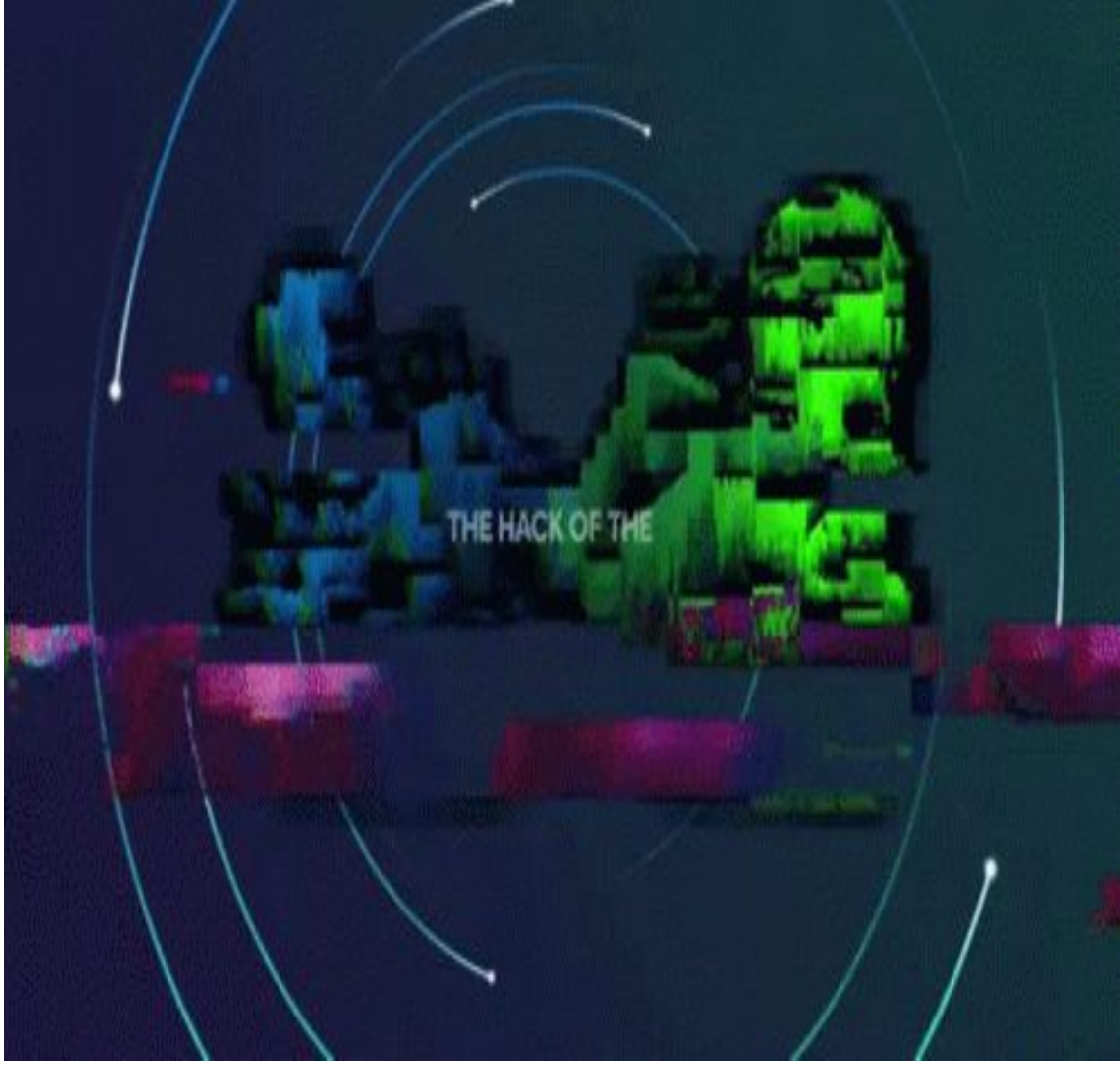
Simplify cyber security

Better and simpler!

T-DOSE 2025
By Maikel Mardjan
June 1 2025

NO|Complexity

About this talk



> Whoami

Maikel Mardjan:

- Architecture & Design of complex IT systems.
- 29+ years of work experience in the IT Industry.
- Master degree (MSc) Electrical Engineering, of Delft University of Technology.
- Master (MSc) Business Studies of University of Groningen.
- Master Business Management (MBM) – TSM Business School

I still love to do hands-on programming to learn, make and break things. I love solving complex IT challenges to make people happier!

