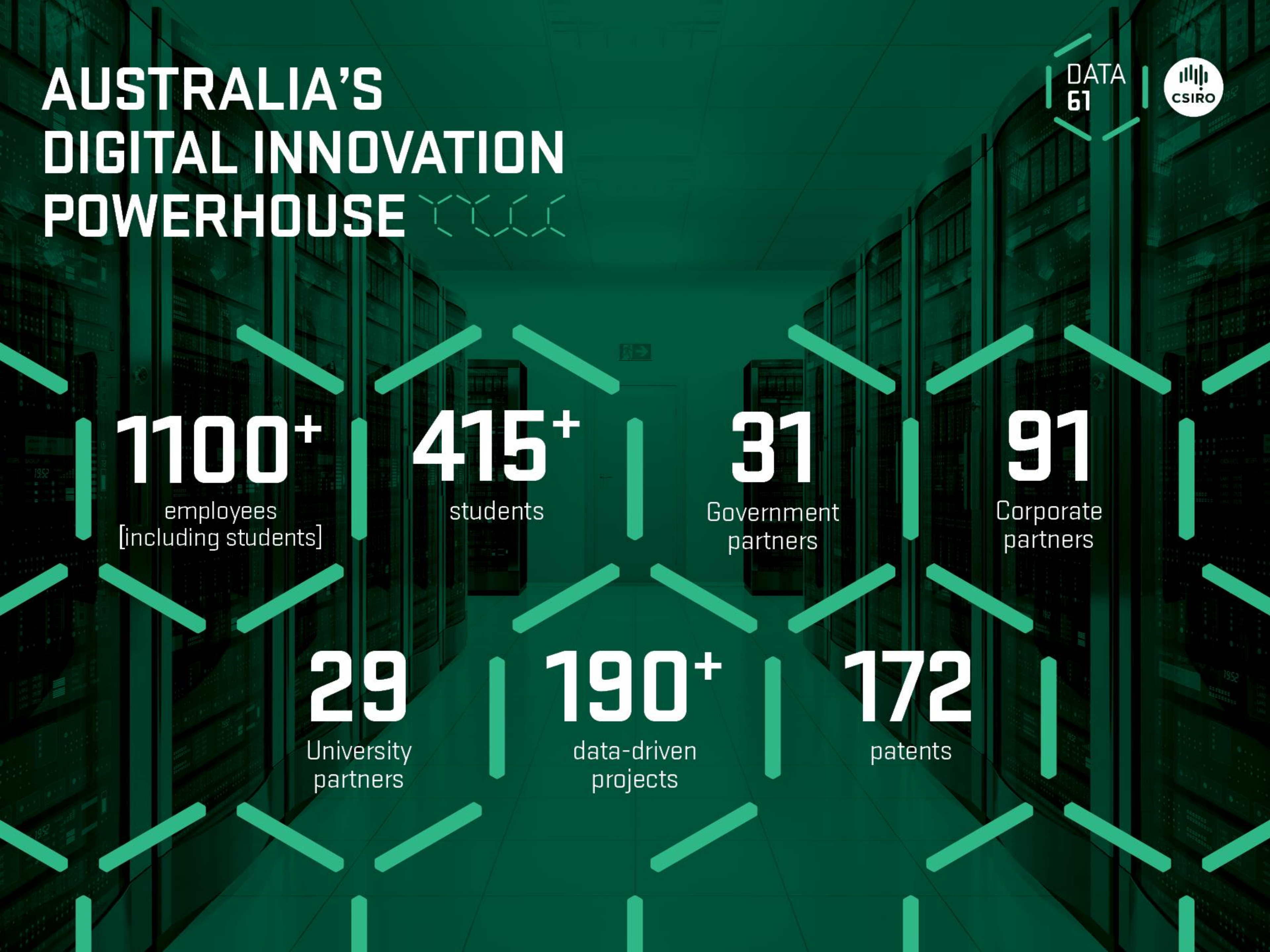
Adelaide, 21 - 22 March, 2019

CSIRO DATA 61

Australian Government
Department of Defence
Science and Technology

DEFENCE INDUSTRY & INNOVATION
NEXT GENERATION TECHNOLOGIES FUND

AUSTRALIA'S DIGITAL INNOVATION POWERHOUSE



1100^{+}
employees
[including students]

