Security & Privacy by Design

Surya Nepal

24 October 2019

www.data61.csiro.au

PbD: Privacy by Design

Privacy by Design (PbD)

- Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian
- the future of privacy cannot be assured solely by compliance with legislation and regulatory Framework
- privacy assurance must become an organization's default mode of operation.

Privacy vs Utility

Privacy is not dead – you're just doing it wrong.

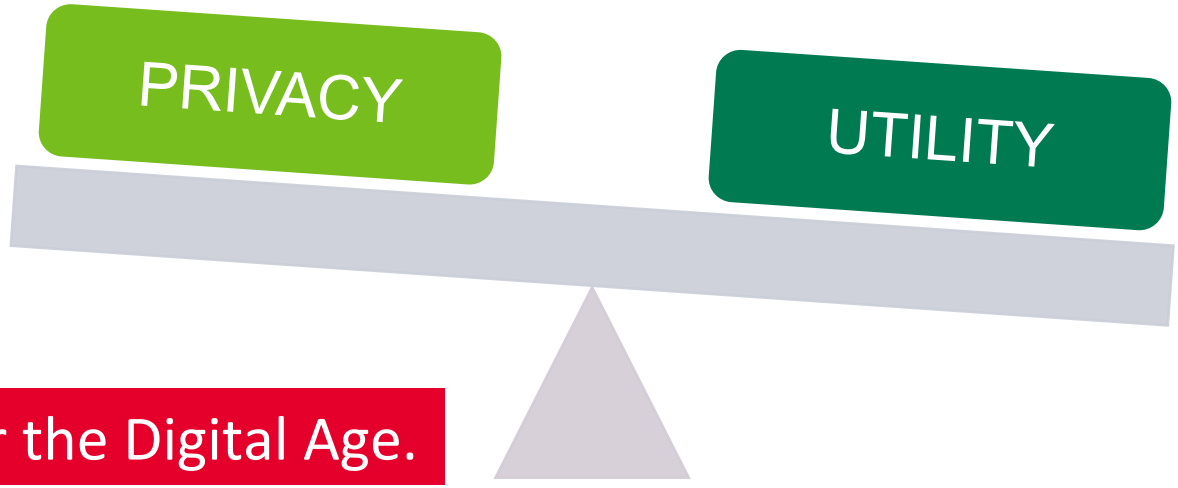
Privacy is dead — get over it.

Privacy is the price for free.

Data is the new oil.

General Data Protection Regulation (GDPR).

Data Science.



Digital Rights - Human Rights for the Digital Age.

Five Safes


Safe Projects
Is this use of the data appropriate?
Safe People
Can the researchers be trusted to use it in an appropriate manner?
Safe Data
Is there a disclosure risk in the data itself?
Safe Settings
Does the access facility limit unauthorised use?
Safe Outputs
Are the statistical results non-disclosive?

SbD: Security by Design

Open Web Application Security Project SbD principles

- Minimize attack surface area
- Establish secure defaults
- Principle of Least privilege
- Principle of Defence in depth
- Fail securely
- Don’t trust services
- Separation of duties
- Avoid security by obscurity
- Keep security simple
- Fix security issues correctly

Microsoft’s Secure Development Lifecycle (SDL)

- Define Security Requirements
- Define Metrics and Compliance Reporting
- Perform Threat Modeling
- Establish Design Requirements
- Define and Use Cryptography Standards
- Manage the Security Risk of Using Third-Party Components
- Use Approved Tools
- Perform Static Analysis Security Testing (SAST)
- Perform Dynamic Analysis Security Testing (DAST)
- Perform Penetration Testing
- Establish a Standard Incident Response Process

Security vs Usability

Humans are the weakest link in the information security chain.

