UNIVERSITY OF OSLO

TEK5530 Measurable Security for the Internet of Things

Takeaway - main points from each lecture L1-L15

https://bestructured.com/intrusion-detection-intrusion-prevention-and-antivirus-the-differences/

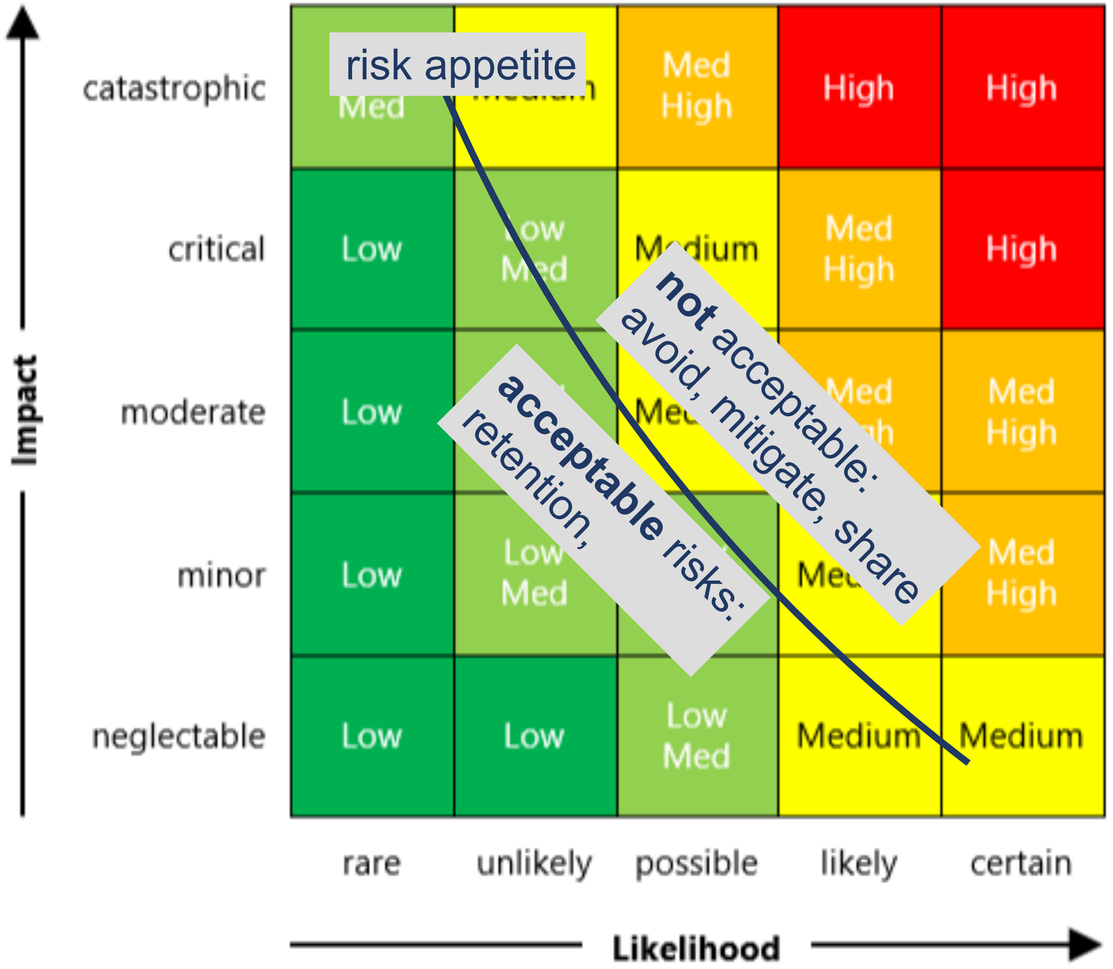
Josef Noll
Professor
Department of Technology Systems

UNIVERSITY
OF OSLO

Take-away L1 Introduction

- Risk analysis
  - Likelihood
  - Impact

- Risk analysis for IoT
  - Likelihood “you are going to be hacked”
  - Exposure



Take-away L2 Internet of Things

- Things
  - NFC/RFID
  - Sensors
  - Gateways & Backend-systems
- Internet
  - IPv4, IPv6
  - limitations of IoT: bandwidth, latency, reliability, processing power, battery
- Semantics
  - machine-readable understanding
  - context, reasoning

