



Advanced Cybersecurity Essentials Workshop

Dr. Amin Hasbini

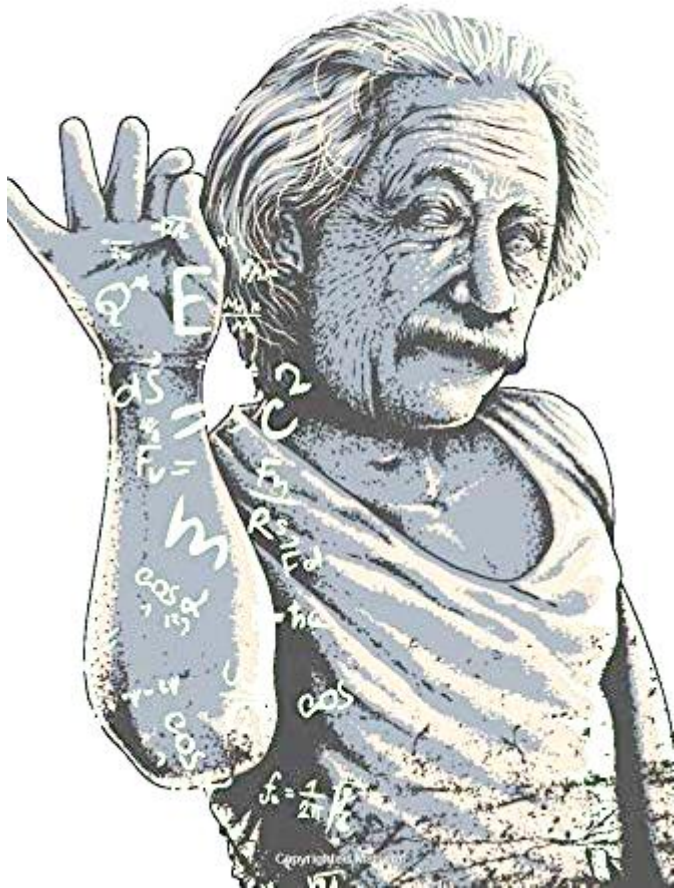
Intro?

Dr. Amin Hasbini

Why am I doing this course?

- Pleasure
- Learning
- Just curious

The goal of this course/workshop



This document is TLP RED

First and Foremost for Cyberwarriors only

1. This is no magic or secret sauce
2. It's a continuous knowledge acquisition/maintenance process!
3. In most cases, It's not even about knowing the information
4. There will always be much more to learn!

Disclosure / Disclaimer

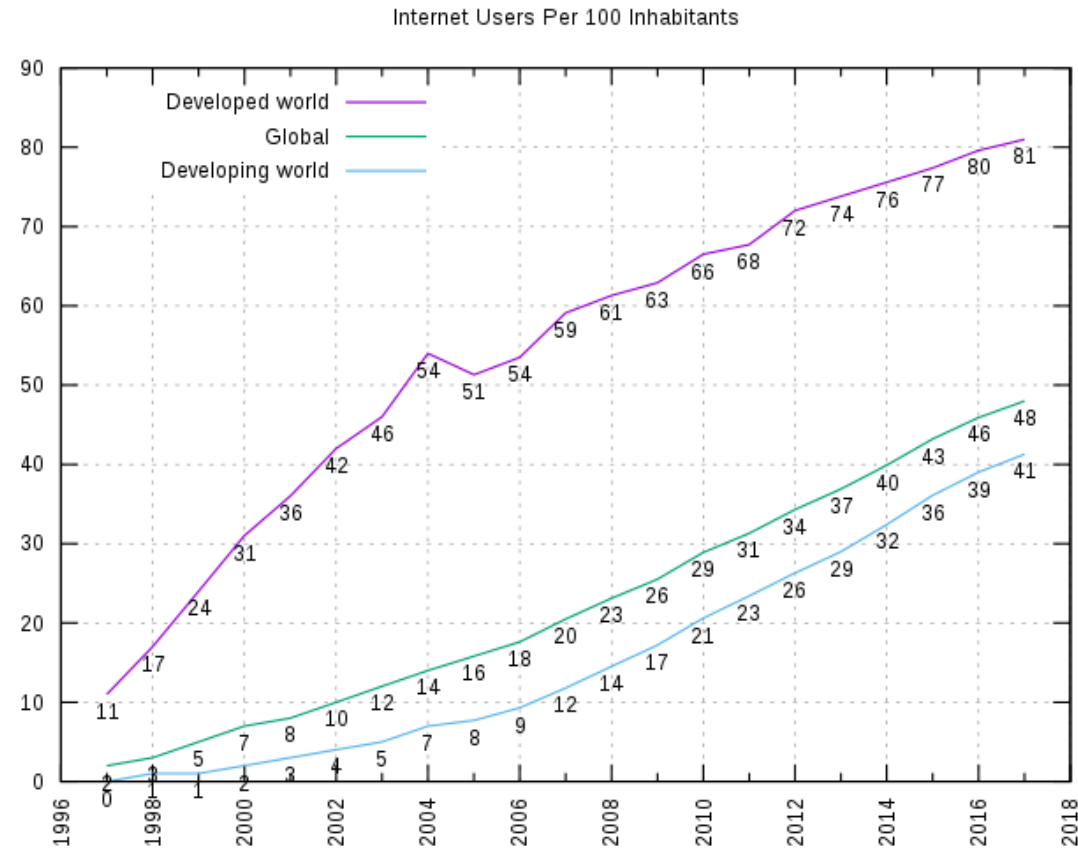
- No criminal activities please
- No misuse of knowledge
- We are Ethical Whitehat Hackers
- What this course/workshop is offering
- What this course/workshop does not offer
- 2-way communication?
- Sessions format? Break?

Material that will make your life easier sometimes

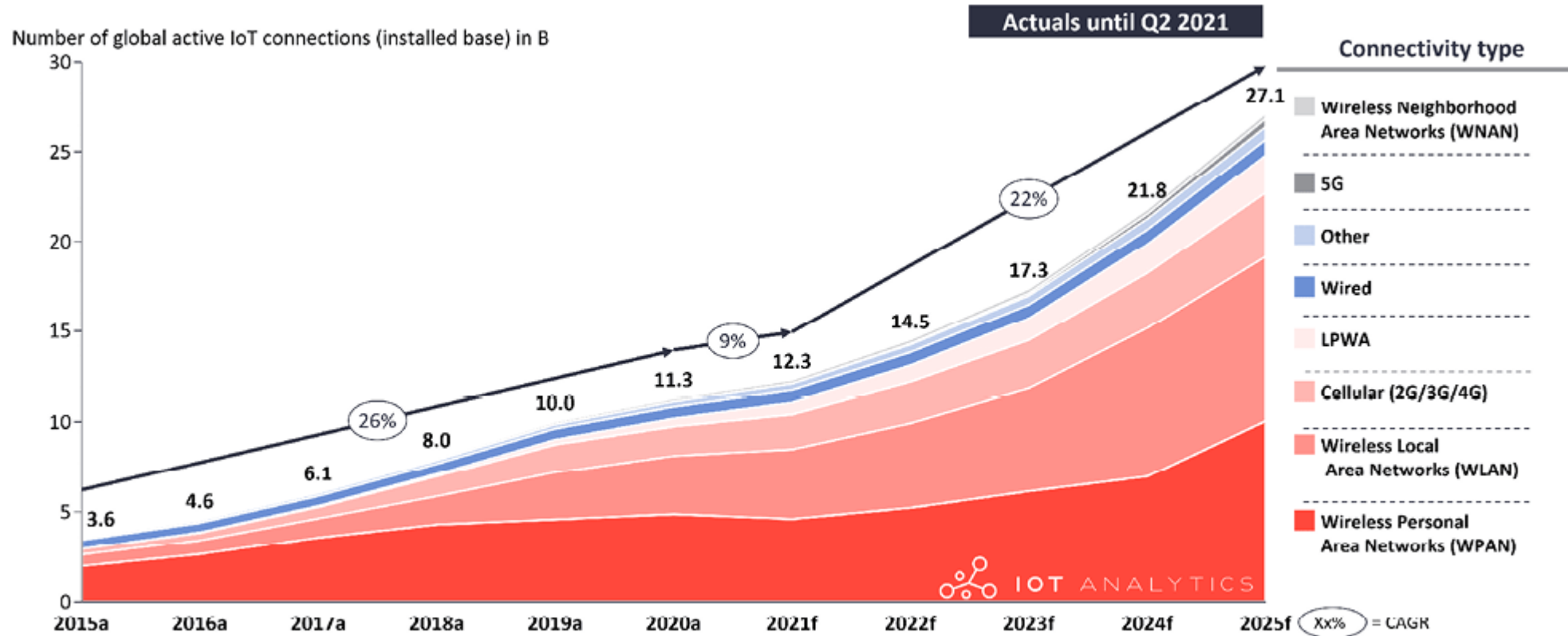
- Internet speed
- Specs 4 CPUs, 8GB RAM, SSD
- Vmware

Setting the scene

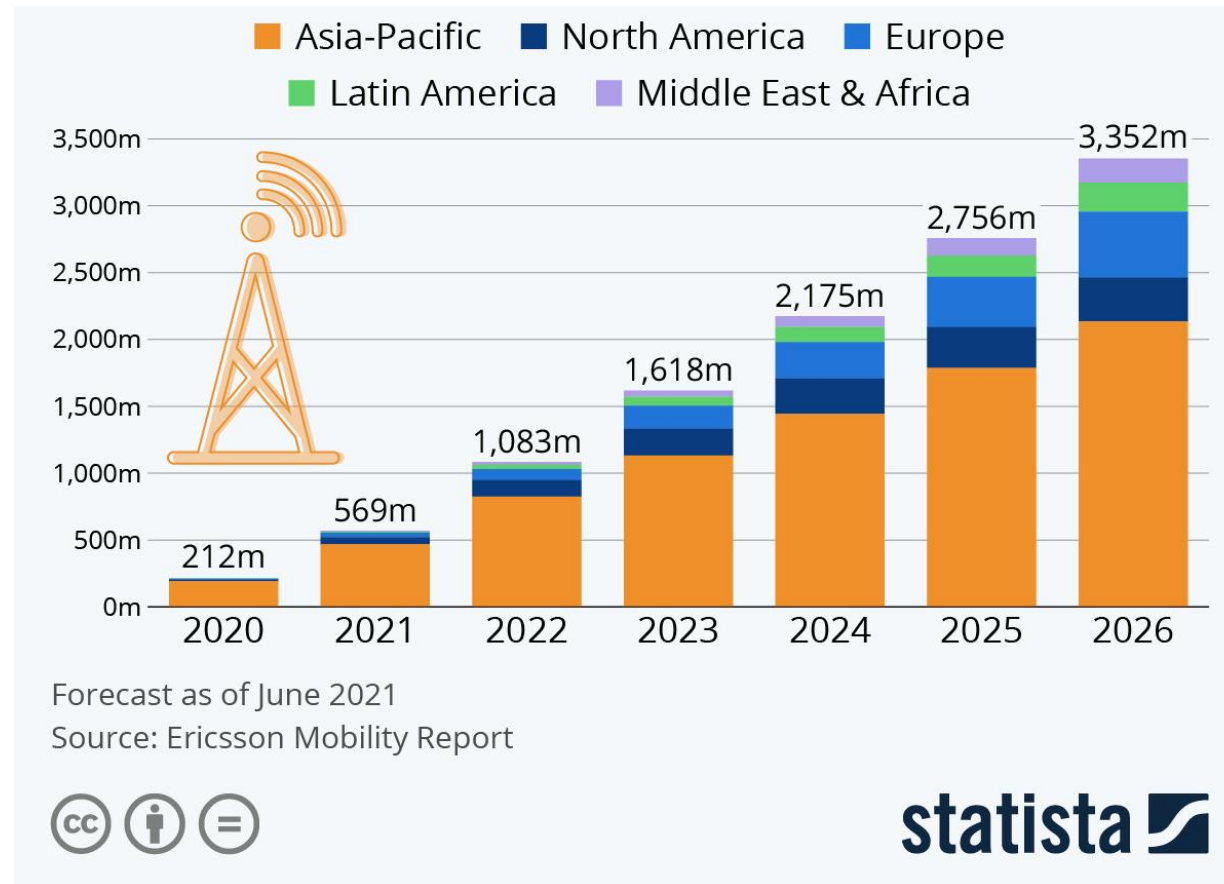
Growth of internet users



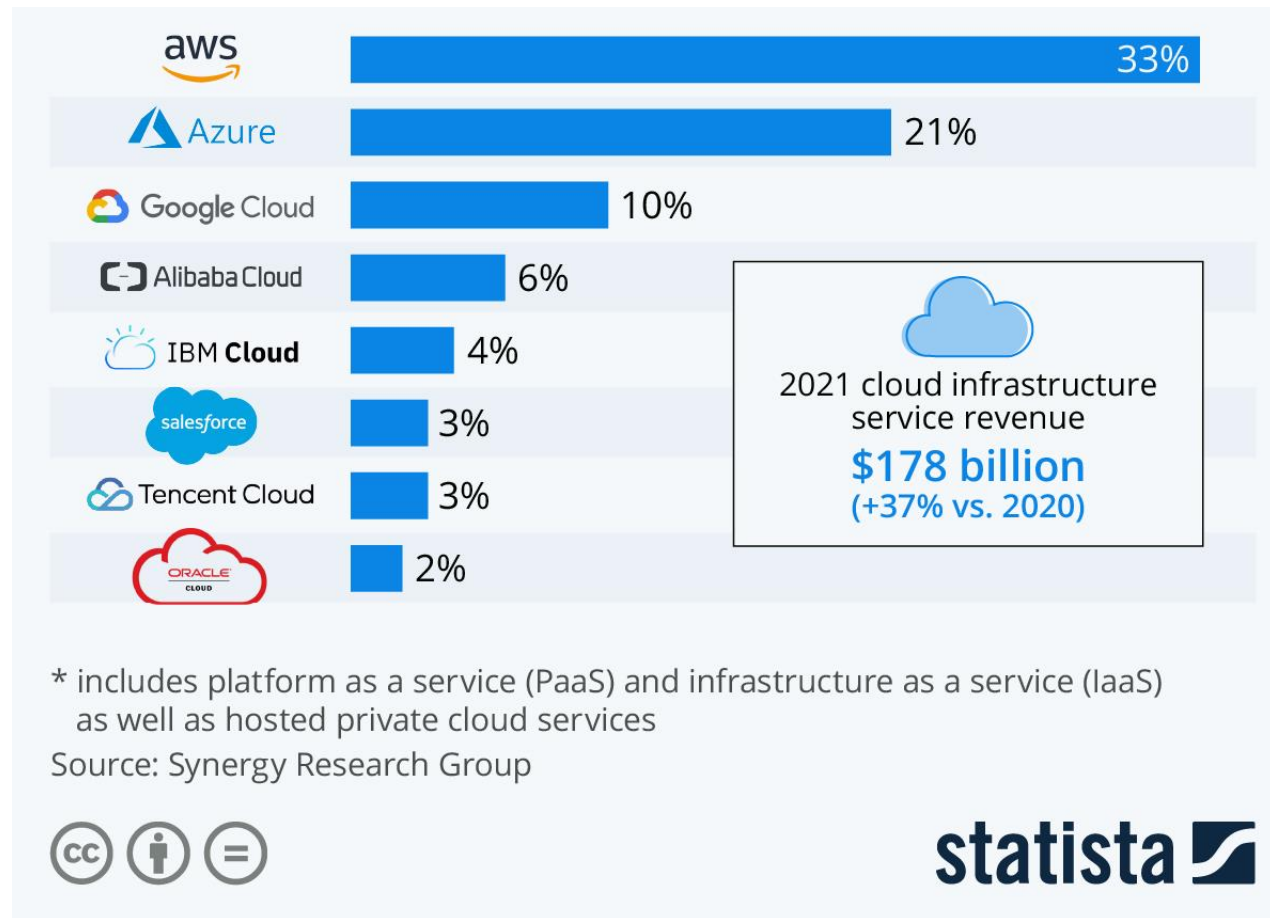
Global IoT market forecast (in billion connected IoT devices)