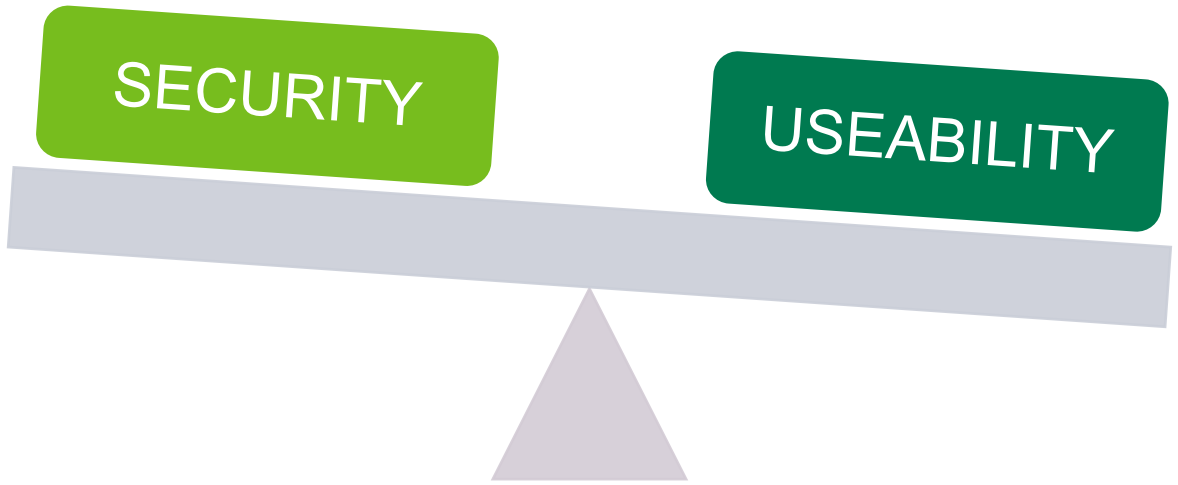
Developers are the Enemy.

Encryption is not the enemy.