- 5G
  - eMBB, mIoT, URLLC
  - network slicing

- Energy networks
  - Smart Grid & energy twins
  - Just transition

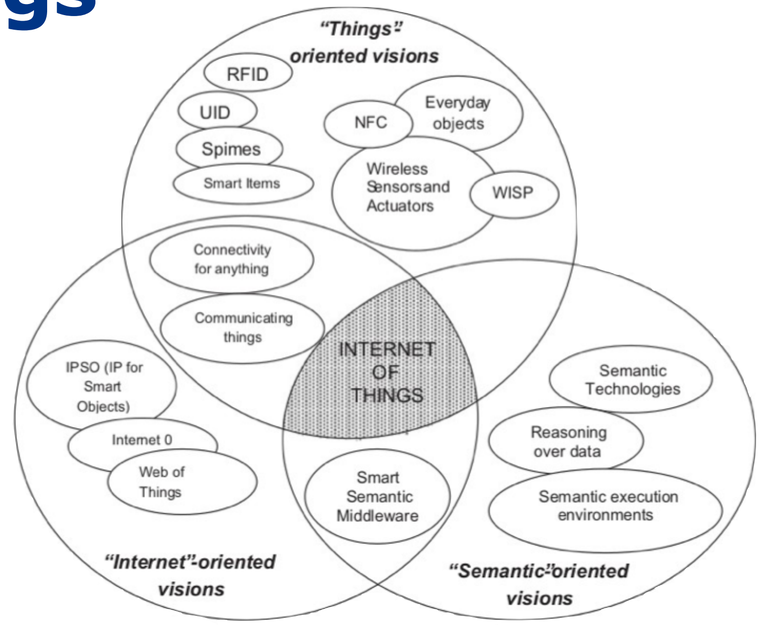
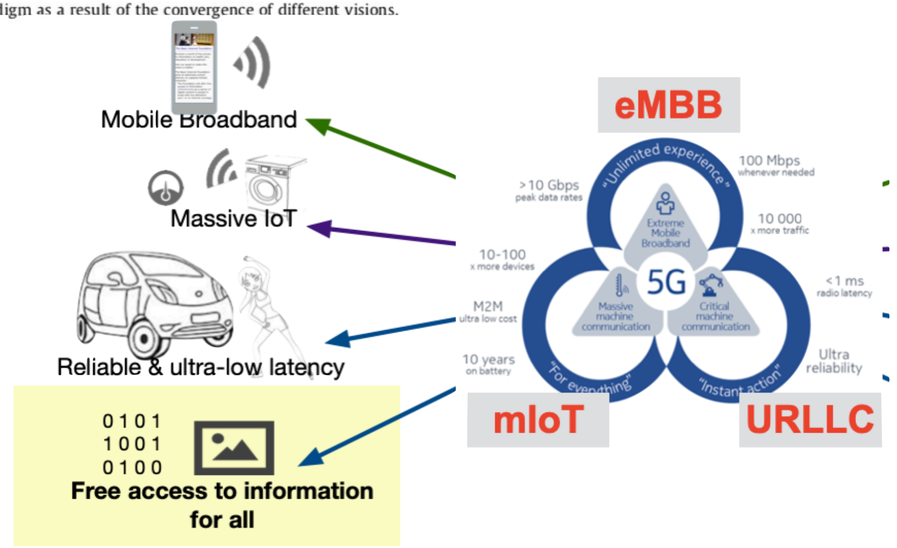


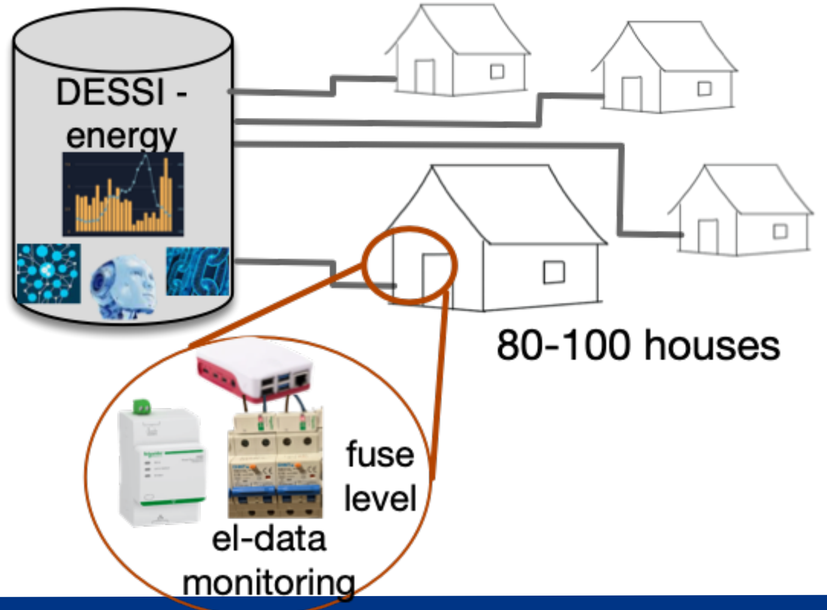
Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.



