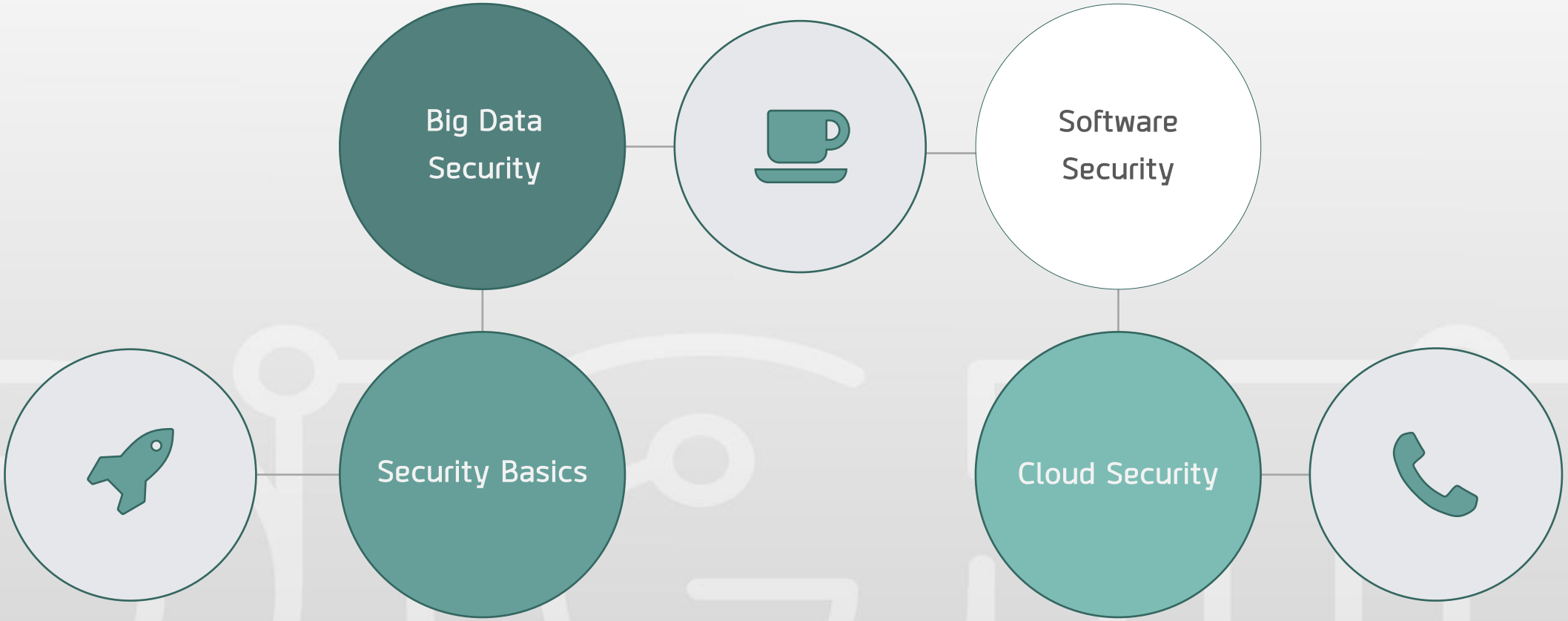
Data Science and Security

Sirapat Boonkrong

sirapat@g.sut.ac.th

Digital Arts & Science
DIGITECH

Topics


Big Data Security
Software Security
Security Basics
Cloud Security

Security Basics

Sirapat Boonkrong

sirapat@g.sut.ac.th

Digital Arts & Science
DIGITECH

"The quality or state of being secure –

to be free from danger"

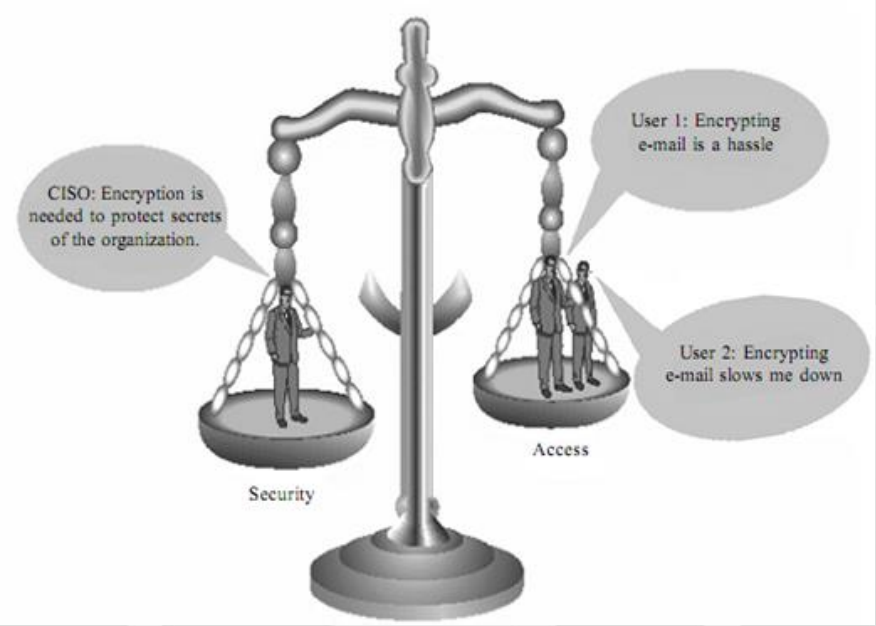
Photo Source: https://www.shutterstock.com

What is "Cyber Security"?

