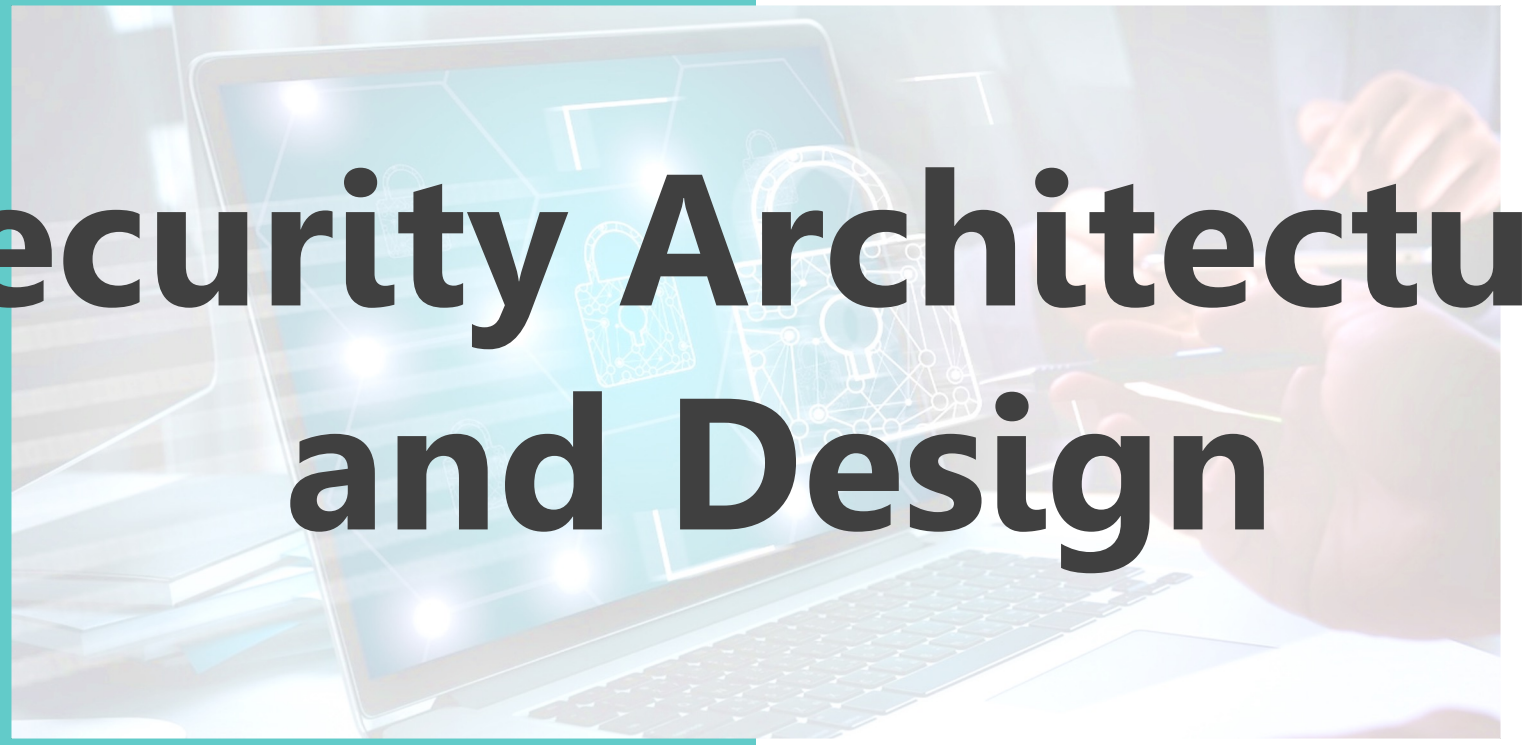
KBTG
KASIKORN
BUSINESS-TECHNOLOGY GROUP

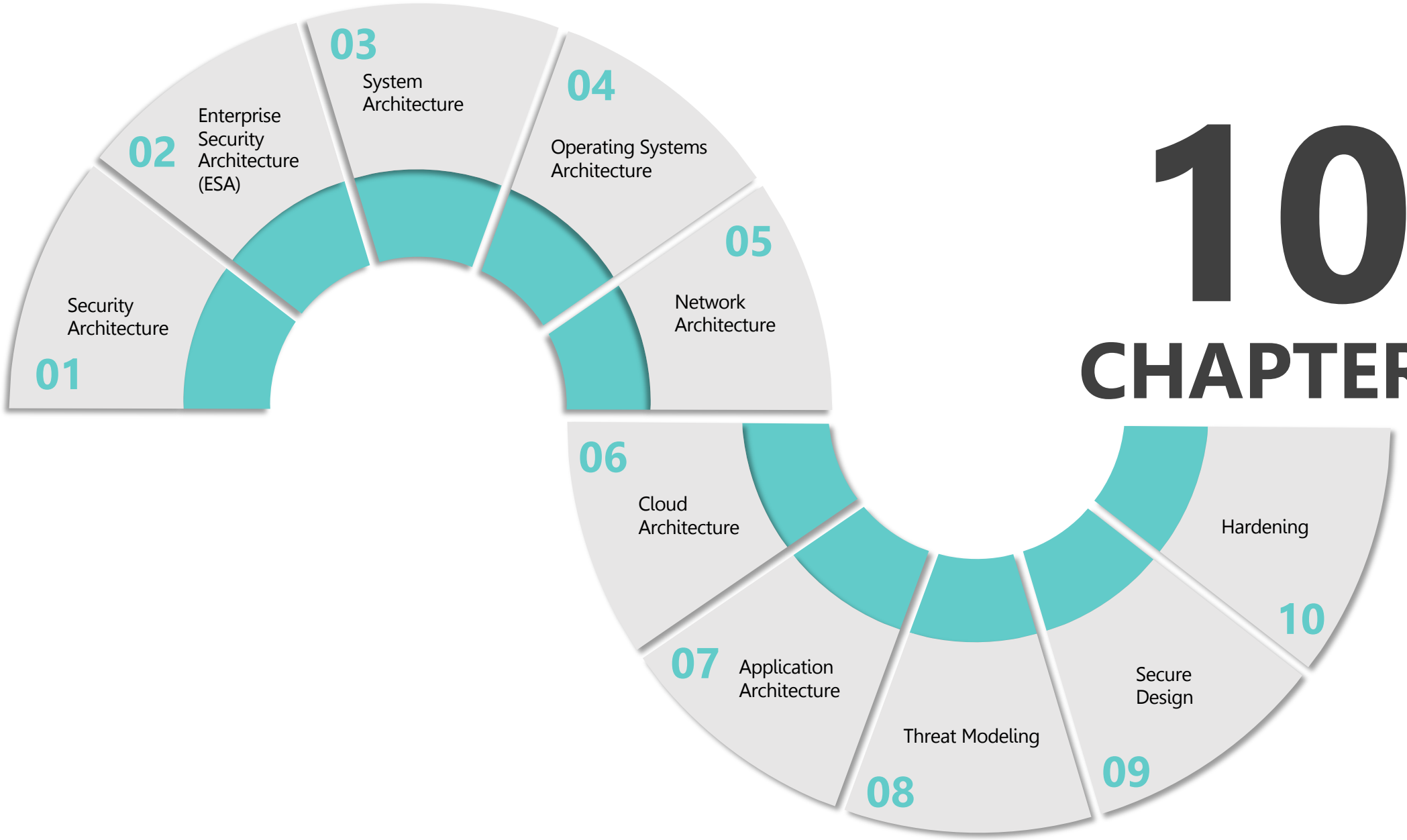


Security Architecture and Design

Cybersecurity Bootcamp
2024

Disclaimer

This learning material is addressed and used only for Cybersecurity Bootcamp 2024 and should not be used or relied upon for any other purposes. Our learning material is not to be disseminated to or used by any third party in whole or in part without prior consent and permission from Kasikorn Technology Group Secretariat Company Limited (KBTGSec). Accordingly, we will not accept or take any responsibility or liability for any party or any person, whether or not such material is shown, disseminated, obtained, or possessed to such party or person since such material is only for educational purposes. We reserve all of our rights, including but not limited to intellectual property rights in our learning material, such as presentations, spreadsheets, system techniques, ideas, concepts, information, forms, electronic tools, forming parts of the materials, etc.



10 CHAPTERs

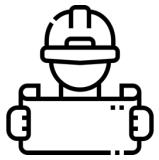
A.

Key Objectives

Key Objectives of this topic

01 Security Architect

Develop expertise in designing secure systems, aligning security solutions with organizational goals, and collaborating with stakeholders to ensure comprehensive security measures.

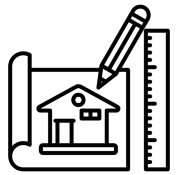


02 System Architect

Master the design and optimization of server, network, cloud, operating system, and application architectures, ensuring they meet performance, reliability, and security requirements.

03 Principles

Understand and implement secure design principles, threat modeling techniques, and system hardening practices to mitigate security risks effectively.



01

Introduction to Security Architect

Security Architect

What is Security Architect ?

Security architect jobs combine hardware and software knowledge with programming, research, and policy development. Security architects anticipate potential threats and design systems to preempt them.

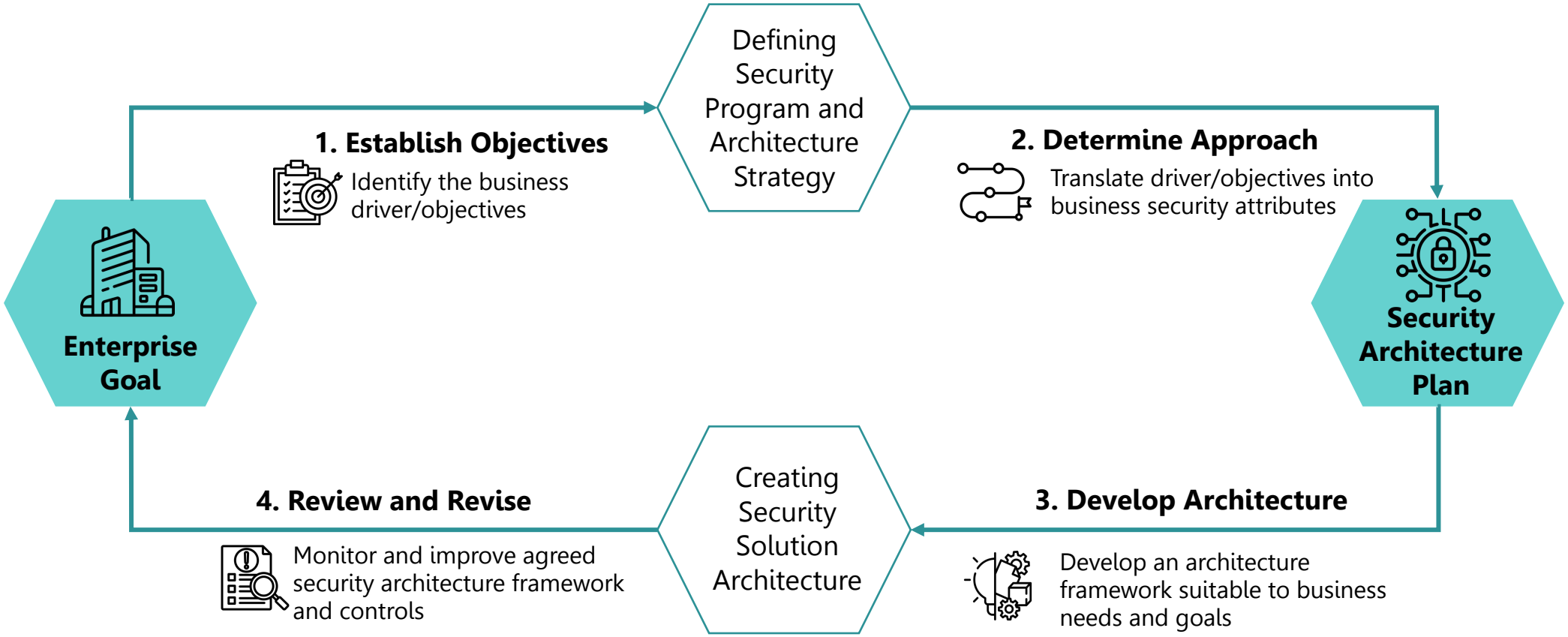
Cybersecurity architecture developed from the need to control and monitor data: who or what holds data, and how it is exchanged across networks and channels. Security architects, also called cybersecurity architects, coordinate the lifecycle of information technology processes and policies.

Why Security Architect do ?