Take-away L3 Security in IoT

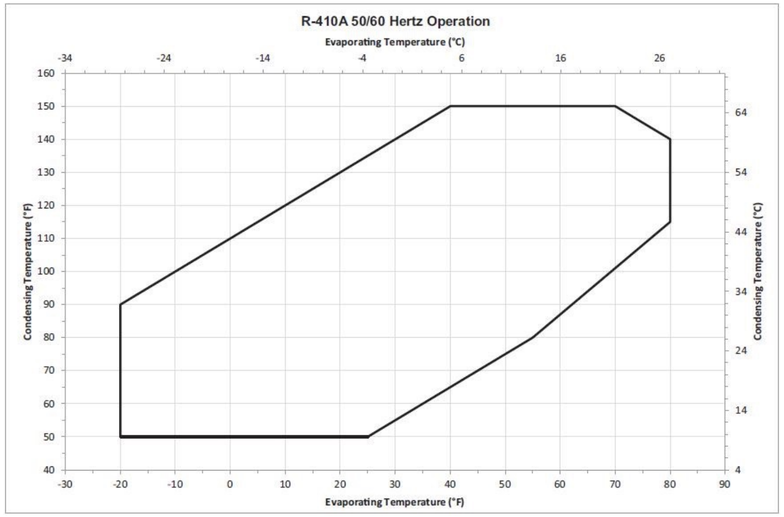
- Security challenges in IoT
  - examples/classes of IoT
  - limitations of IoT: bandwidth, latency, reliability, processing power, battery
  - security challenges
- Smart home example
  - alarm, monitoring,

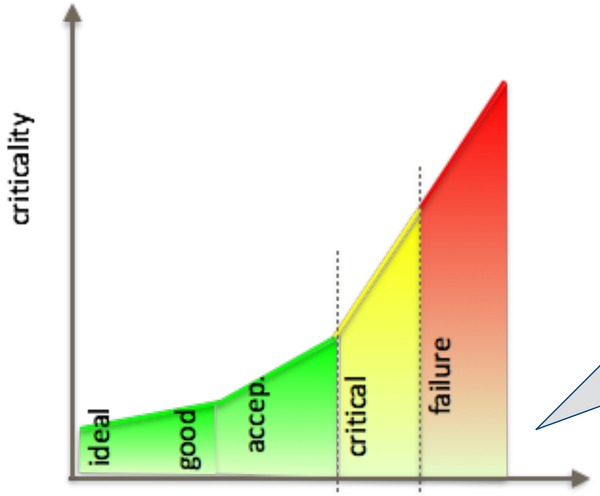
- Threats & vulnerabilities
  - physical access, authentication
  - DDoS, Botnet, malware, data breach, man-in-the-middle
- Defence
  - Gateway
  - Monitoring



Take-away L5 Security Semantics

- IoT System components, Security functionality & Security attributes
- IoT Lifetime security functionality
  - Operations
  - Development, Audit, Maintenance
  - Decommissioning
  - Mechanisms, Humans, Physical, Privacy protection
- Internet, Things, Semantics
  - Semantics vs Syntax
- Operating envelope
  - Meaning, examples
  - communication