*"**Cybersecurity** is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access."*

Another Definition of "Security"

- A "well-informed sense of assurance that the information risks and controls are in balance." –Jim Anderson, Inovant (2002)



Source: http://www.expertsmind.com/questions/balancing-security-and-access-information-security-30116480.aspx

Unbalanced View

Cybersecurity Professionals

are accustomed to securing access to their networks and applications.

Digital Transformation

leads to an explosion of connected environments where perimeter protection is no longer enough.

Photo Source: https://www.shutterstock.com

Types of Security

Physical Security

Personal Security

Operations Security

Network Security

Information Security

Physical Security
The protection of personnel, hardware, software, networks and data from physical actions

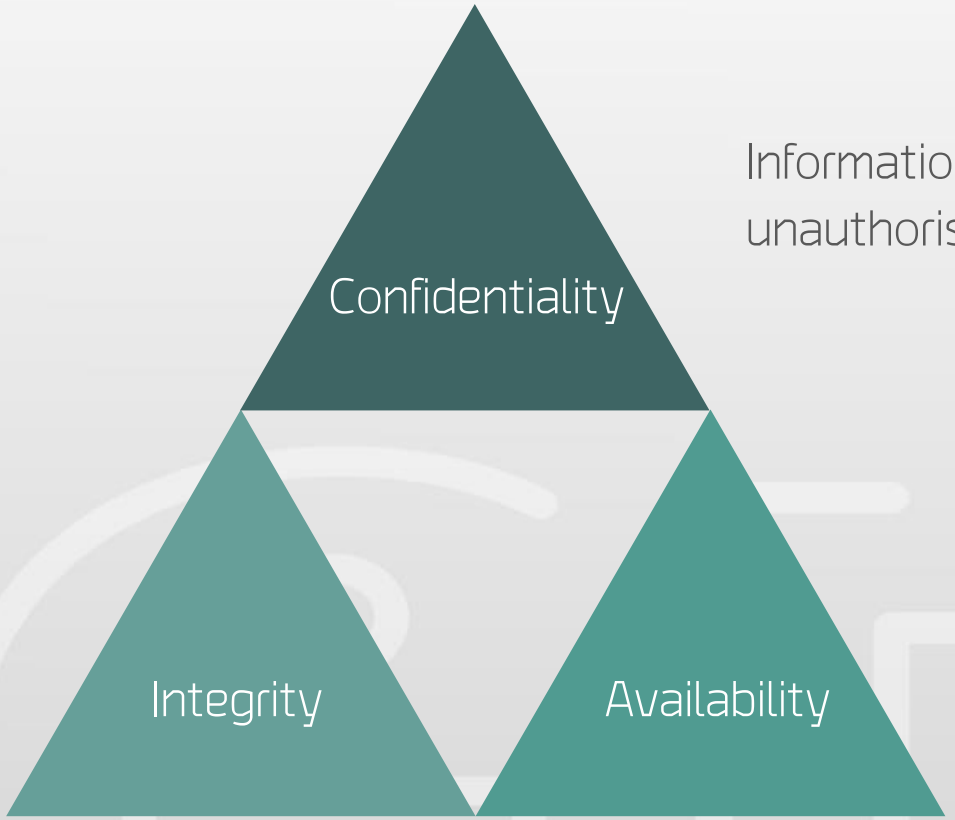
Personal Security
The protection of personal data and identity

Operations Security
The protection of critical information or pieces of data deemed useful for adversaries

Network Security
The protection of network assets and network traffic

Information Security
The protection of data of any form

CIA Model



Information is not available to unauthorised people or entities.

Information is complete and accurate and protected from corruption.

Information is accessible and usable when authorised users require it.