- Driven by business requirements rather than technical consideration
- Aligns business risks and risk appetite
- Directly trace able to business objectives
- Designed from the project outset to be cost – effective
- Meets regulatory, audit, and compliance requirement by design

Security Architect

Security Architect and Enterprise Architect



02

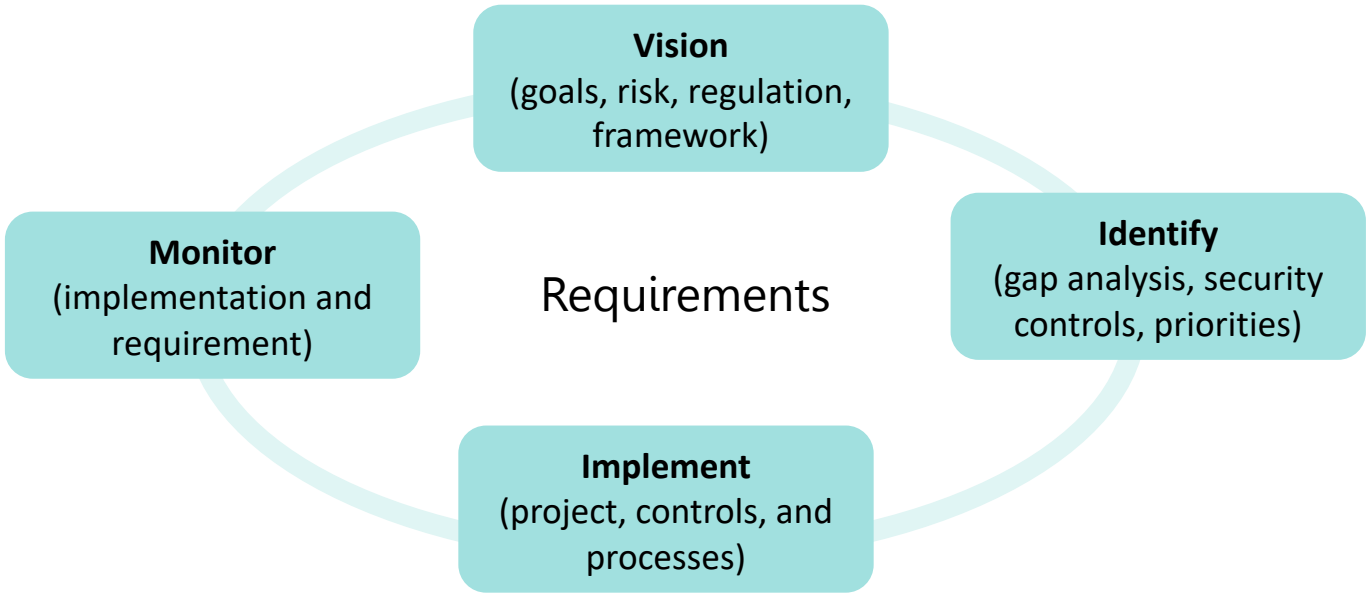
Enterprise Security Architecture (ESA)

Enterprise Security Architecture (ESA)

What is Enterprise Security Architecture (ESA) ?

Enterprise security architecture (ESA) is the methodology and process used to develop a risk-driven security framework and business controls. The focus of an enterprise architect should be to align information security controls and processes with business strategy, goals and objectives.

ESA life cycle management



https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/esa-what-is-it-and-how-does-it-work

Enterprise Security Architecture (ESA)

NIST Cybersecurity Framework 1.1 vs 2.0

NIST Cybersecurity Framework 1.1

NIST Cybersecurity Framework 2.0

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Enterprise Security Architecture (ESA)

NIST Cybersecurity Framework 2.0

Govern

- Organizational Context
- Risk Management Strategy
- Roles, Responsibilities, and Authorities
- Policy
- Oversight
- Cybersecurity Supply Chain Risk Management

Identify

- Asset Management
- Risk Assessment
- Improvement

Protect

- Identity Management, Authentication, and Access Control
- Awareness and Training
- Data Security
- Platform Security
- Technology Infrastructure Resilience

Detect

- Continuous Monitoring
- Adverse Event Analysis

Response

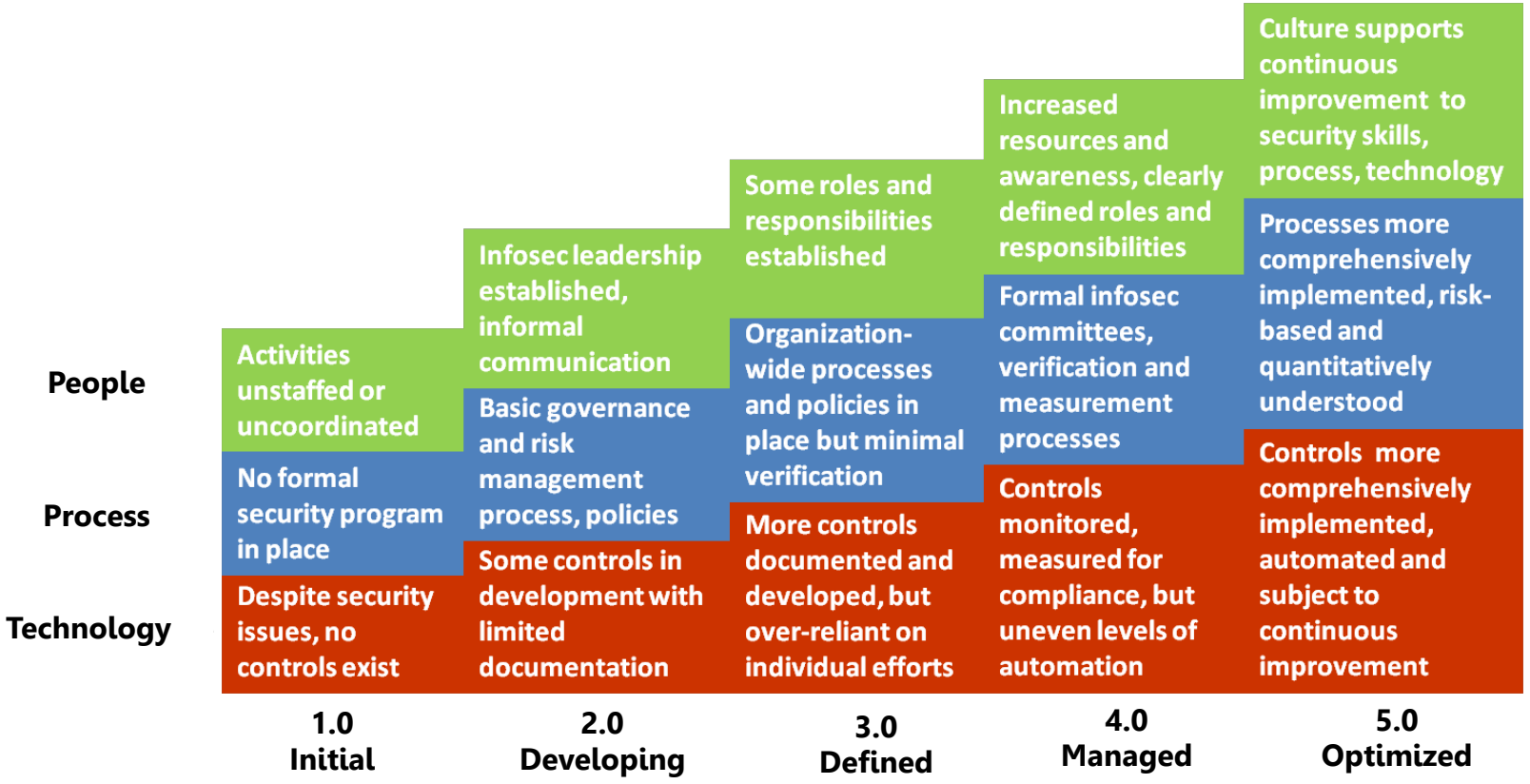
- Incident Management
- Incident Analysis
- Incident Response Reporting and Communication
- Incident Mitigation

Recover

- Incident Recovery Plan Execution
- Incident Recovery Communication

Enterprise Security Architecture (ESA)

Security Maturity Level



B.

Key Takeaway – 01 Security Architect

Key Takeaway for 01 Security Architect

Security Architect

- Security architecture involves designing and implementing security solutions to protect organizational assets and data.

Enterprise Security Architect

- Security architects focus on designing secure systems, while enterprise security architects develop comprehensive security strategies for large-scale enterprises.

03

System Architecture

System Architecture

What is System Architecture ?

The architecture of a system reflects how the system is used and how it interacts with other systems and the outside world. It describes the interconnection of all the system's components and the data link between them. The architecture of a system reflects the way it is thought about in terms of its structure, functions, and relationships.

What is "System" we talk about ?

Server

Email server, File server,
Web server,
Database server

Operating System

Monoliths, Layered,
Microkernel, and Hybrid
Architecture

Network

Network Architecture
Internet Architecture
Network Zoning

Cloud

Private cloud
Public cloud
Hybrid cloud

Application

Tightly coupled
Coupled
Loosely coupled

System Architecture - Servers

Several types of servers

Mail Server

send and receive e-mails between parties

File Server

File servers are centralized locations for file storage and are accessed by many clients

Web Server

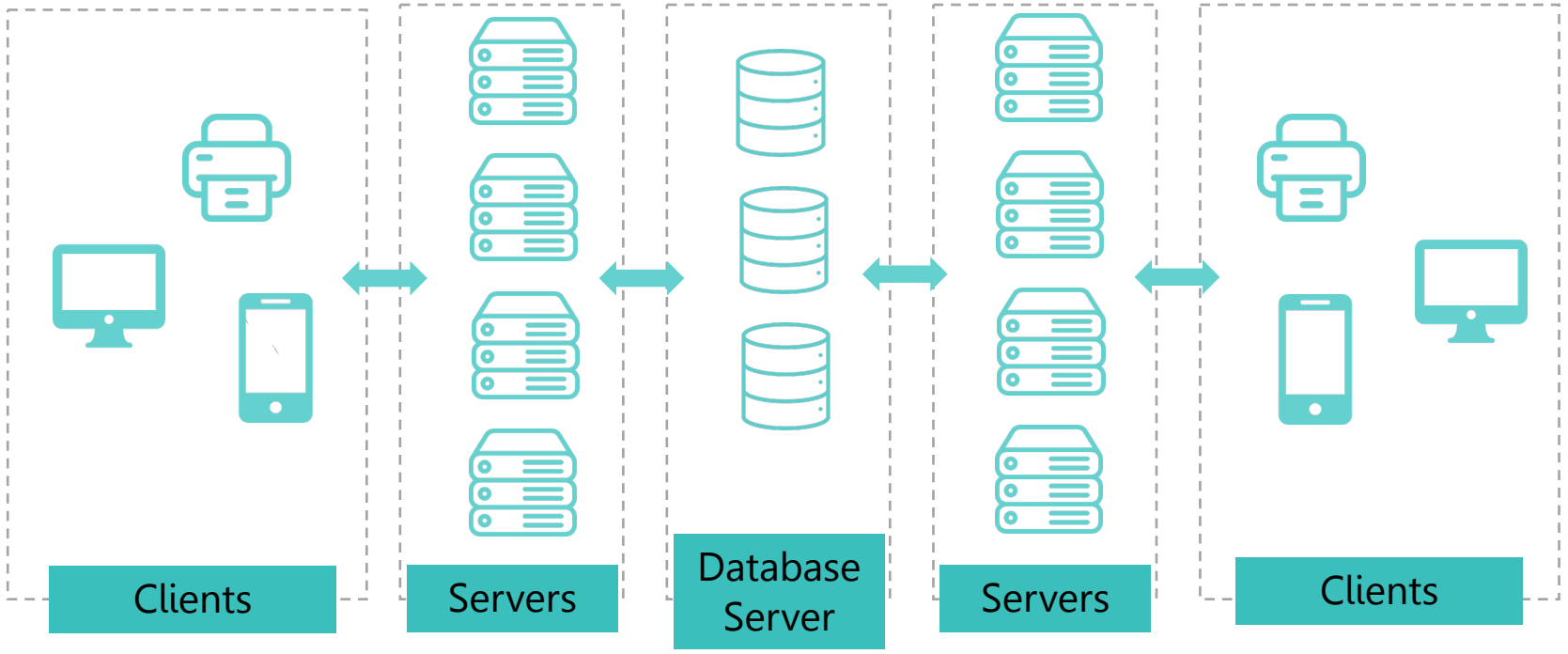
These high-performance servers host many different websites, and clients access them through the Internet

Database Server

A database server helps users or companies store, manage, retrieve, update or change files, information logs and other forms of digital data

System Architecture - Server

Client-Server diagram shows the basics of the architecture



The Client-Server Model

04

Operating Systems Architecture

Operating Systems Architecture

What is Operating Systems Architecture ?

The operating system provides an environment for the users to execute computer programs. Operating systems are already installed on the computers you buy for eg personal computers have windows, Linux, and macOS, mainframe computers have z/OS, z/VM, etc., and mobile phones have operating systems such as Android, and iOS. The architecture of an operating system consists of four major components hardware, kernel, shell, and application

Key terms of Operating System

Application

The application represents the software that a user is running on an operating system it can be either system or application software e.g. slack, sublime text editor, etc.

Shell

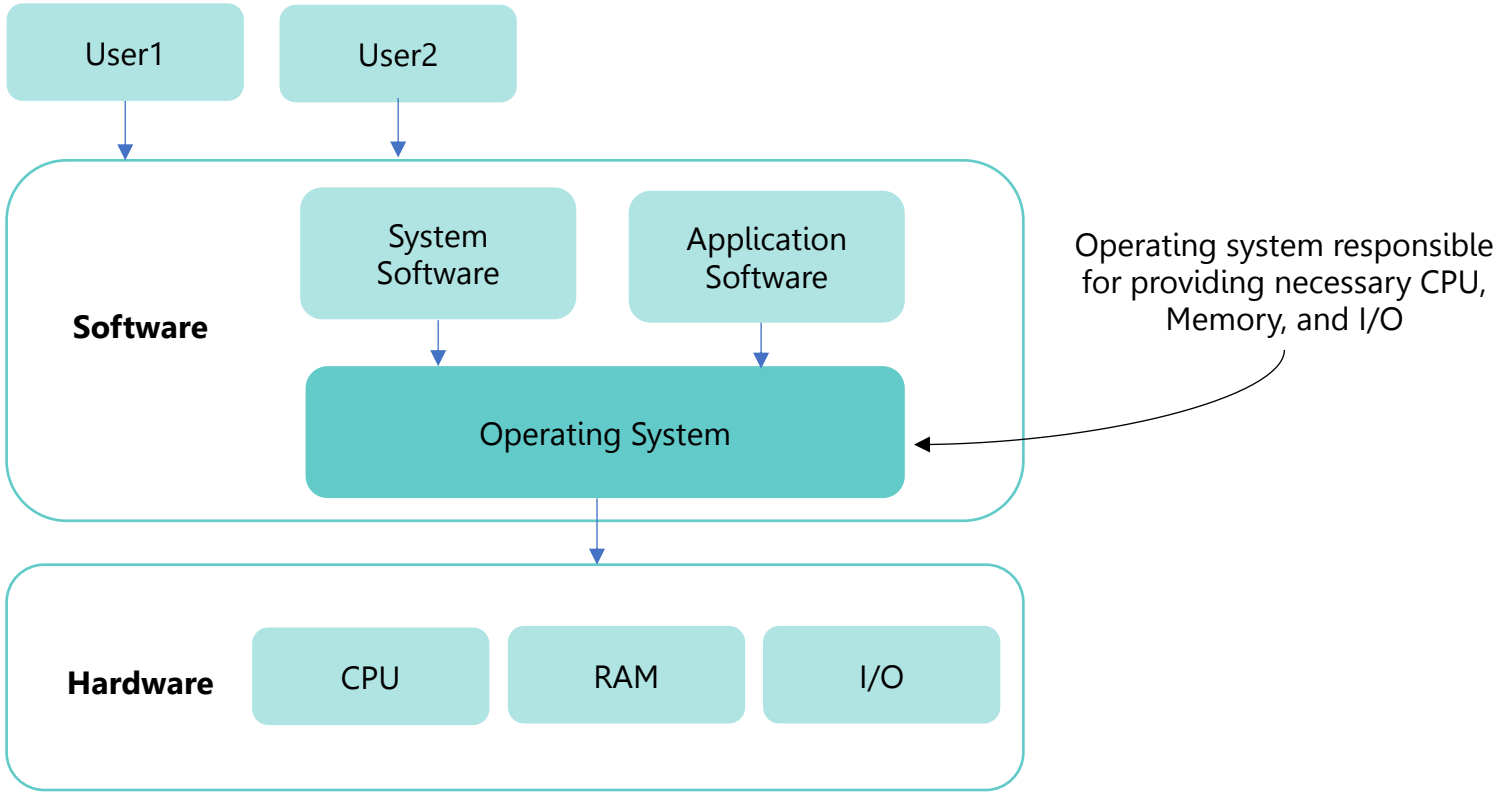
The shell represents software that provides an interface for the user where it serves to launch or start some program for which the user gives instructions.
It can be of two types first is a command line and another is a graphical user interface for.