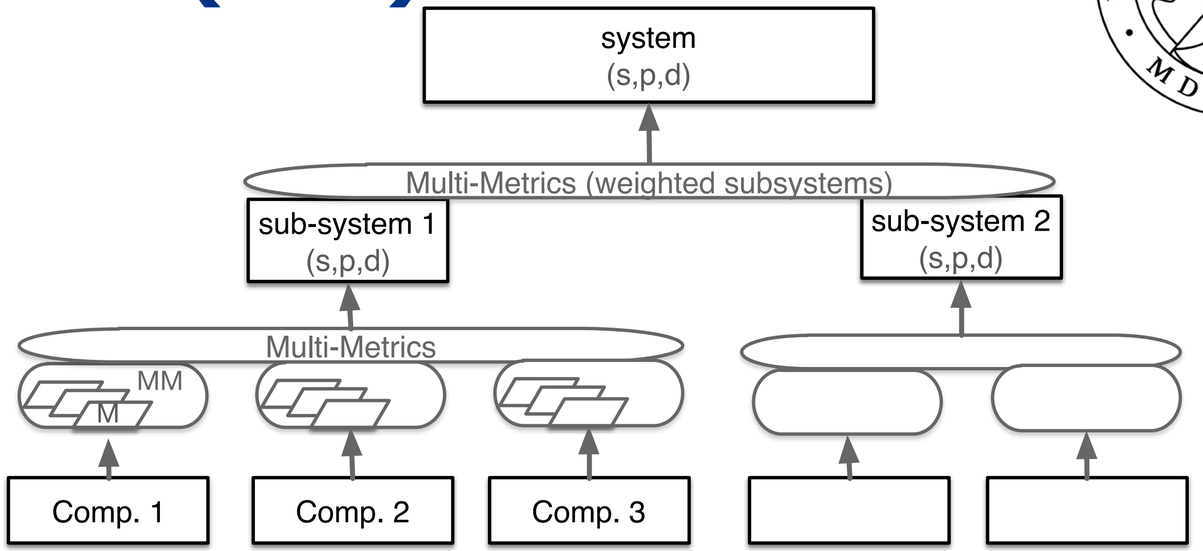




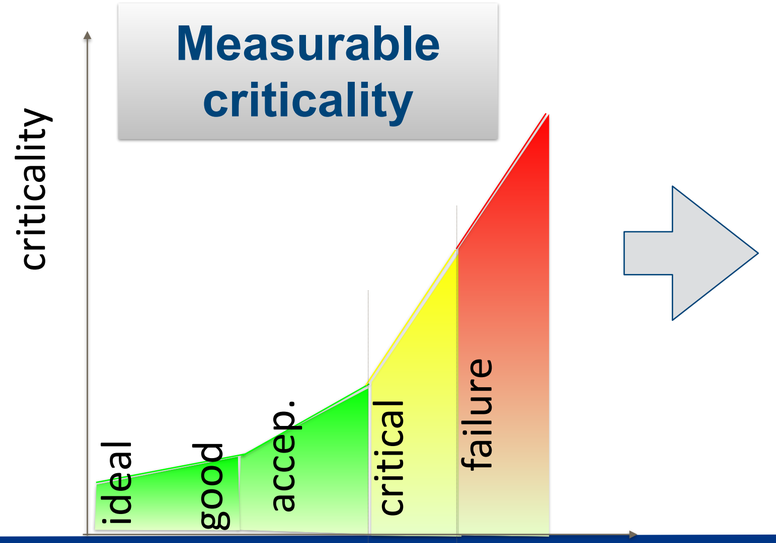
1) How does he Operating Envelope look like applying criticality?
2) How can the criticality be applied for SPD?

Take-away L6 Multi-Metrics (MM) Method

- Accountable security - MM
  - principle operation
- Privacy: Loan of vehicle
  - difference of scenarios 1-3 (privacy, speeding, crash)



- Privacy labels
  - which data, sharing
  - integrity, storage
  - ownership, further distribution



to measurable: security, privacy and dependability

SPD level	SPD vs SPD_{Goal}
(67,61,47)	(●,●,●)
(67,61,47)	(●,●,●)
(31,33,63)	(●,●,●)

Take-away L7 Multi-Metrics (MM) Method

- Applications: Smart Meters
- Communication: Smart Meter System
- SPD
  - from components and functionalities
  - to SPD functionalities
- Operation envelop
- Weighting in MM
- Combining sub-systems through MM