Security of Data Science and Data Science for Security

Sirapat Boonkrong

sirapat@g.sut.ac.th

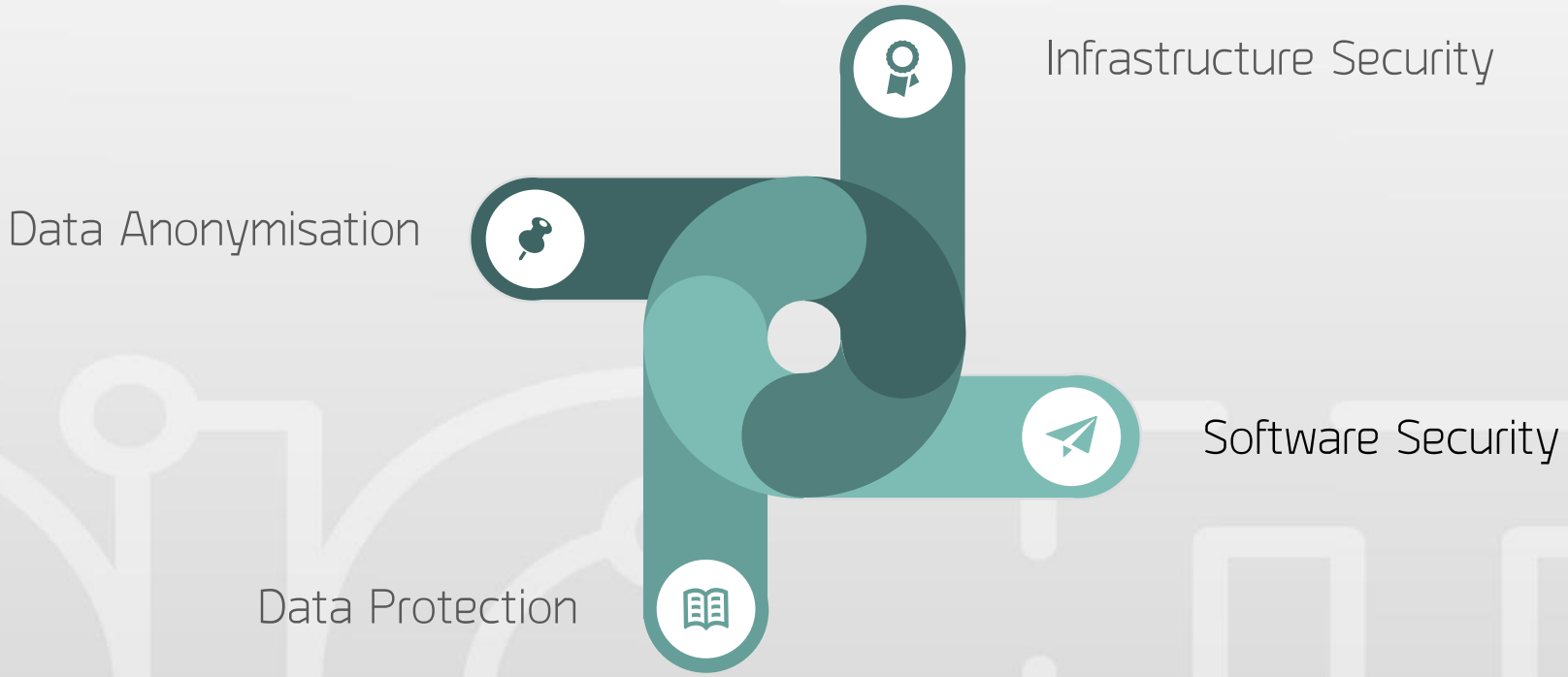
Digital Arts & Science
DIGITECH

Question

What is the difference between "security of data science" and "data science for security"?

Let's discuss this for a moment.

Security of Data Science



Data Science for Security

Big Data Security

Sirapat Boonkrong

sirapat@g.sut.ac.th

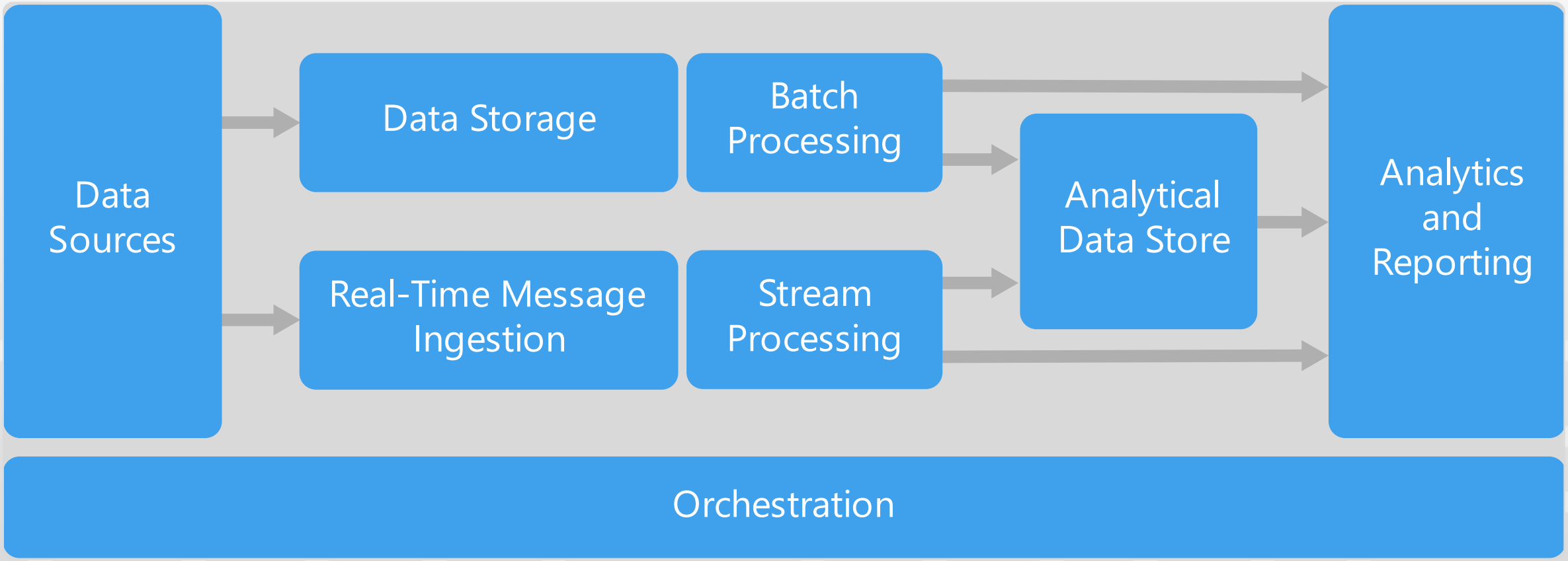
Digital Arts & Science
DIGITECH

Google Data Centre Security

Watch the video and state as many security measures you see as you can.