Kernel

Kernel represents the most central and crucial part of the operating system where it is used for resource management i.e. it provides necessary I/O, processor, and memory to the application processes through inter-process communication mechanisms and system calls.

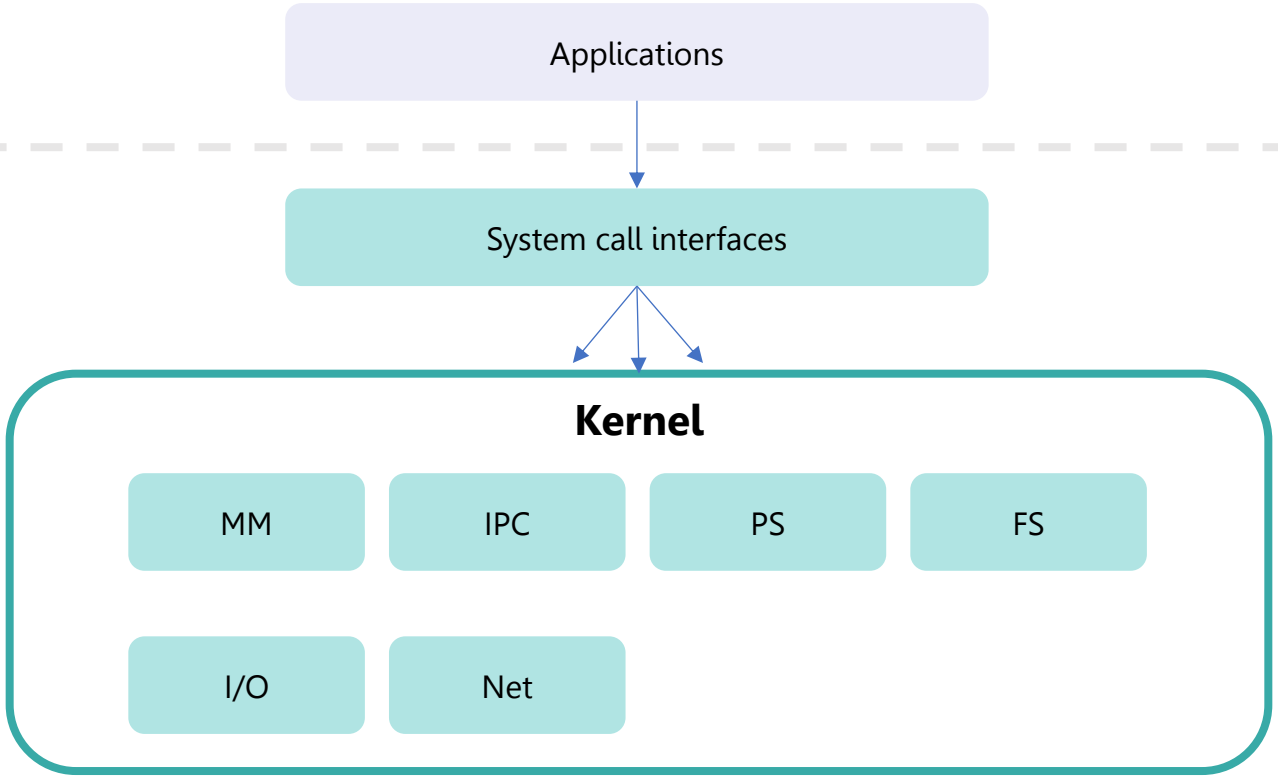
Operating Systems Architecture

The architecture of an operating system



Types of Architectures of Operating System

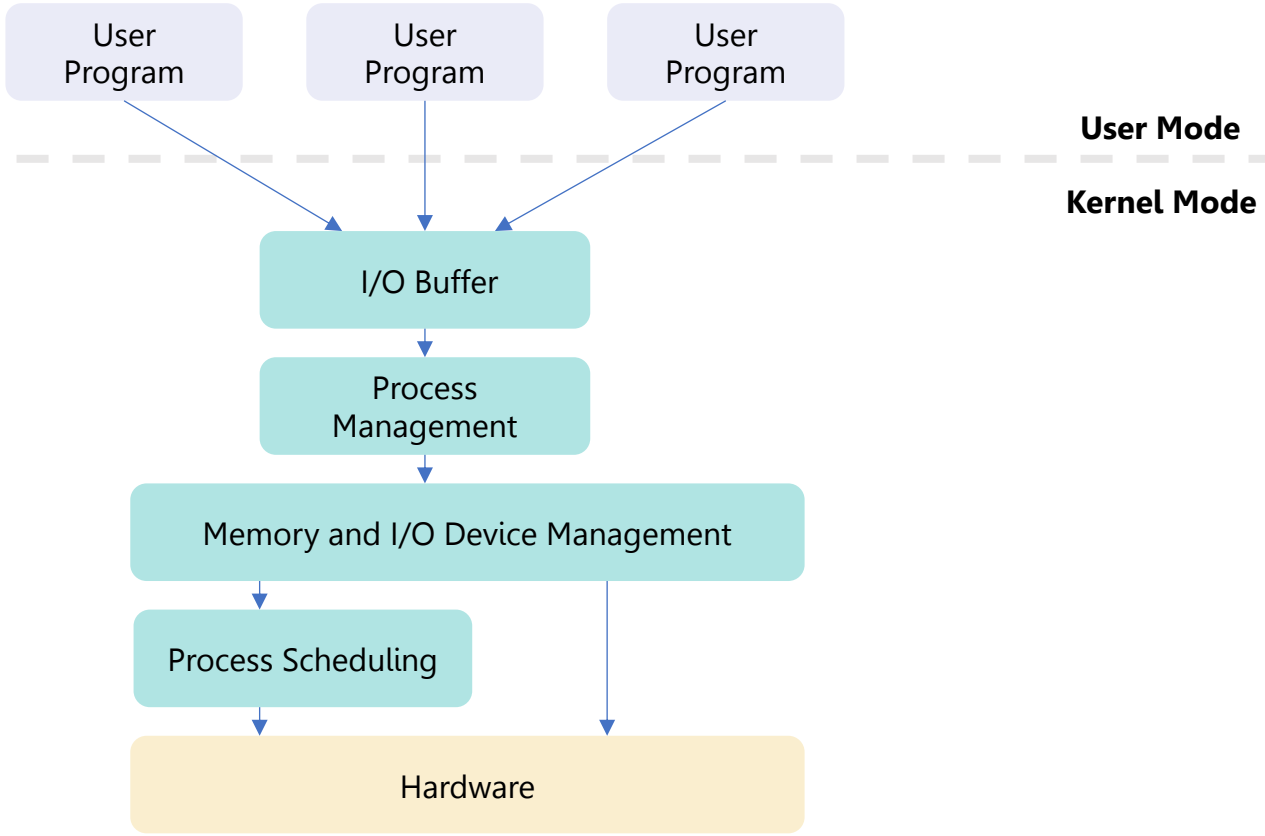
1) Monolithic Architecture



MM – Memory Scheduler
IPC – Interprocess Communication
PS – Process Scheduler
FS – File System
I/O – Input/Output Manager
Net – Network Manager

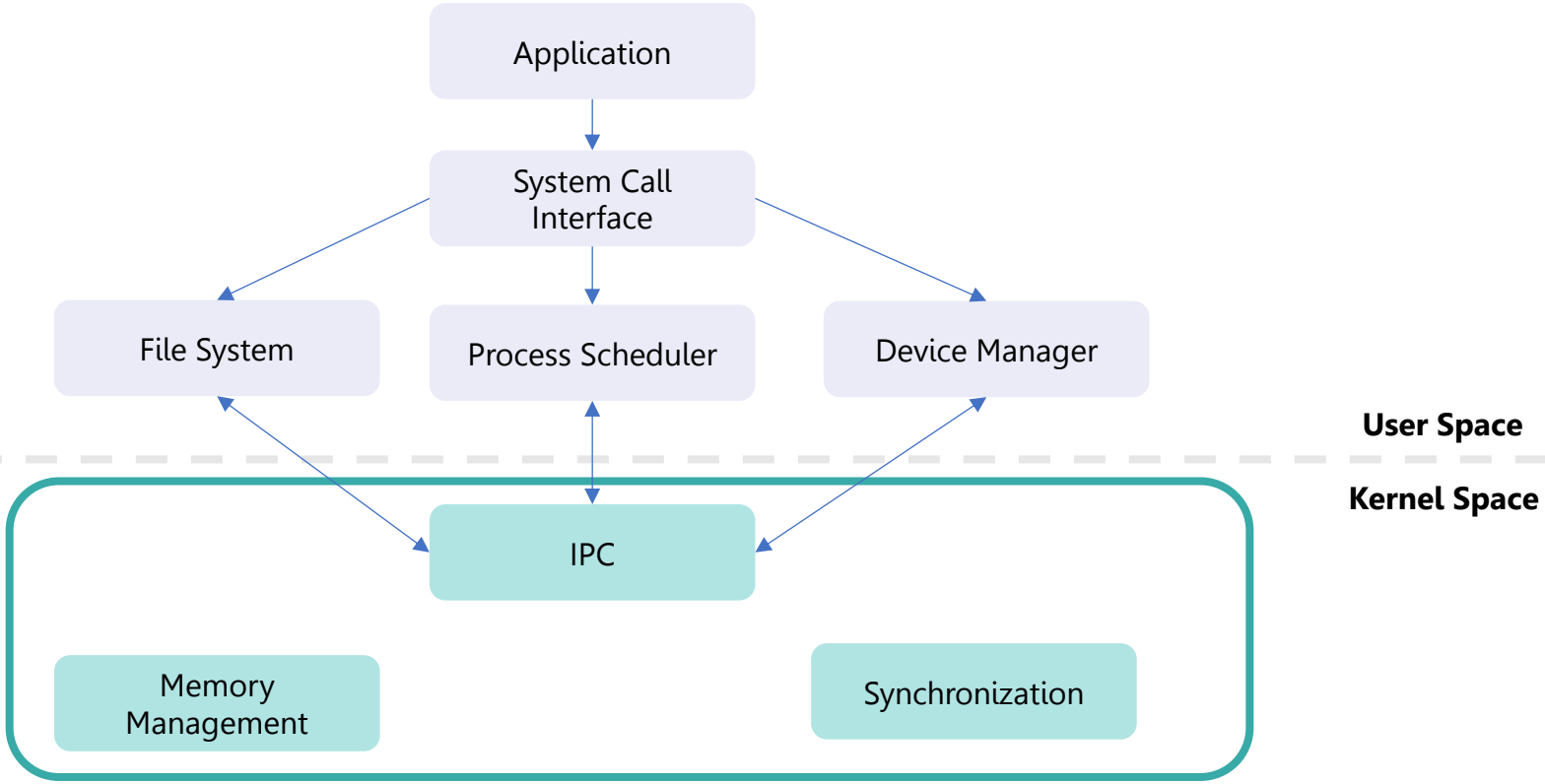
Types of Architectures of Operating System

2) Layered architecture



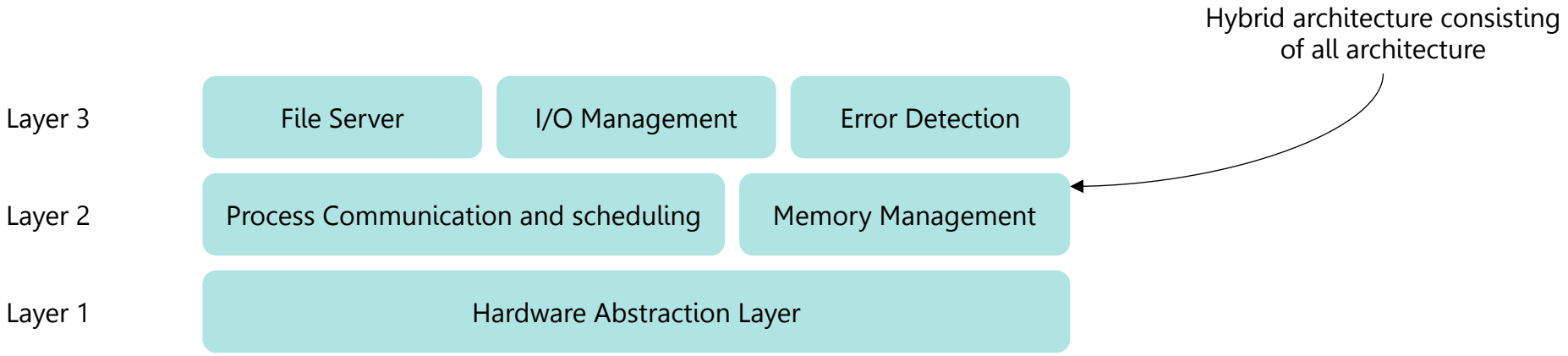
Types of Architectures of Operating System

3) Microkernel Architecture



Types of Architectures of Operating System

4) Hybrid Architecture



05

Network Architecture

Network Architecture

What is Network Architecture ?