THE Open GROUP
TOGAF™ 9 Certified

CISSP® Certified Information Systems Security Professional

TU Delft Delft University of Technology

university of groningen

tsm business school

OWASP Open Web Application Security Project

Cyber security breaches have a severe impact on our daily activities.

- ➔ 2019 Capital One data breach (Large US Bank): largest data breaches impacting personal information of over a 100 million individuals.
- ➔ December 2020: Ransomware on the dutch municipality ‘Hof van Twente.’ Very advanced attack (at least for people not familiar with IT in general), since the very strong password used was very hard to determine ‘Welkom2020’
- ➔ 2023: The Dutch police reported 147 organisations in the Netherlands fell victim to ransomware attacks.
- ➔ 2024 / 2025: More IT outages, more breaches and more nasty disasters!

Major incidents are caused by tools that should save us!

CrowdStrike disaster: July 2024

➔ The largest outage in the history of information technology and "historic in scale".

The American cybersecurity company CrowdStrike distributed a faulty update to its Falcon Sensor security software that caused widespread problems with Microsoft Windows computers running the software. Roughly 8.5 million systems crashed and were unable to properly restart.

(https://en.wikipedia.org/wiki/2024_CrowdStrike-related_IT_outages)

Facts?

- ➔ Only a fraction of security incidents are publicly reported and known.
- ➔ Decent software testing and BCDR is often lacking. Testing simple ‘happy paths’ is often already complicated enough and takes lots of resources (time and money).
- ➔ We have ~~a blind~~ trust in expensive cyber software solutions that lack transparency.
- ➔ Non disclosure agreements prevent transparency and learning from mistakes.
- ➔ Using expensive security software, highly paid skilled resources and very expensive IT security companies does not prevent major incidents.
- ➔ We have culture of hiding incidents from the public eye.
- ➔ We have no choice for using leaky governmental systems, banking, shopping and more.

We are doomed to use proprietary systems that will be hacked….

Why is good cyber security still so hard to accomplish?

We are trained and brainwashed by commercial vendors to advocate for complex, expensive cyber security solutions that are costly to implement and lack transparency.

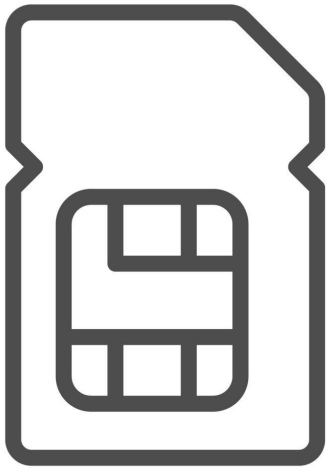
We need simpler solutions, we need to use solutions that are transparent and we can trust.

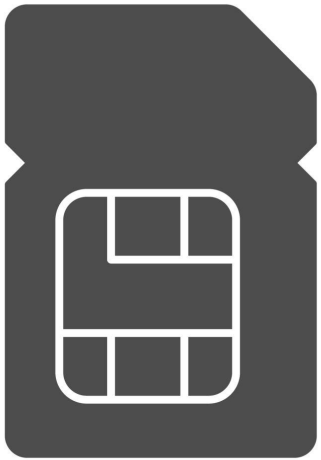
Reducing *complexity* means greater transparency so reduced business risks!

Complex IT and Simple IT: A definition

An unified definition of what ‘Complex IT’ is does not exist.

Complexity is not ‘soft’. It is tangible and measurable!