Big Data

Typical Big Data Architecture



Source: https://docs.microsoft.com/en-us/azure/architecture/guide/architecture-styles/big-data

General Big Data Security Issues

Insecure Computation

Insecure Data Storage

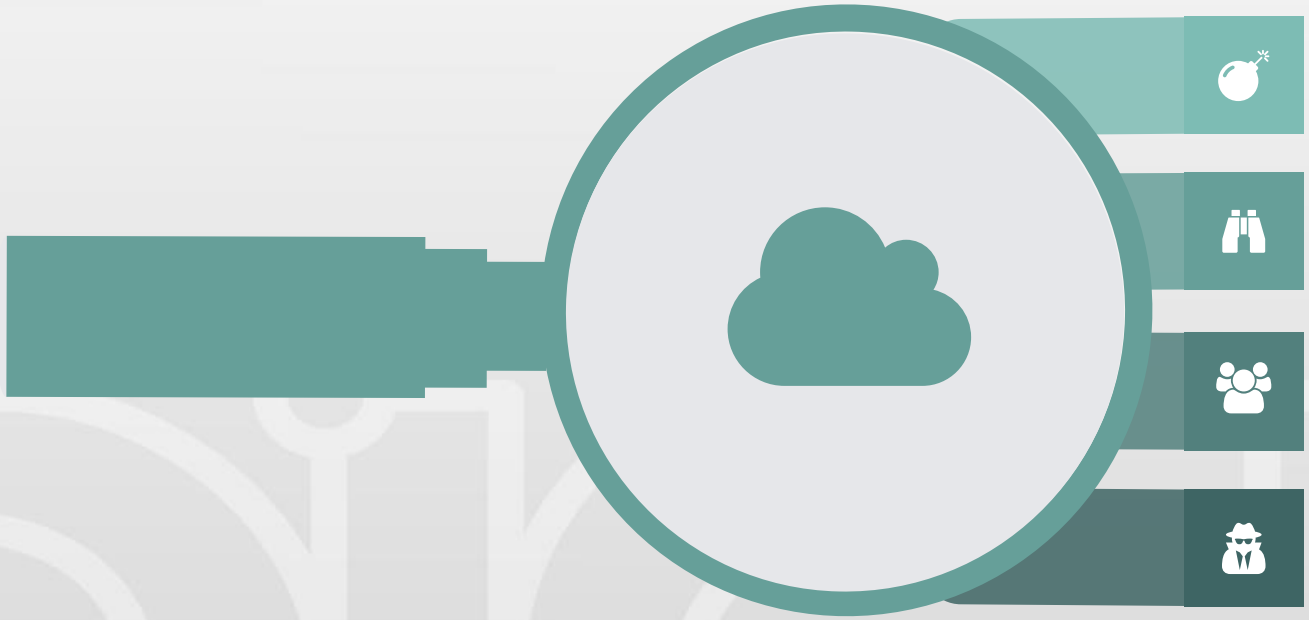
Input Validation and Filtering

Granular Access Control

Privacy Concerns in Data Mining and Analytics

Big Data Security Challenges

Four Pillars of Security



Perimeter (Authenticating)

Access (Authorising)

Visibility (Auditing)

Data (Architecting)