415^{+}
students

31
Government
partners

91
Corporate
partners

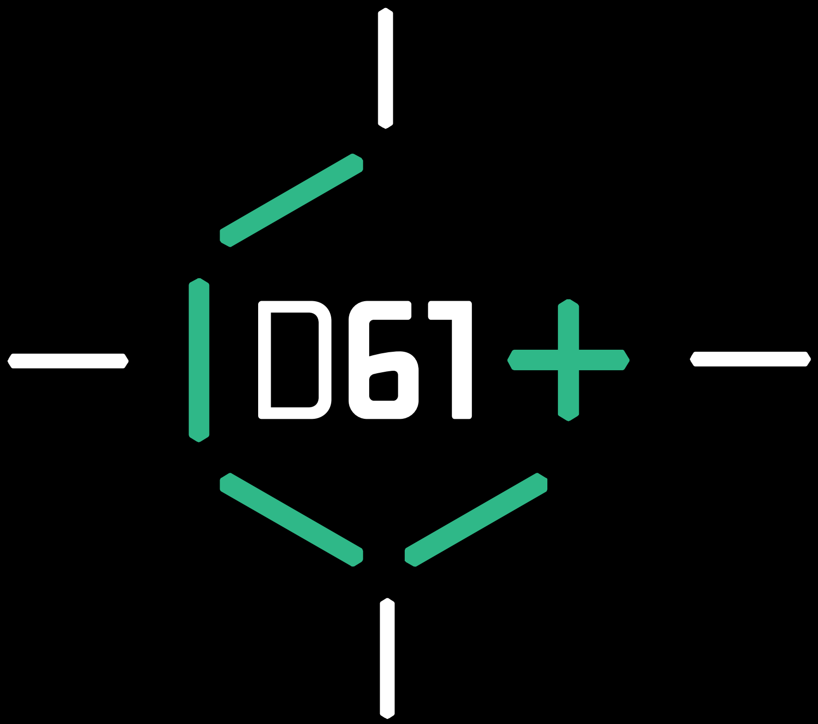
29
University
partners

190^{+}
data-driven
projects

172
patents

Industry – Academia Collaboration

Automate and simplify the cyber security necessary for our data driven future.