Global 5G adoption in 2022 and forecasts in millions

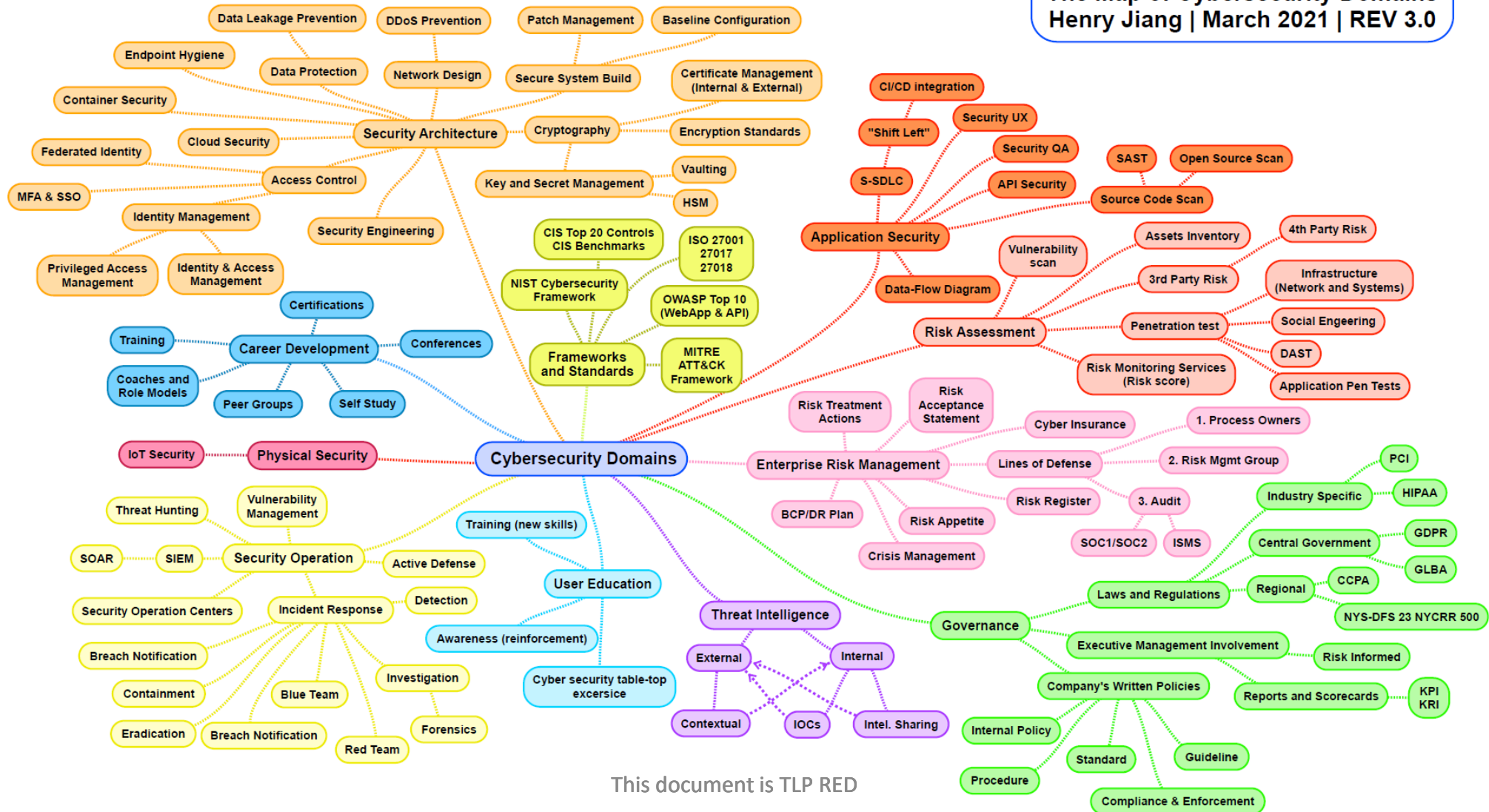


Worldwide cloud market share as of Q4/2021



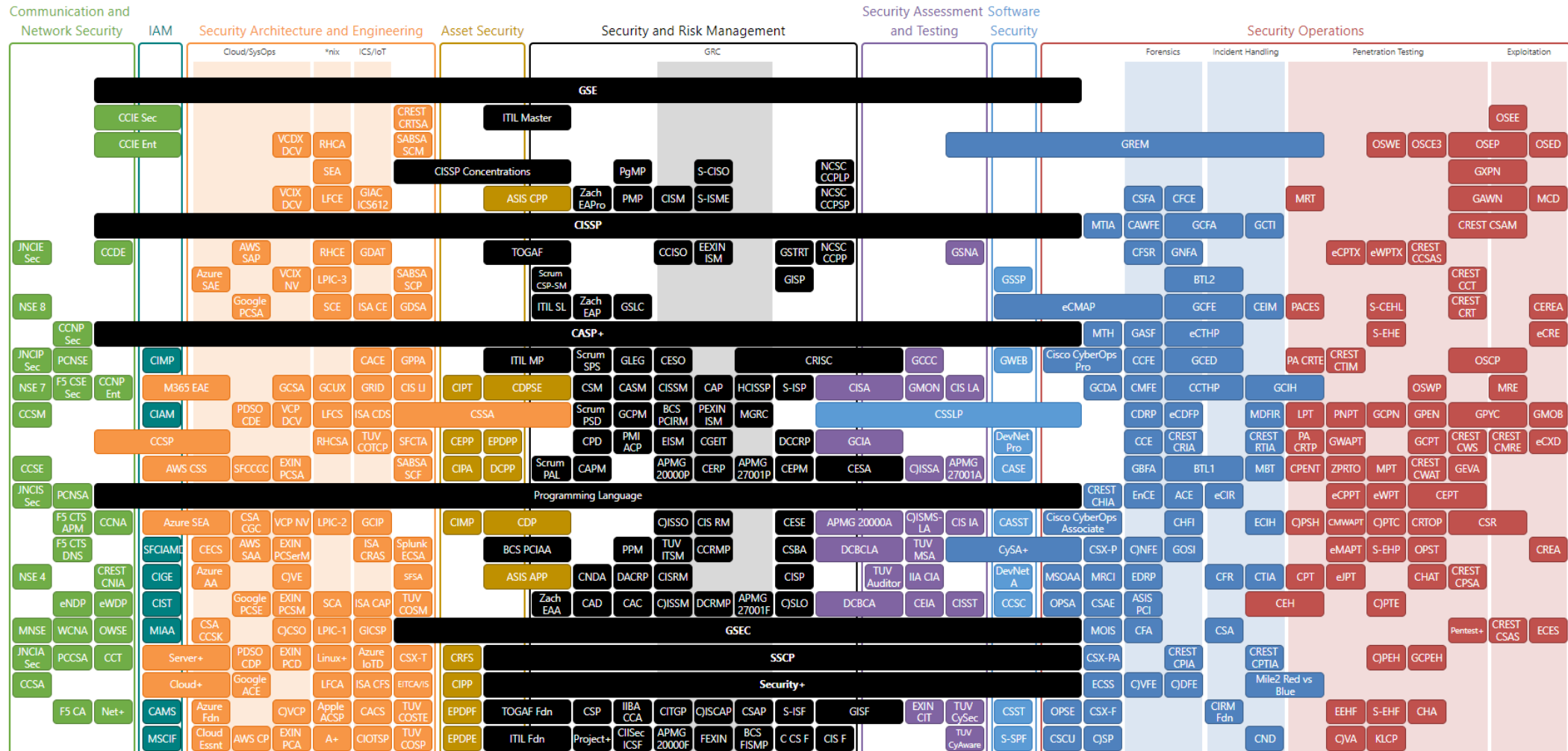
The cybersecurity domains map

The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.0



This document is TLP RED

The cybersecurity certifications map



399 certifications listed | July 2021



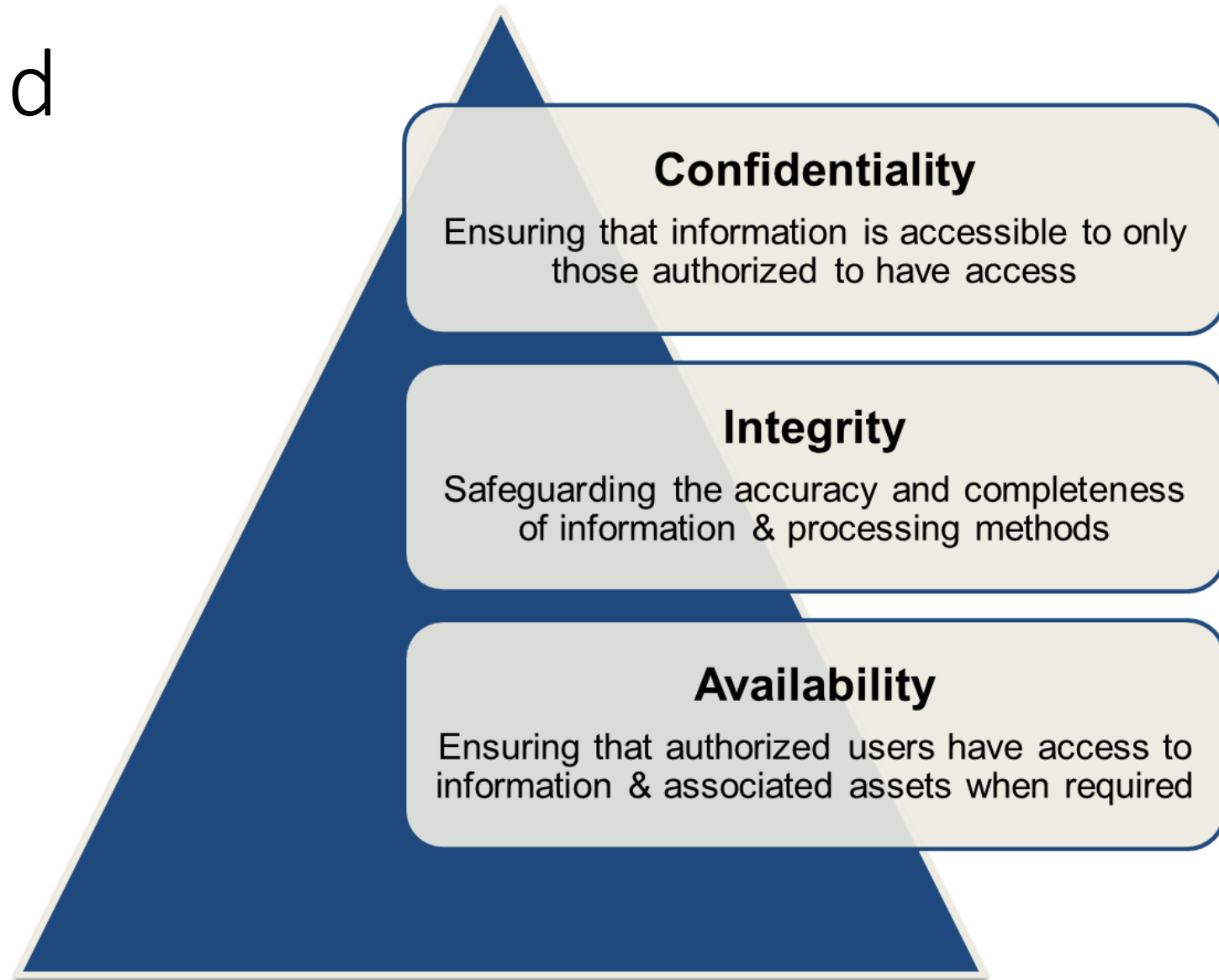
Module 1 Networks and Systems security basics

Dr. Amin Hasbini

CIA

5min: what is CIA?

The CIA triad



CIA priorities per environment

#	Enterprise IT environment	Industrial OT environment
1	Confidentiality	Availability
2	Integrity	Integrity
3	Availability	Confidentiality

AAA

5min: what is AAA? AAAA?

The AAA model

- Authentication
 - Who are you?
 - "I am user student and my password ILoveMom123 proves it"
- Authorization
 - What can you do? What can you access?
 - "User student can access host NT Server with Telnet"
- Accounting
 - What did you do? How long did you do it? How often did you do it?
 - "User student accessed host NT Server with Telnet 15 times"
- Auditing? (AAAA)

Encryption algorithms

Symmetric encryption

Symmetric and Asymmetric

5min: what is symmetric encryption?