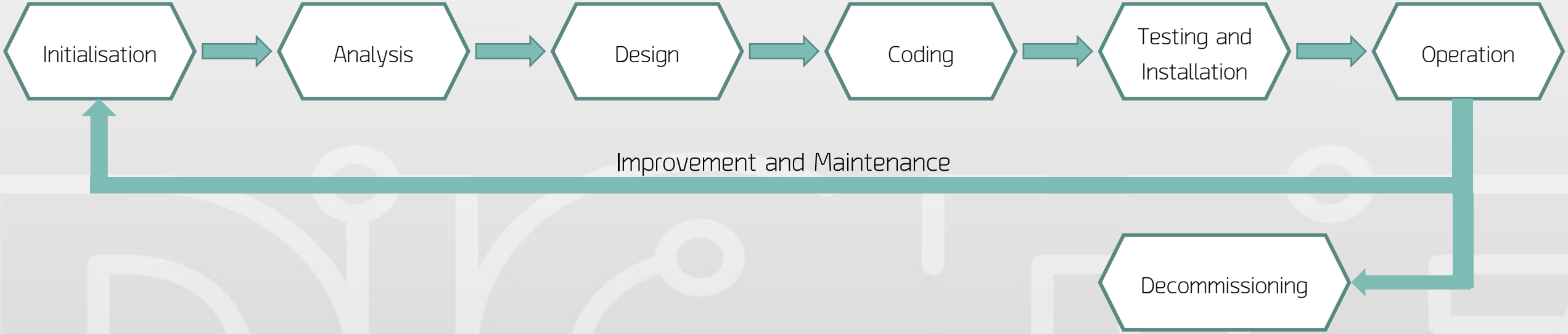
Software Security

Sirapat Boonkrong

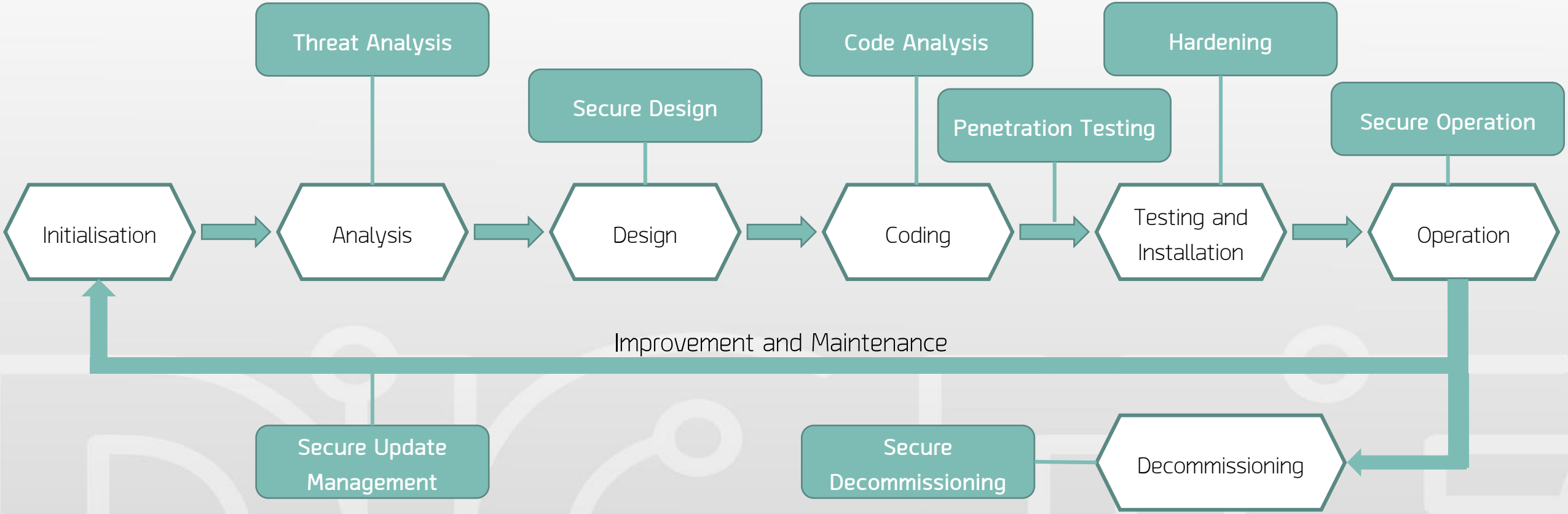
sirapat@g.sut.ac.th

Digital Arts & Science
DIGITECH

System Development Life Cycle (SDLC)



Secure System Development Life Cycle (SecSDLC)



OWASP

Developers should check their applications and services for the following problems.

- Incorrect or lack of input validation and data sanitation so that an attacker can trick an interpreter or query engine to do things that were not intended.
- Incorrect implementation of authentication and session management.
- Exposure of sensitive data
- Incorrect implementation of the mechanisms to restrict what an authenticated user is allowed to do.