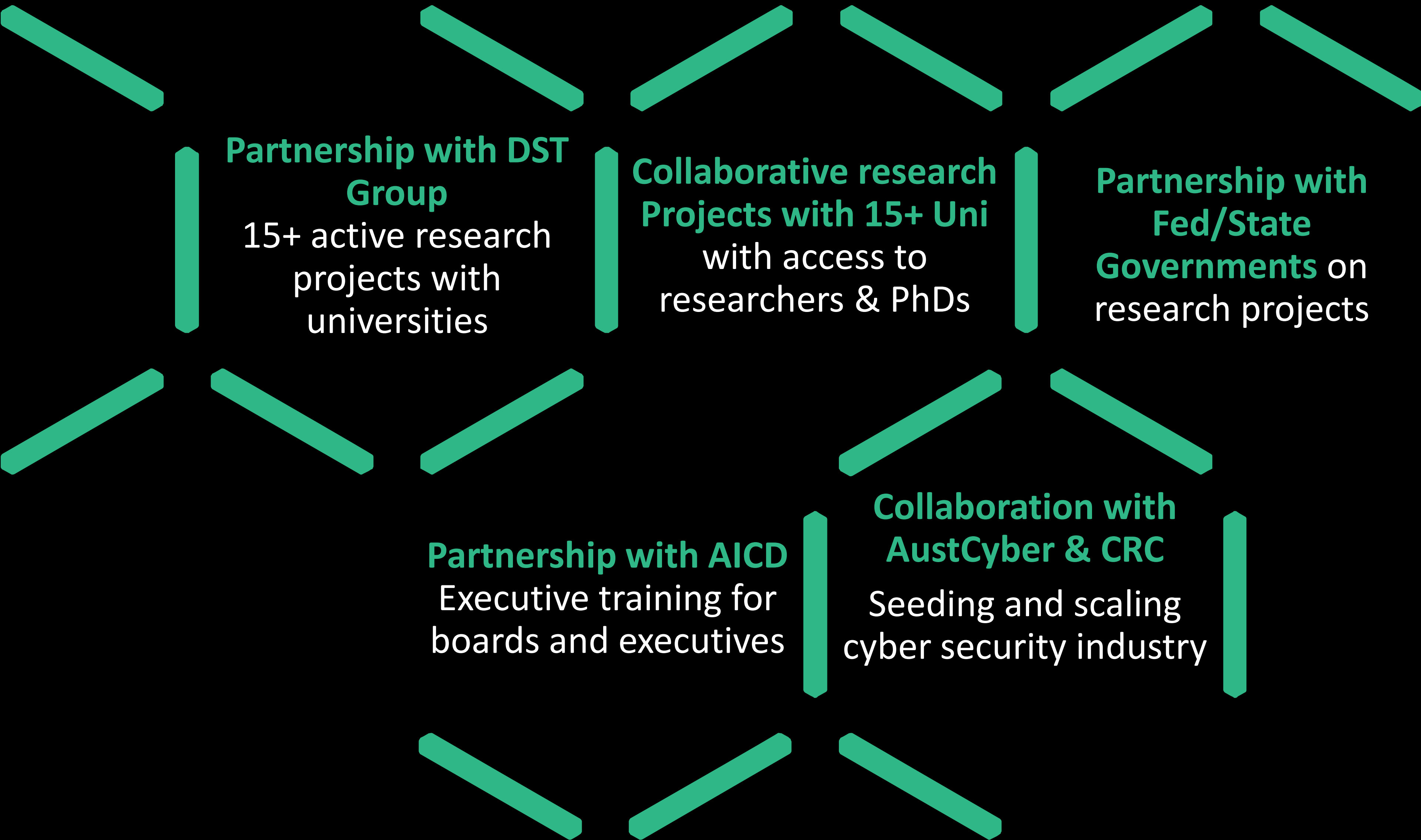
CORPORATIONS

ACADEMIA
Current University
Collaboration
Agreements - DUCA

GOVERNMENTS
Federal, State and
Territory Govts

STARTUPS/SME

D61+ Cybersecurity Network



Partnership with DST Group
15+ active research projects with universities

Collaborative research Projects with 15+ Uni with access to researchers & PhDs

Partnership with Fed/State Governments on research projects

Partnership with AICD
Executive training for boards and executives

Collaboration with AustCyber & CRC

Seeding and scaling cyber security industry

Research Challenges & Themes

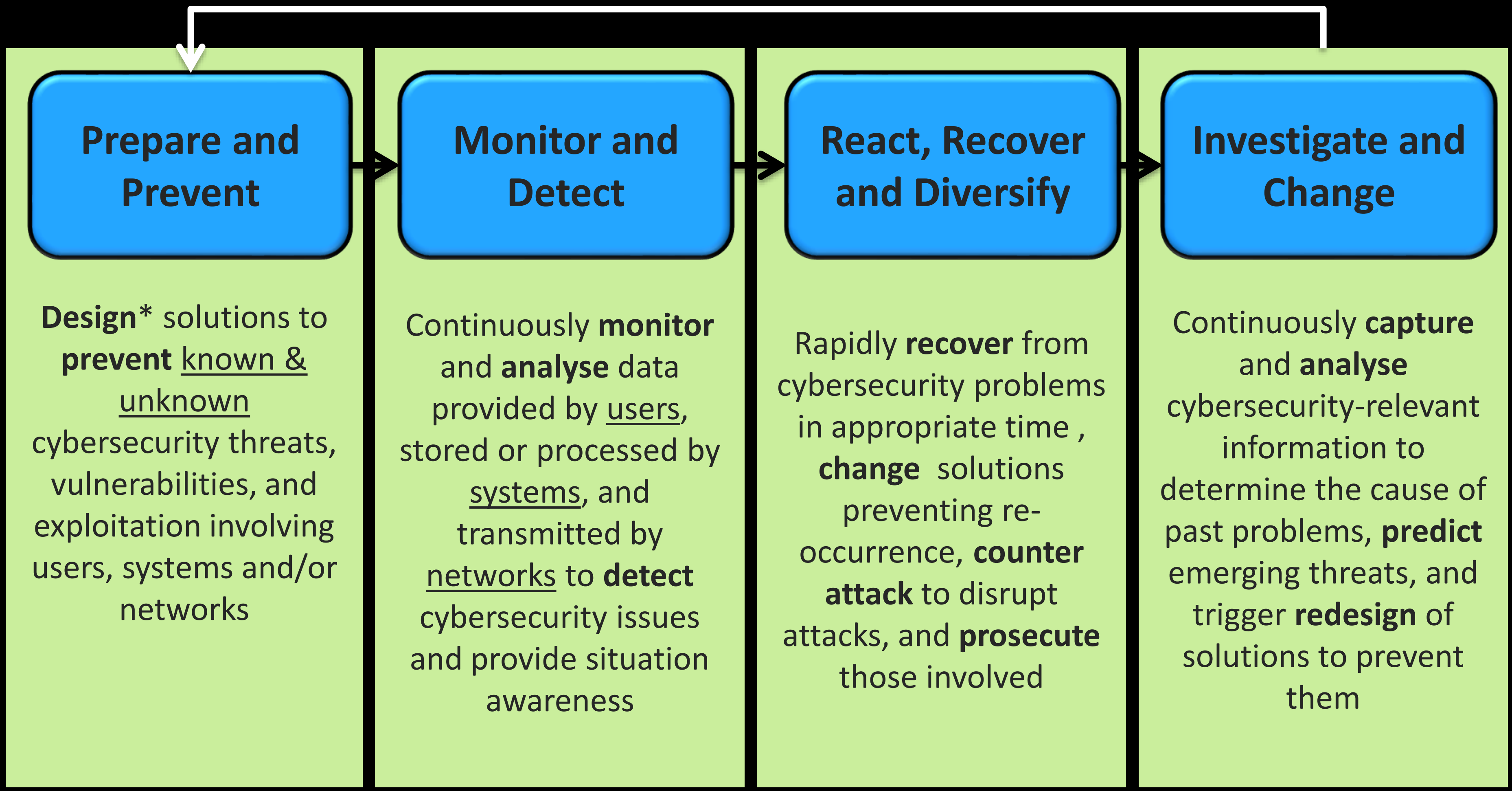
Research challenges, defined together with our defence partner, DST Group