Symmetric encryption: RC4, AES, DES, 3DES, QUA



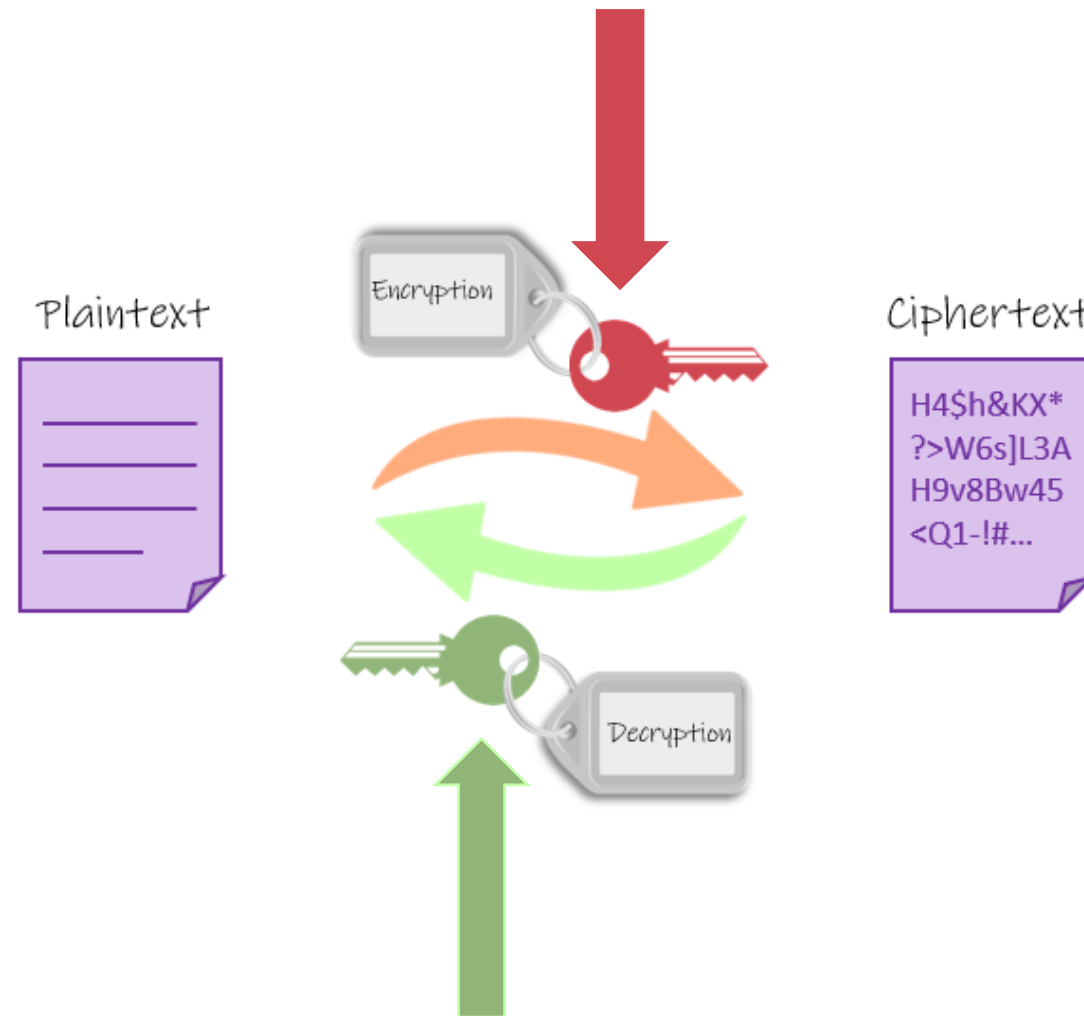
Asymmetric encryption

5min: what is asymmetric encryption?

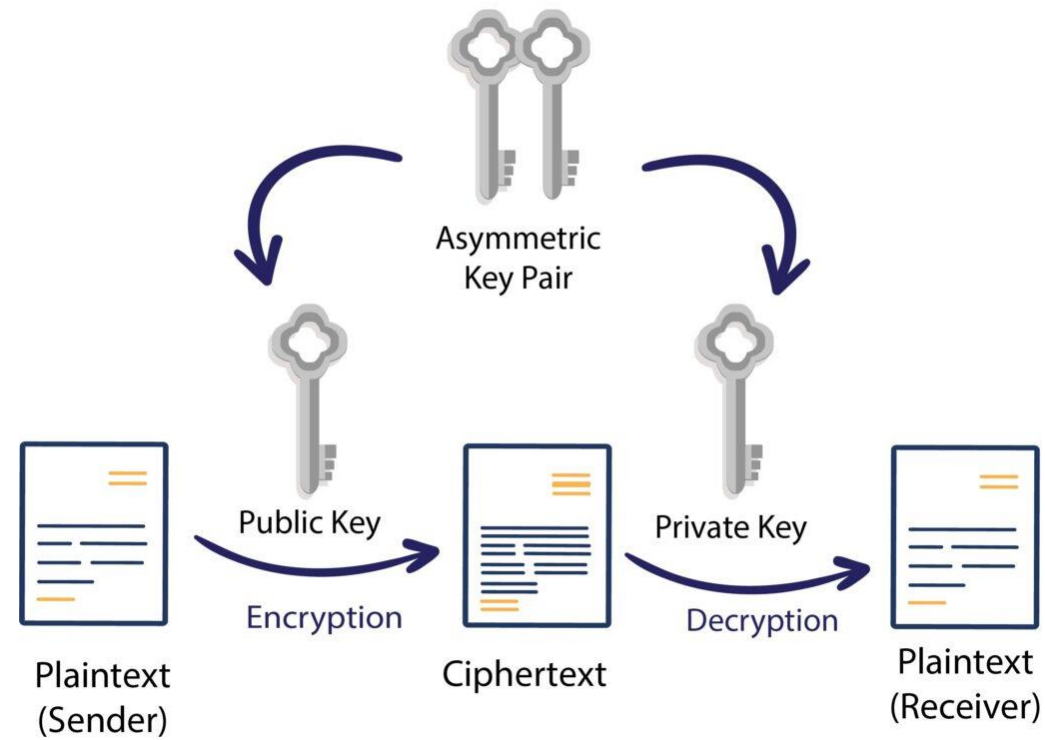
Asymmetric encryption

- Every user
 - Public key
 - Private key
- Encrypt with Public key, Decrypt with Private key => Encryption
- Encrypt with Private key, Decrypt with Public key => Signature

Examples RSA, Diffie-Hellman, ECC, El Gamal, DSA



Asymmetric Encryption



Symmetric Encryption



Asymmetric Encryption



Symmetric Vs Asymmetric algorithms

Attributes	Symmetric	Asymmetric
Keys	One key is shared between two or more entities	One entity has a public key, and the other entity has a private key
Key Exchange	Out-of-band	Symmetric key is encrypted and sent with message; thus, the key is distributed by in-bound means
Speed	Algorithm is less complex and faster	Algorithm is more complex and slower
Number of Keys	Grows exponentially as users grow	Grows linearly as users grow
Use	Bulk encryption, which means encrypting files and communication paths	Key encryption and distributing keys
Security Service Provided	Confidentiality	Confidentiality, authentication, and non-repudiation

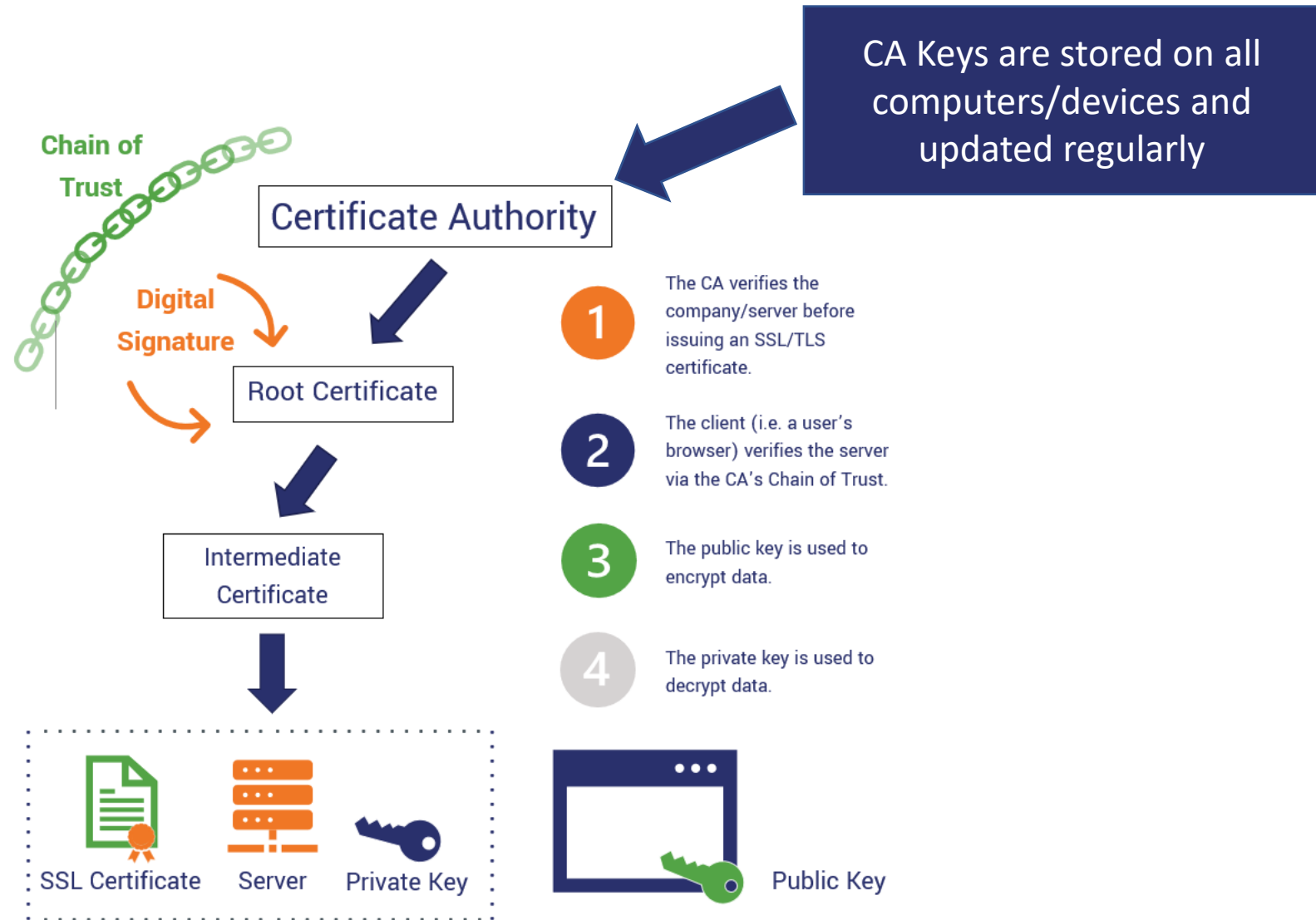
More examples => symmetric or asymmetric?

- The mailbox letters?
- HTTPS to my bank?
- Mobile app communication with my favorite shopping platform?

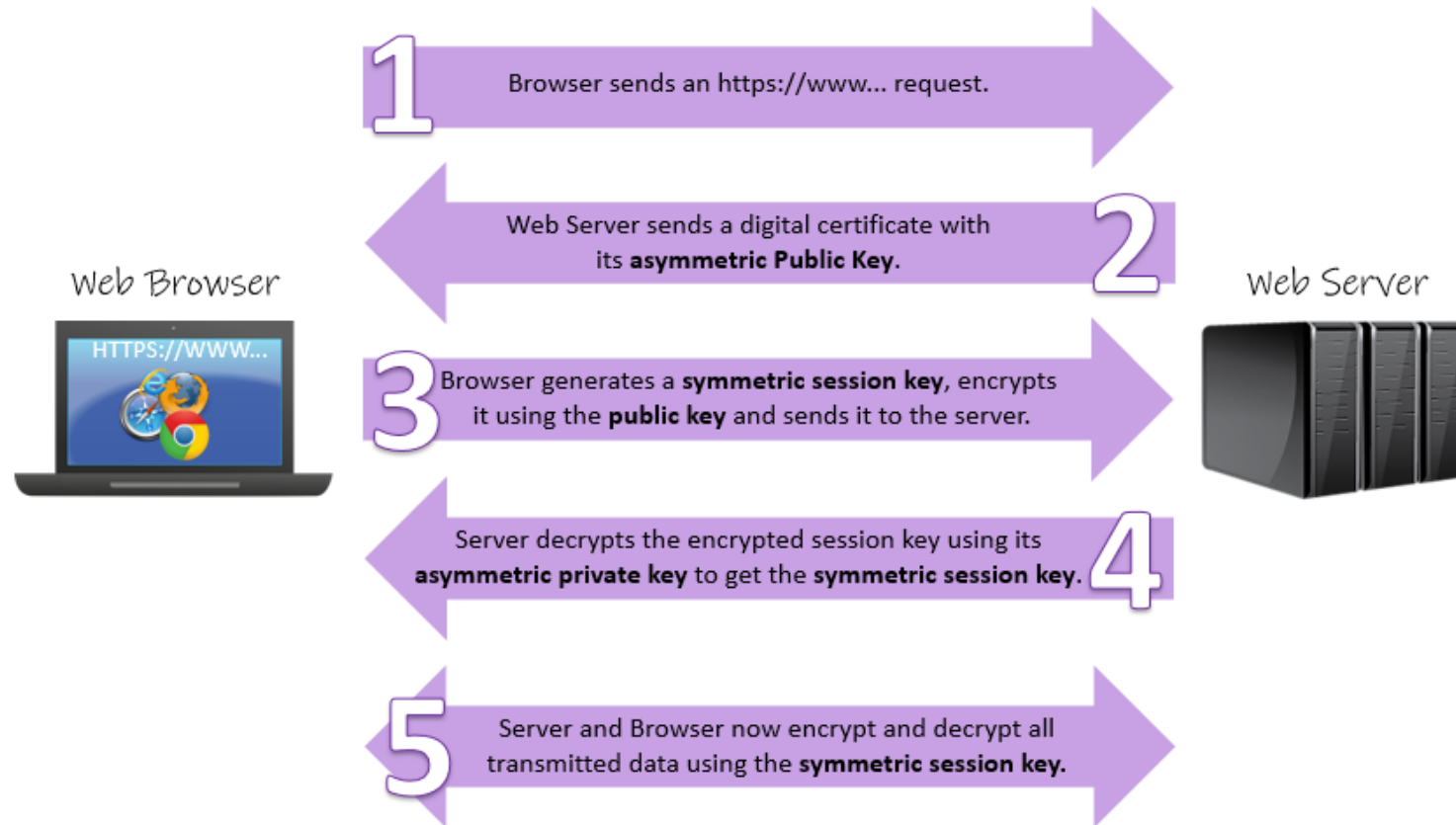
Public Key Infrastructure (PKI)

5min: what is PKI?

PKI



Example SSL/TLS handshake

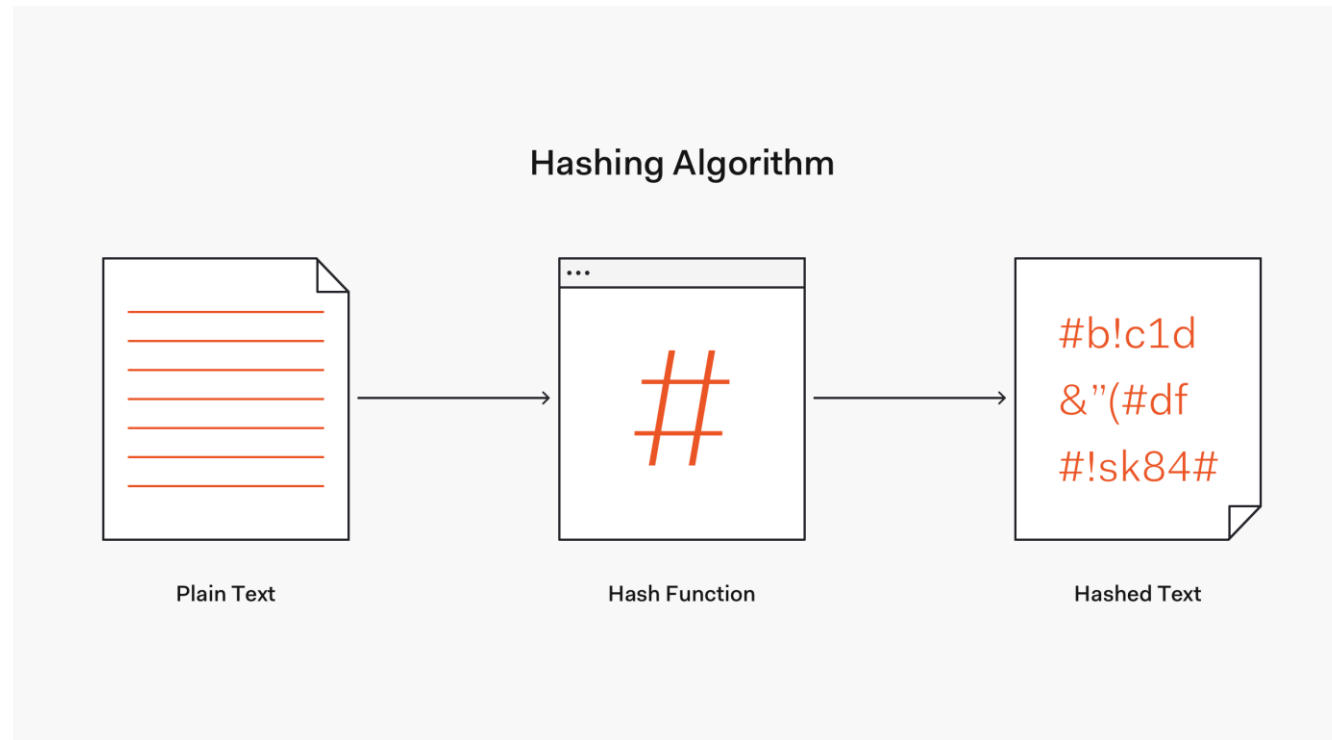


5min: How can I see the certificates store on Windows?