Network architecture refers to the way network devices and services are structured to serve the connectivity needs of client devices.

- Network devices typically include switches and routers.
- Types of services include DHCP and DNS.
- Client devices comprise end-user devices, servers, and smart things.

Network Architecture

Key Components of Network Architecture Design

Hardware

- Routers
- Switches
- Servers
- Firewall

Network Protocols

- Internet Protocol (IP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

Transmission Media

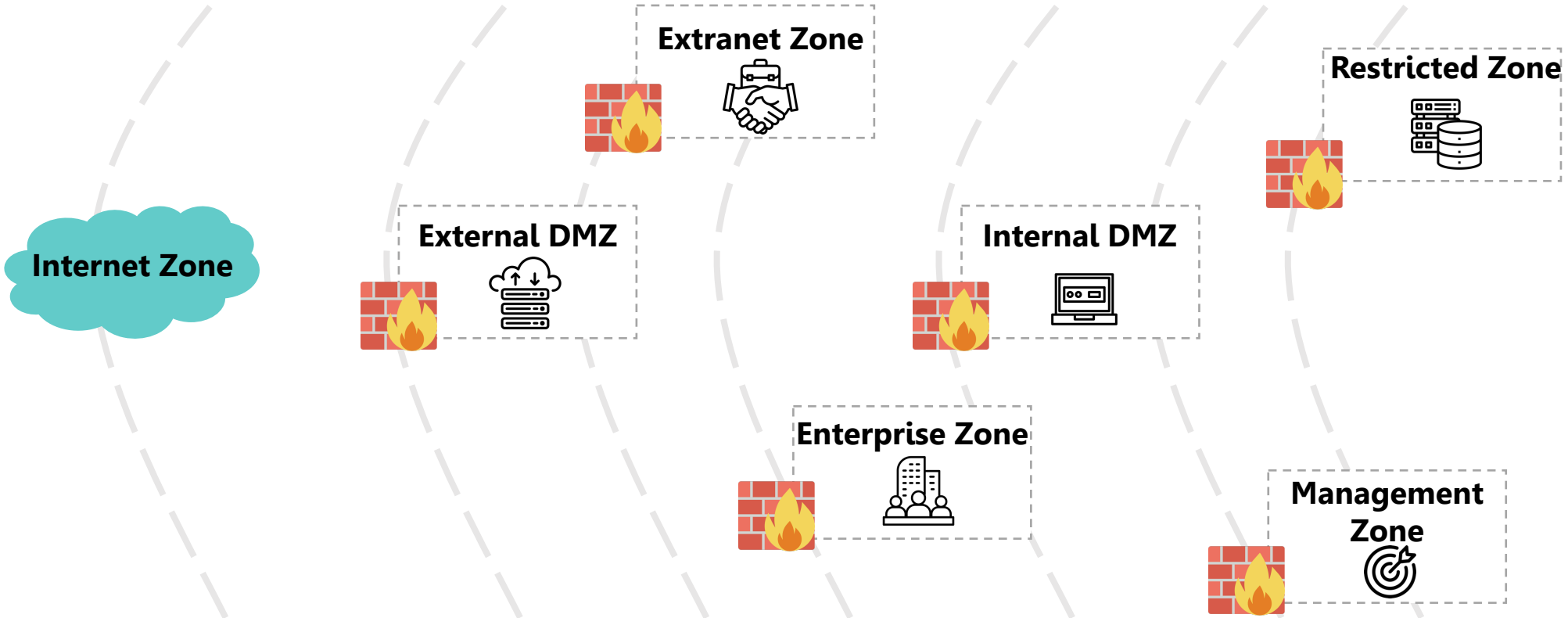
- Wired networks
- Wireless networks

Network Topologies

- Mesh Network
- Hybrid Network
- Software-Defined Networking (SDN)
- Peer-to-Peer (P2P) Network
- Tree (Hierarchical) Network
- Virtual Network (Overlay Network)
- Cloud (Multi-tenant)
- Hybrid-Cloud
- Multicloud

Network Architecture

Network Zoning



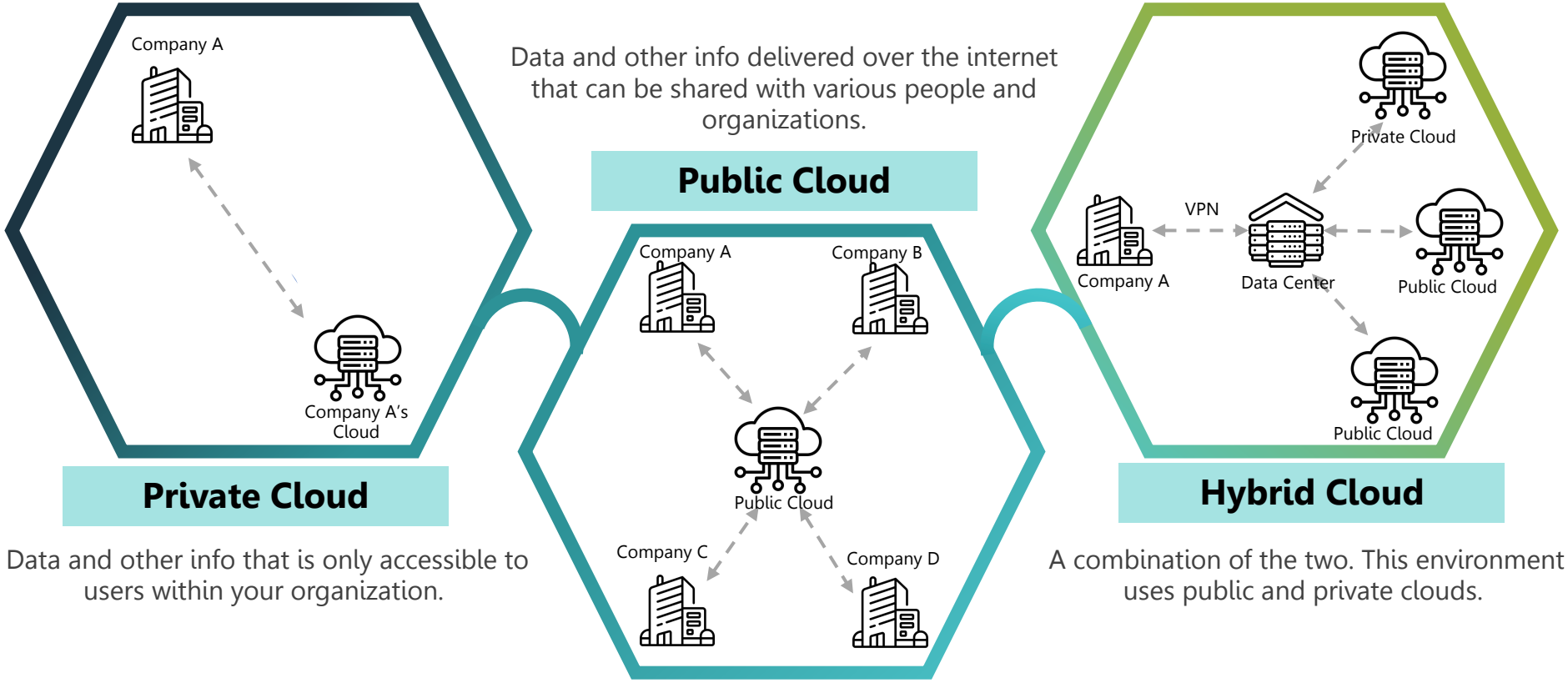
https://medium.com/@aman.bansal93/security-zoning-in-network-architecture-ff7693b91556

06

Cloud Architecture

Cloud Architecture

Different Cloud Architecture Models



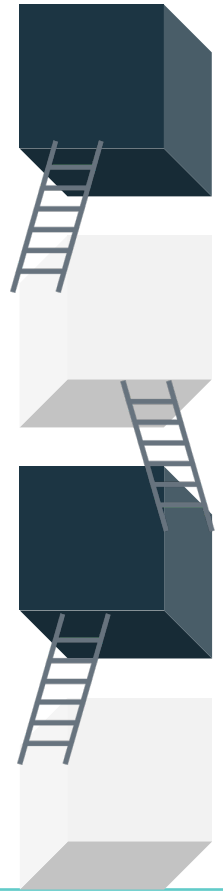
Cloud Architecture

Different Types of Cloud Computing Layers

SaaS
Users

PaaS
Software Developer

IaaS
System Admin



Application Layer
(Business Application, Web Services, Multimedia)

Gmail | Facebook | SalesForce | Youtube

Platform Layer
(Social Framework)

Amazon Simple | Google App Engine

Infrastructure Layer
(Storage, Virtual Machine)

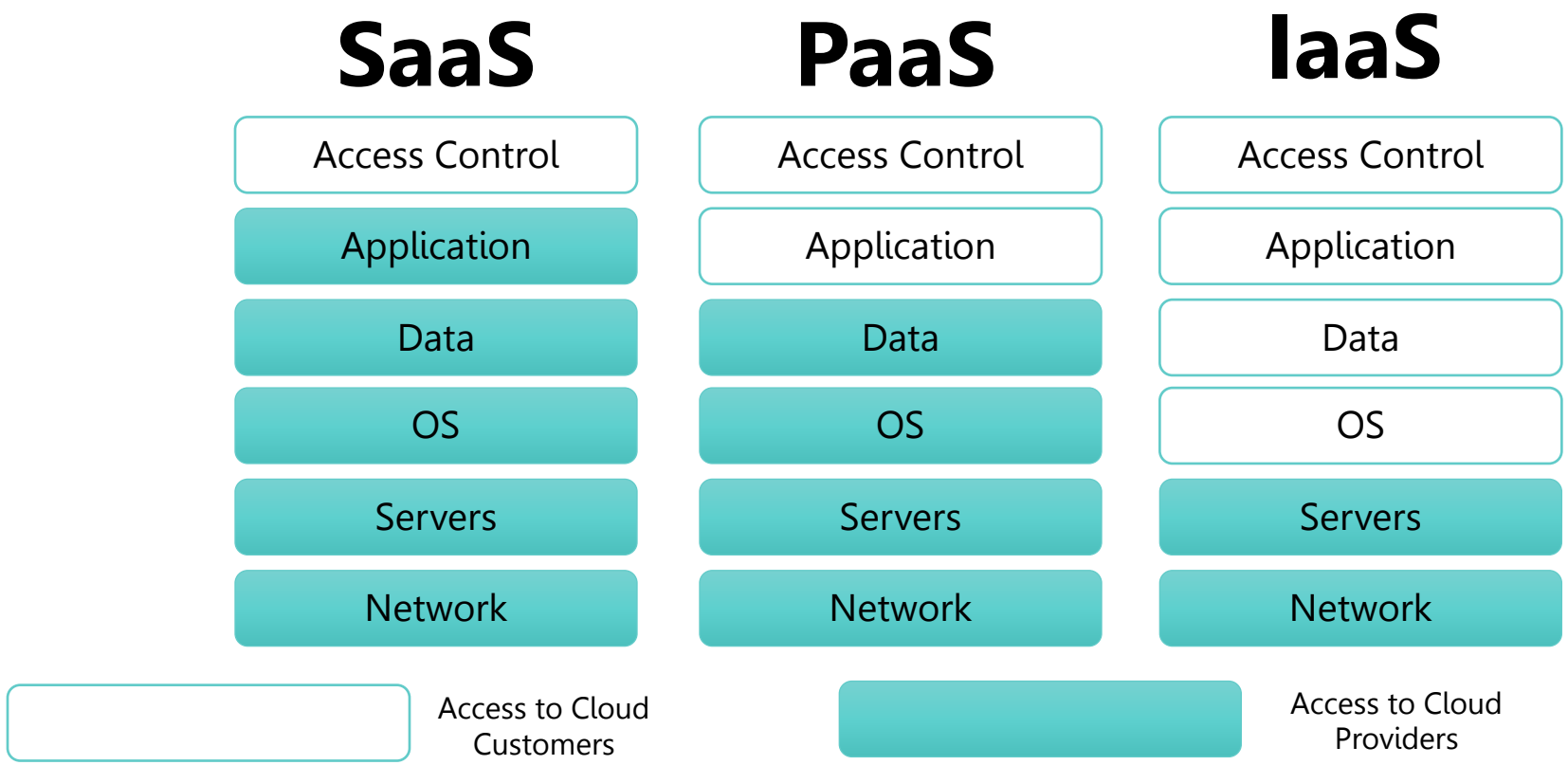
Amazon Web Service | Flexiscale | Rack Space

Datacenter Layer
(CPU, Bandwidth, Disk, Memory)

Data Centers

Cloud Architecture

Different Types of Cloud Computing Layers - Controls



07

Application Architecture

Application Architecture

What is Application Architecture ?

An application architecture describes the patterns and techniques used to design and build an application. The architecture gives you a roadmap and best practices to follow when building an application, so that you end up with a well-structured app.

When deciding which application architecture to use for a new application, or when evaluating your current architecture, start by determining your strategic goals.