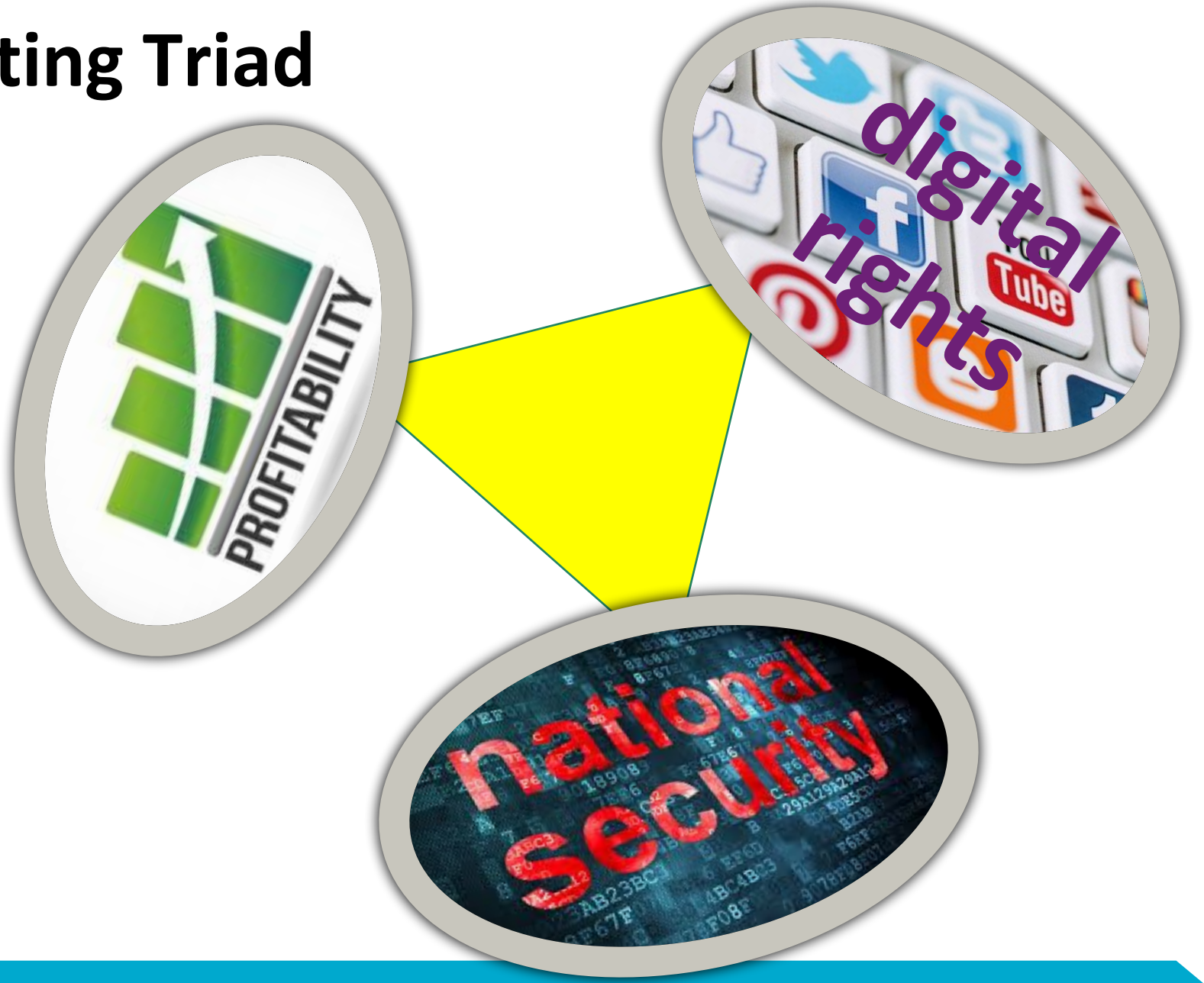
Human-Centric Security

Usable Security

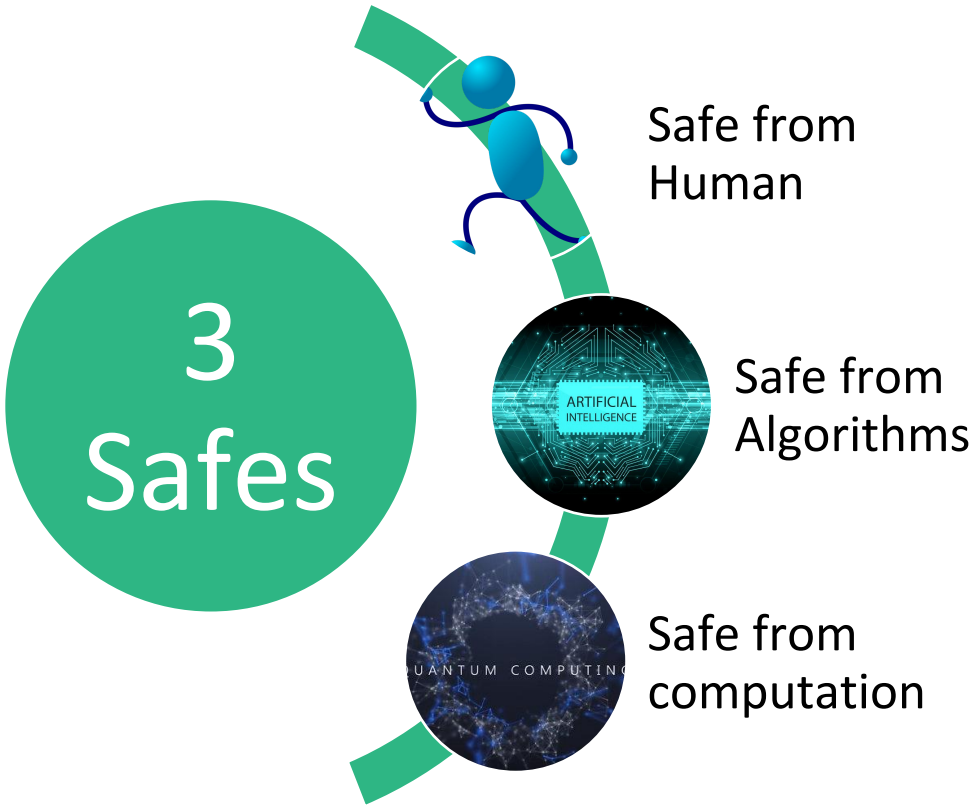
Usable Authentication

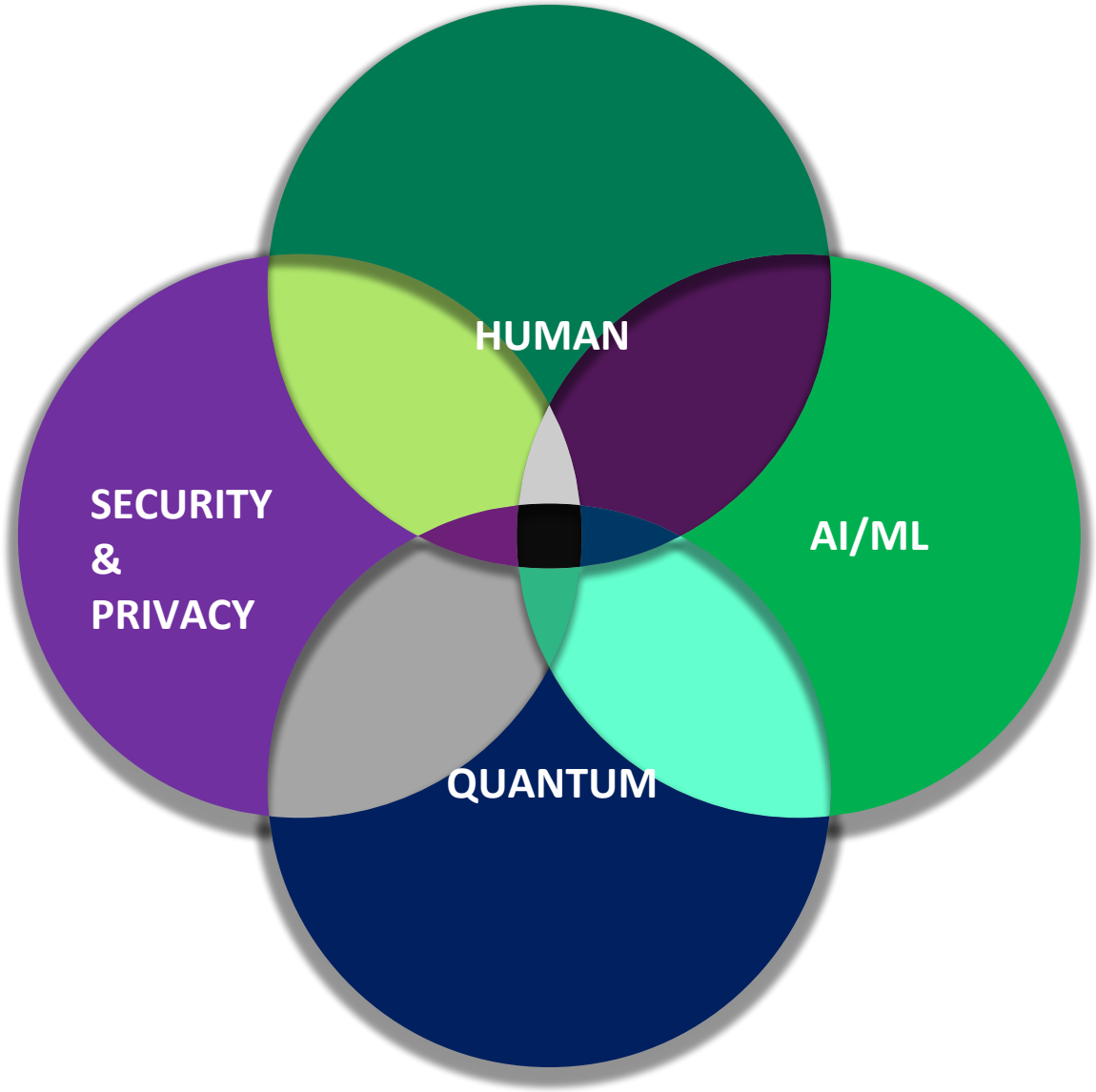