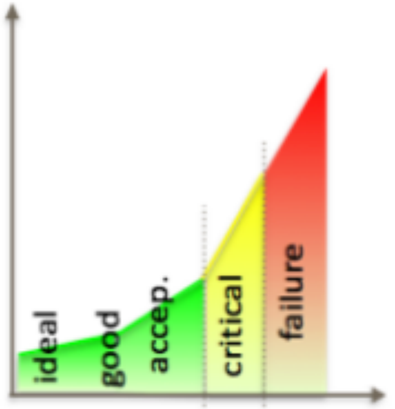


Table 8 Sub-systems and components weights

Sub-system	Sub-sys. Weight	Component	Comp. Weight
AMS	80	Remote Access	70
		Authentication	80
		Encryption	80
Radio link	50	Mesh	60
		Message Rate	80
		Encryption	40
Mobile link	20	Mobile link	70
		Encryption	40

Take-away L8 Risk-Exposure Model

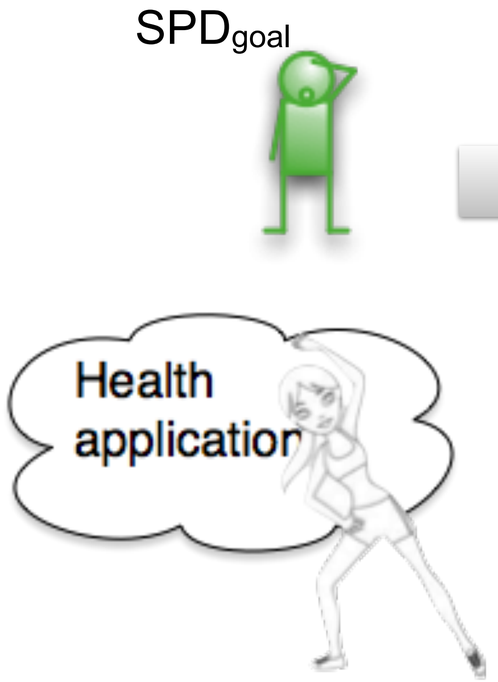
- Why not Impact & Frequency/Likelihood risk analys
- Risk-Exposure model components
  - Exposure: Connectivity & Protection level
  - Connectivity: C1 (isolated) … C5 (full Internet)
  - Protection level: P1 (lowest) … P5 (highest)
- Protection: data encryption, communication protection, SW security, HW security controls, Monitoring, Access control, Cryptography, Physical security
- Home control, explain
  - external supervision vs in-house solution

Catastrophic	A	C	E	F	F
Major	A	B	D	E	F
Moderate	A	B	C	E	E
Minor	A	A	B	D	D
Insignificant	A	A	A	C	C
Impact/ Exposure	E1	E2	E3	E4	E5

Courtesy: Manish S

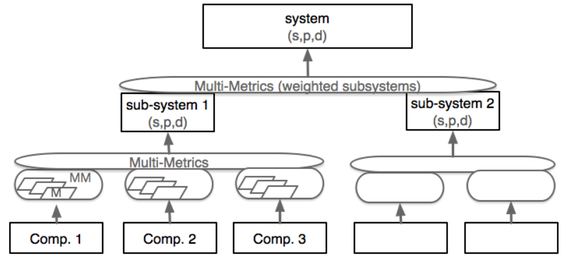
Main Take-away L9 System Security

- Application-driven SPD_{goal}
  - Provide examples and justify
- how to perform the Multi-Metrics Method
  - Components, sub-systems, Multi-metrics
  - Result of Multi-Metrics
- Shortcomings of Multi-Metrics?



versus

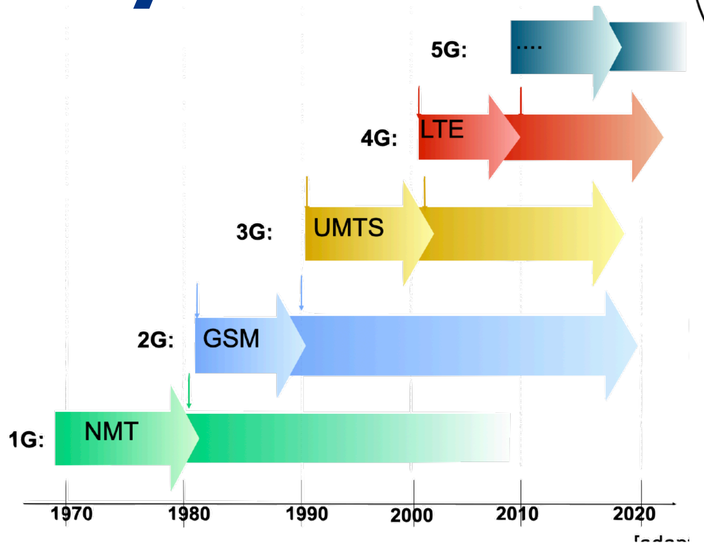
$System_{SPD}$



system of systems

$|SPD_{Goal} - SPD\ level| = \leq 10$, green.
$|SPD_{Goal} - SPD\ level| = > 10, \leq 20$, yellow.
$|SPD_{Goal} - SPD\ level| = > 20$, red.