- Use of insecure configurations as a result of insecure default configurations

Cyber Security Teams

RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

YELLOW TEAM

- Software Builders
- Application Developers
- Software Engineers
- System Architects

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

Source: https://hackernoon.com/

Cloud Security

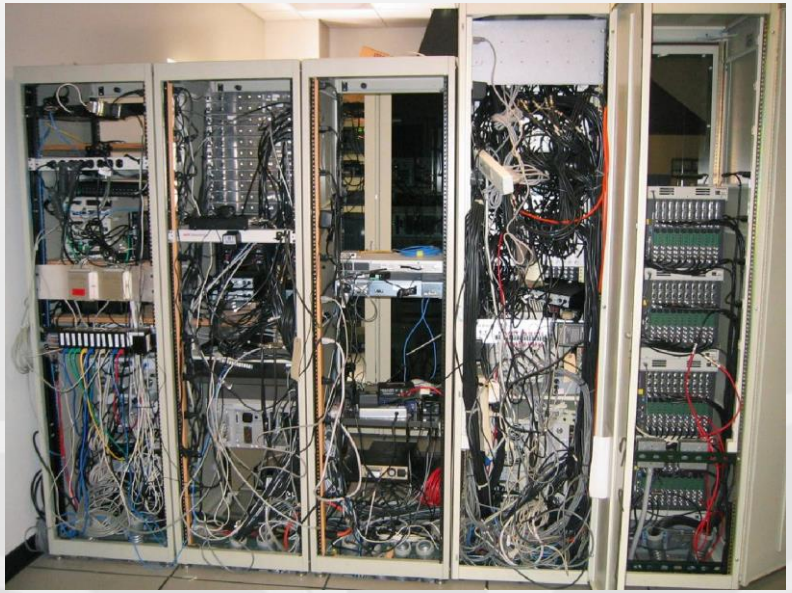
Sirapat Boonkrong

sirapat@g.sut.ac.th

Digital Arts & Science
DIGITECH

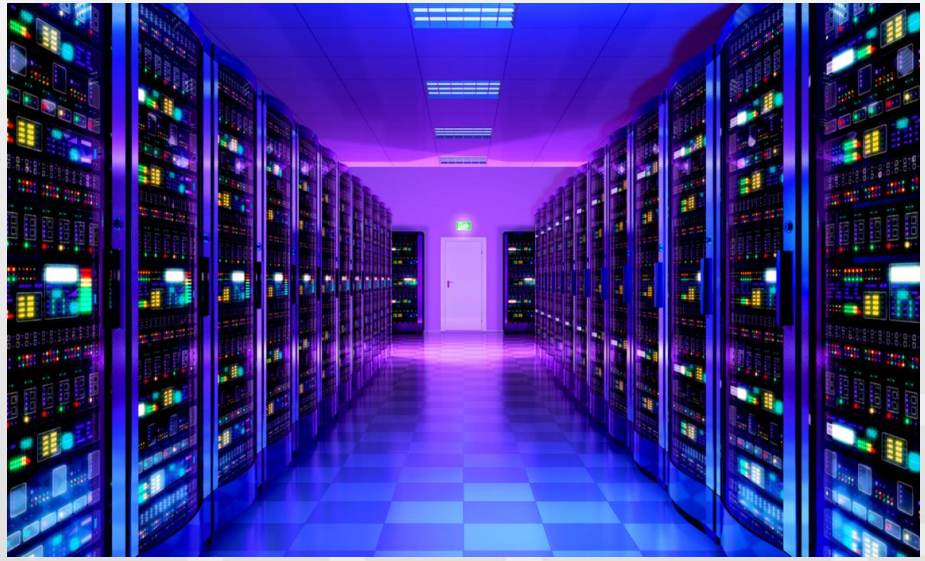
Infrastructure has Changed

Buying Own Hardware



Source: https://www.techrepublic.com/pictures/real-world-server-room-nightmares/12/