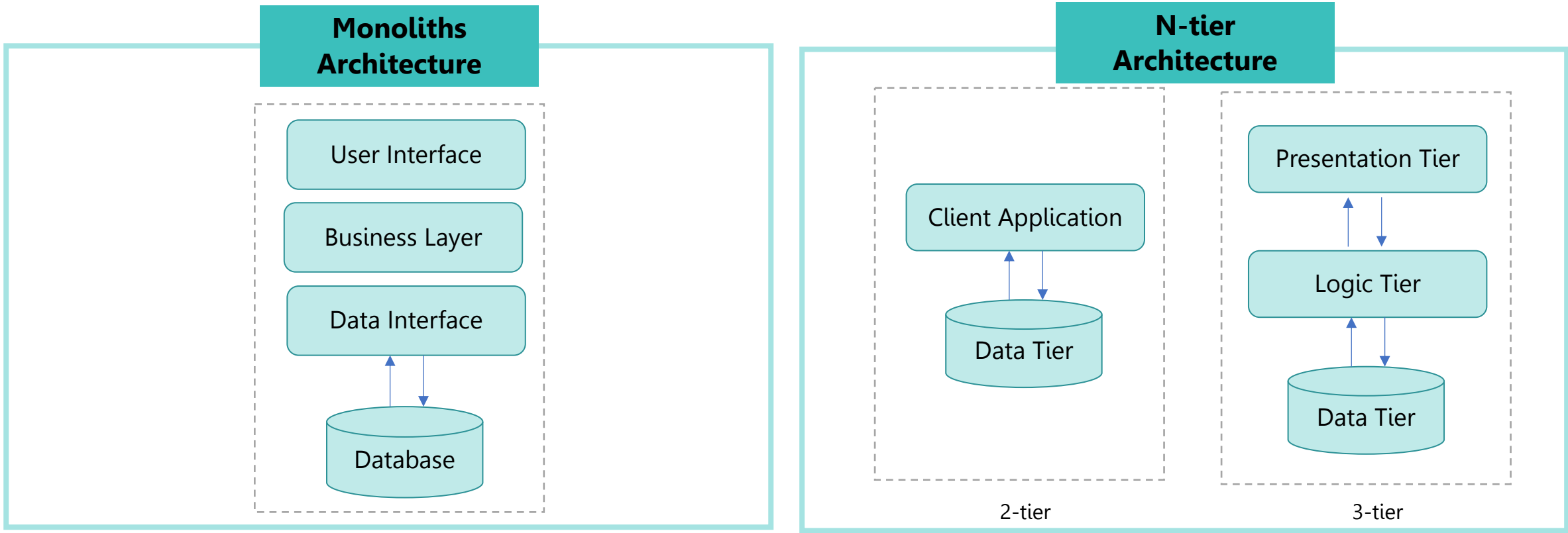
Then you can design the architecture that supports your goals, instead of choosing an architecture first and trying to make an application fit within that structure.

5 types of application architectures

Tightly Coupled	Decoupled	Loosely Coupled
Monoliths Architecture N-tier Architecture	Microservices	Event-driven Architecture Service-oriented Architecture

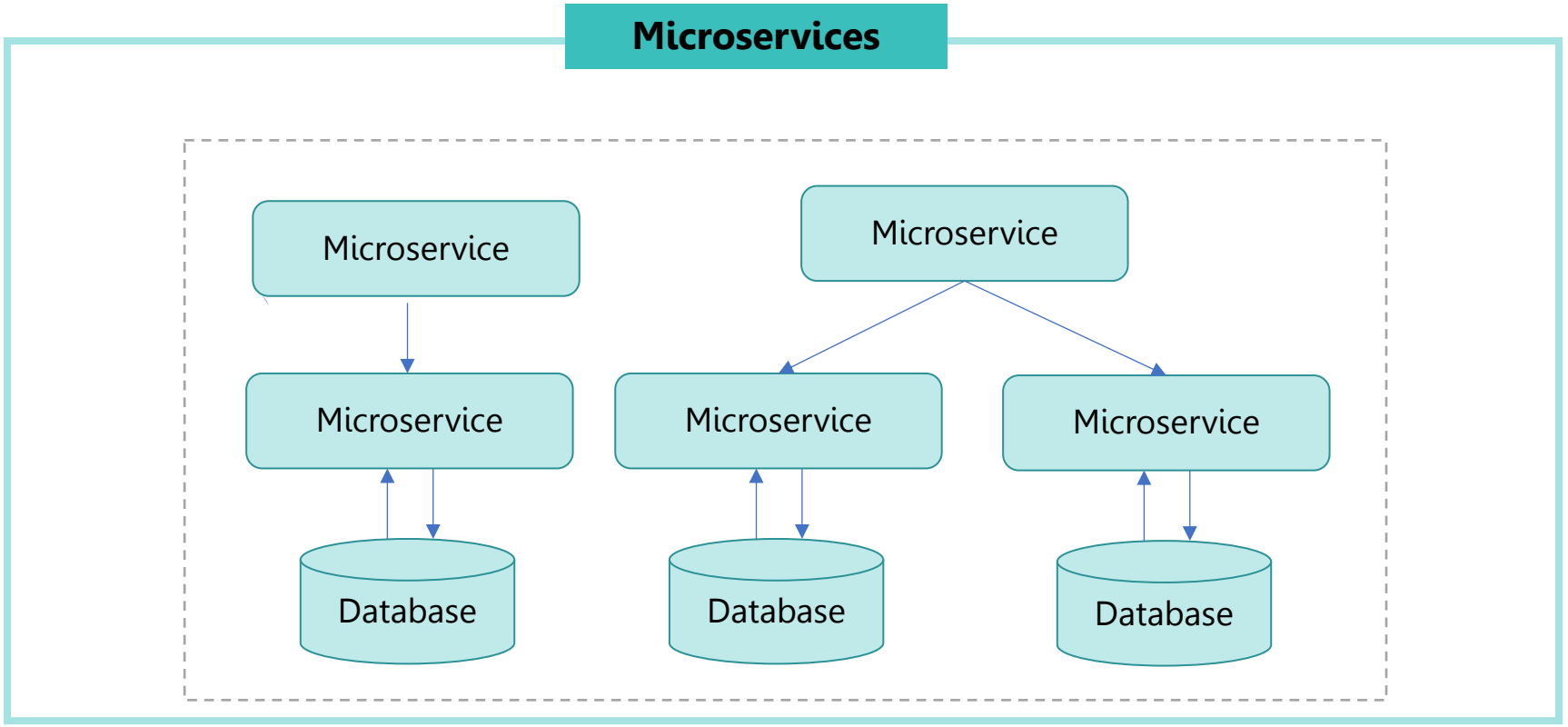
Application Architecture

Different types of application architectures - Tightly Coupled



Application Architecture

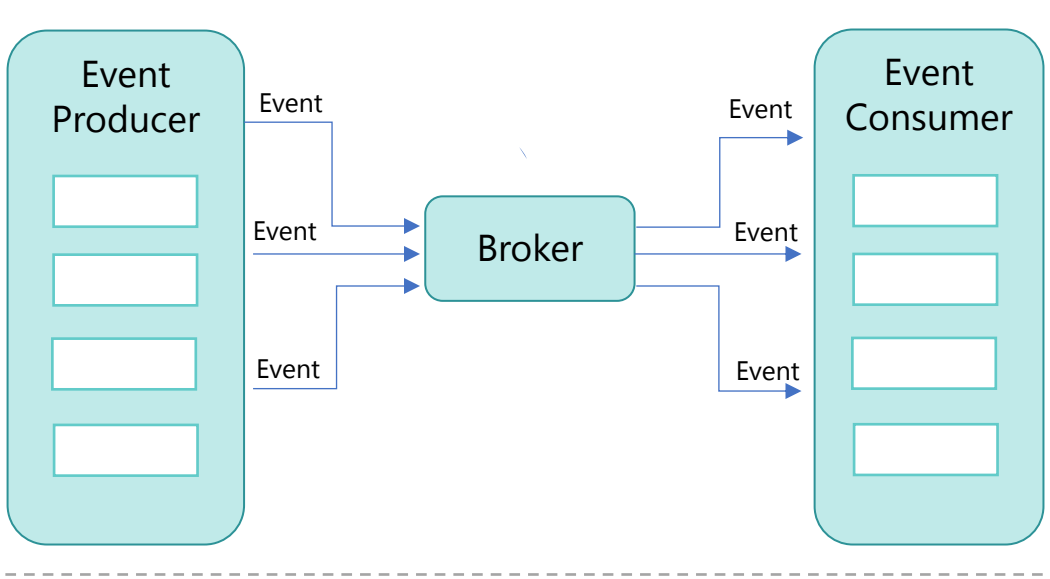
Different types of application architectures - Decoupled