- *Building trustworthy and resilient cyber systems.*
- *Risk-based cyber approaches and shared awareness.*
- *Strengthening the human and social dimension of cyber security.*

Research themes within ***D61+ network***

- *Trustworthy Systems*
- *Automating Cybersecurity and Resilient Systems*
- *Cyber-Physical Systems Security*
- *Quantitative Cybersecurity Risk Management*
- *Data Security and Privacy*
- *Data and Decision Trustworthiness*
- *Usable Human-centric Security*

Cybersecurity Lifecycle



Prepare and Prevent

Design* solutions to **prevent** known & unknown cybersecurity threats, vulnerabilities, and exploitation involving users, systems and/or networks

Monitor and Detect

Continuously **monitor** and **analyse** data provided by users, stored or processed by systems, and transmitted by networks to **detect** cybersecurity issues and provide situation awareness

React, Recover and Diversify

Rapidly **recover** from cybersecurity problems in appropriate time , **change** solutions preventing re-occurrence, **counter attack** to disrupt attacks, and **prosecute** those involved

Investigate and Change

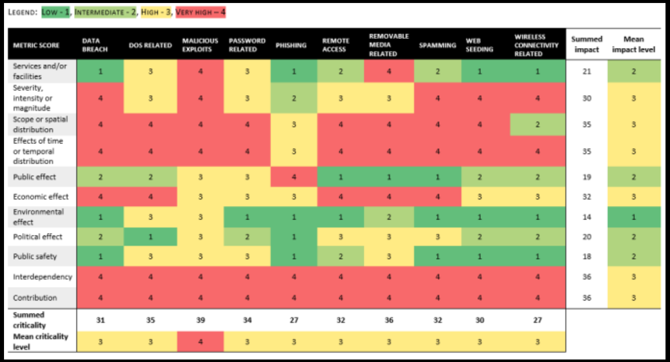
Continuously **capture** and **analyse** cybersecurity-relevant information to determine the cause of past problems, **predict** emerging threats, and trigger **redesign** of solutions to prevent them

Example Cyber Projects

Government: State and Federal

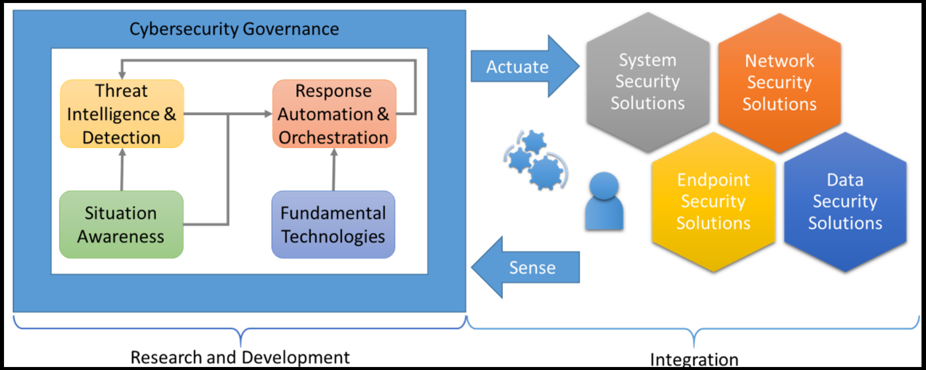
DATA 61 CSIRO

- Governing Cybersecurity by Identifying High Risk Threats
- Cybersecurity Incident Response Orchestration (CIRO)
- Whole-of-Government Secure Data Sharing Framework