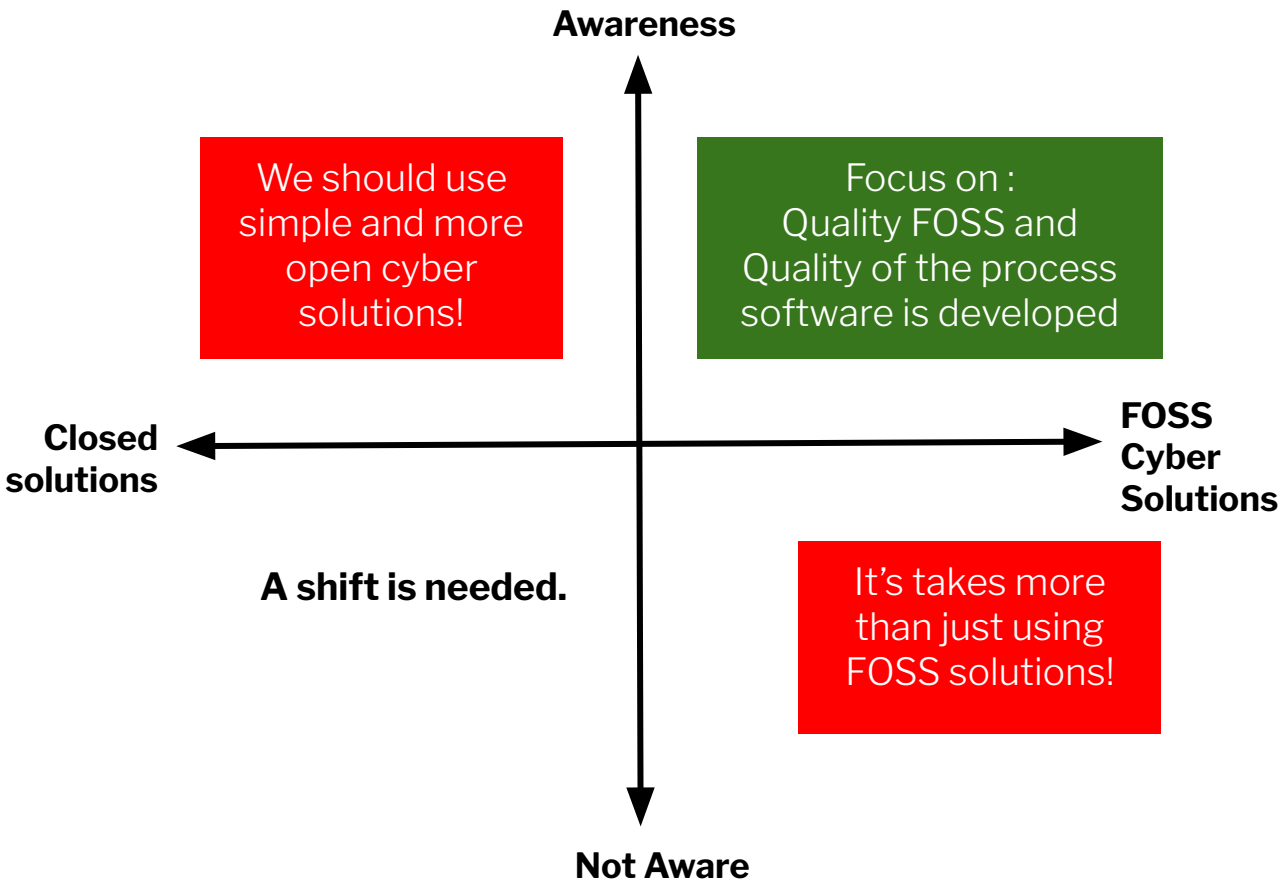
SO why…

- ➔ Why do we embrace every new IT hype as the holy grail for solving our cyber security problems?
- ➔ Why do we not aim to build more on open solutions that are simple to use and to adjust?
- ➔ Why do we not get the basics rights? Risks will always remain, but…knowing and understanding your thread model is a start!