Hashing algorithms

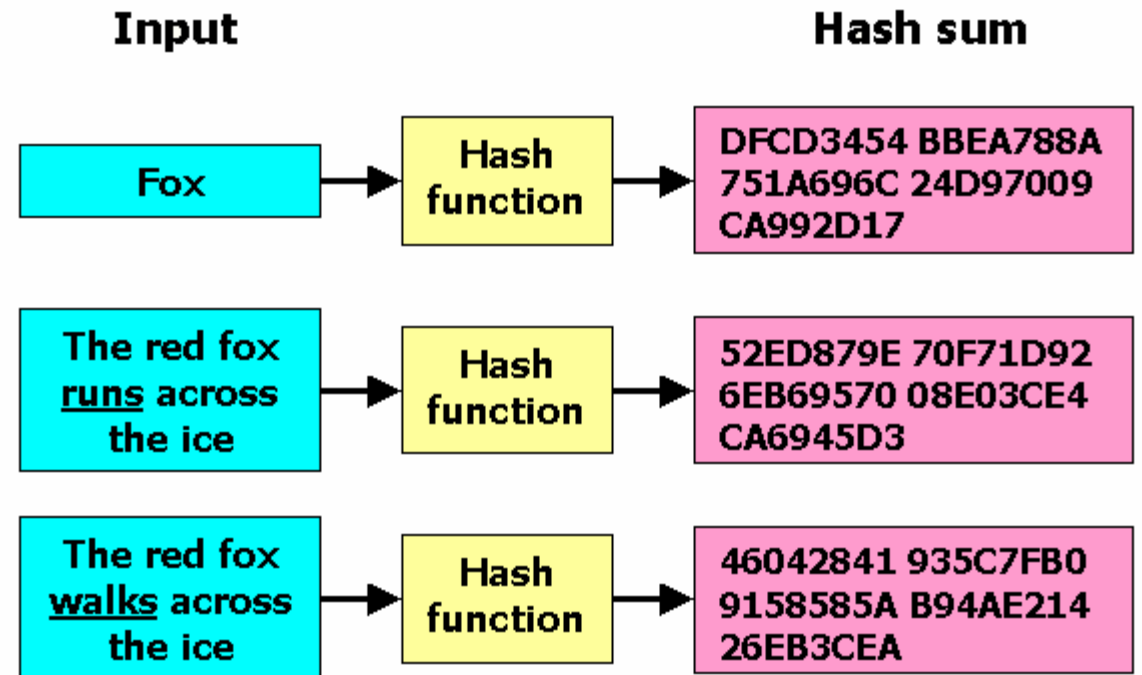
5min: what is a hash? MD5? SHA1?

Hashing algorithms



Example hashing algorithms

- MD5 = 128 bits (Designed in 1991)
- MD6 = up to 512 bits.
- SHA-1 = 160 bits.
- SHA-224 = 224 bits.
- SHA-256 = 256 bits.
- SHA-384 = 384 bits.
- Tiger = 192 bits.
- Whirlpool = 512 bits.



Example use of research hashes

- Securelist
- Virustotal!

LAB1

- Send me a PGP encrypted file
- Steps
 1. Download/run the required toolset
 2. Generate PGP key
 3. Import my PGP public key
 4. Encrypt file
 5. Send me the file
 6. Send me your PGP public key
 7. Wait for my reply

Homework

- Lab PGP 13min:
<https://drive.google.com/file/d/1NBU6zmAtBcp2Y1Fs6jtHk5NQgXGnUe0a/view>
- Additional multi-factor authentication examples for online services explained ~11min: <https://www.youtube.com/watch?v=fzUVrz0ixn8>

Need a volunteer for a Public key / Private key connection simulation



User1 wants to communicate with user2, he already has his Pub2

1. User 1 applies PGP algorithm using Pub2 => ?
2. User 1 applies PGP algorithm using Priv1 => ?
3. User 1 applies PGP algorithm using both Pub2 and Priv1 => ?

A last look at the PGP toolset

- PGP is an example implementation of public key / private key
- PGP Integration
- PGP and cloud?

<https://gnupg.org/software/swlist.html>

A last look on the critical role of PKI and CAs

- DM
- RU

Any last questions?

CIA, AAA, AAAA

Encryption, Hashing, Public key/Private key, PKI

Main cybersecurity organizational concepts

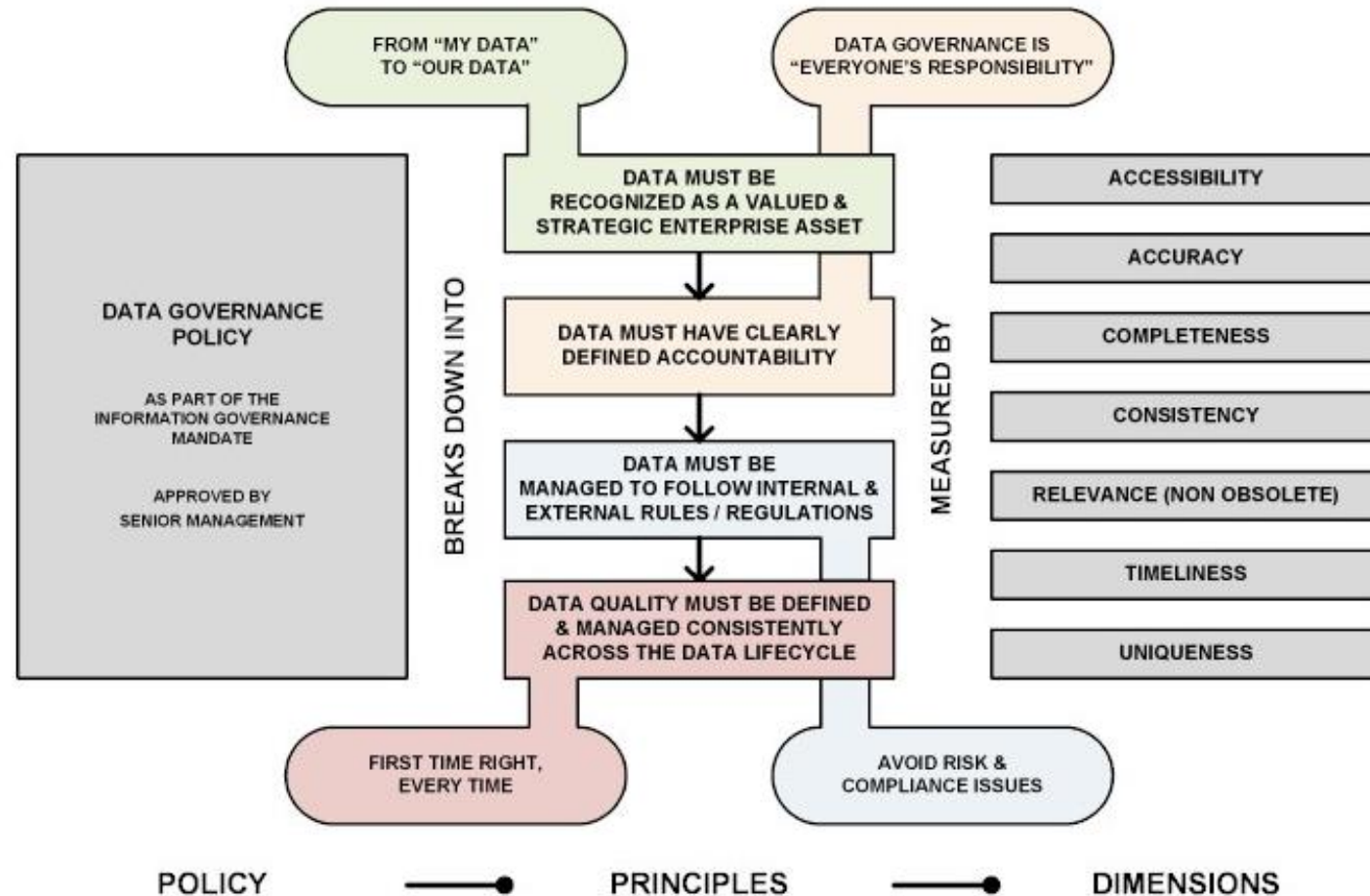
Data Protection (e.g. GDPR)

- Lawfulness, fairness, and transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

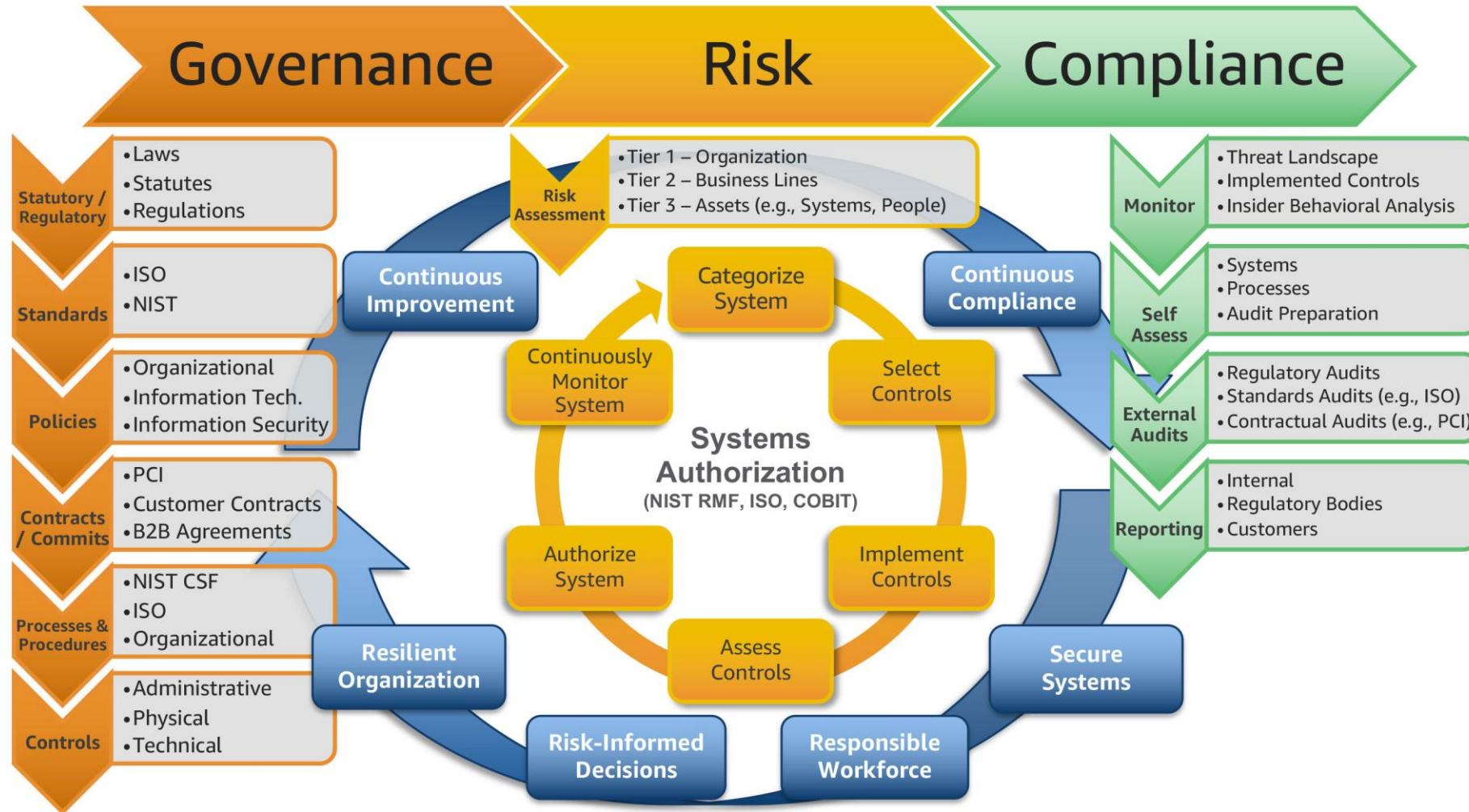
Data governance

- Recognizing data as an asset
- Data ownership and accountability
- Following standardized rules and regulations
- Managing data quality consistently
- Change management
- Data audit

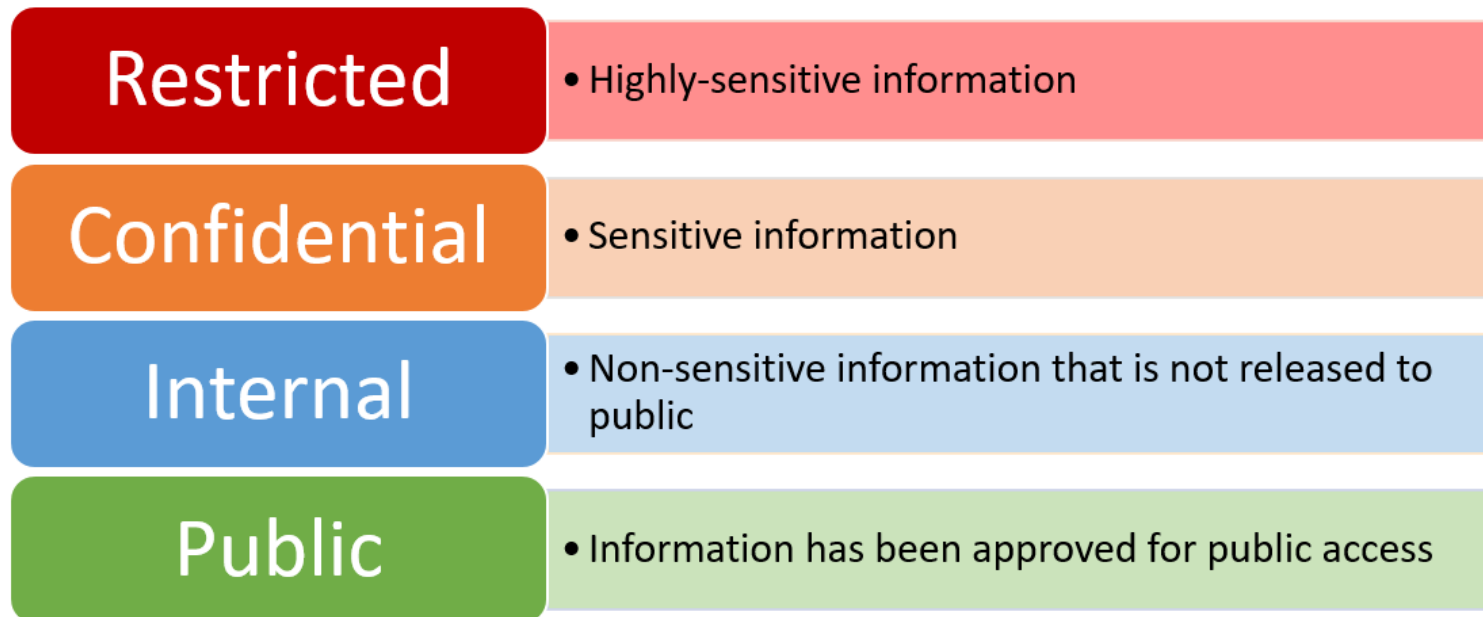
Data governance policy example



Risk and Compliance



Data classification



<https://newsletter.icto.um.edu.mo/data-classification-and-you/>

Identity and access management (IAM)