Legend: 🟩 Low - 1, 🟩 Intermediate - 2, 🟨 High - 3, 🟥 Very high – 4

Metric score	Data breach	DOS related	Malicious exploits	Password related	Phishing	Remote access	Removable media related	Spamming	Web seeding	Wireless connectivity related	Summed impact	Mean impact level
Services and/or facilities	1	3	4	3	1	2	4	2	1	1	21	2
Severity, intensity or magnitude	4	3	4	3	2	3	3	4	4	4	30	3
Scope or spatial distribution	4	4	4	4	3	4	4	4	4	2	35	3
Effects of time or temporal distribution	4	4	4	4	3	4	4	4	4	4	35	3
Public effect	2	2	3	3	4	1	1	1	2	2	19	2
Economic effect	4	4	3	3	3	4	4	4	3	3	32	3
Environmental effect	1	3	3	1	1	1	2	1	1	1	14	1
Political effect	2	1	3	2	1	3	3	3	2	2	20	2
Public safety	1	3	3	3	1	2	3	1	1	1	18	2
Interdependency	4	4	4	4	4	4	4	4	4	4	36	3
Contribution	4	4	4	4	4	4	4	4	4	4	36	3
Summed criticality	31	35	39	34	27	32	36	32	30	27		
Mean criticality level	3	3	4	3	3	3	3	3	3	3		



Cybersecurity Governance

Threat Intelligence & Detection

Response Automation & Orchestration

Situation Awareness

Fundamental Technologies

Actuate

Sense

System Security Solutions

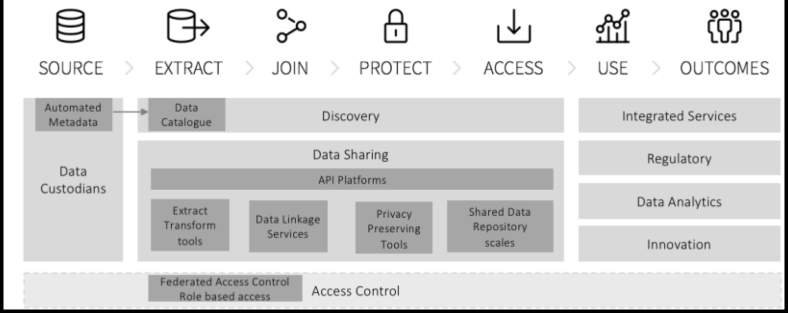
Network Security Solutions

Endpoint Security Solutions

Data Security Solutions

Research and Development

Integration



SOURCE > EXTRACT > JOIN > PROTECT > ACCESS > USE > OUTCOMES

Automated Metadata

Data Catalogue

Discovery

Data Custodians

Data Sharing

API Platforms

Extract Transform tools

Data Linkage Services

Privacy Preserving Tools

Shared Data Repository scales

Integrated Services

Regulatory

Data Analytics

Innovation

Federated Access Control Role based access

Access Control

NSW GOVERNMENT

Queensland Government

Machine Learning & AI for Cyber

Automating cyber defence and addressing skill shortage

DATA 61 CSIRO

- Adversarial Machine Learning
  - Prevent attack to the learning itself
- Deep Learning for Cyber
  - ML applied to detect bugs and anomalies
- Autonomous Cyber Operation
  - Apply AI planning and autonomic computing to cyber defence

Australian Government
Department of Defence
Defence Science and Technology Group

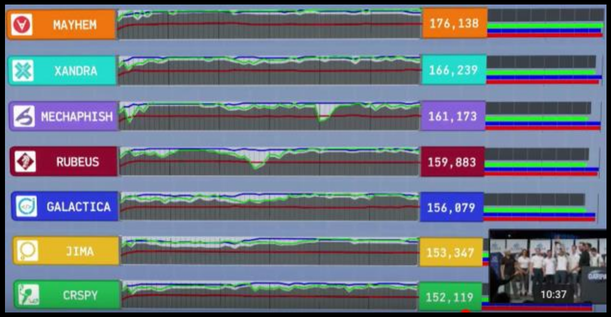
THE UNIVERSITY OF MELBOURNE

SWINBURNE UNIVERSITY OF TECHNOLOGY

Australian National University

AI for Cybersecurity

- *“The need for automated, scalable, machine-speed vulnerability detection and patching is large and growing fast as more and more systems—from household appliances to major military platforms—get connected to and become dependent upon the internet.” - DARPA CGC*