How to transform? - Two shifts are needed

1. From complex to simple

2. From Closed to open solutions

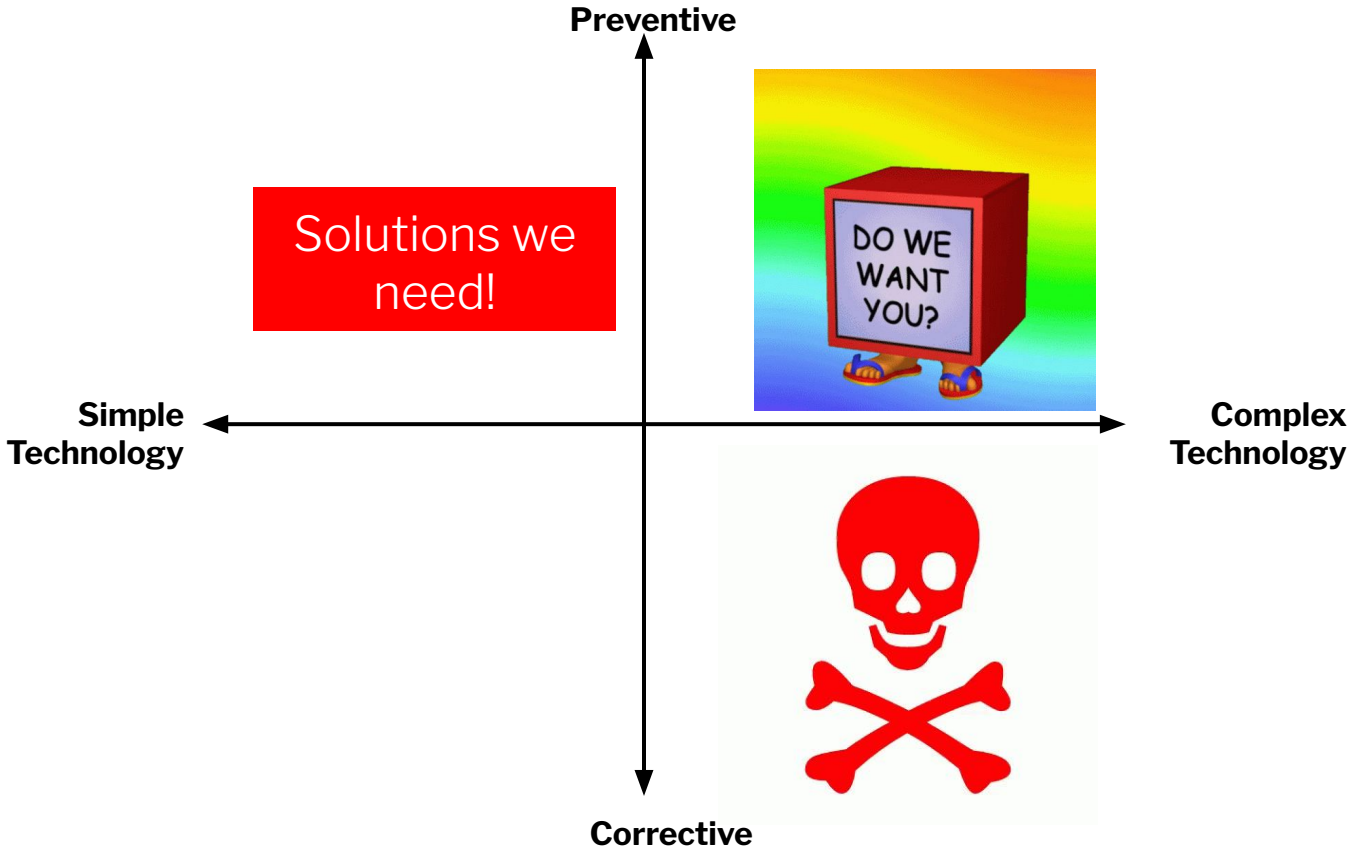


Software quality is not black or white

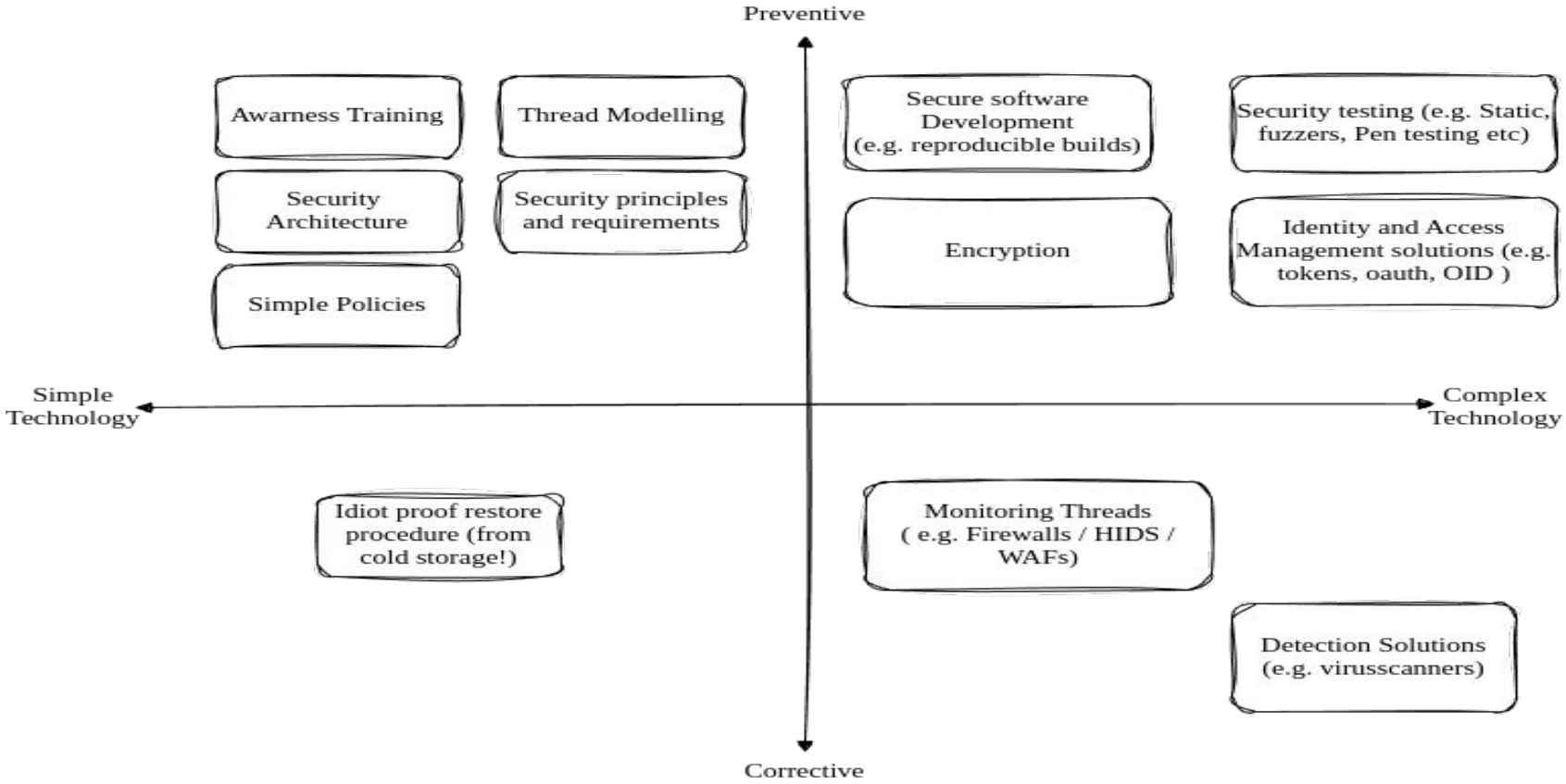
But for security software consider minimal:

- ➔ OpenSSF Best Practices Badge Program (e.g. https://www.bestpractices.dev/en/projects/54#analysis)