Infrastructure as a Service



Source: http://www.justinhallcomics.com/what-is-a-network-server/

Early 200s → Mid 200s → Today

Cyber Crime has Changed

Single Actors

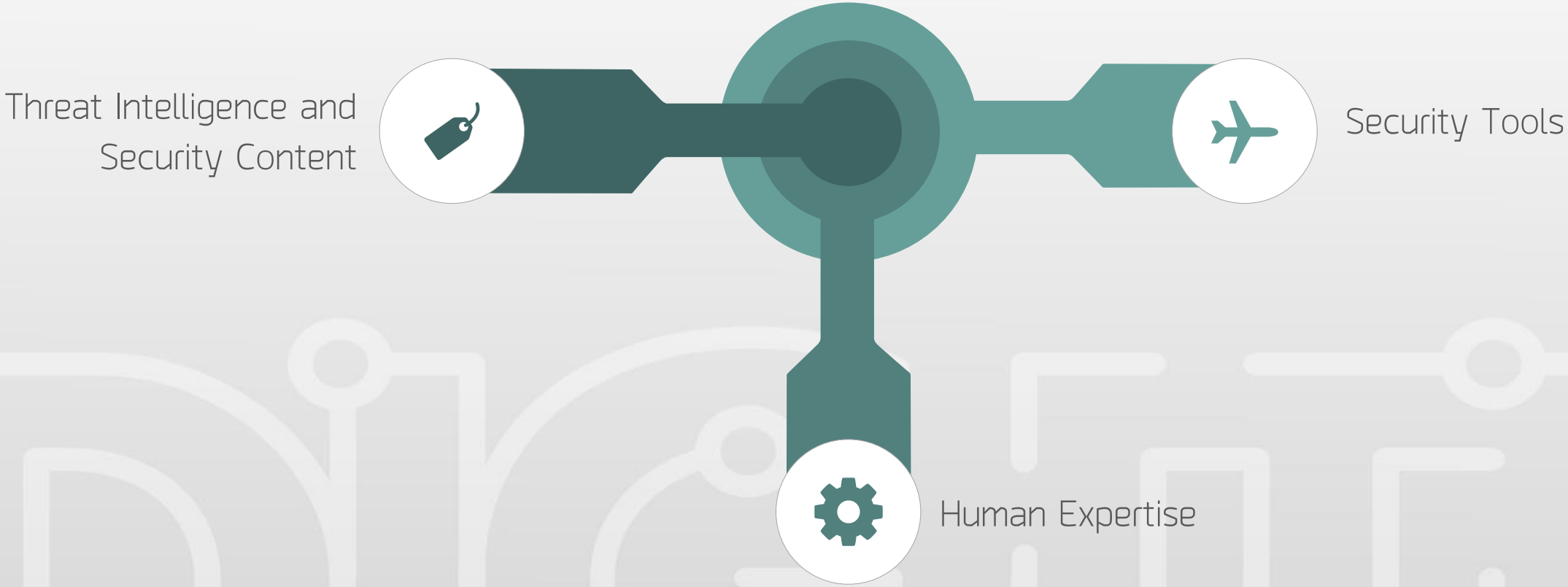
Organised Groups

Early 200s

Mid 200s

Today

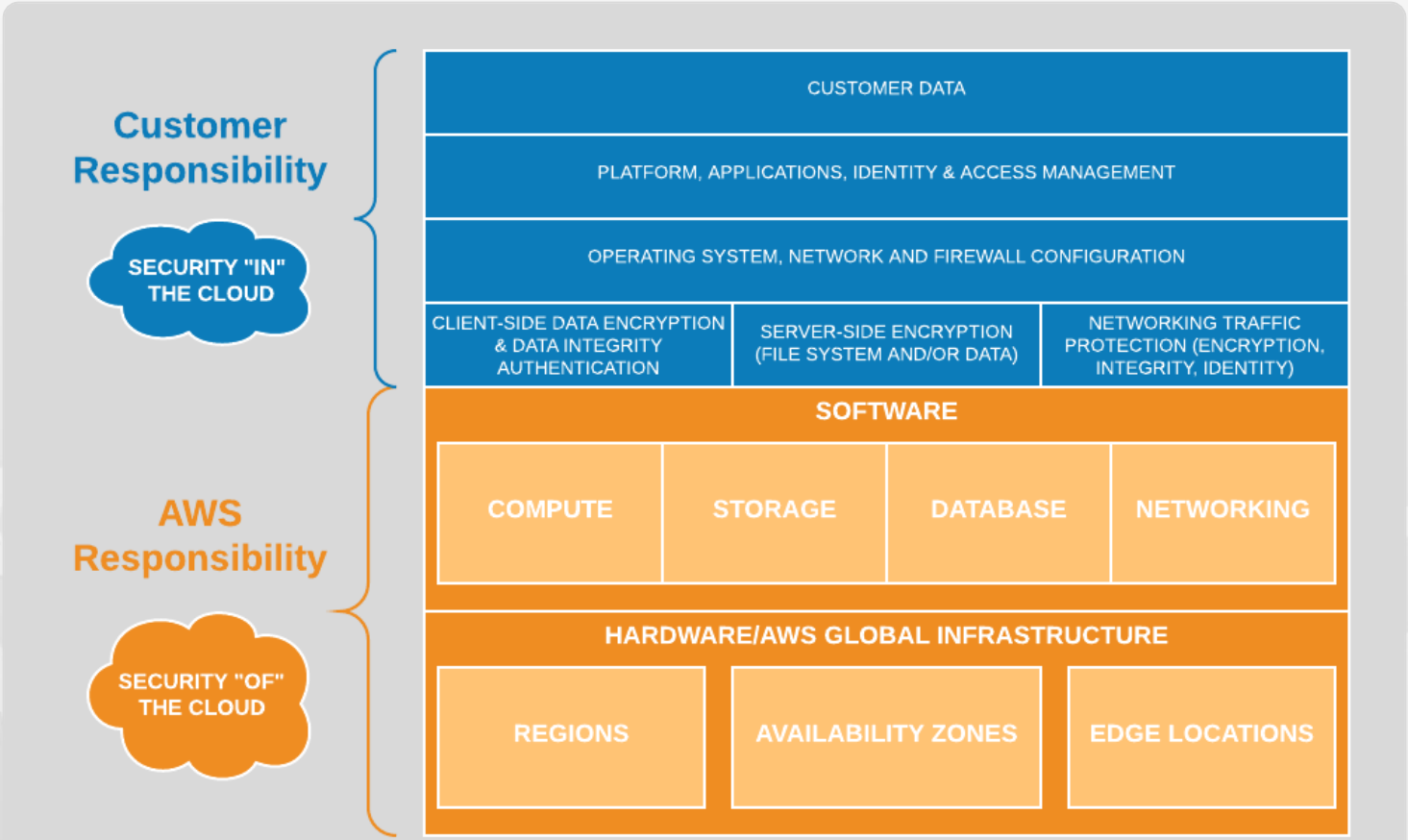
Basic Cloud Security Challenges



Technical Cloud Security Challenges

1. Loss of Visibility
2. Compliance Violations
3. Lack of Cloud Security Strategy and Architecture
4. Insider Threats
5. Contractual Breaches
6. Insecure API
7. Misconfiguration of Cloud Services

Shared Responsibility Model



Shared Responsibility Model

	Infrastructure-as-a-service (IaaS)	Platform-as-a-service (PaaS)	Software-as-a-service (SaaS)
People	You	You	You
Data	You	You	You
Applications	You	You	CSP
Operating system	You	CSP	CSP
Virtual networks	You	CSP	CSP
Hypervisors	CSP	CSP	CSP
Servers and storage	CSP	CSP	CSP
Physical networks	CSP	CSP	CSP

Source: https://kinsta.com/blog/cloud-security/

Best Practice (1)

1

Keep it simple and thus secure (KISS)

2

You can only secure system that you fully understand.

3

- Prefer simplicity over complexity
- Ensure others understand the design
- Use standardised tools
- Draw high-level diagrams

Best Practice (2)