MAYHEM	176,138
XANDRA	166,239
MECHAPHISH	161,173
RUBEUS	159,883
GALACTICA	156,079
JIMA	153,347
CRSPY	152,119

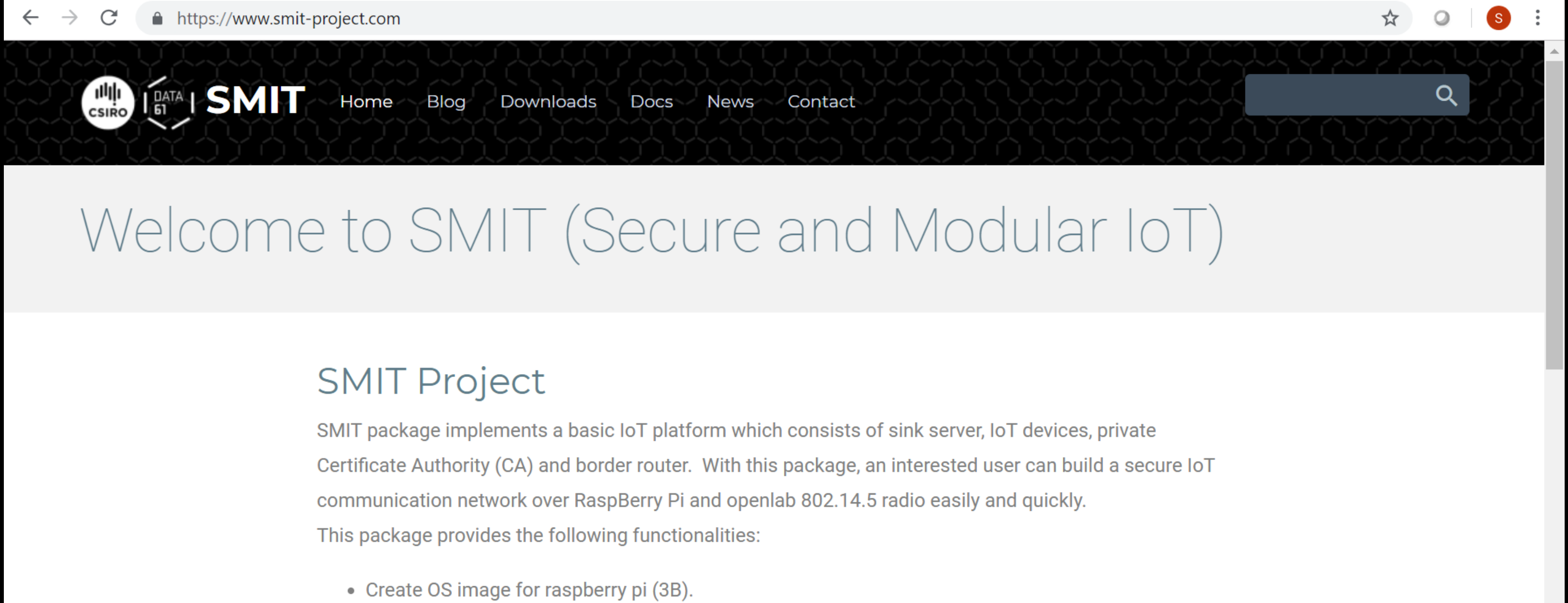
https://www.darpa.mil/program/cyber-grand-challenge

- *Australia’s AI for Cybersecurity Infrastructure*
  - *Various labs, cyber ranges, national research infrastructure..*

SCIENCE AND INDUSTRY ENDOWMENT FUND

IoT Security

Protect from the biggest security threat



https://www.smit-project.com

SMIT Home Blog Downloads Docs News Contact

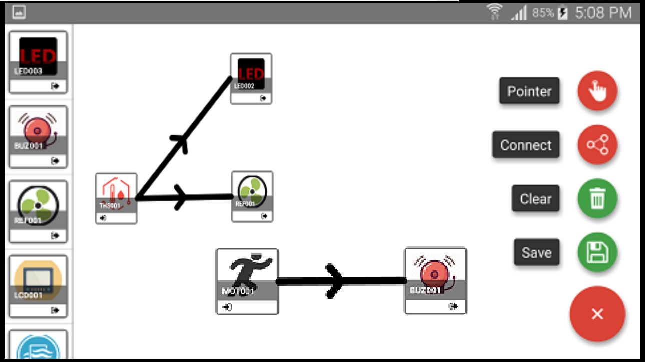
Welcome to SMIT (Secure and Modular IoT)

SMIT Project

SMIT package implements a basic IoT platform which consists of sink server, IoT devices, private Certificate Authority (CA) and border router. With this package, an interested user can build a secure IoT communication network over RaspBerry Pi and openlab 802.14.5 radio easily and quickly.