- ➔ OpenSSF Scorecard (e.g. https://securityscorecards.dev/viewer/?uri=github.com/borgbackup/borg)
- ➔ Reproducible Builds (https://reproducible-builds.org/)

Simple or Complex?



Simple or Complex?

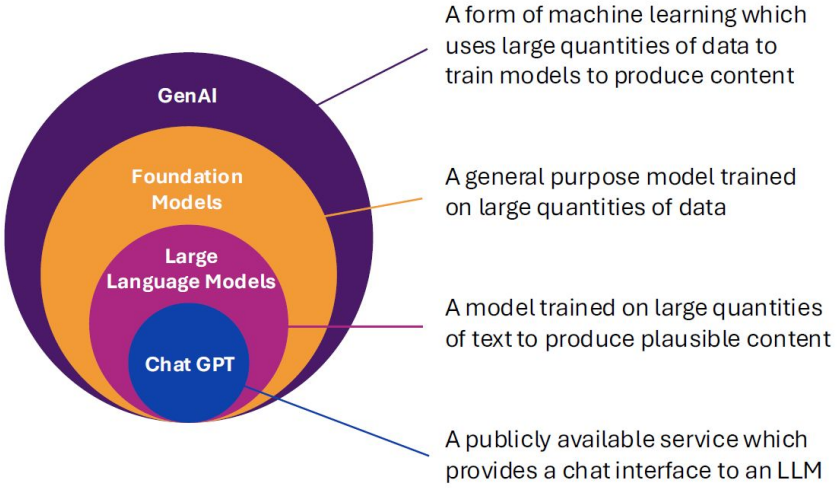


AI can and will help! (A bit)

Adapt AI and use the benefits to make FOSS cyber solutions simpler and better!