1

Require strong authentication

2

Use credential-based authentication and user session management to grant access

3

- Use password manager
- Use 2FA or MFA
- User SSO service

Overview of Cloud Security

Source: https://kinsta.com/blog/cloud-security/

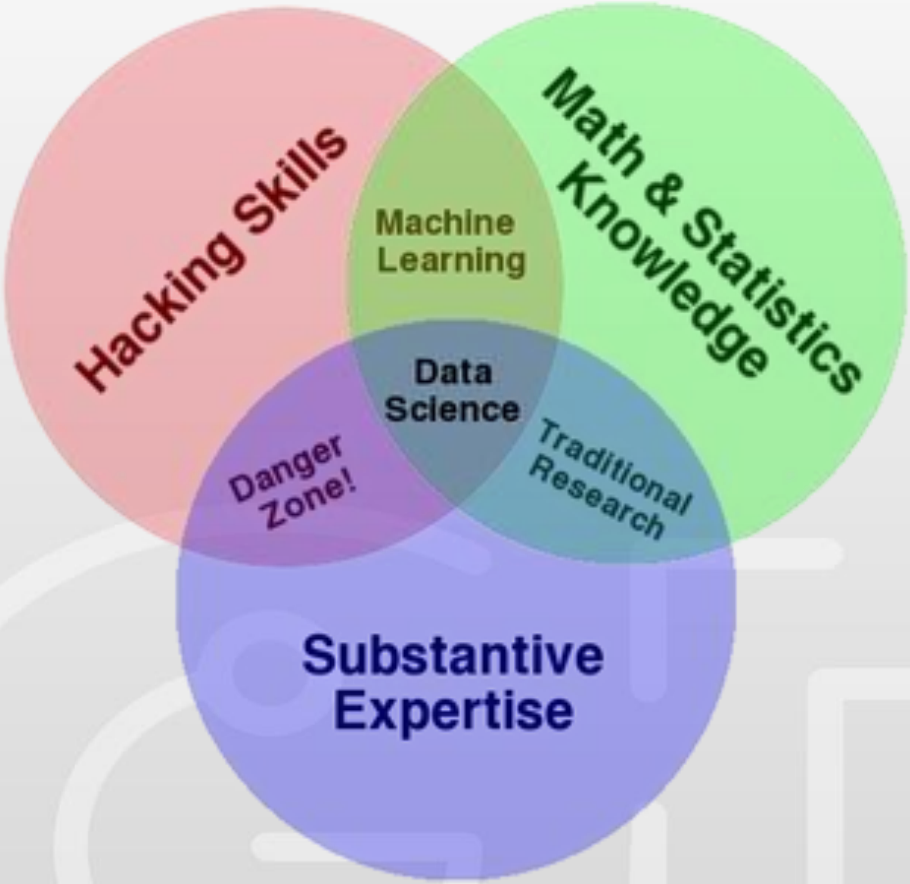
Data Science for Security

Sirapat Boonkrong

sirapat@g.sut.ac.th

Digital Arts & Science
DIGITECH

Data Science Venn Diagram

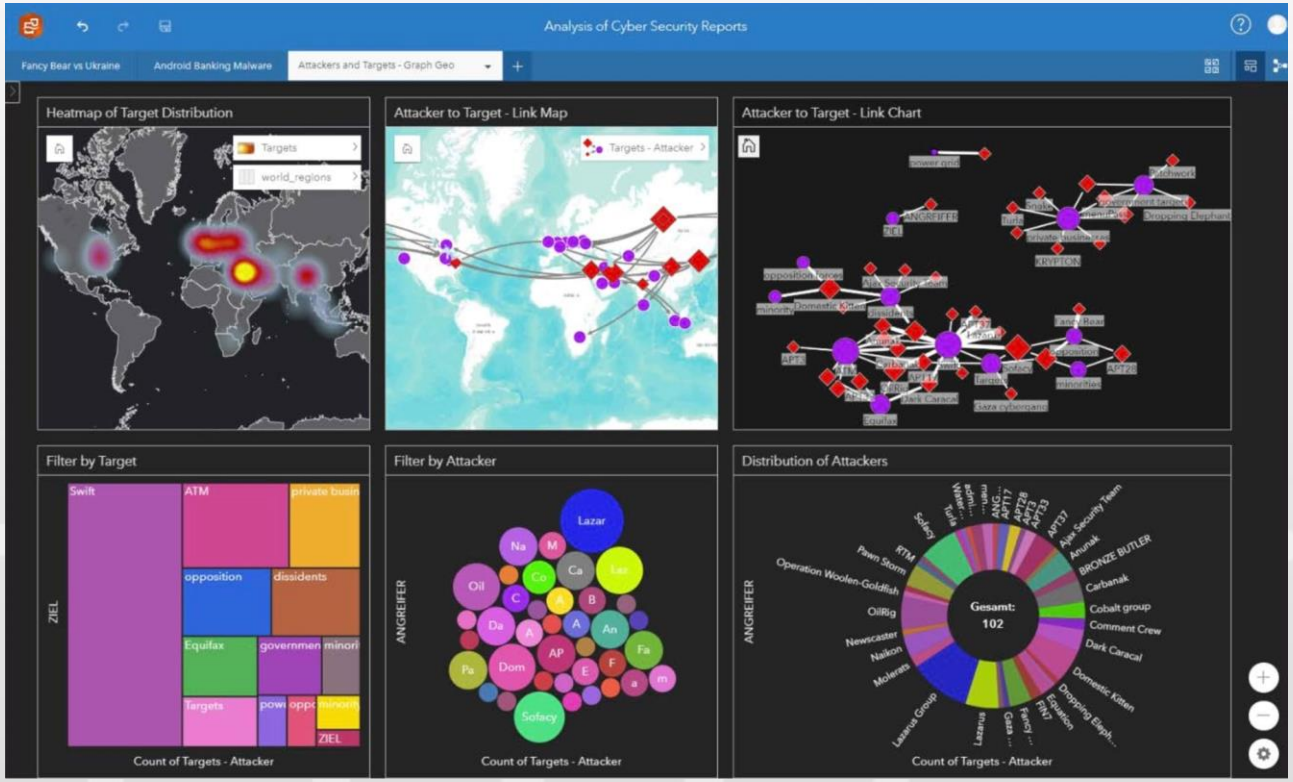


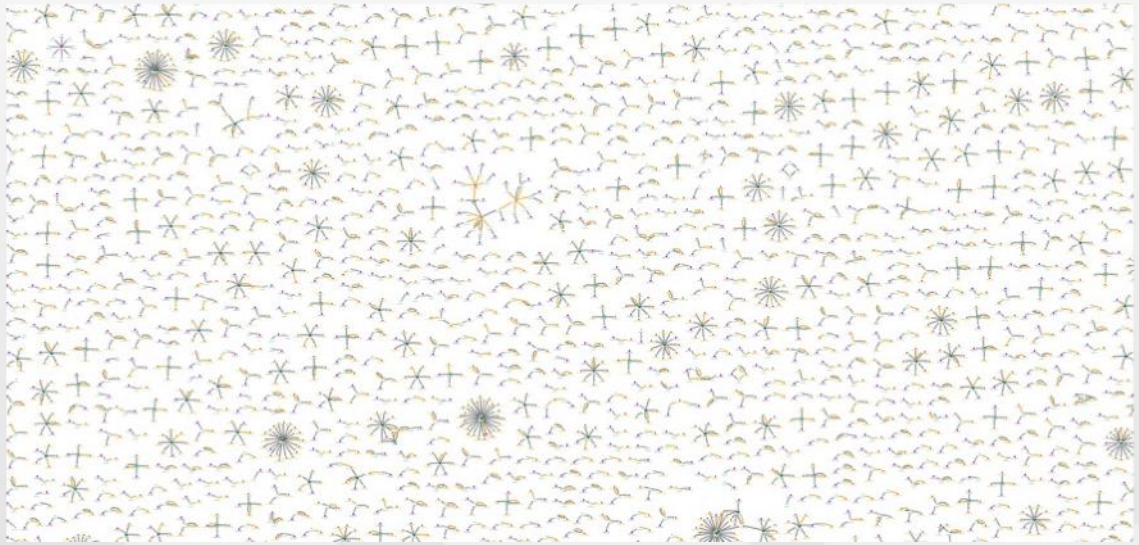
Source: http://drewconway.com/zia/2013/3/26/the-data-science-venn-diagram

Cyber Security Data Science Personas

Cyber Security Data Science Process

Examples of Cyber Security Visualisation





Digital Arts & Science
DIGITECH

Summary

Basics of Security

Security of Data Science and Data Science for Security

Finish

Big Data Security

Software Security

Cloud Security

Thank You

44