This package provides the following functionalities:

- Create OS image for raspberry pi (3B).



Secure IoT Device Mashup

DARPA
HACMS

Trustworthy Systems

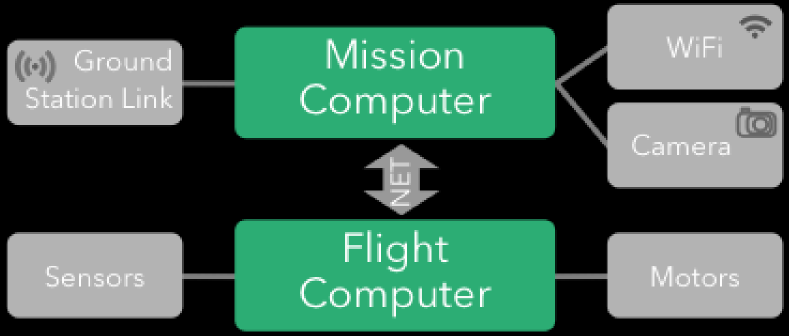
Building high-assurance cyber-physical systems

Aim
- Protecting autonomous vehicles from cyber attacks

What
- Air vehicles: quadcopter, Boeing optionally-piloted helicopter
- Ground vehicles: robot, autonomous army trucks

How
- Formalised architecture
- Synthesised code
- Verified isolation (seL4 and CAmkES)

Results
- Vehicles running high-assurance software
- Resist attacks by Red Team



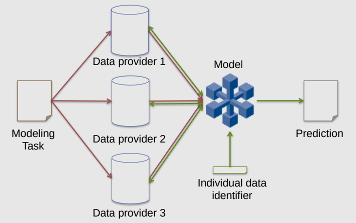
Confidential Computing

National and Enterprise Borders

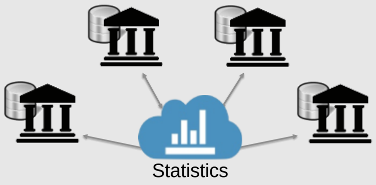
Machine learning and joint analytics over fully encrypted data

- Learn valuable insights from sensitive data from multiple organisations without putting the data together using
  - Partial Homomorphic Encryption
  - Secure Multiparty Computation:
  - Irreversible Aggregation

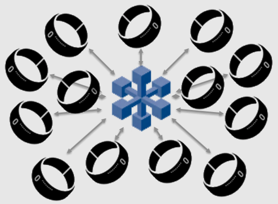
Partners: UK bank, Singapore bank, Australian government agencies



Predictive Analytics



Data aggregation



Device Analytics

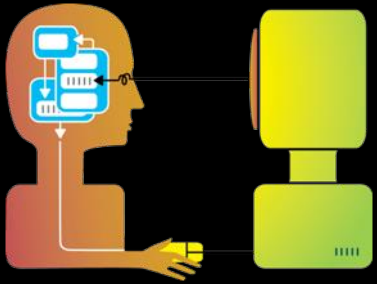
Usable Security

Develop Security protocols considering the Weakest link (Human) in the Loop

- Observations-resistant password systems
  - Password systems that are secure even if someone watches
  - Discovering computing problems that are easy for humans

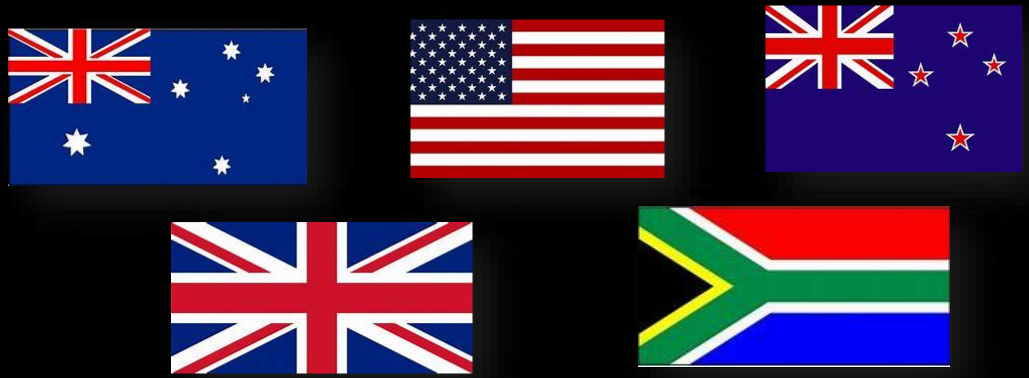
- Simulating human behavior when operating a security system