AI and LLMs can and will simplify some cyber security challenges:

- Assists with creating better FOSS security tools. Especially creating nicer UIs. LLMs can speed up the process of creating more user friendly UIs so that security tool usage will become simpler.
- Assist with creating better test suites for software. Writing tests for code makes software often more robust and increases quality. Manual writing test for security aspects is time consuming and boring work.



AI to the rescue?

Many hyped AI security products overpromise and do not work:

- LLMs are trained on yesterday's attack patterns and solutions , not on today's challenges.
- Most threat models and security architectures are not published as open access on the internet.
- Security is not a product, but a process. A security product can never replace the human factor. The human factor within cyber defense is crucial.
- Risk assessments can not be outsourced to an AI-agent or tool. Risk assessments are context specific and involve humans, processes, business systems and more.
- Most AI solutions require unhealthy network requirements. Aka It only requires our private trusted VPN tunnel...

Yes we can! Join the project.

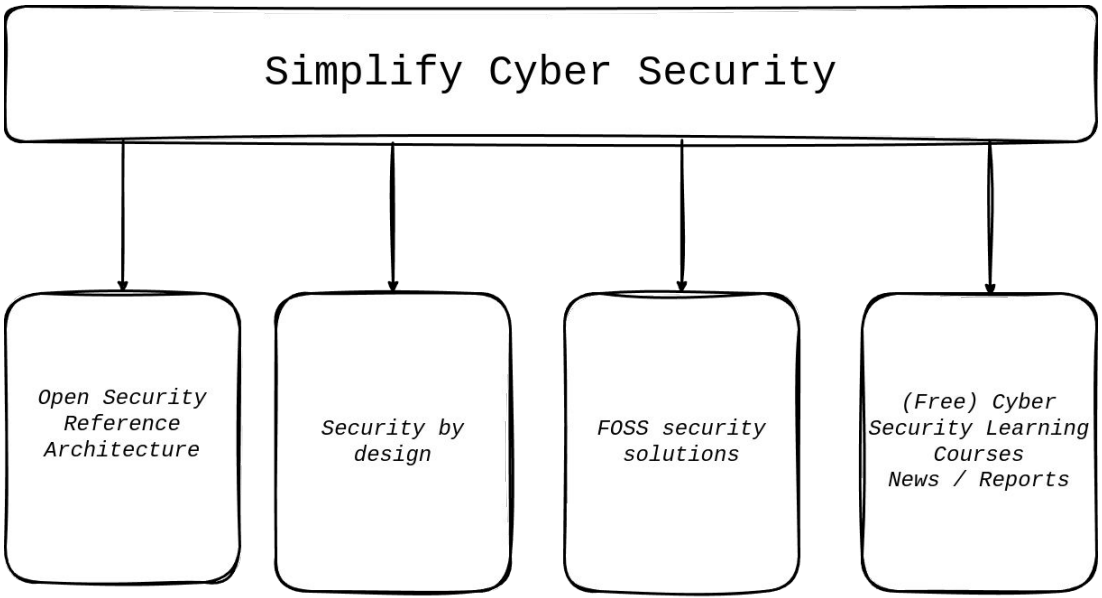
You don’t have to be a security expert to contribute, every contribution is welcome!

Check the Github repository: https://nocomplexity.com/documents/simplifysecurity/intro.html

Share your knowledge to be used and reused:

- Blueprints for simple cyber solutions
- FOSS Solutions building blocks

And more!



Summary

- ➔ You are the problem
- ➔ We did not improve cyber security solutions the last 25 years, so stop putting energy in it.
- ➔ Good Open cyber solutions are possible, but a key problem is how money is earned within the commercial cyber security industry.
- ➔ The problem with today's broken IT environments is not technical. Advocate by your local government for public money means open solutions. So we all benefit! Check https://publiccode.eu/en/
- ➔ You are the solution!

