DEEPSEC

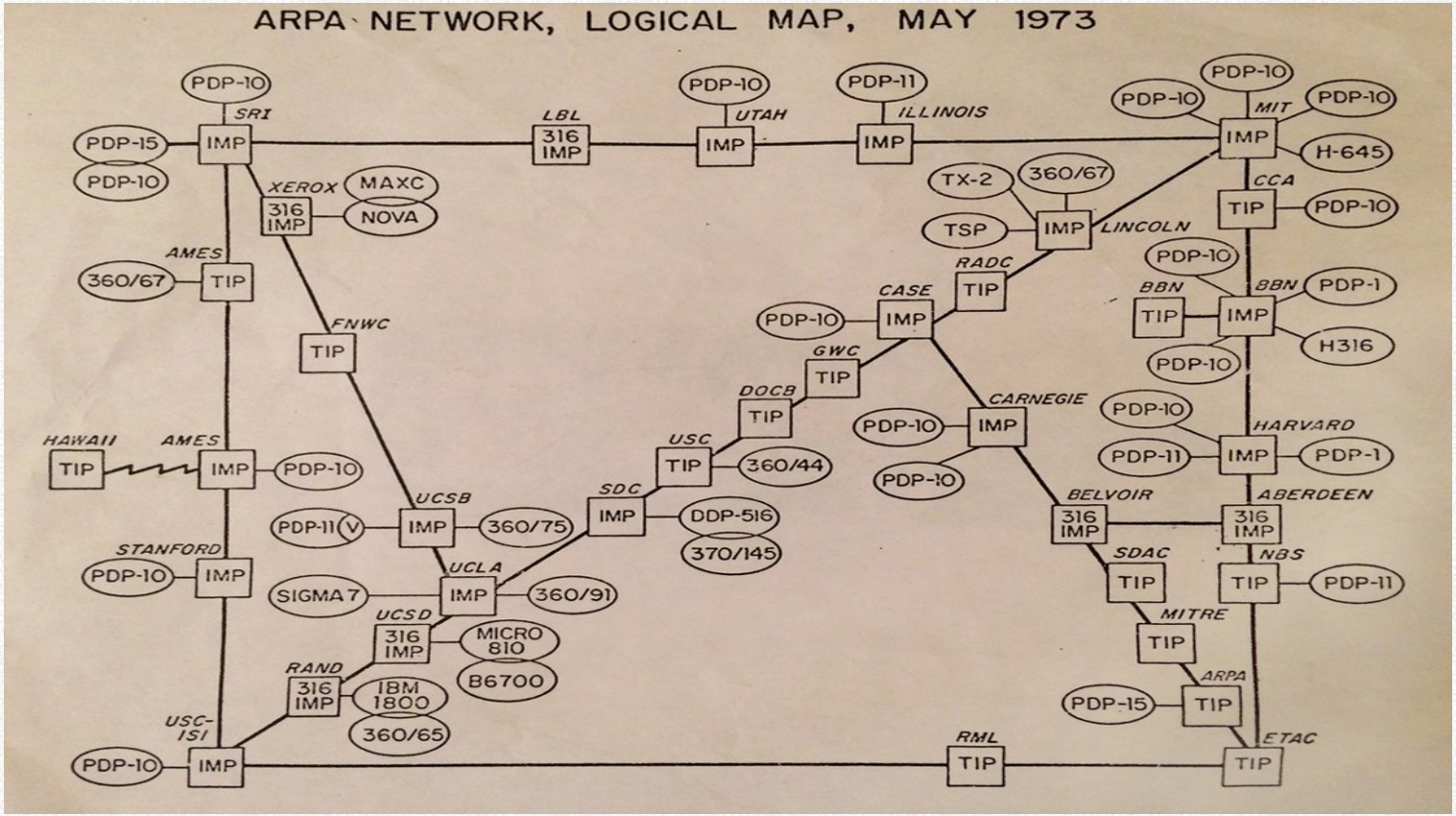
DevSecBioLawOps and the current State of Information Security

René 'Lynx' Pfeiffer,

DeepSec In-Depth Security Conference 2020

Background

First a bit of History



History continued

- 1960s : Organisation use passwords
- 1970s : Worm/virus PoC, CREEPER & Reaper
- 1980s : War dialling & war games, Morris worm, CERT founded
- 1990s : Firewalls to the rescue!
- 2000s : Governments catch up!
- 2010s : Data leaks on the scale of nuclear disasters
- 2020s : Invention of using the prefix *Dev* to solve every problem
- 2021+ : ?