- Single Identity (one record per person in the Person Registry)
- Single Credential (one username and password per identity)
- Standards based
- Platform agnostic
- Secure
- Highly Available
- Logging and Auditable Transactions
- Measurable performance metrics

IAM example technologies

- MFA Multifactor authentication
- OTP One time passwords (SMS/APP/Token...)
- SSO Single Sign On

Monitoring and operations

Security operations center (SOC)

SOC manager: Supervises the SOC team and reports to the chief information security officer (CISO)

Security analyst: Provides real-time risk management and security intelligence

SIEM engineer: Oversees SIEM (security information and event management) administration, incident response, and vendor management

Forensic investigator: Analyzes incident data, evidence, and behavior analytics

Incident responder: Conducts initial investigations and threat assessments using incident response plans (IRPs)

Compliance auditor: Ensures SOC procedures remain in compliance with government regulations and industry standards



Vulnerability assessment and management

- **Step 1: Discover:** Identify and map all of your assets across all of your computing environments
- **Step 2: Assess:** Understand exposure of all of your assets including vulnerabilities, misconfigurations and other security health indicators
- **Step 3: Prioritize:** Understand your exposures with context so you can prioritize remediation based on asset criticality, vulnerability severity and threat context
- **Step 4: Remediate:** Prioritize which exposures to address first and then use the appropriate remediation process
- **Step 5: Measure:** Measure and then benchmark your exposure so your teams can make better business and technology-related decisions

Incident response and digital forensics - process

- **Acquisition:** In this step, investigators create an exact duplicate of the media in question, usually using a hard drive duplicator or specialized software tools. The original media is secured to prevent any tampering.
- **Analysis:** Forensic specialists then analyze the duplicated files or technology, logging all the evidence they discover that supports or contradicts a hypothesis. Ongoing analysis is conducted to reconstruct events and actions in an incident, helping them reach conclusions about what happened and how hackers compromised systems.
- **Reporting:** Once a digital forensics investigation is completed, the findings and conclusions analysts uncovered are delivered in a report that non-technical personnel can understand. These reports are passed on to those who commissioned the investigation, and usually wind up in the hands of law enforcement.

Incident response and digital forensics - Evidence

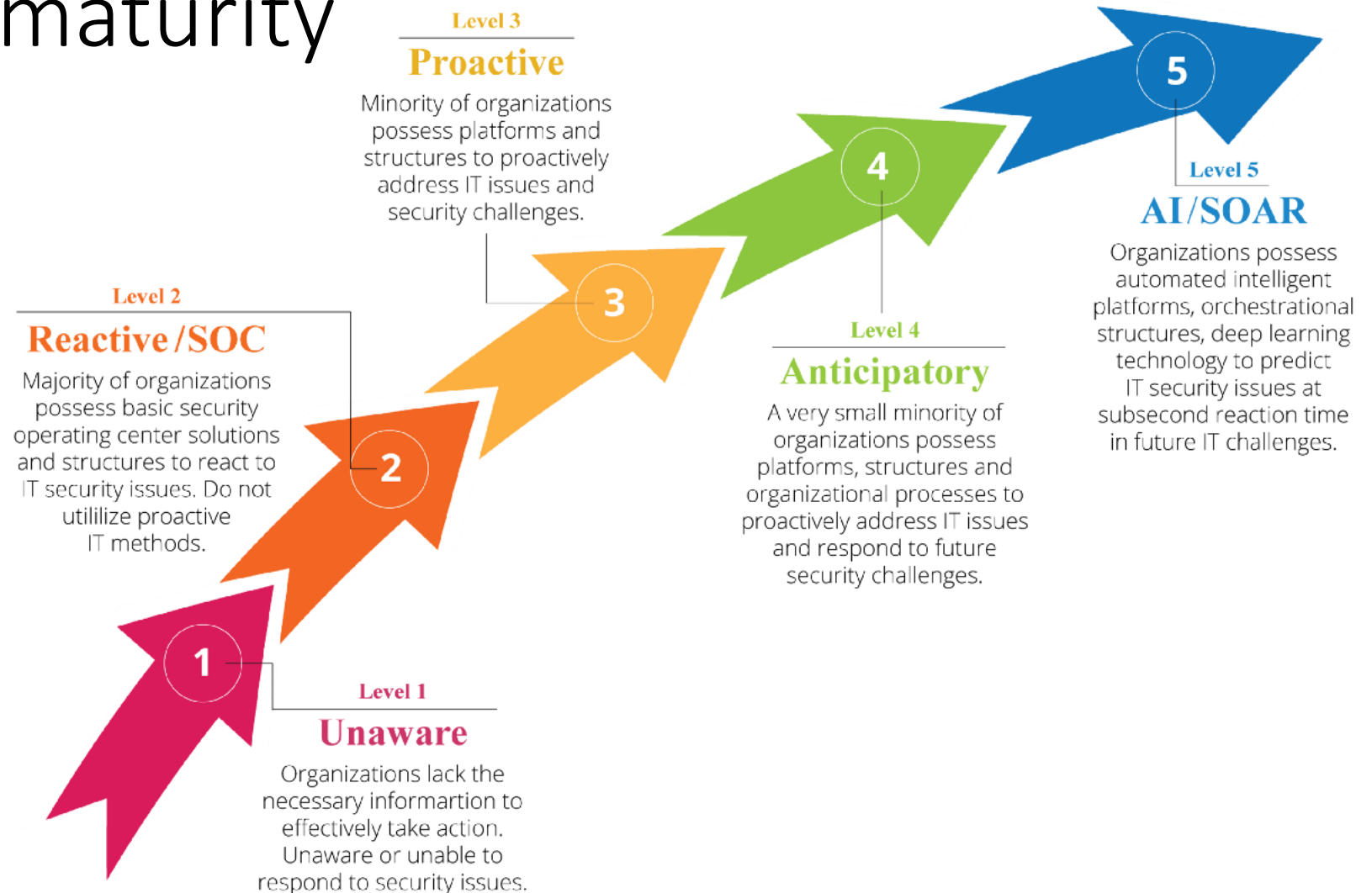
- It is admissible in court
- It is authentic
- It is complete
- It is reliable
- It is believable

Orchestration and Instrumentation- Cybersecurity maturity

- Low maturity

SOC: security operations center

SOAR: security, orchestration,
automation, response



Other main cybersecurity Hardware and software concepts

Endpoint security

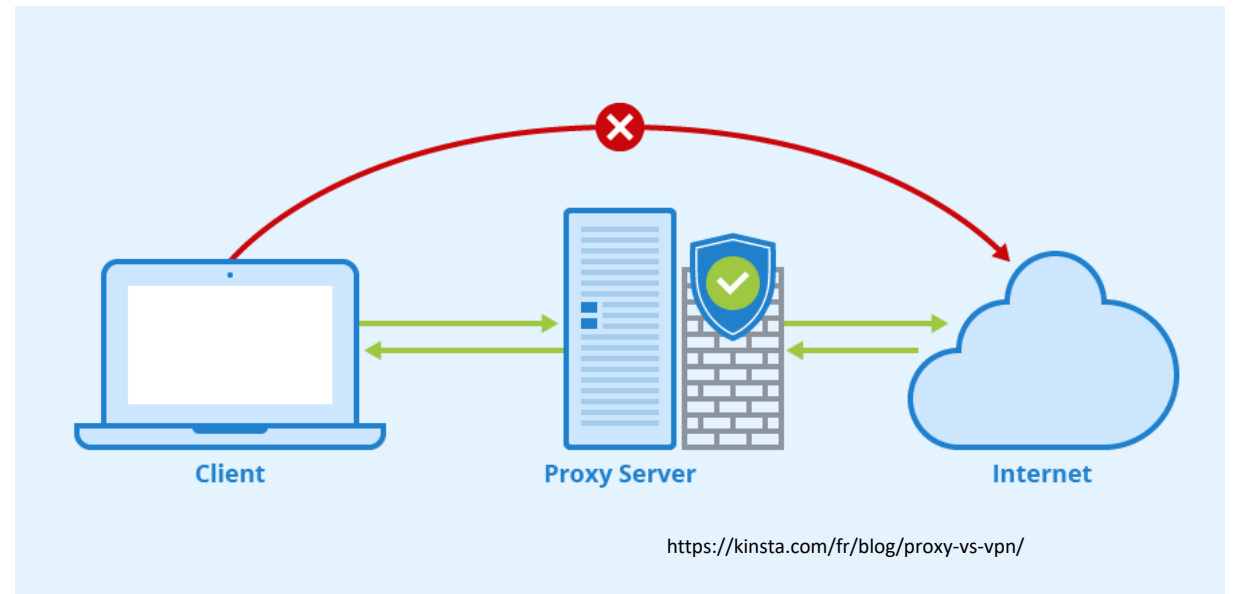
- File security
- Web security
- Email security
- Mobile security
- Heuristic security (usage of online resources)
- Cloud-based security
- Application control, whitelisting
- Memory anti-exploitation techniques
- Anti-fraud, risk compliance
- Patch and vulnerability management
- Firewall, network security
- Password manager, parental control...

Network security

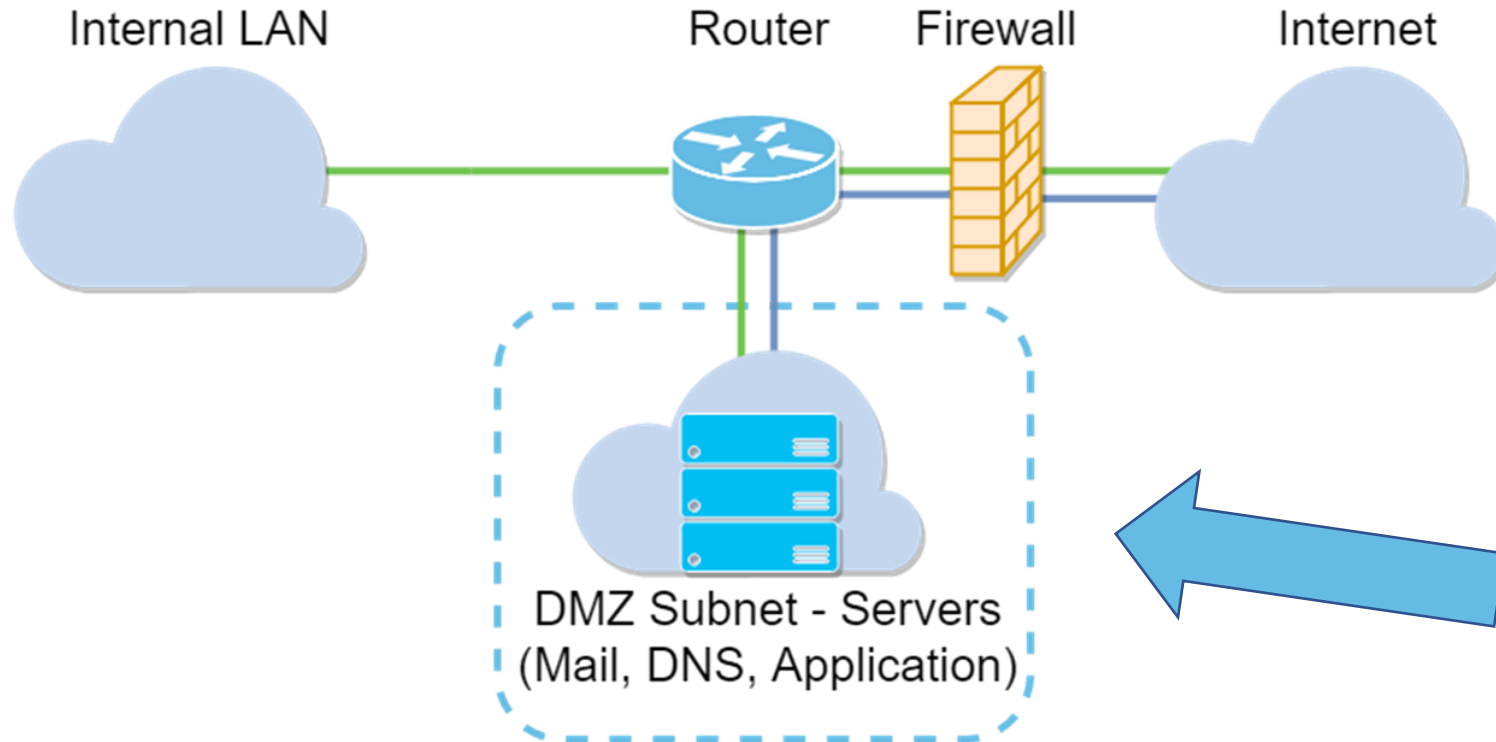
- Denial of service /Distributed (DoS/DDoS)
- Scanners
- Enterprise Proxy services
- Man in the middle (MITM)
- Switching security, spanning-tree, ARP-injection
- Routing security, BGP...
- Wireless security, jamming, encryption, authentication, authorization...