Conflicting Triad

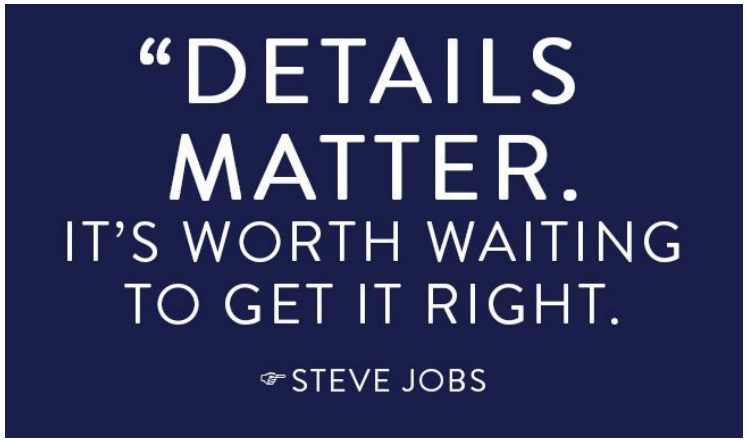


Ephemerality

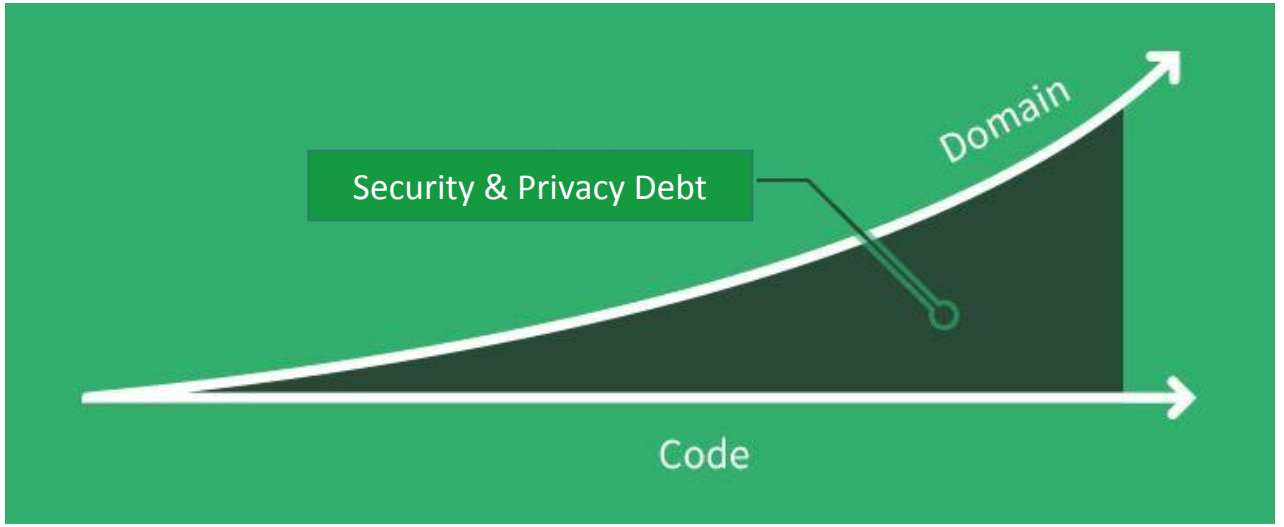




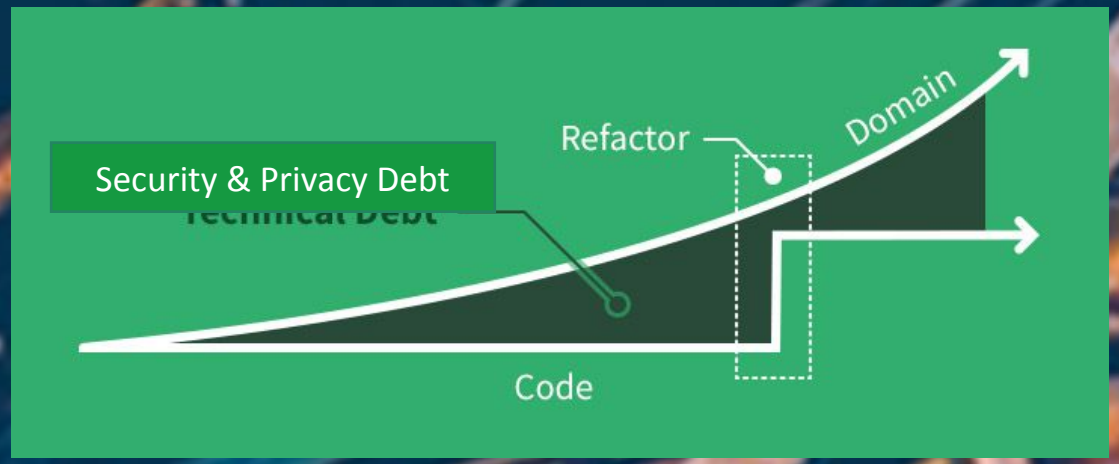