- Computer Science
- Telecommunications
- Mathematics
- Physics
- Chemistry
- Engineering
- Psychology
- Law
- Linguistics
- Sociology
- Economics
- Logistics
- Administration
- Accounting
- …

- How to get started with information security?
  - Spoiler: Nowadays you can start anywhere.
- How to acquire the necessary skills in one lifetime?
  - Companies looks for experts in their mid-20s with decades of experience.
  - Constant degradation of education programmes.
- How to stay up-to-date?
  - `git pull` not feasible for human brain.
  - Trends and buzzwords cloud important knowledge.

Silo Mentality

Silos rule the World

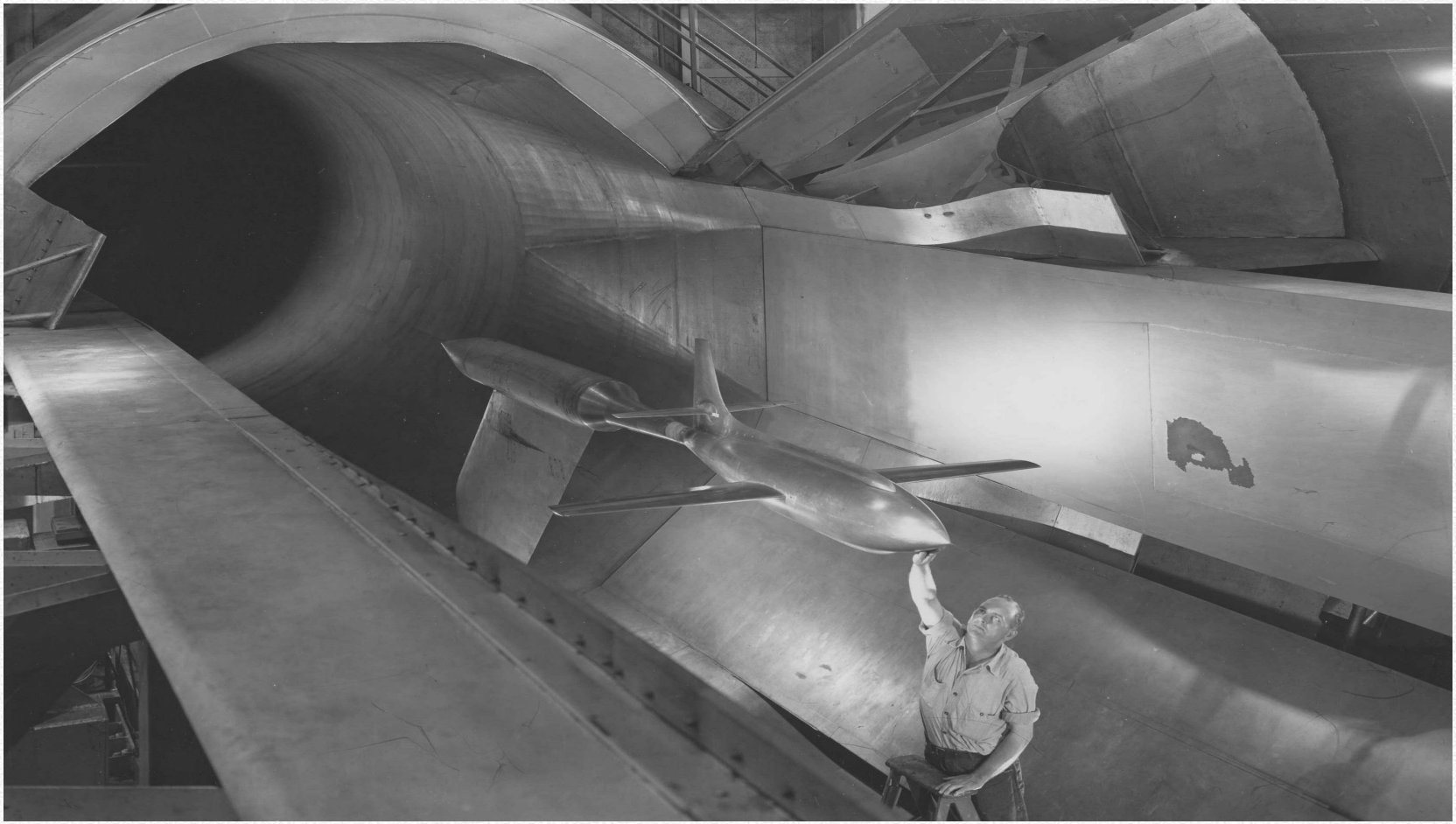
- Information technology requires specialisation
  - Background knowledge is mandatory
  - Toolchains (programming languages, frameworks, …)
- No new phenomenon
  - Gottfried Wilhelm Leibniz († 1716) probably last universal expert
  - Specialisation is best practice in other fields
- Accelerated by pace of technology
  - Moore's Law
  - 13 HDMI specs, 11+ generations of CPUs, millions of apps, …