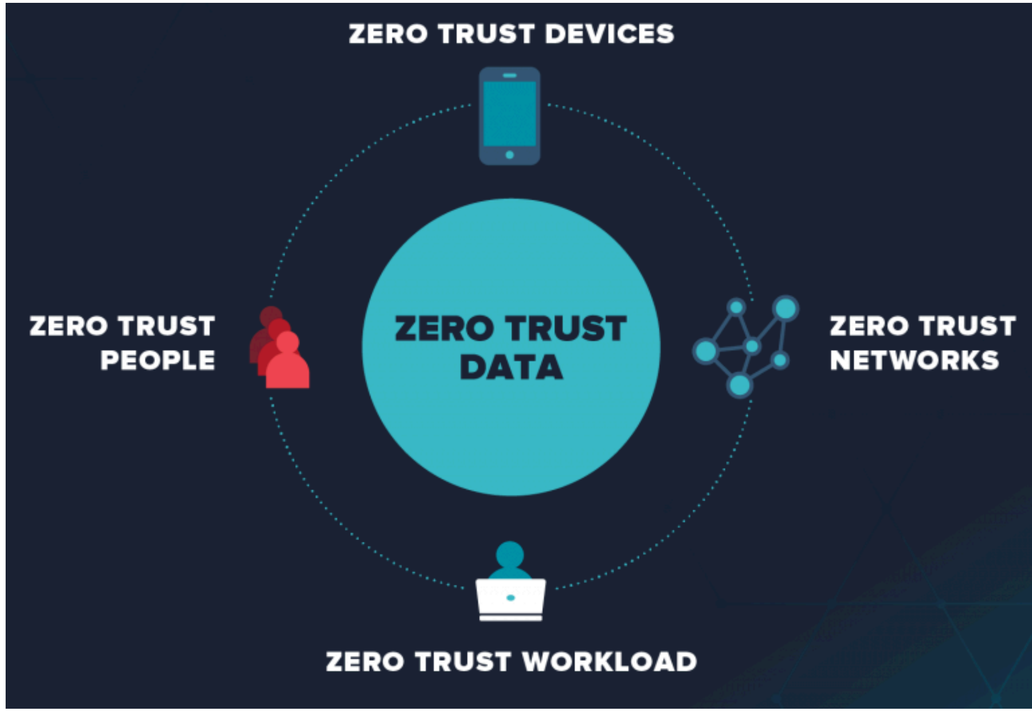
Take away from L10 Mobile Security



- Key characteristics of mobile systems
  - 1G - analog - voice
  - 2G - digital - voice & SMS
  - 3G - voice & mobile data
  - 4G - mobile broadband (MBB)
  - 5G - eMBB, massive IoT, URLLC (reliable, low latency)
- Security considerations
  - 2G - IMSI catcher (mobile authenticates to network)
  - 3G - mutual authentication
  - 4G - all IP security
  - 5G - increased attack surface (cloud computing, IoT devices)

Take away from L11 ZeroTrust Architecture

- Why zero trust
  - "your system is hacked already"
  - "no user or device is trusted until they have proved otherwise"
  - what do you do in case of hacking/ ransomware?
- Domain examples
  - Hospital architecture
  - IT-deployment, docker-based
  - Cloud access
- Rollen i organisasjon