Proxy

- Control internet usage
- Bandwidth control
- Privacy/Security
- Data leak prevention
- Data monitoring and logging



Firewall



DMZ: Demilitarized Zone, services partially accessible from outside/internet

Small test:

demoui.asus.com

[fortigate.fortidemo.com \(demo/demo\)](http://fortigate.fortidemo.com/demo/demo)

VPN (Virtual private network)

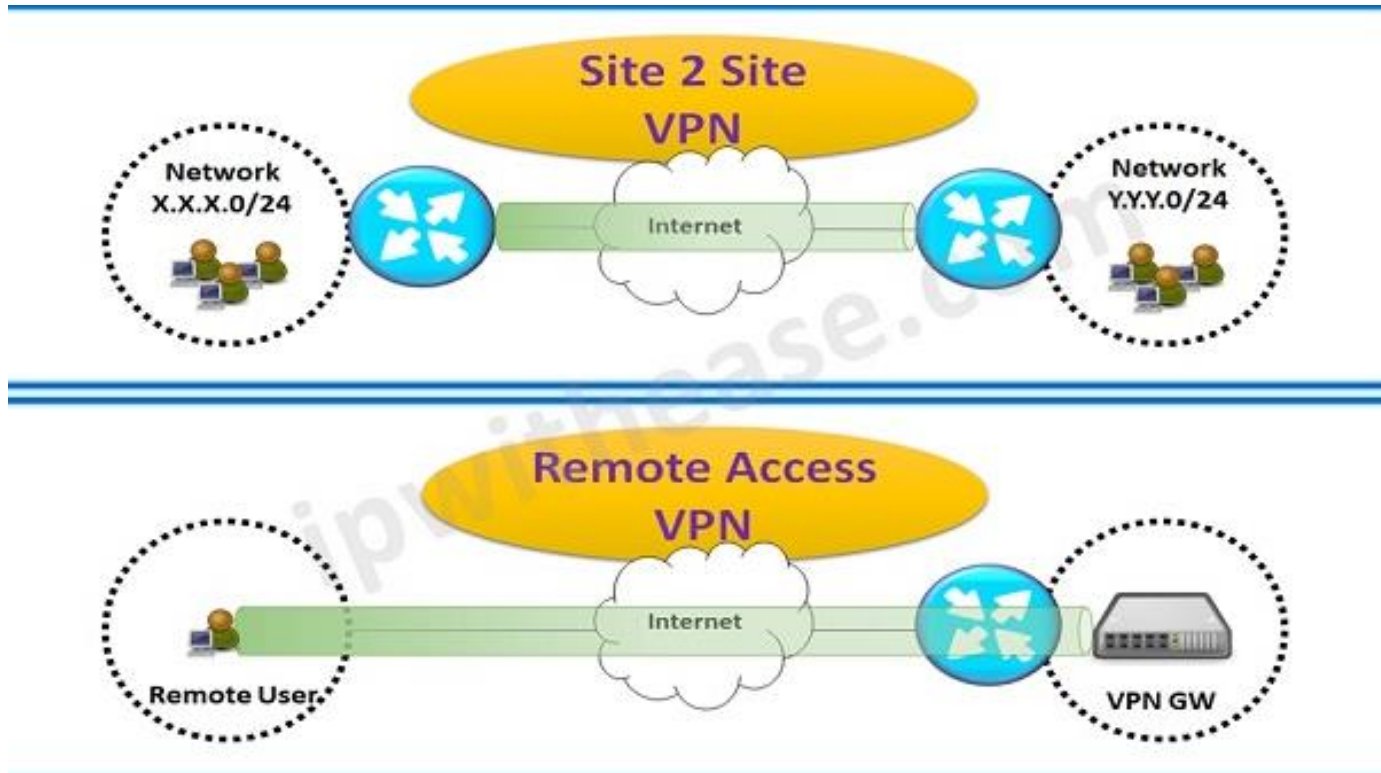


<https://community.fs.com/fr/blog/what-is-vpn-router-and-why-you-need-it.html>

This document is TLP RED

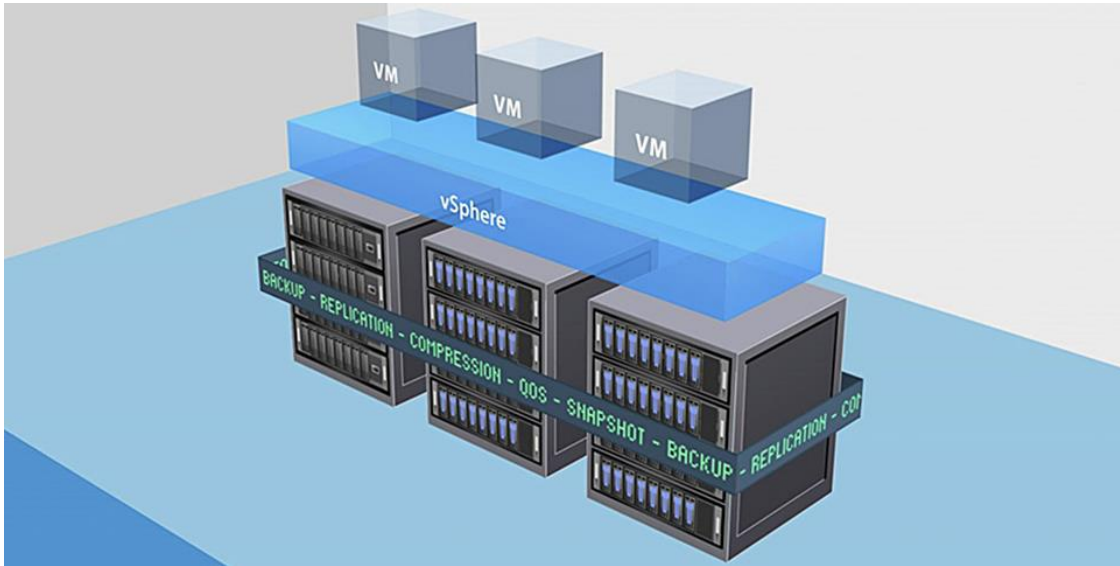
Small test:
demoui.asus.com
fortigate.fortidemo.com (demo/demo)

Site-to-site Vs remote access VPN



Datacenter security

- Virtualization security
- Virtual firewalls/switches/routers

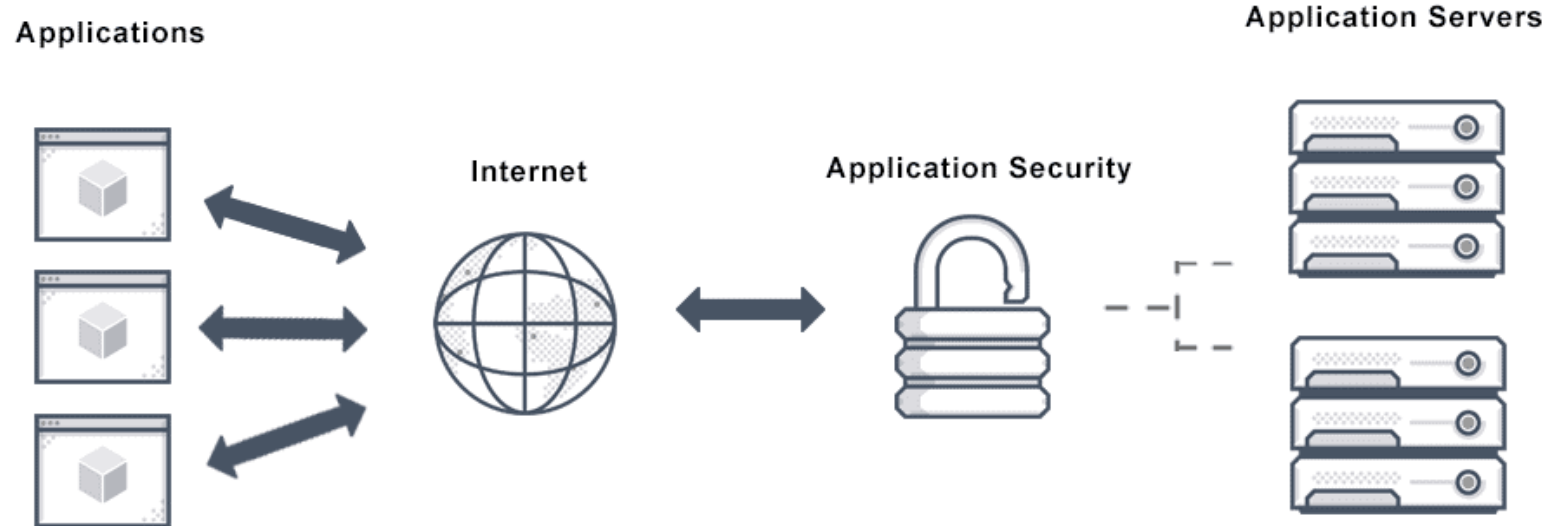


<https://www.vmware.com/fr/products/vsphere/data-center-consolidation.html>



<https://www.fs.com>

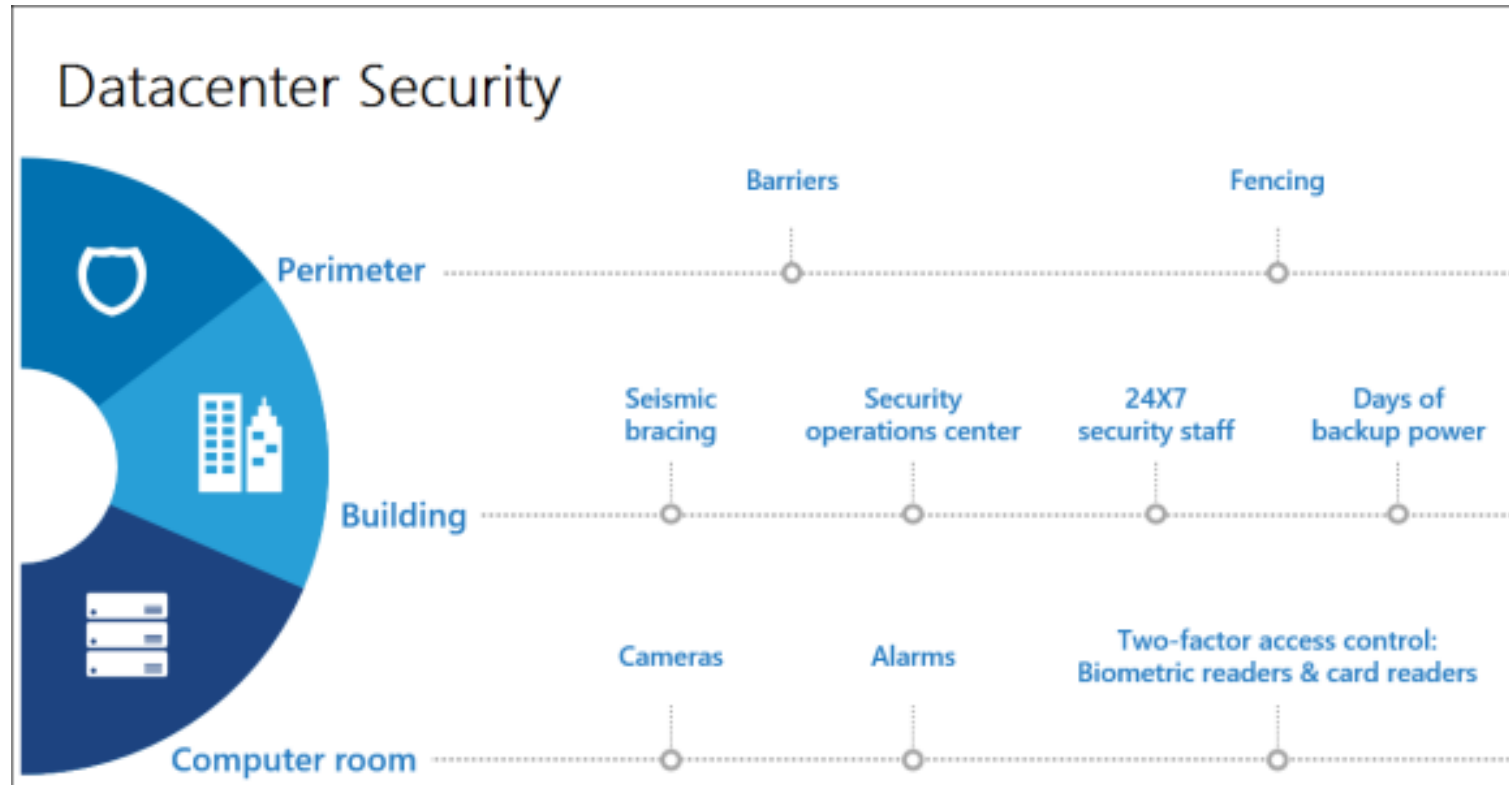
Software and application security



<https://avinetworks.com/glossary/application-security/>

This document is TLP RED

Physical security



+Cooling
+Fire prevention

<https://expertslab.wordpress.com/2017/07/10/physical-security/>

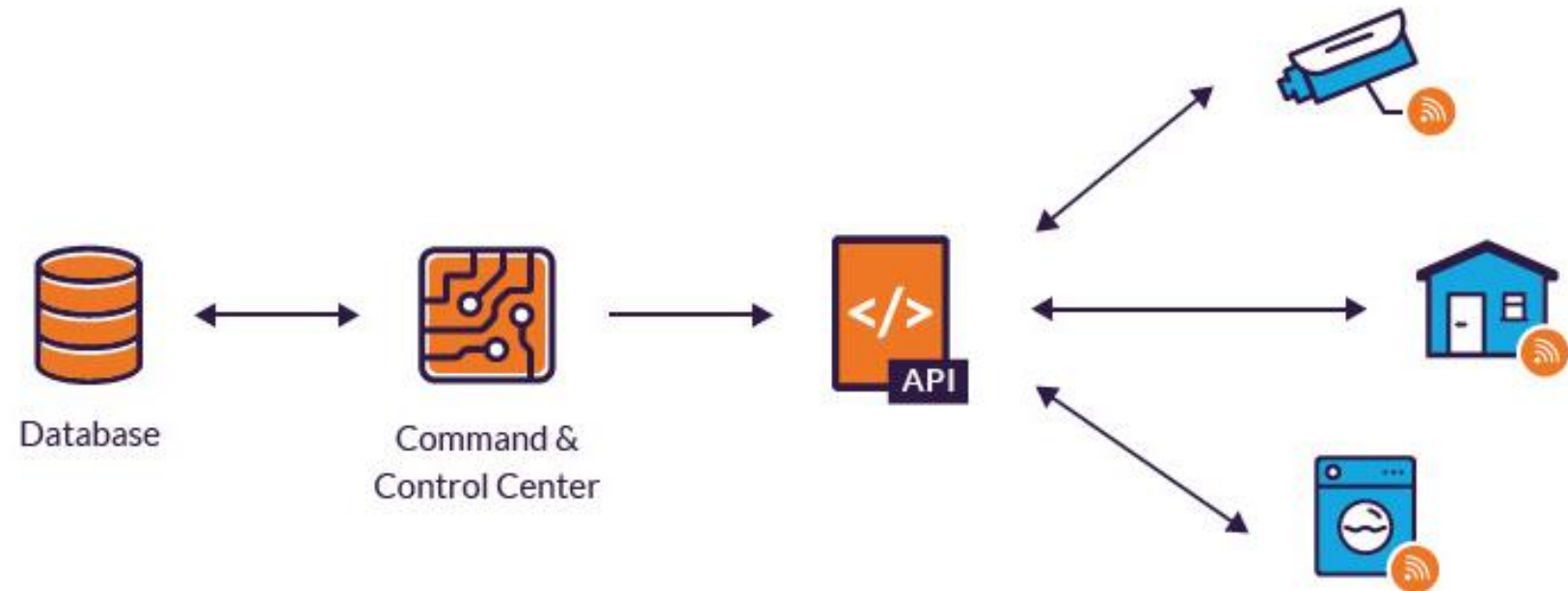
Disaster recovery planning

- Plan, Policy
- Procedures
- Controls
- Testing



IoT security

- Low maturity domain



<https://www.imperva.com/learn/application-security/iot-internet-of-things-security/>