Adding Mindsets

- Silos create or solve problems depending on mindset
  - Requires respect of other experts
  - Communication and common language mandatory
- Information technology is often different
  - My silo is better than yours!
  - Your silo blocks progress in my silo!
  - My silo is most important for the project!

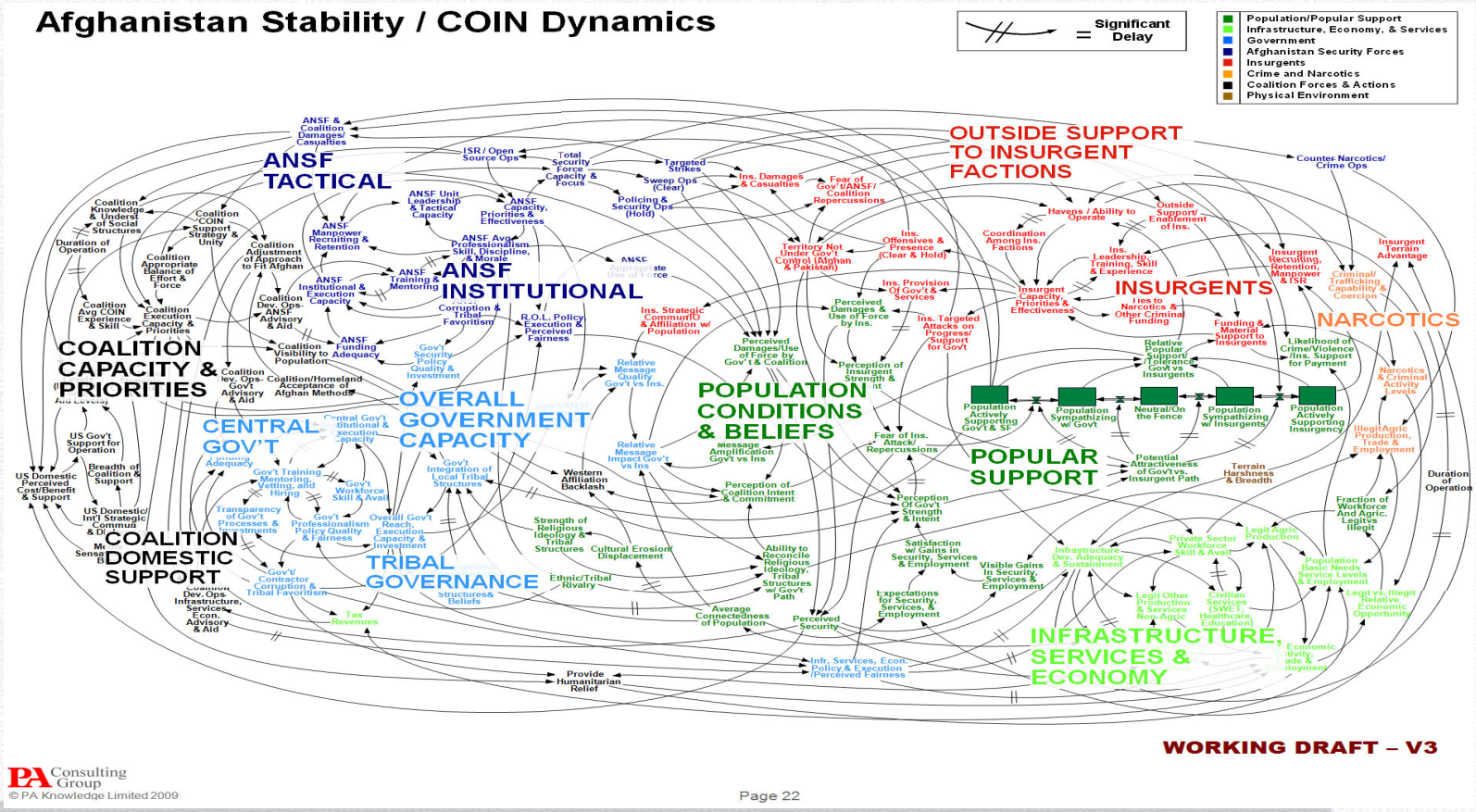
Example: Serverless Computing

- Serverless is a “new” “technology” for development/production
  - Serverless has servers
  - Serverless means “I don’t care about the platform”
  - Serverless means “let somebody else worry about the details”
- Valid approach for certain scenarios
- Adding silo mindsets
  - Serverless = administrator-less
  - Vendor lock-in
  - The *S* in computing is for security.



We live in complex Worlds

DEEPSEC



- Creating words beginning with *Dev* does not solve anything
- Teams will always have to cover a spectrum of knowledge
  - Make sure team members can communicate
  - Make sure everyone respects each other
  - Keep overhead and administration as low as possible
- Accommodate for *sensible* knowledge transfer
  - Transferring decades of experience is impossible
  - Use didactic methods