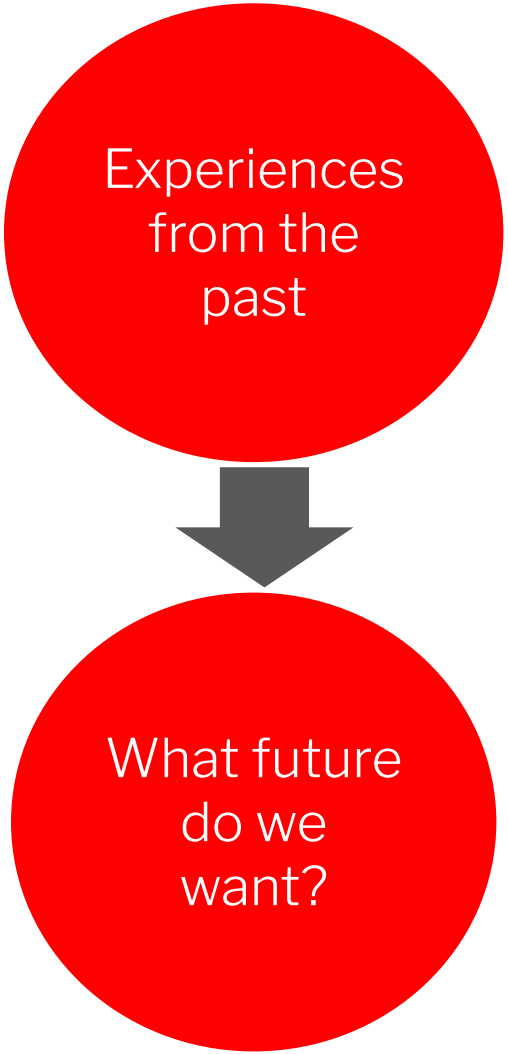
Questions and discussion

Thank you!

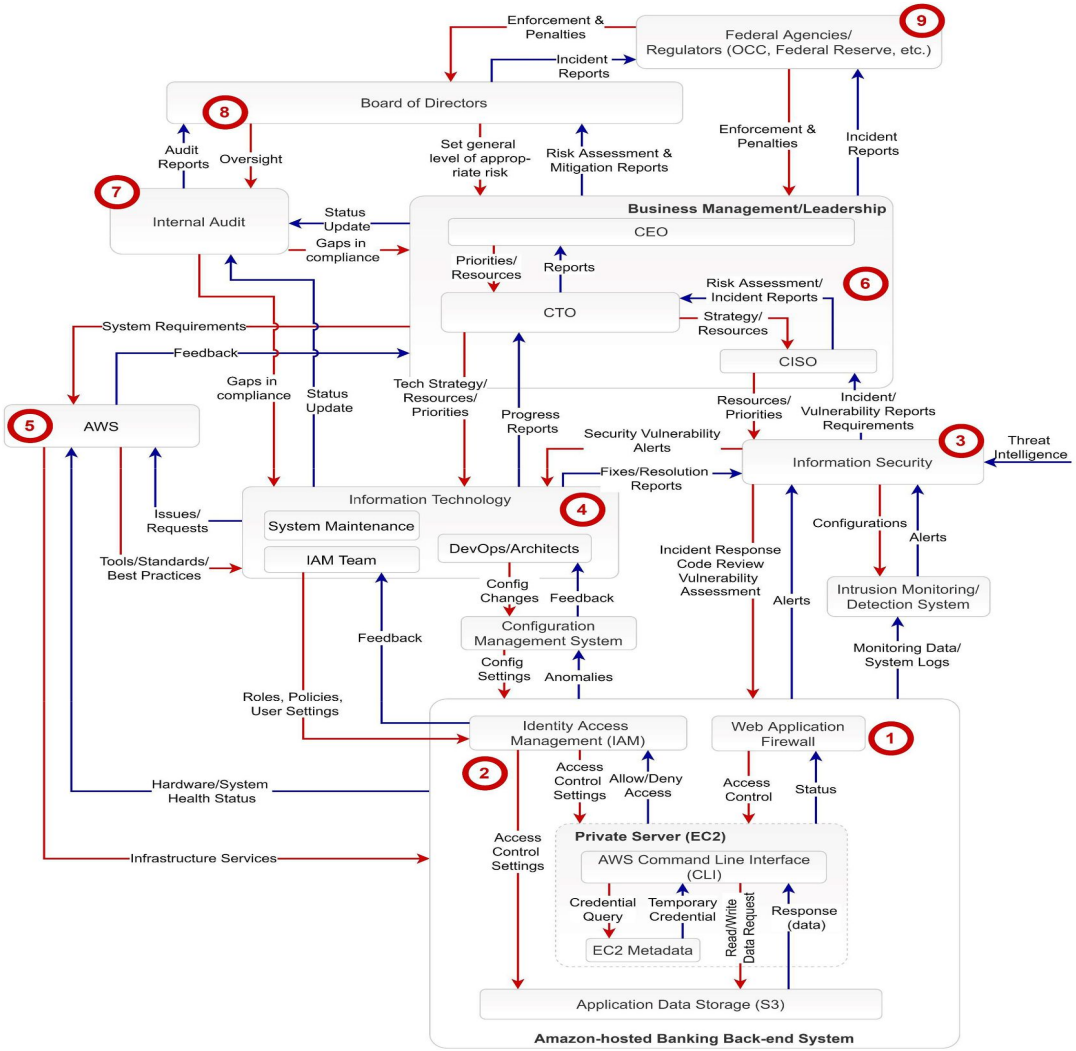
Continue the discussion online by joining the growing community and help by creating more quality open solutions that do work.