S&P Drift

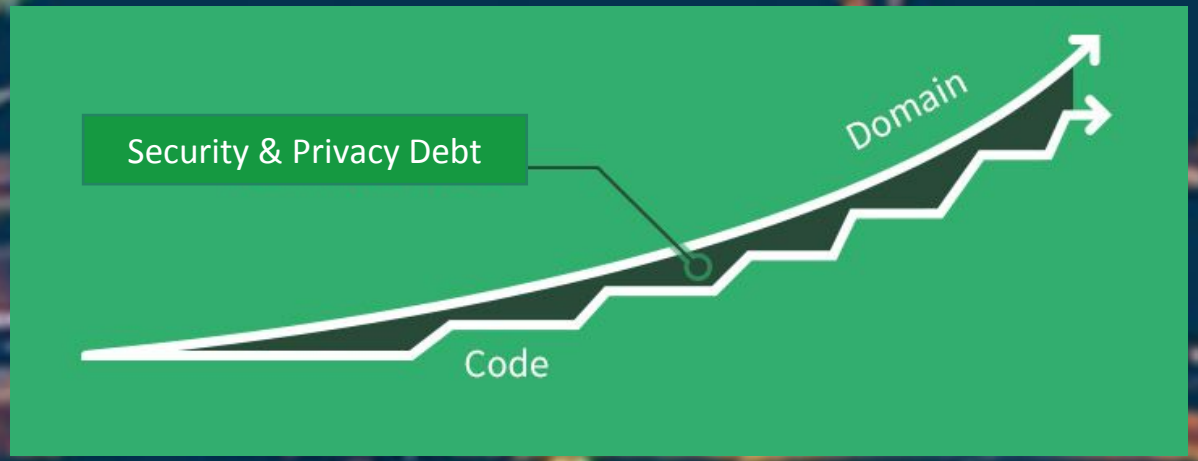

“DETAILS
MATTER.
IT’S WORTH WAITING
TO GET IT RIGHT.
STEVE JOBS

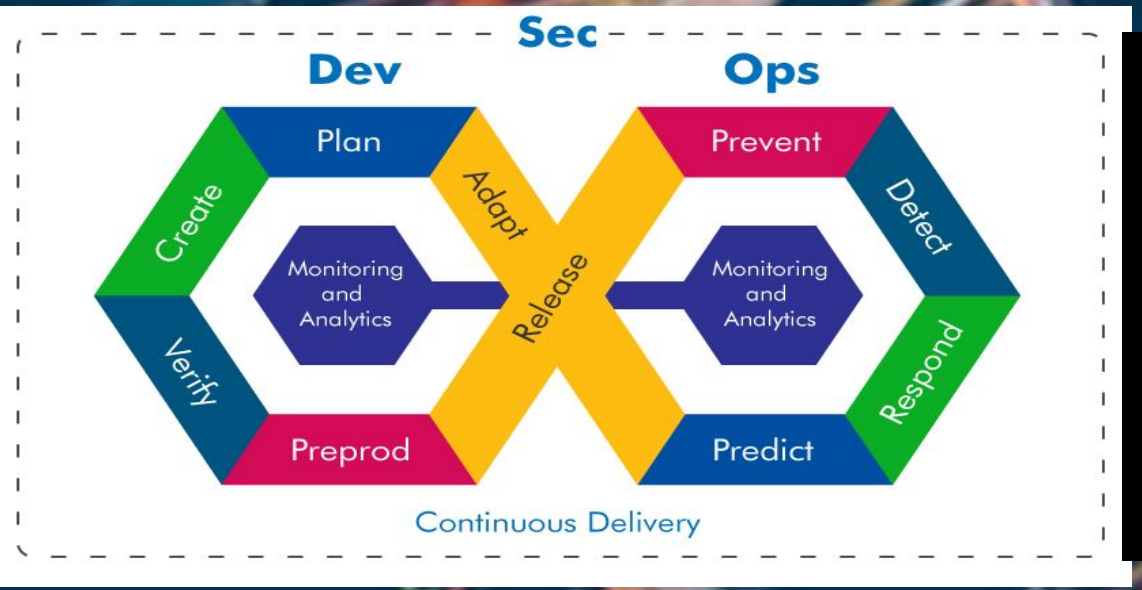