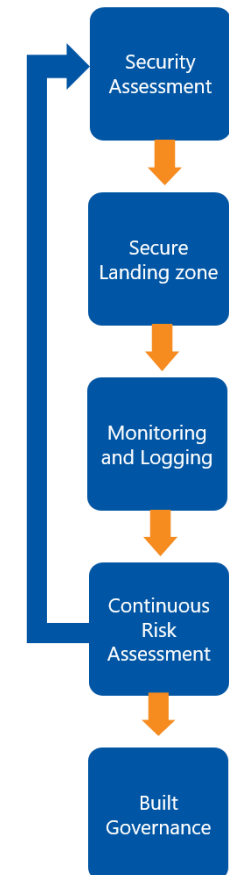
Cloud security

- Low maturity domain



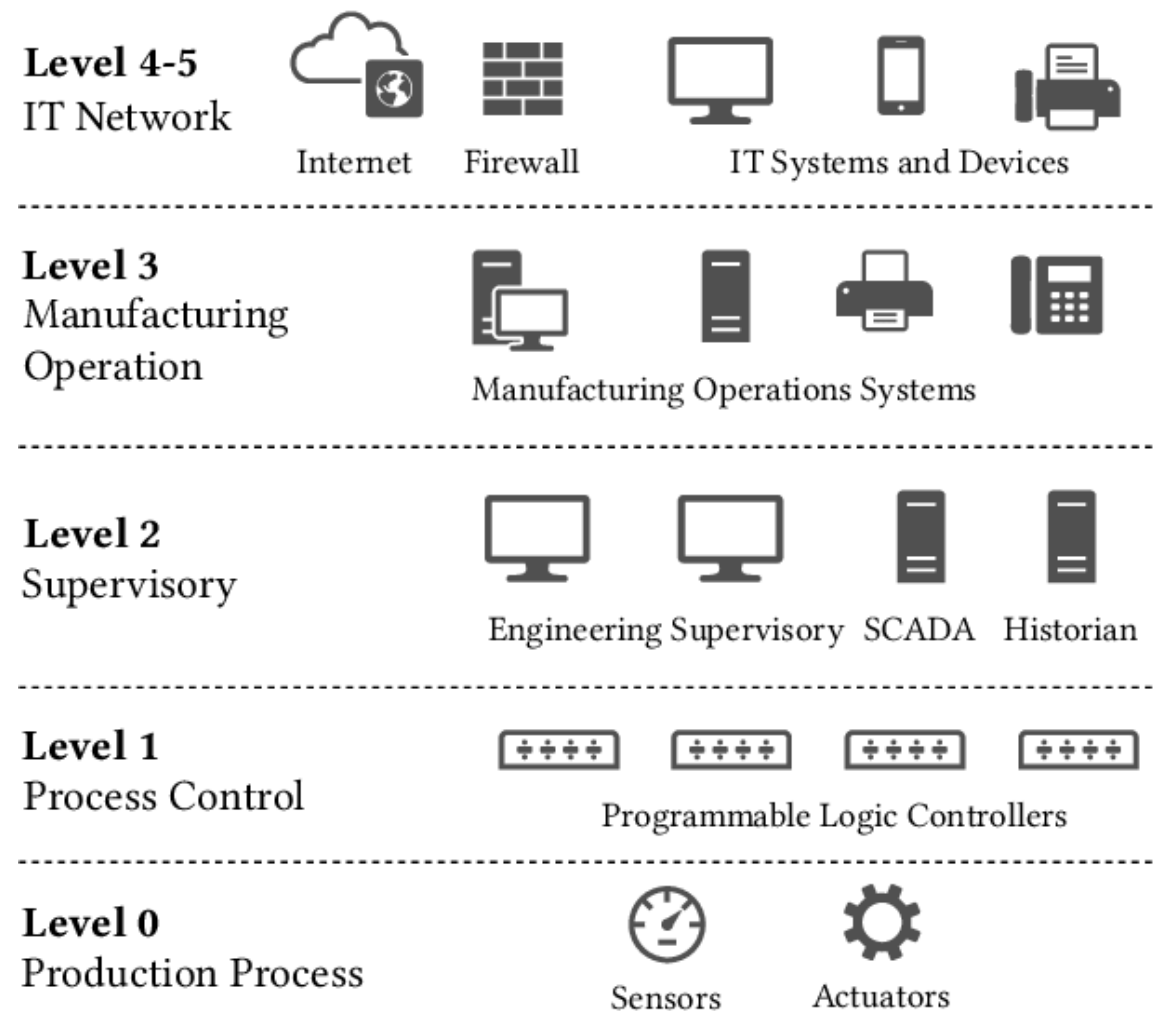
1	- MULTI FACTOR AUTHENTICATION - ZERO TRUST MODEL	- IAM POLICY - CONDITIONAL ACCESS
2	- ACCESS CONTROL - AWARENESS TRAINING	- IAM ROLES AND GROUPS - INFORMATION CLASSIFICATION & PROTECTION
3	- PROTECTIVE TECHNOLOGIES - DETECTION PROCESS	- AUDIT REPORTS - REGULAR PATCH MANAGEMENT
4	- GOVERNANCE - RISK MANAGEMENT STRATEGY	- ANOMALIES AND EVENTS - THREAT DETECTION
5	- ASSETS MANAGEMENT - BUSINESS ENVIRONMENT	- RISK ASSESSMENT - CONTINUOUS MONITORING AND ALERTS
6	- ENCRYPTED VOLUMES - KEY MANAGEMENT SYSTEM	- ENCRYPTION FOR VPN - PROXY, NAT GATEWAYS, LOAD BALANCERS
7	- THREAT PREVENTION - RISK AND COMPLIANCE	- OS HARDENING - REGULAR SECURITY UPDATES
8	- SEGREGATED NETWORK WITH UNIQUE ROUTING - ENVIRONMENT SEGMENTATIONS	- NOC AND SOC SEGMENTATIONS - FIREWALL AND DMZ