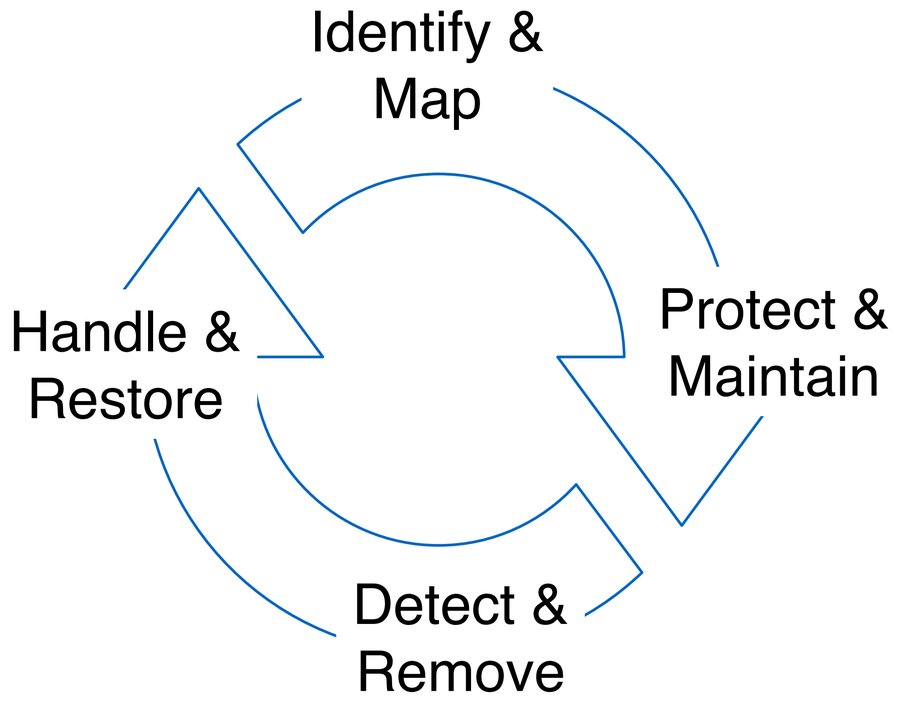


https://dtc1.com/how-to-set-up-a-zero-trust-network/

Take away from L13 Intrusion Detection

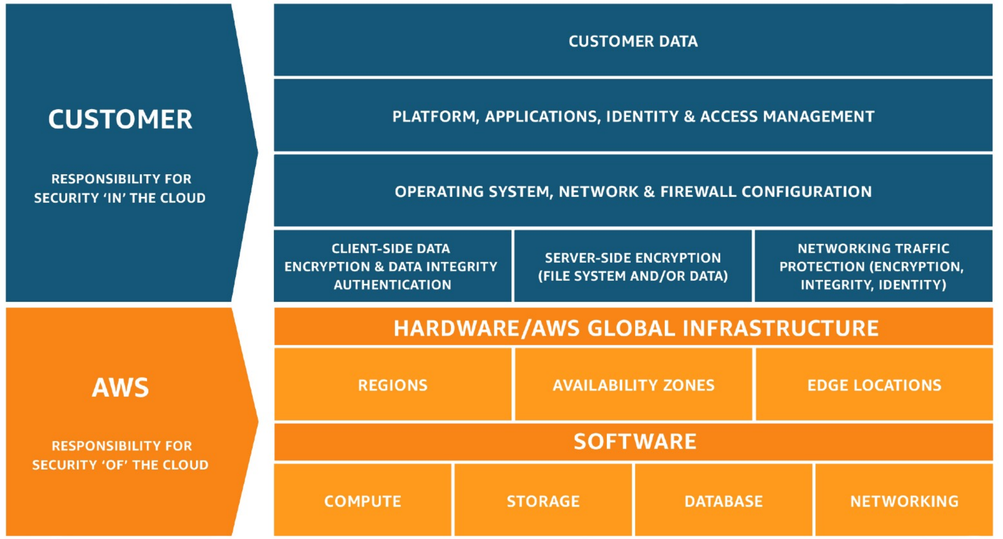
- NSM Principles for ICT security (v2.0)
  - what do these terms include?

- Intrusion Prevention System (IPS)
  - stop potential threats before breaching the system
- Intrusion Detection System (IDS)
  - Mitigate the damage



Take away from L14 Cloud & Cloud Security

- Delivery models
  - Infrastructure (IaaS), Platform (PaaS), Software (SaaS) as a Service



- Responsibility of Cloud provider, and of Customer

- Cyber vs Cloud Security
  - Threats, reasons, main defence

Take away from L15 Group Work

- Application goals of your scenario
  - Security, Privacy, Dependability goals
  - System analysis

- Main topics
  - functionality, threats, defence

- Main 3-5 take-aways
  - lessons learned