Slides **are** published online: Check Simplifysecurity.nocomplexity.com

Appendix
Backup Slides



More budget and more expensive cyber technology does not help to mitigate cyber security risks.



Example: From the 2019 Capital One data breach:

Capital One functional control structure; nine key controls are noted—all of them failed.

Yes they used AWS hosted back-end systems.

(https://dl.acm.org/doi/pdf/10.1145/3546068)

“Simplicity is a great virtue but it requires hard work to achieve it and education to appreciate it. And to make matters worse: complexity sells better”

— Edsger Dijkstra

- 2023: The Dutch police reported 147 organisations in the Netherlands fell victim to ransomware attacks.

  February 2021: The German Chaos Computer Club has reported more than fifty data leaks. Government institutions and companies from various business sectors were affected. Researchers had access to over 6.4 million personal data records.

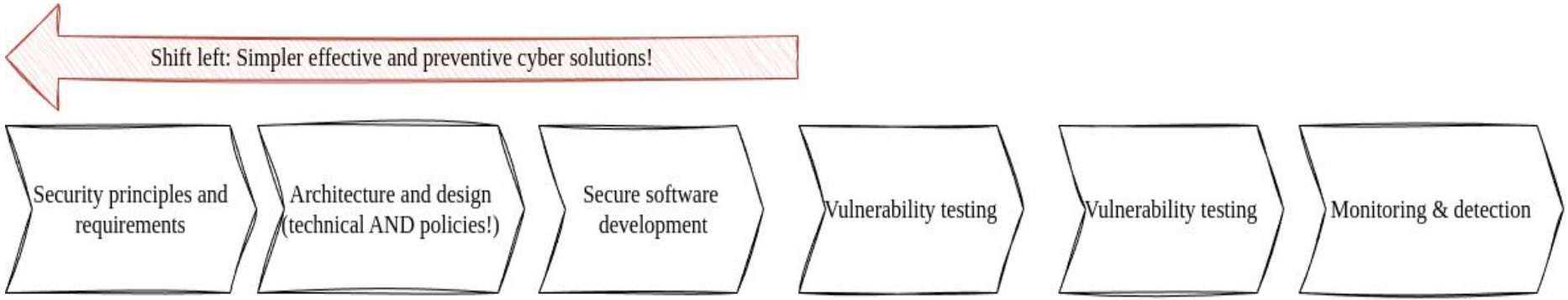
- June 2021:More than 1 billion people's personal records stolen from the Shanghai National Police

  Database.

- 2021 Microsoft Exchange Server data breach: 250,000 servers fell victim to the attacks, including servers belonging to around 30,000 organizations in the United States, 7,000 servers in the United Kingdom as well as the European Banking Authority and other institutions.

(https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach)

Shift Left



- ➔ We need a shift to simpler thinking about cyber security defense measurements.
- ➔ This means more emphasis on what works from a preventive perspective.
- ➔ Preventive security measurements are often less technical

Aiming for complex, complicated or simple?

➔ The way we build and ship software these days is mostly ridiculous, leading to apps using millions of lines of code to open a garage door, and other simple programs importing 1,600 external code libraries—dependencies—of unknown provenance.

Think complex CICD pipelines, github-actions, many dependencies(!), Exploding SBOMs , orchestration over containers and virtualized networks using COSTS software that is vulnerable by design.

We know the current situation is untenable.