If you wait for the
perfect
conditions,
you'll never get
anything done.

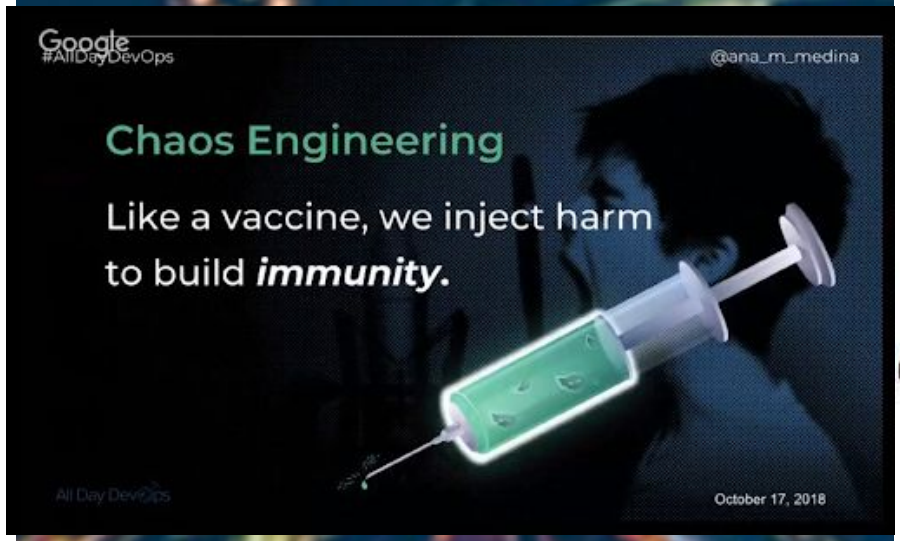

Security & Privacy Debt
Domain
Code

Iterative S&P Design









THANK YOU

Data61
Surya Nepal
Group Leader, Distributed Systems Security

t +61 2 9123 4567
e firstname.surname@data61.csiro.au
w www.data61.csiro.au/lorem