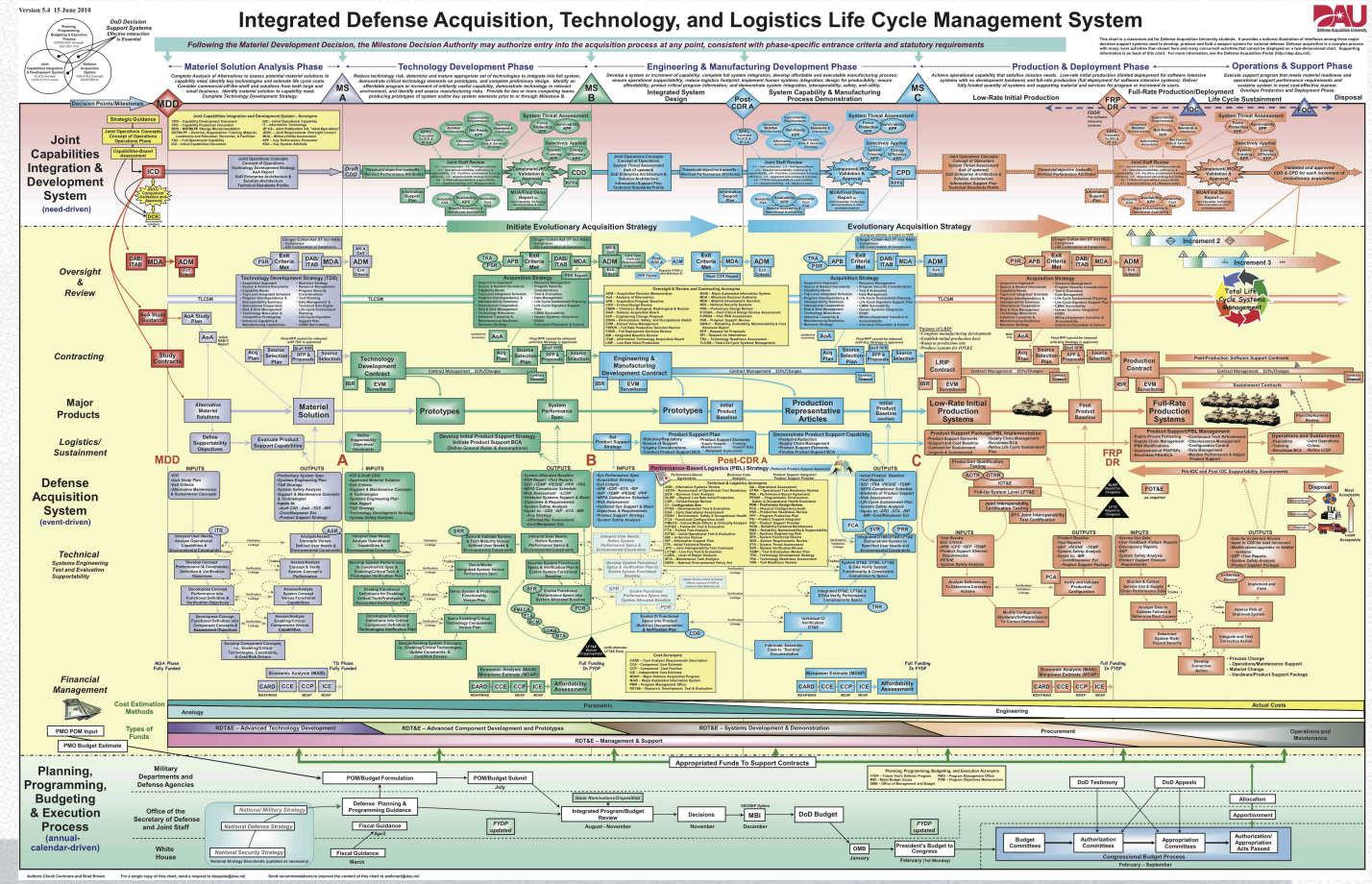
Leave Room for Criticism

- One Method to bind Them All
  - Doesn't exist.
  - Apollo 11 didn't use Scrum or Agile
- Use what works best for your team
  - Personalities dictate how your team operates
  - Be able to address and implement change

Rediscover the Lost World of Facts

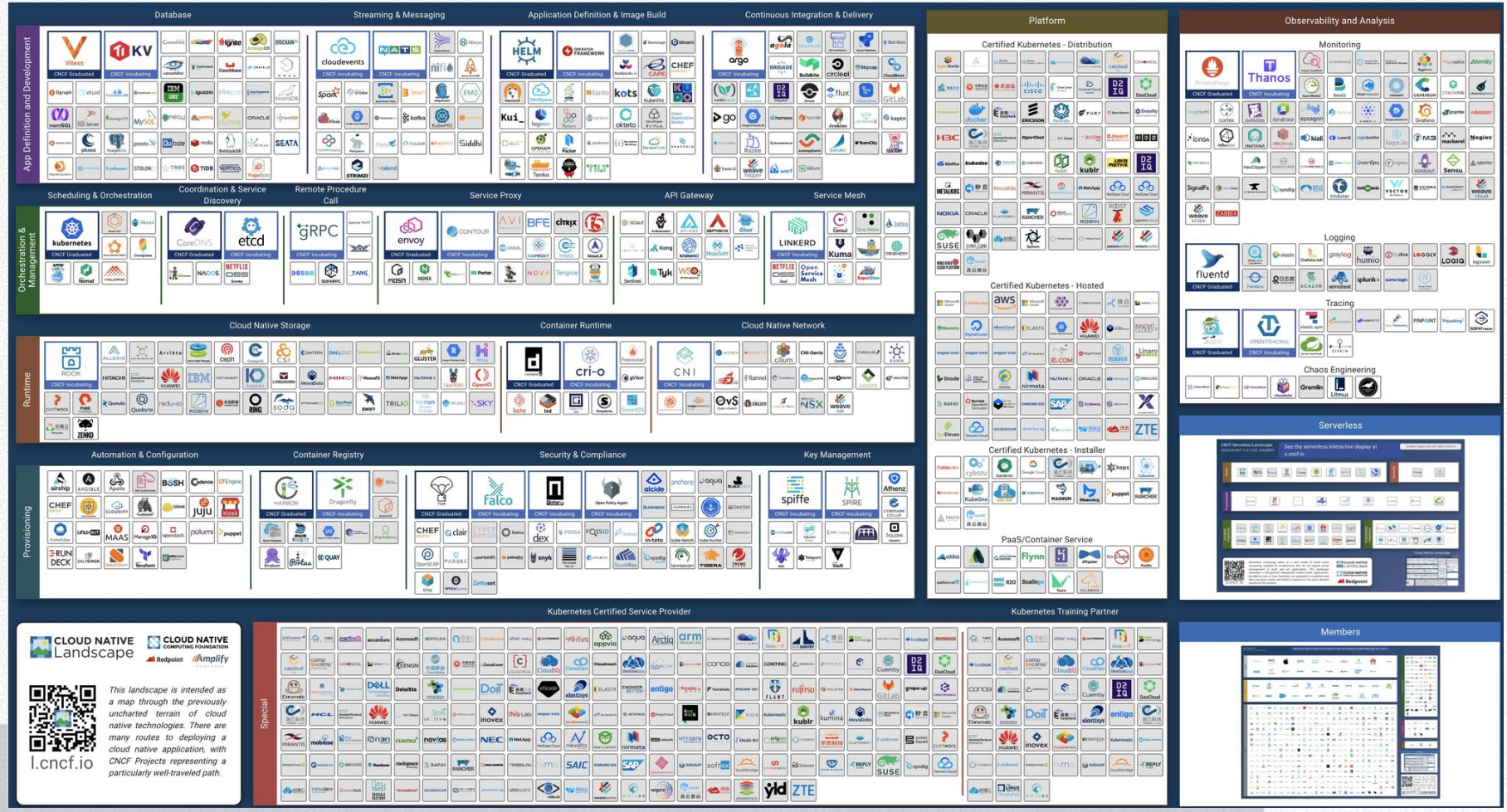
- Information security leans on evidence
- Good metrics are few and far between
  - Few “experts” can read numbers or deal with mathematics
  - 95% of all visualisations give the remaining 5% a bad reputation
- Create processes for fact-finding
  - Question all your tools and frameworks
  - Question all your vendors
  - Eliminate assumptions as completely as possible