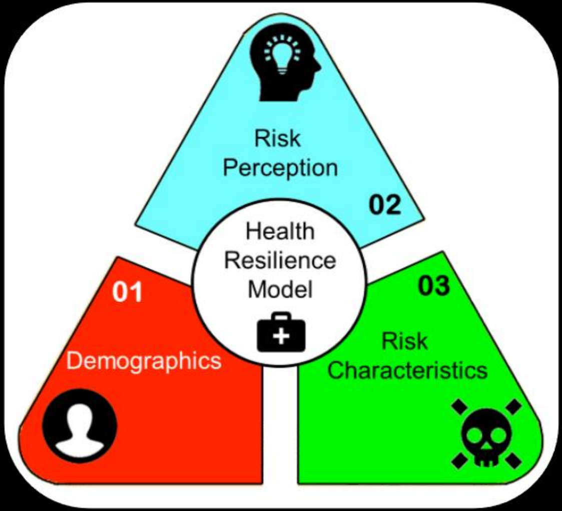
- Usable security also applicable to
  - group authorization, message integrity



Transforming online risk resilience hardening

- Develop an international online health resilience model
- Multi-national online resiliency benchmarking experiment



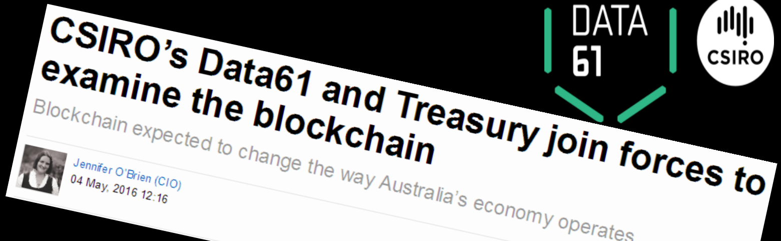


Testing people's resilience to fraudulent websites under stressor conditions

One More Thing…

Blockchain: Resilience and trustworthiness *without* a trusted third party

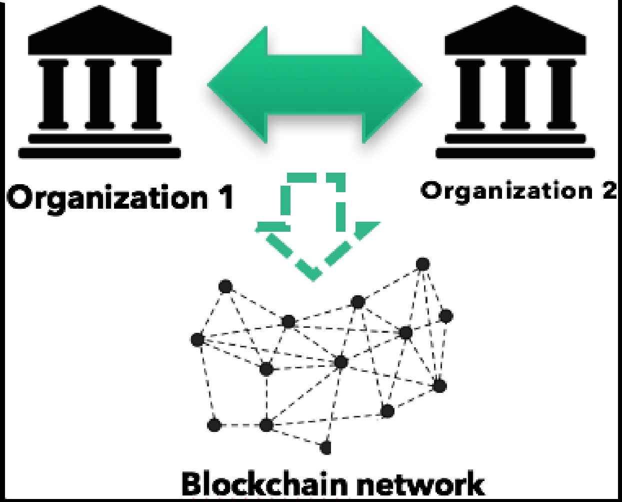
- System designs with blockchain
  - Cross-org business processes
  - Architecture tradeoffs; Standards
- Trustworthy blockchain
  - Mathematically-proven “smart contract” linked with legal contracts
  - Empirical studies
- Applications: IoT security, government registries, (food) supply chain security, cross-boarder trade facilitation and fraud detection



CSIRO’s Data61 and Treasury join forces to examine the blockchain

Blockchain expected to change the way Australia’s economy operates

Jennifer O'Brien (CIO)
04 May, 2016 12:16



ISO/TC 307

Blockchain and distributed ledger technologies

Acknowledgements

- Gareth Parker and Liming Zhu
- All keynote Speakers and Invited Speakers
- Organising Committee
  - Marthie Grobler (Data61)
  - Anton Uzunov (DSTG)
  - Brigitte Biscotto (Data61)
  - Lisa Nguyen (Data61)
  - Siqi Ma (Data61)
  - Chadni Islam (University of Adeliade/Data61)
- All other student volunteers

Thank you

Surya Nepal, Research Group Leader
Distributed Systems Security
Surya.Nepal@data61.csiro.au

www.data61.csiro.au