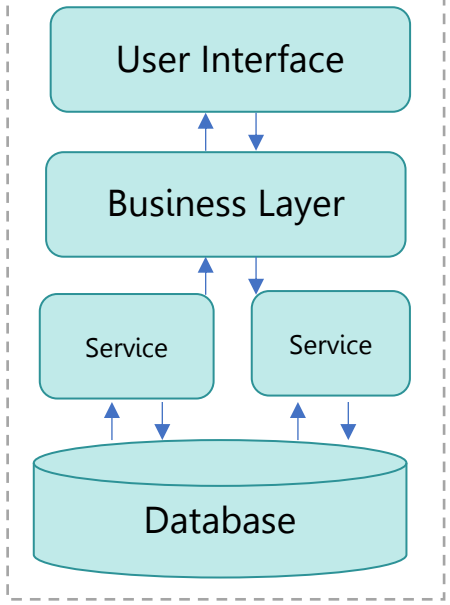
Application Architecture

Different types of application architectures - Loosely Coupled

Event-driven Architecture

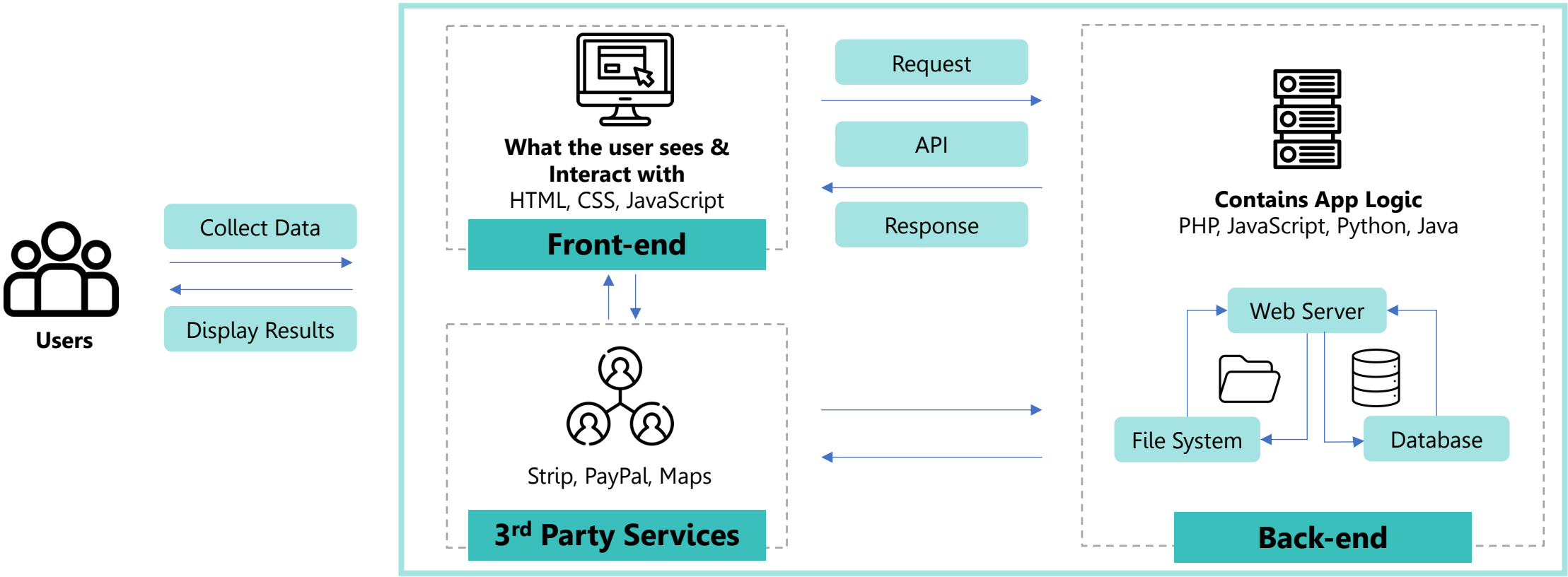


Service-oriented Architecture



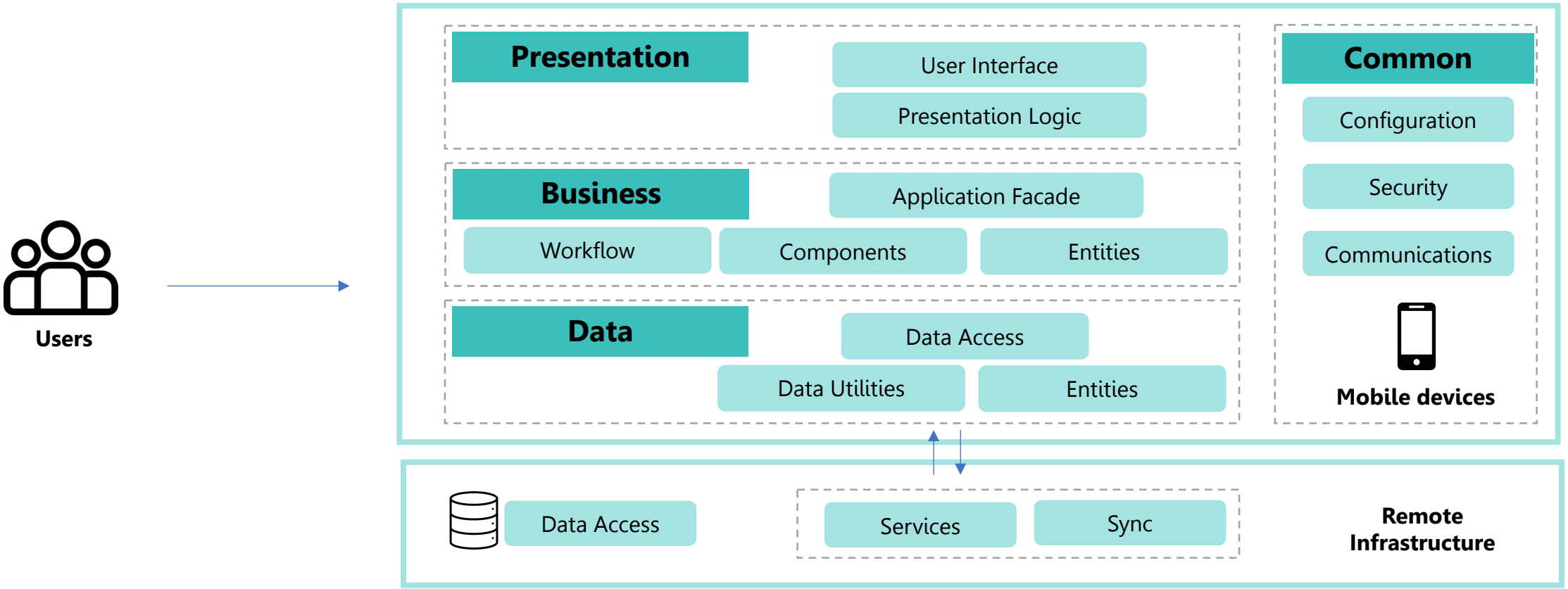
Application Architecture

Different types application architectures – Web application architecture



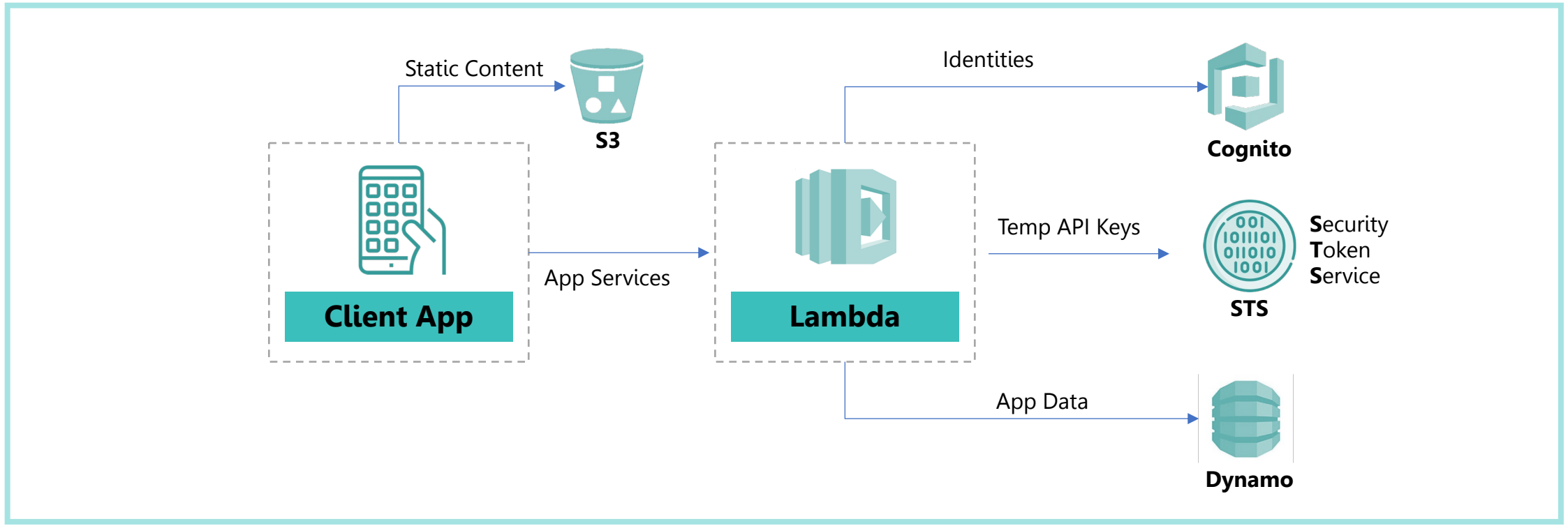
Application Architecture

Different types application architectures – Mobile application architecture



Application Architecture

Different types application architectures – Serverless application architecture (AWS)



B.

Key Takeaway – 02 System Architect

Key Takeaway for 02 System Architect

Server Architecture	• Design resilient servers with top-notch security. • Keep data safe and performance high.
OS Architecture	• Keep OS updated, secure, and tight. • Harden defenses, keep threats out of sight.
Network architecture	• Secure networks for seamless communication. • Keep data confidential, always in motion.
Cloud Architecture	• Cloud security, compliant and robust. • Encrypt, control, and integrate with trust.
Application Architecture	• Build apps strong, scalable, and smart. • Secure code, encryption, play your part.

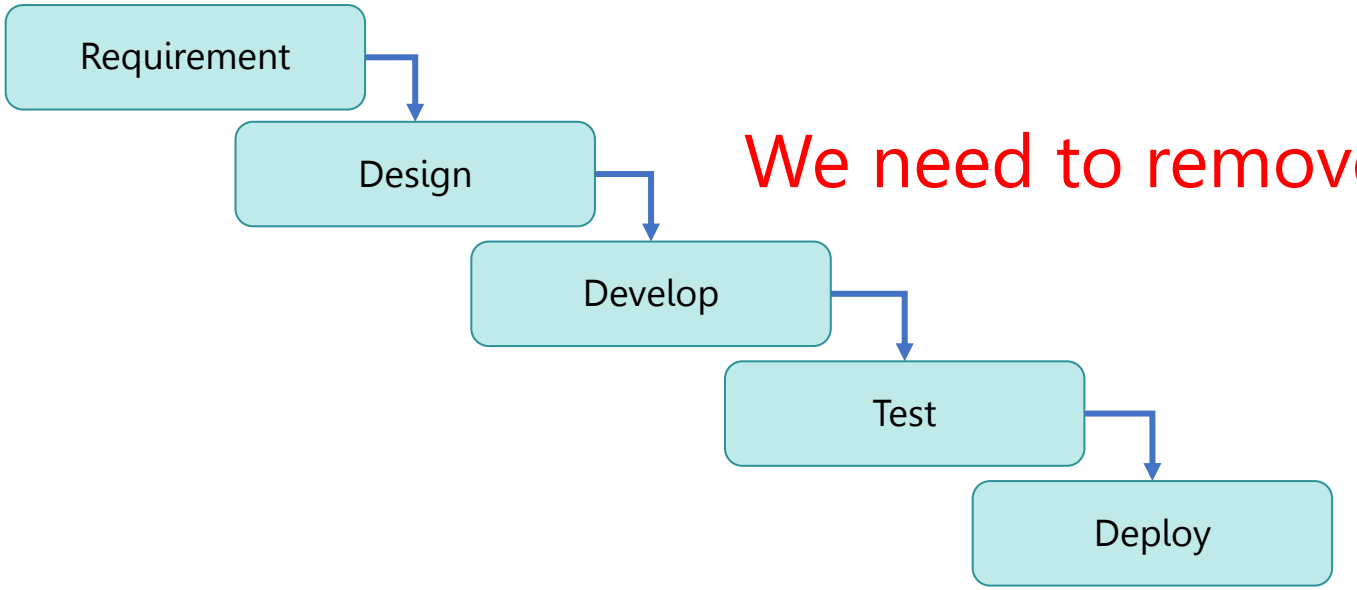
Application Architecture - DevSecOps

Goal of doing DevSecOps

1. **Increasing**
   - Throughput = Money
   - Generated terms of sales
2. **Reducing**
   - Inventory : investment made in producing products
   - Operational expenses = cost necessary to turn inventories into finished product

Waterfall model

- Sequential
- No iteration
- Slower release



We need to remove bottle neck

Application Architecture - DevSecOps

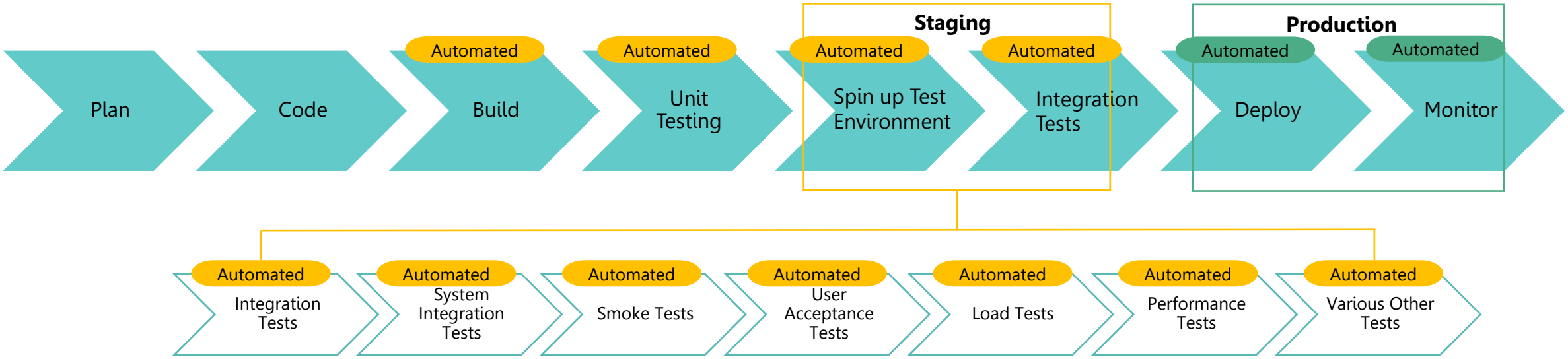
Agile Development Process

- Enhanced speed through iteration development
- Encourage breaking down large feature into more time-bound manageable chucks
- Facilitated the need for sprints retrospectives, and collaborative development

Application Architecture - DevSecOps

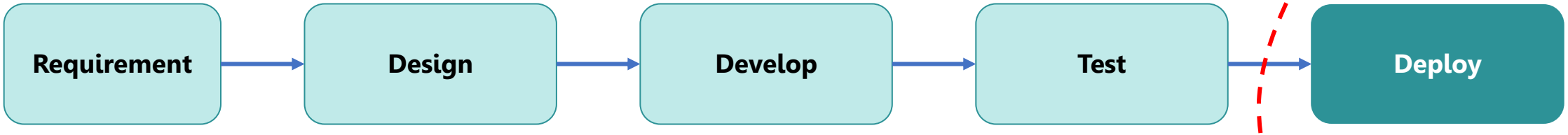
CI and CD

- **Continuous Integration (CI)** => Developers integrate code into a shared repo (Git) multiple times a day. Each integration triggers and is verified by automated tests resulting in an automated build.
- **Continuous Deployment (CD)** => Builds on CI. Code built by CI is deployed to a target environment through a series of automated deployment steps



Application Architecture - DevSecOps

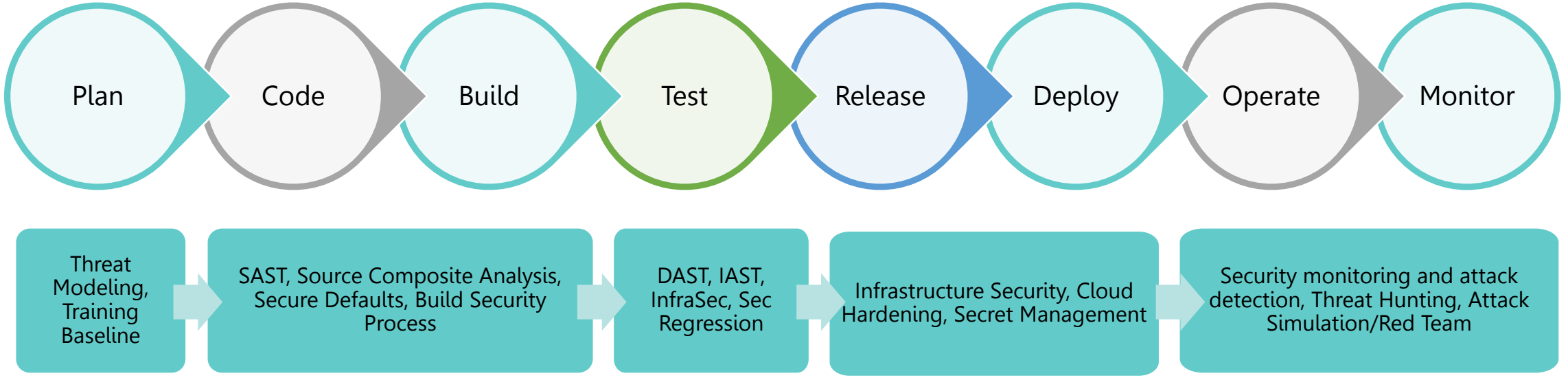
Security is very waterfall



Security is still viewed as a Gatekeeper process

Application Architecture - DevSecOps

Security adding to DevOps



Application Architecture - DevSecOps

Benefits of DevSecOps

- DevSecOps is an approach that integrates security into the software development process, providing several benefits
- Early detection of security vulnerabilities and issues, reducing the risk of security breaches.
- Improved collaboration between development, operations, and security teams, leading to faster and more efficient software development.
- Continuous security monitoring and testing, ensuring that security measures are up-to-date and effective.

Best Practices for Implementing DevSecOps

- Implement security measures and practices throughout the software development lifecycle, from design to deployment.
- Automate security testing and monitoring processes to detect vulnerabilities and issues in real-time.
- Provide security training and awareness programs for developers and other team members to ensure a security-focused mindset.