Why all of the Suggestions won't work (I) DEEPSEC



Why all of the Suggestions won't work (II)

DEEPSEC



Any questions?

René was born in the year of Atari's founding and the release of the game Pong. Since his early youth he started taking things apart to see how they work. He couldn't even pass construction sites without looking for electrical wires that might seem interesting. The interest in computing began when his grandfather bought him a 4-bit microcontroller with 256 byte RAM and a 4096 byte operating system, forcing him to learn assembler before any other language. After finishing school he went to university in order to study physics. He then collected experiences with a C64, a C128, two Amigas, DEC's Ultrix, OpenVMS and finally GNU/Linux on a PC in 1997 (let's leave out the wonderful world of Windows 3.11/95/NT4). He is using Linux since this day and still likes to take things apart und put them together again. Freedom of tinkering brought him close to the Free Software movement, where he puts some effort into the right to understand how things work – which he still does.

René is currently occupied with system administration (old school, I know), teaching at the University of Applied Sciences Technikum Wien and Burgenland, conducting secure coding/design trainings, security/penetration/compliance testing, and writing lecture notes.

About DeepSec

DEEPSEC

The DeepSec In-Depth Security Conference (IDSC) is an annual European two-day in-depth conference on computer, network, information, and application security. DeepSec aims to bring together the leading security experts from all over the world. DeepSec IDSC is a non-product, non-vendor-biased conference event. Prior to the conference there are two-day trainings held by experts in their respective field.

The intended target audience is : Security Officers, Security Professionals and Product Vendors, IT Decision Makers, Policy Makers, Security-/Network-/Firewall-Admins, Hackers and Software Developers.

Contact Information

DEEPSEC

- DeepSec web site https://deepsec.net/
- DeepSec blog https://blog.deepsec.net/
- Contact information https://deepsec.net/contact.html
- We prefer end-to-end encrypted (E2EE) communication such as:
  - Gnu Privacy Guard (GPG)
  - Signal messenger
  - Threema messenger
  - GSMK CryptoPhone

Sources

- Ensor, Phil (Spring 1988). "The Functional Silo Syndrome" (PDF).
- Article "Pentagon's Craziest PowerPoint Slide Revealed", Wired magazine, 13 September 2010.
- Article "Hey New York Times: a causal loop diagram is not a PowerPoint fail", blog of David Liu, 17 July 2013.
- Missile silo (for ICBMs), Vandenberg AFB, CA, USA. Picture from the U.S. National Archives.
- Article "Breaking the Sound Barrier - Fast As You Can", nasa.gov, 16 February 2017.
- Twitter account @SimpsonsOps.