Implementation Approach

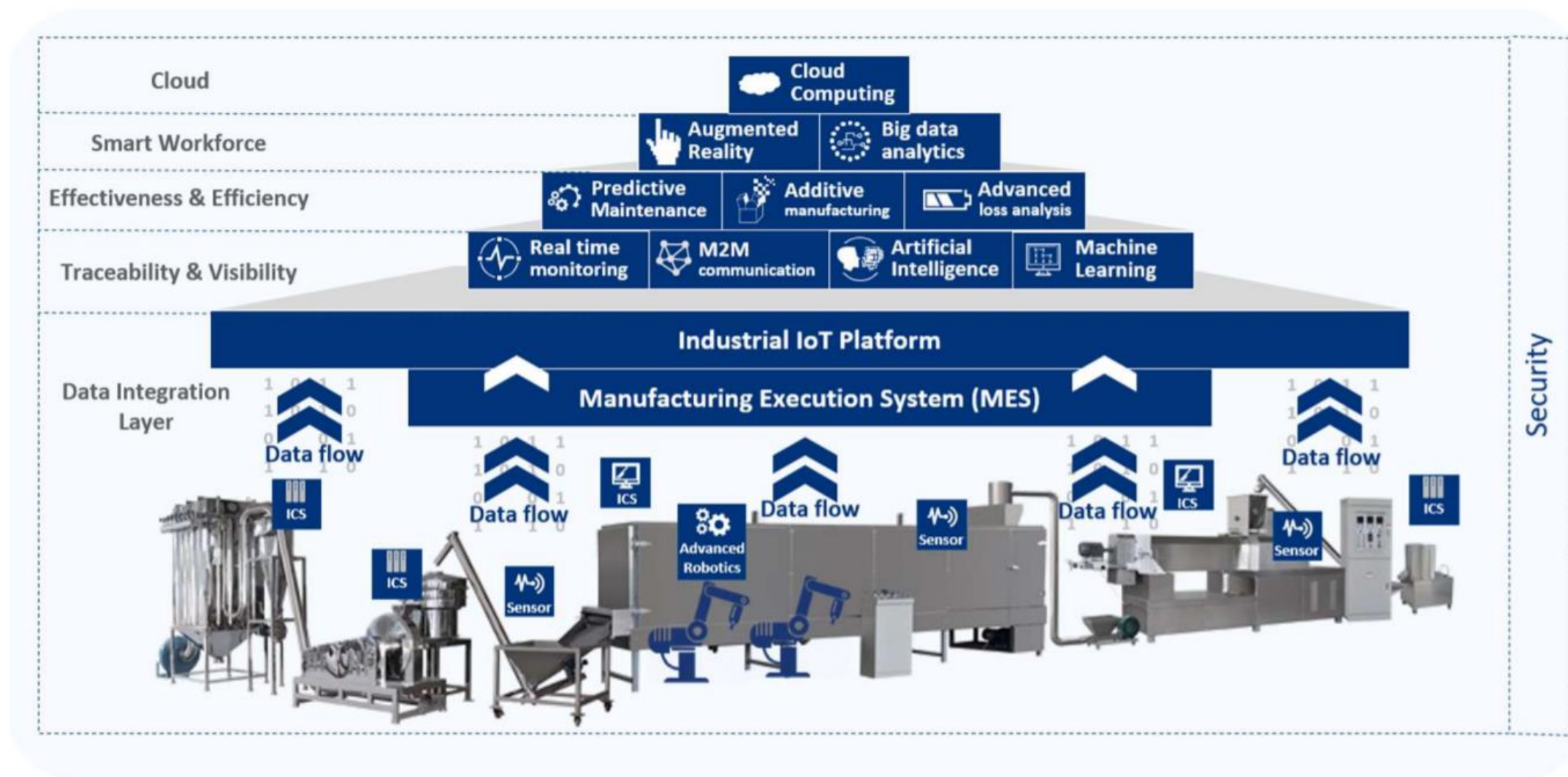


Industrial security

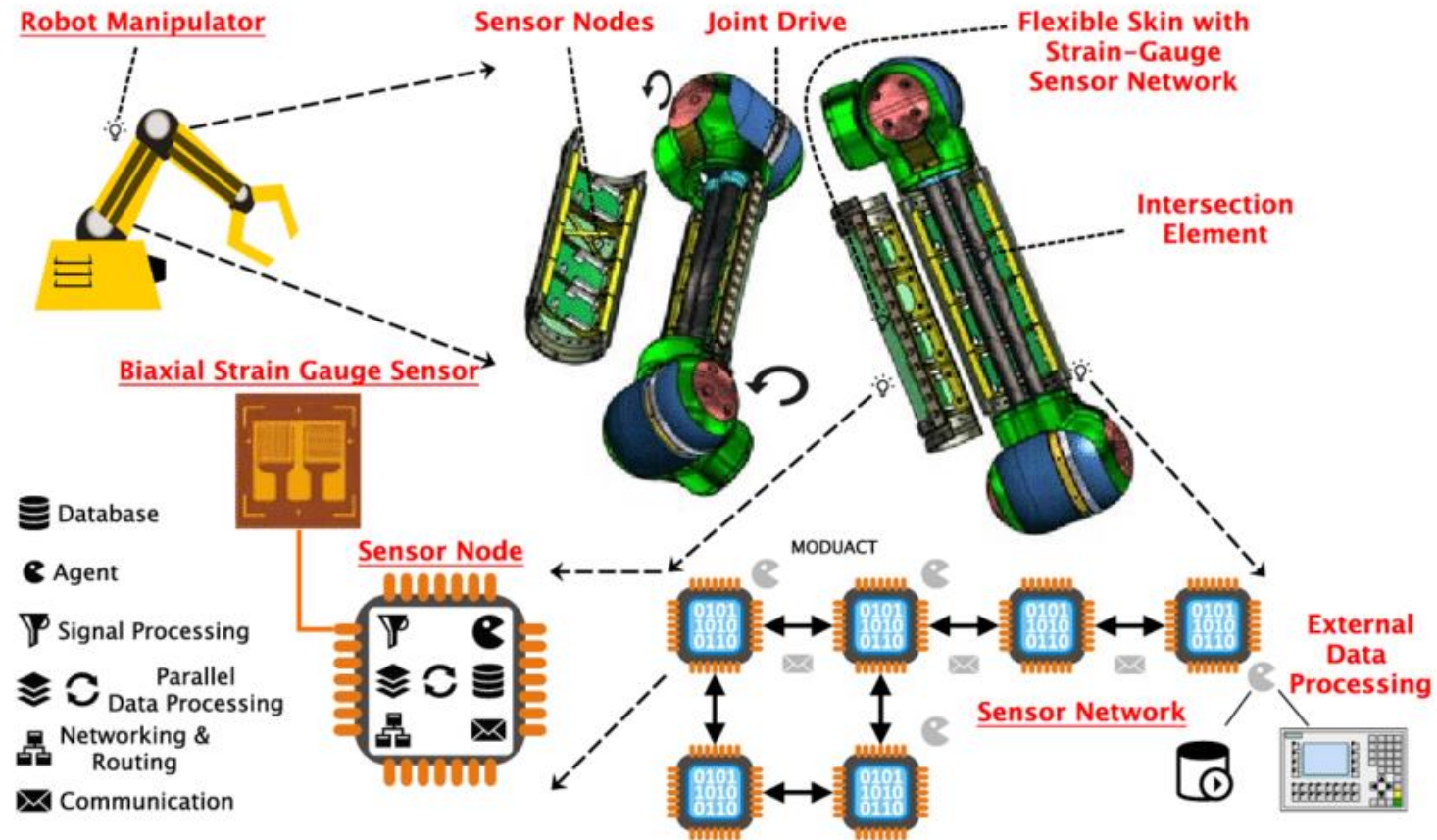
- Low maturity domain



Industrial IOT / IIOT security

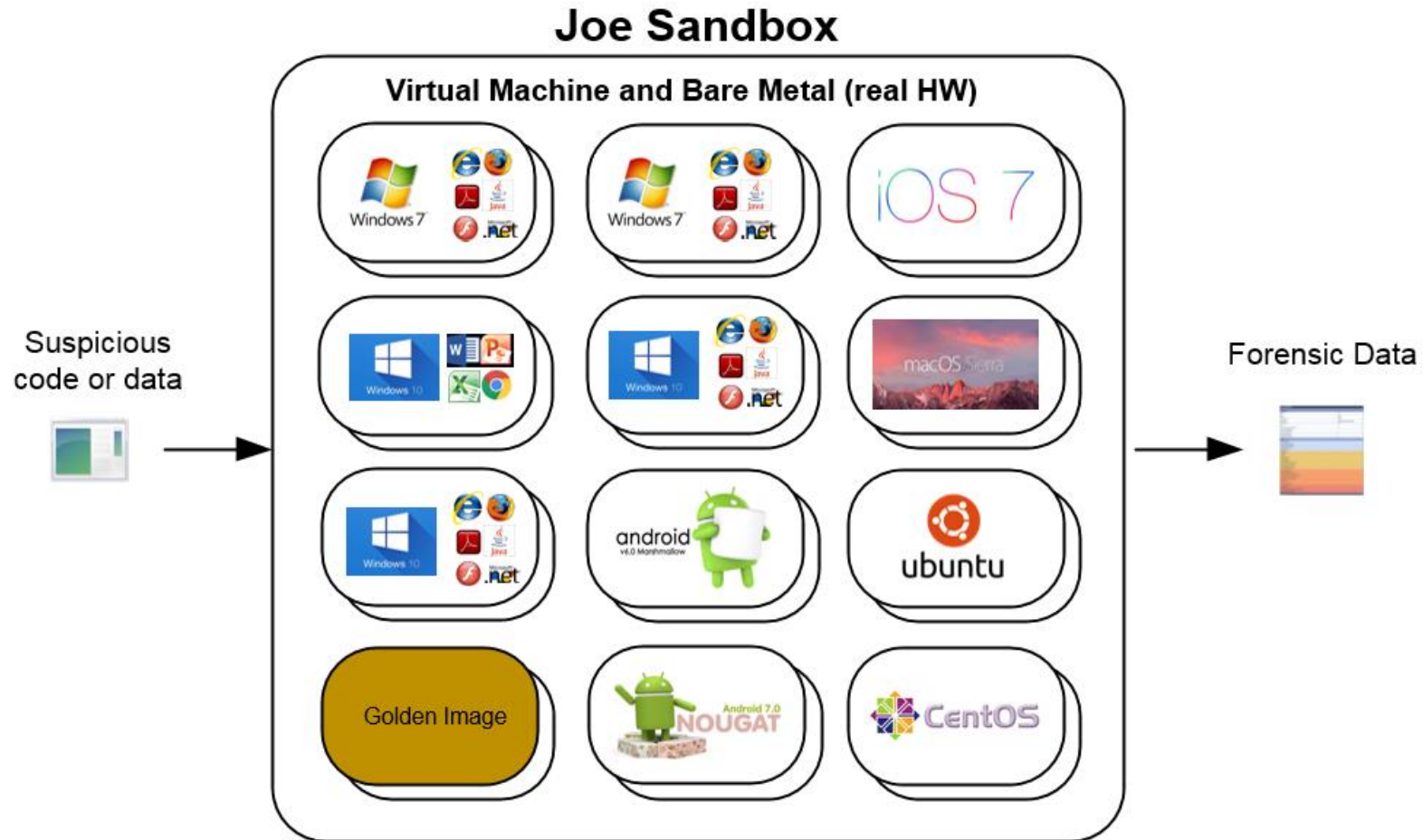


Securing a robotic arm



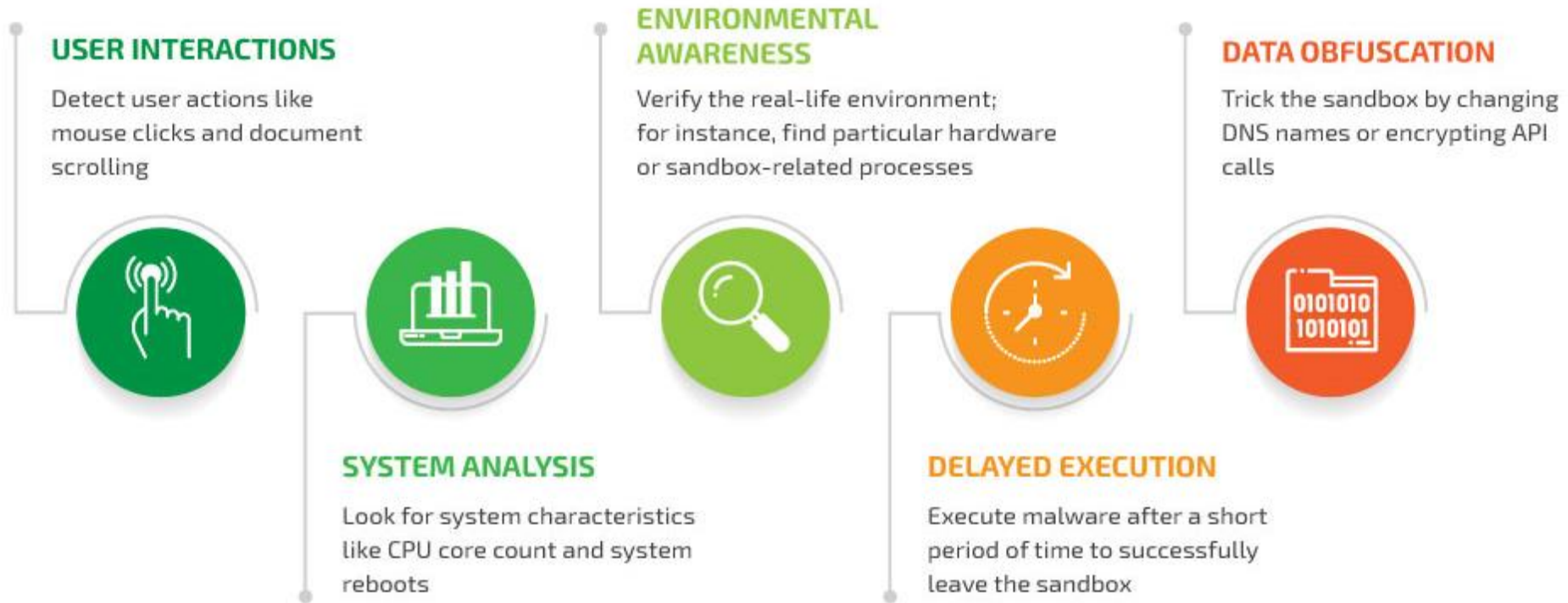
Additional important concepts

Sandboxing and malware analysis



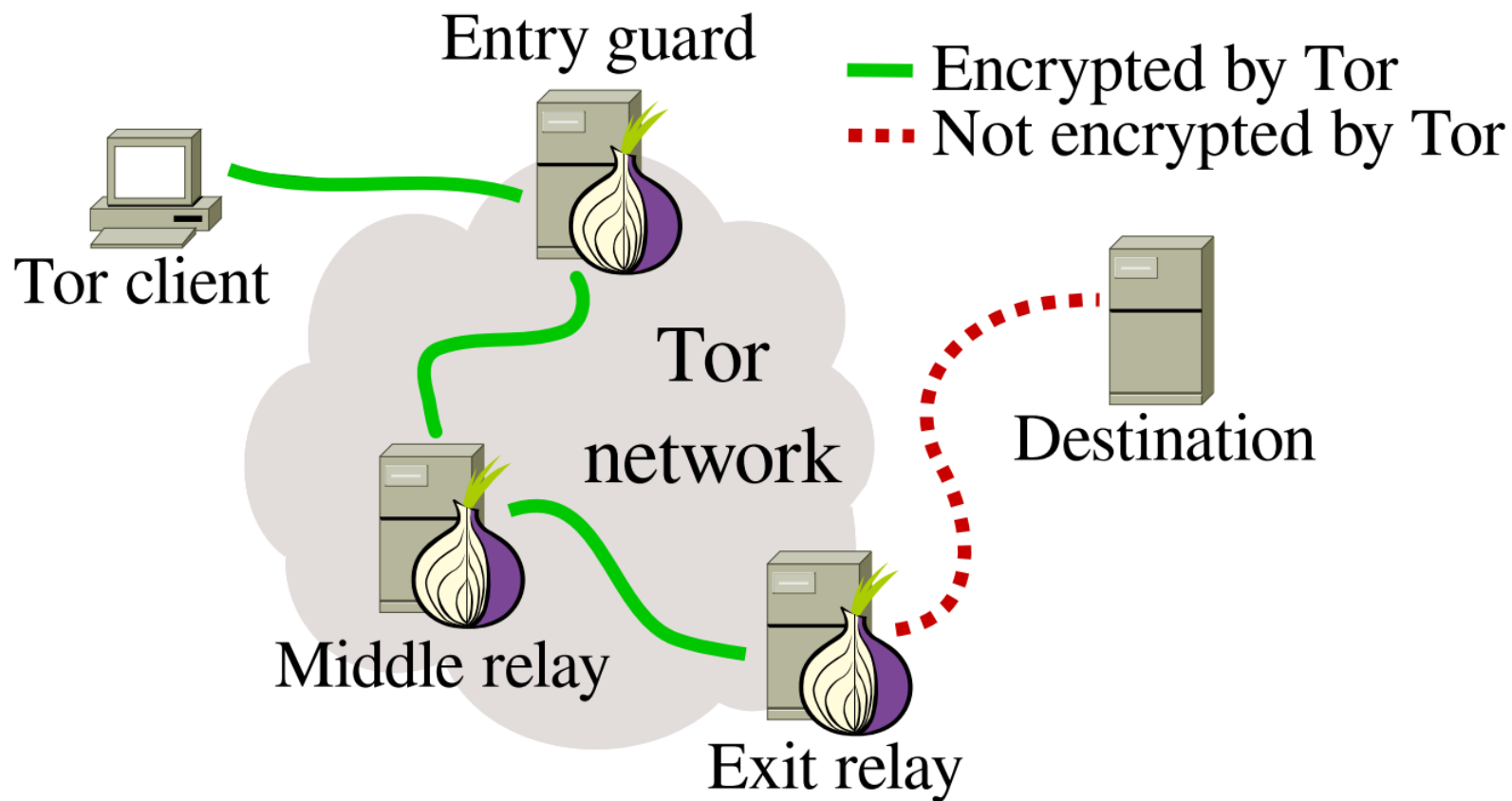
Test:
app.any.run
hybrid-analysis.com
Joe sandbox
Cuckoo sandbox

Sandbox evasion techniques [?]



www.apriorit.com

Onion routing / Darknets / TOR



Darknet sites XYZ.onion

<https://twitter3e4tixl4xyajtrzo62zg5vztmjuricljdp2c5kshju4avvoid.onion>

ETC

- Wireless security
- Hardware security
- Firmware security

Systems hardening

Examples of systems hardening

Servers	Operating systems	Applications	Databases
■ Install all security patches ■ Two different network interfaces ■ Keep backups of all data and files	■ Install latest service packs ■ File and file system encryption ■ Run services with least privileged accounts	■ Install all security patches ■ Implement an SSL architecture ■ Install a web application firewall	■ Locking and expiring unused accounts ■ Role-based access control privileges ■ Perform periodic data-base security audits

<https://www.techtarget.com/searchcio/tip/What-CIOs-need-to-know-about-hardening-IT-infrastructure>

Business cybersecurity needs, role of CISO/CSO

Wikipedia: A chief information security officer (CISO) is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

Role

- Advising on all forms of cyber risk and plans to address them
- Board, management team, and security team coaching
- Vendor product and service evaluation and selection
- Maturity modeling operations and engineering team processes, capability and skills
- Board and management team briefings and updates
- Operating and Capital budget planning and review, ROSI (Return on security investment)

CISO in case of incident

- Correct handling
- Fast response
- Continuous updates to the important stakeholders

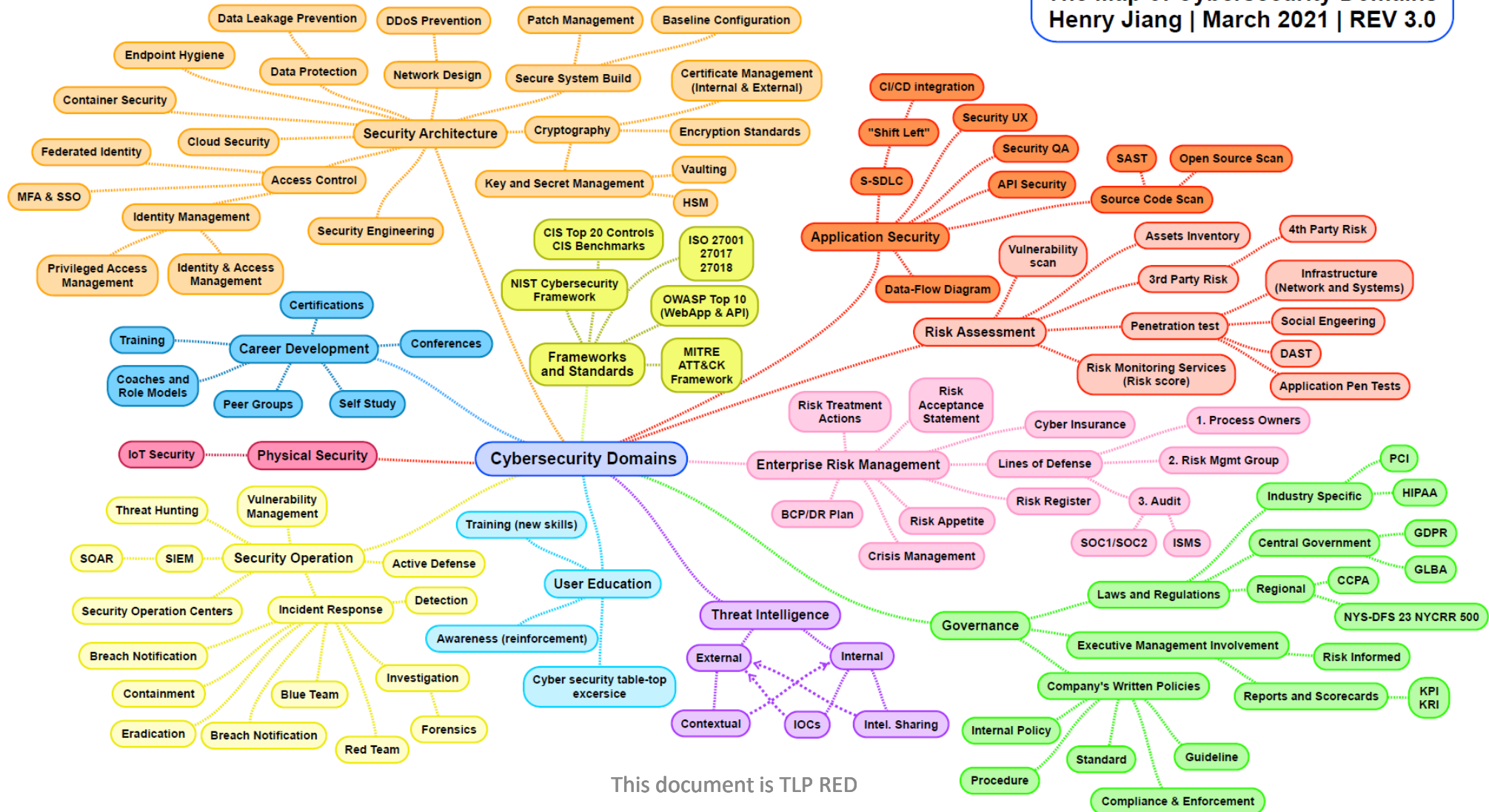
Future outlook discussions,
industry and certifications

Labs/Homework

- Install Ubuntu linux, check bash terminal, gnome desktop
- Import windows 10 VM to virtualization app
- Configure virtual machines for NAT to internet
- Fully update virtual machines

The cybersecurity domains map

The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.0



This document is TLP RED

[illegible]

This document is TLP RED

Lab2 / homework

- Install Ubuntu linux in VM (using downloaded ISO image)
- Explore Linux terminal: <https://hackr.io/blog/basic-linux-commands>
- Install/play ninvaders via terminal
- Online emulators (limited)
 - <https://bellard.org/jslinux/>
 - <https://www.webminal.org/>



End of Module 1

Networks and Systems security basics

Dr. Amin Hasbini