08

Threat modeling

Threat Modeling

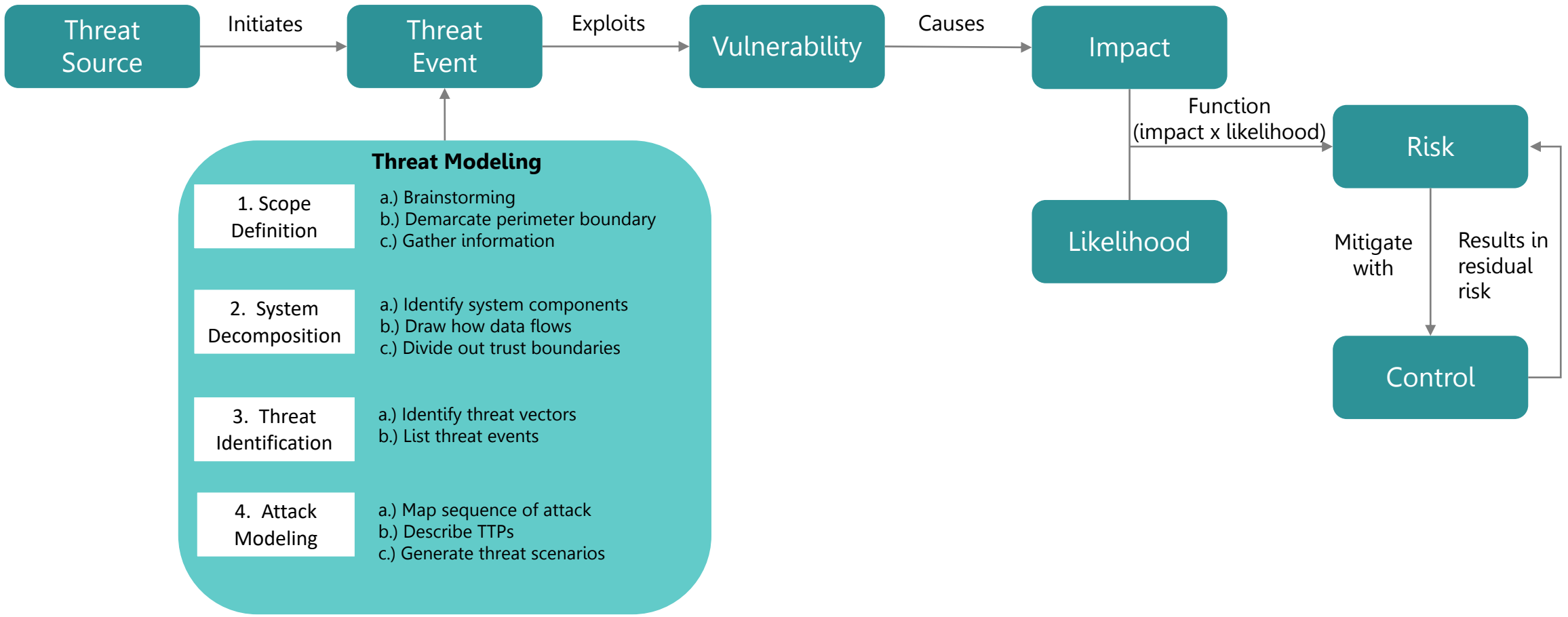
What is Threat Modeling?

- Threat modeling is a process in security architecture and design.
- Identifying and analyzing potential threats to a system or application.
- Organizations can implement effective security measures to mitigate risks and protect against attacks.

Why threat modeling is important?

- Outlining the concern you have as it pertains to a specific system, application, or process
- Making a list outlining the assumptions regarding the threat, which need to be verified as conditions change
- A concrete list of threats
- A list of remediation and elimination steps
- A way to make sure the methods of dealing with the threats are successful and still valid as the threat landscape changes

Threat Modeling fits into Risk Assessment



https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-cyber-threat-modelling.pdf?sfvrsn=a367caff_0

Step 1: Preliminaries and Scope Definition

Task A: Gather Information

Users should gather information pertaining to the system architecture and dependences by referring to system operations manual, software design document (SDD), technical specification or any system-related documentation. Users can also interview the system custodian, system administrator, and database administrator to get their input on the system architecture.

Task B: Demarcate Perimeter Boundary

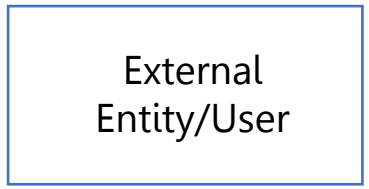
Based on existing network diagrams and architecture drawings, Users should demarcate the perimeter boundary to determine the scope for threat modelling. Some examples of guiding principles to determine what component is within the perimeter boundary may include, but are not limited, to the following:

- Components deployed behind data diodes or “demilitarized zones” (DMZs);
- Components that support the functioning and running of the system at any point in time e.g. servers, databases, client workstations, hosts, switches, routers etc.; and
- Components that support the cybersecurity of the system e.g. firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS).

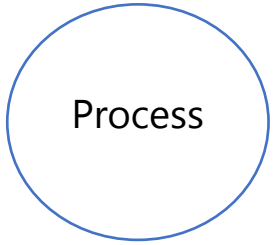
https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-cyber-threat-modelling.pdf?sfvrsn=a367caff_0

Step 2: System Decomposition

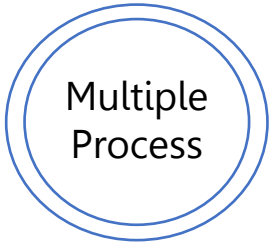
Task A: Identify System Components



An external entity/user is a subject that accesses the system



A process is a component where data manipulation, transformation and/or control takes place.



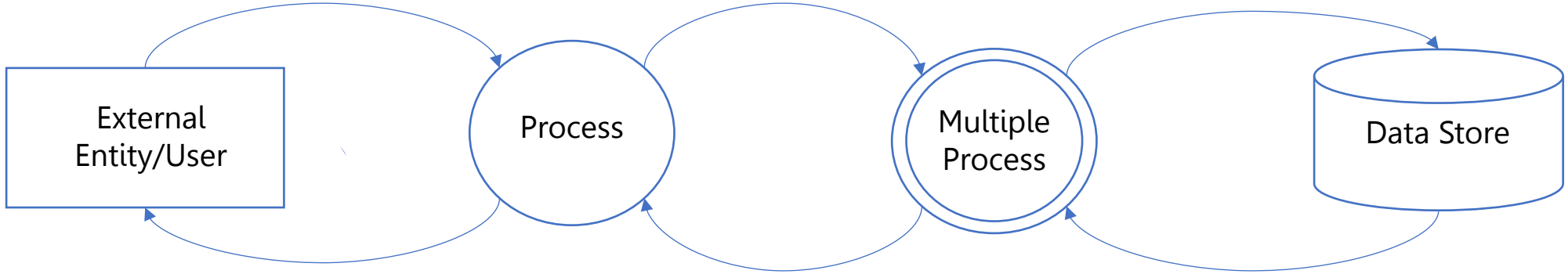
Multiple process is a component where data manipulation, transformation and/or control takes place as a cluster.

A data store is a persistent repository of data required and/or produced by a process.

https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-cyber-threat-modelling.pdf?sfvrsn=a367caff_0

Step 2: System Decomposition

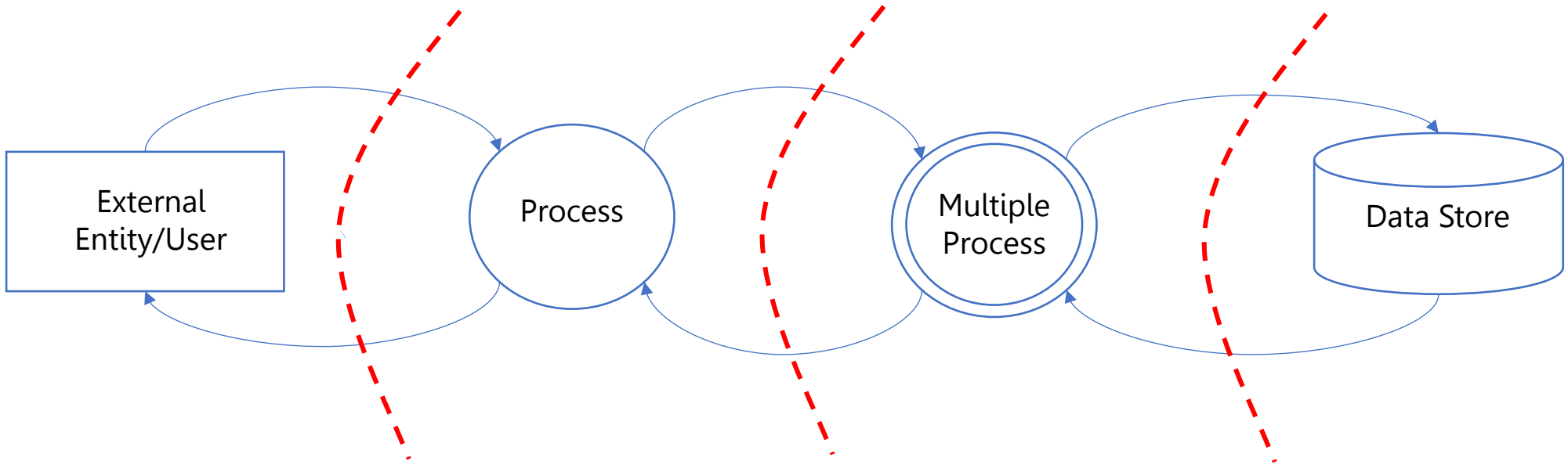
Task B: Draw How Data Flows



https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-cyber-threat-modelling.pdf?sfvrsn=a367caff_0

Step 2: System Decomposition

Task C: Divide Out Trust Boundaries

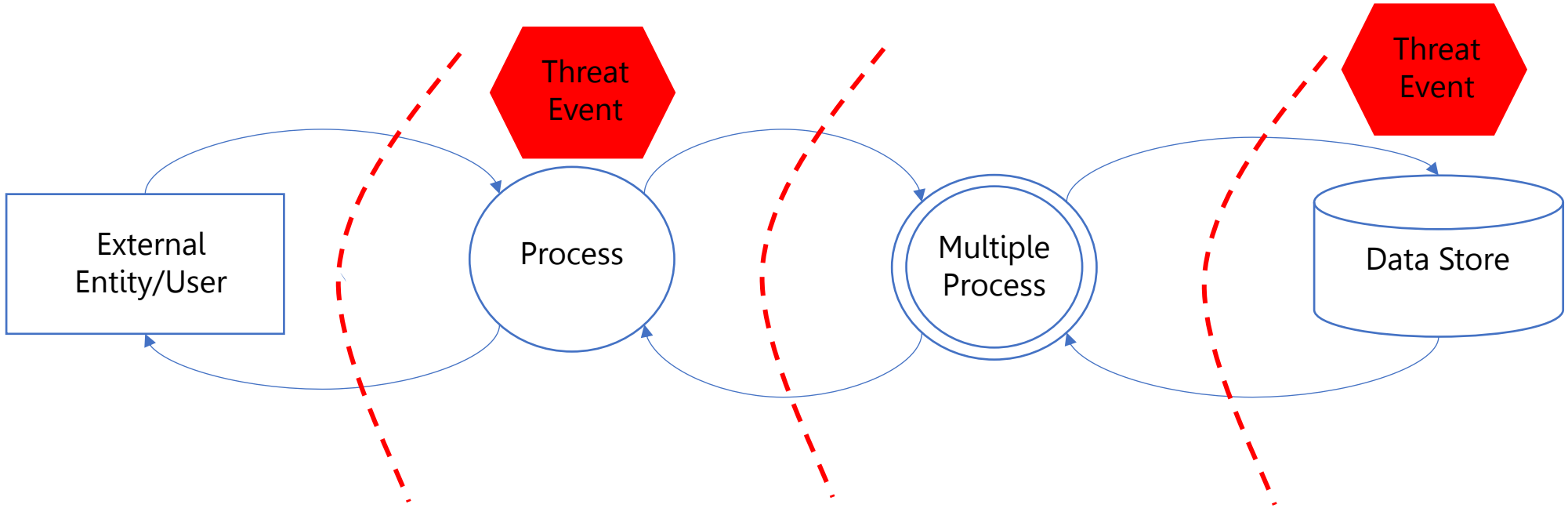


https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-cyber-threat-modelling.pdf?sfvrsn=a367caff_0

Step 3: Threat Identification

Task A: Identify Threat Vectors

Task B: List Possible Threat Events



https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-cyber-threat-modelling.pdf?sfvrsn=a367caff_0

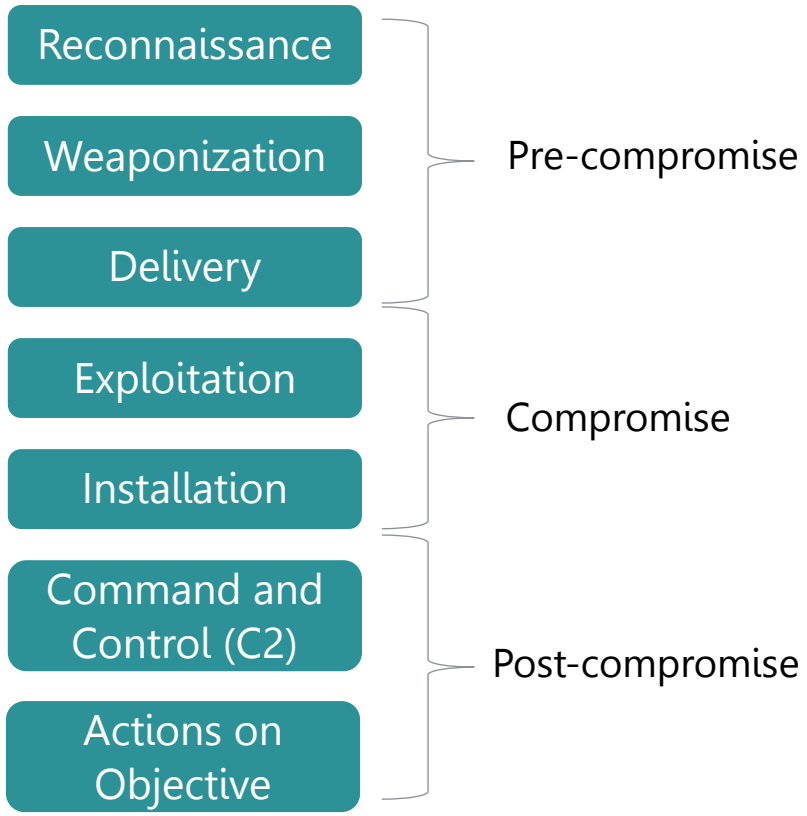
Step 4: Attack Modelling

MITRE ATT&CK

MITRE ID	Name	Description
TA0001	Initial Access	To enter the system
TA0002	Execution	To run malicious code
TA0003	Persistence	To maintain a foothold
TA0004	Privilege Escalation T	To gain higher-level permissions
TA0005	Defense Evasion	To avoid being detected
TA0006	Credential Access	To steal account names and passwords
TA0007	Discovery	To learn about the system environment
TA0008	Lateral Movement	To traverse through the system environment
TA0009	Collection	To gather information of interest
TA0011	Command and Control	To control a compromised system
TA0010	Exfiltration	To steal data
TA0040	Impact	To manipulate, interrupt, or destroy your systems and data

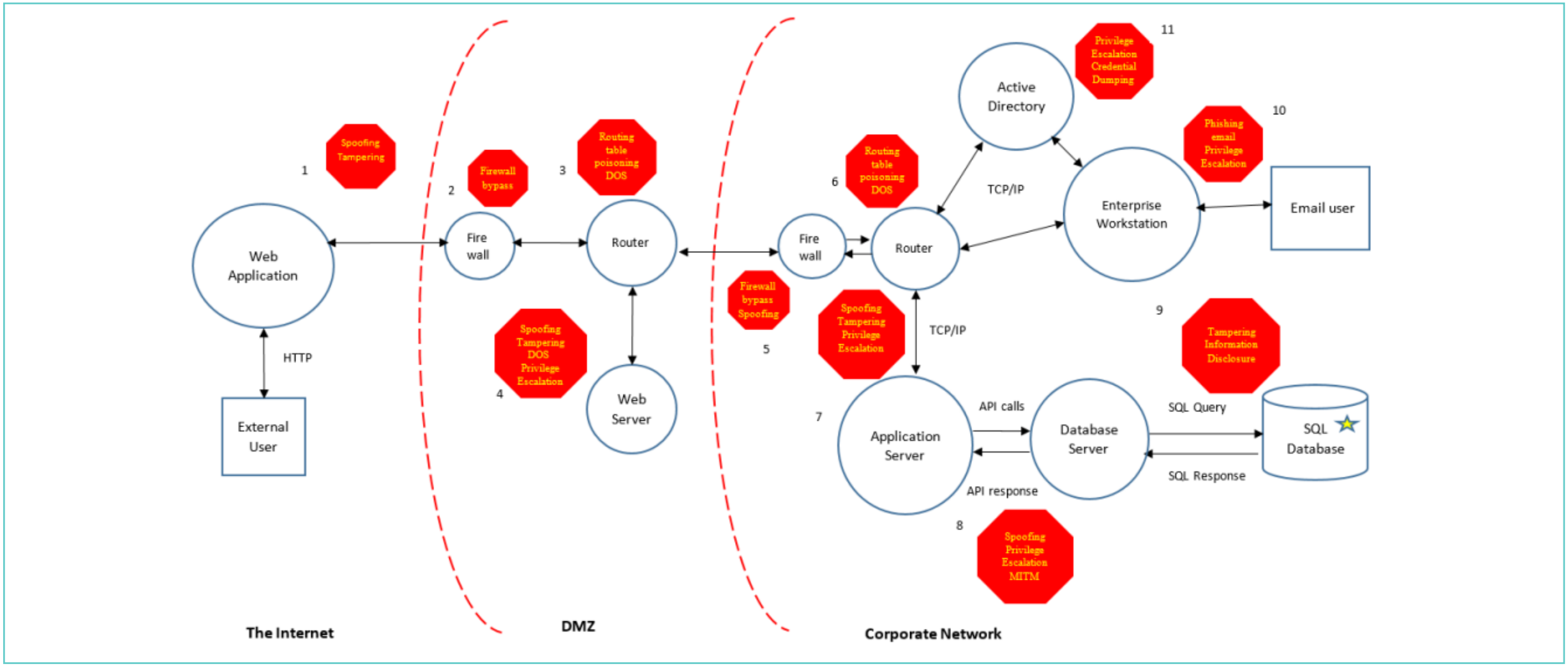
https://attack.mitre.org/matrices/

Lockheed Martin Cyber Kill Chain



https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-cyber-threat-modelling.pdf?sfvrsn=a367caff_0

Step 5: Bringing Everything Together



https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-cyber-threat-modelling.pdf?sfvrsn=a367caff_0

09

Overview of Secure Design

Overview of Secure Design

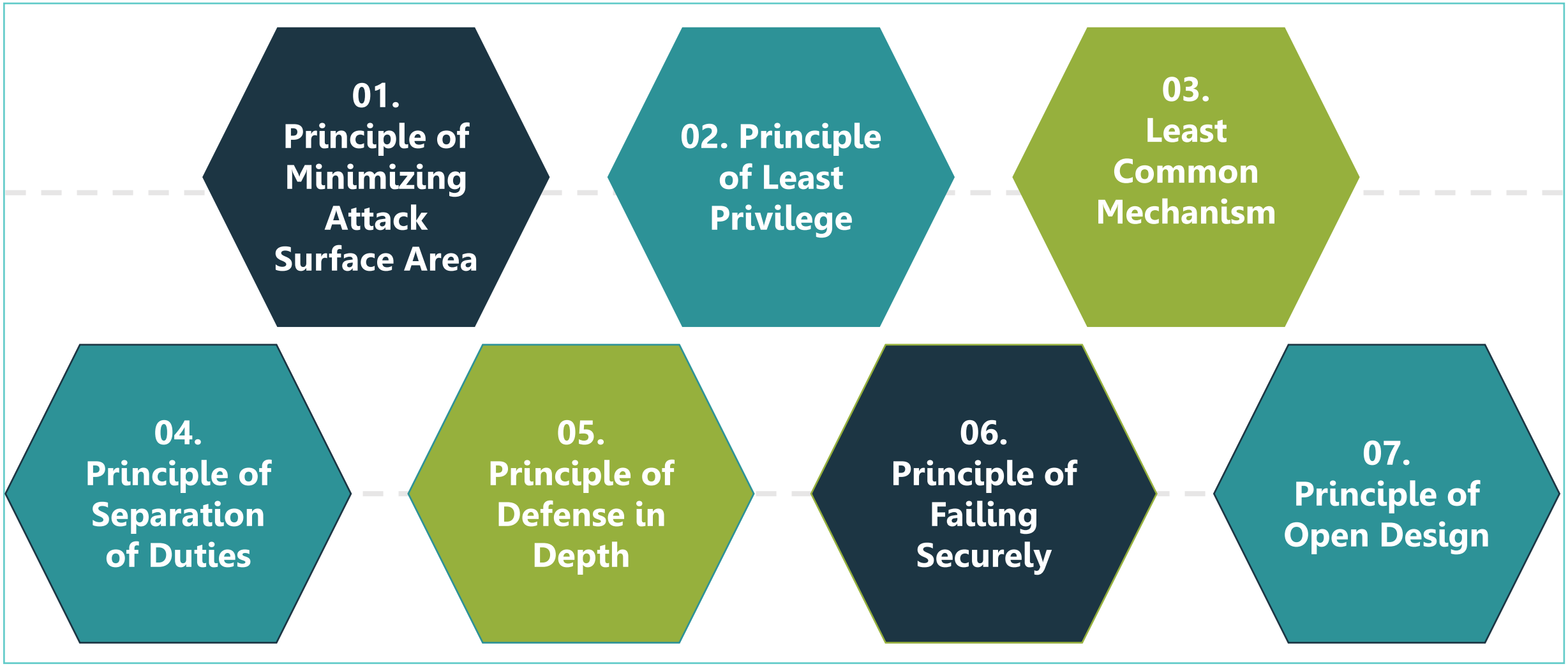
What is Secure Design ?

Secure design principles are essential for building secure systems. It is important to follow key principles to ensure the security of the system and protect sensitive data

Why Secure Design is important?

1. Reduced risk of security breaches and vulnerabilities
2. Lower costs and faster time to market
3. Enhanced customer trust and satisfaction
4. Improved regulatory compliance
5. Stronger culture of security

Security by design principles

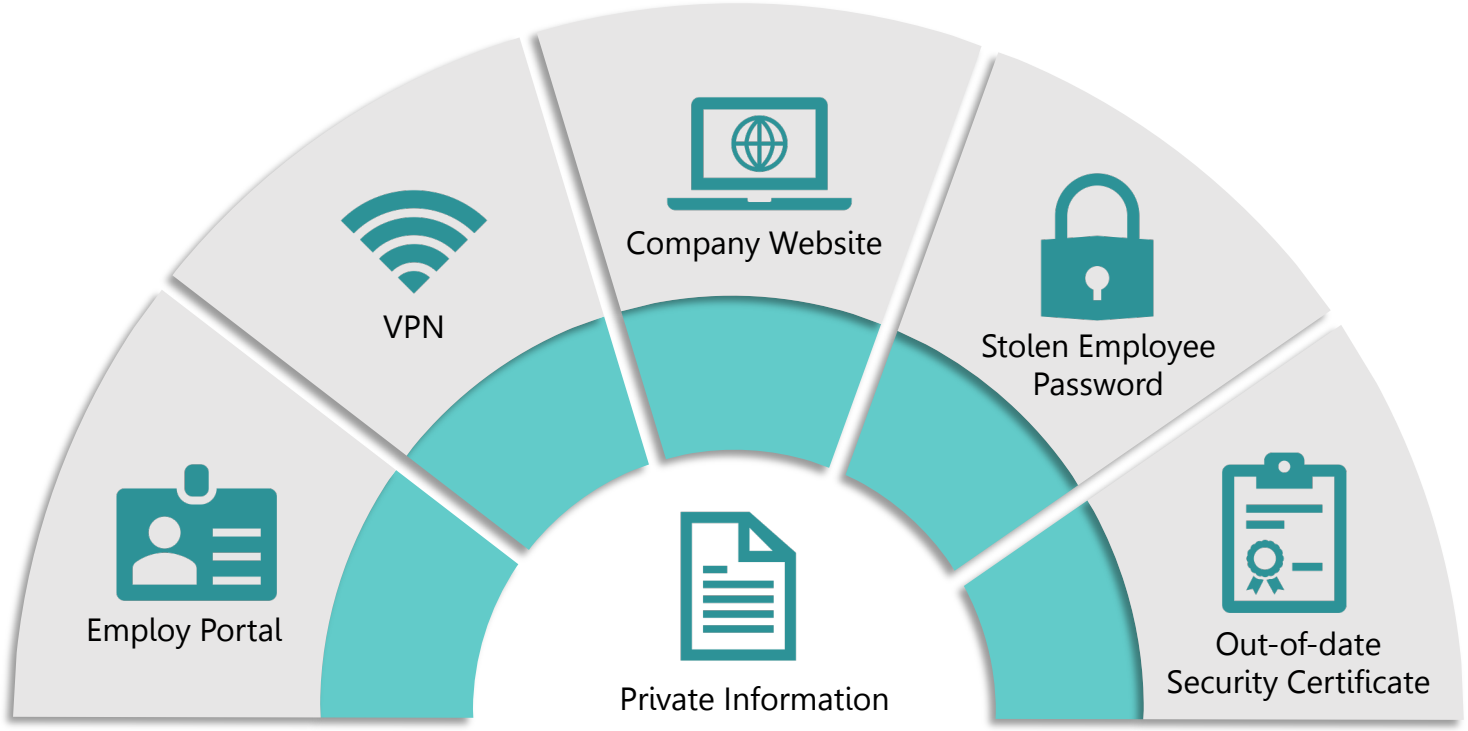


https://www.linkedin.com/pulse/importance-security-design-how-make-part-your-development-

01. Principle of Minimizing Attack Surface Area

What is Attack Surface Area ?

An attack surface is the entire area of an organization or system that is susceptible to hacking. It's made up of all the points of access that an unauthorized person could use to enter the system. Once inside your network, that user could cause damage by manipulating or downloading data.

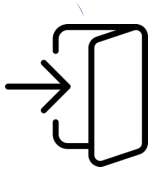


01. Principle of Minimizing Attack Surface Area

Reduce Attack Surface in 5 Steps

No user should have access to your resources until they've proven their identity and the security of their device.

01 Zero Trust



Remove user access to organization network as soon as the person is no longer part of your organization.

02 Access protocols

Use attribute-based access control (ABAC) or role-based access control (RBAC) to ensure data can be accessed by the right people.

03 Authentication

https://www.okta.com/identity-101/what-is-an-attack-surface/

01. Principle of Minimizing Attack Surface Area

Reduce Attack Surface in 5 Steps

Replicas of code and data are a common part of a typical company's attack surface. Use strict protection protocols to keep these backups safe from those who might harm you.

04 Backups

The more firewalls you build, the harder it will be for hackers to get into the core of your business with speed

05 Network Segment

https://www.okta.com/identity-101/what-is-an-attack-surface/

02. Principle of Least Privilege

What is Least Privilege ?

Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform legitimate functions. Privilege itself refers to the authorization to bypass certain security restraints. When applied to people, the principle of least privilege (POLP), means enforcing the minimal level of user rights, or lowest clearance level, that allows the user to perform his/her role.

What are Privileged Accounts ?

Privileged Accounts

Superuser Accounts

Standard user Accounts

02. Principle of Least Privilege

What are the Benefits of Least Privilege ?

01 Enhanced Data Protection, System Integrity

02 Restricted Malware Spread

03 Decreases the Likelihood of Catastrophic Harm

04 Reduces Attack Surface, Third-Party Risks

05 Increases End-User Efficiency

06 Facilitates Compliance and Auditing, Provides Better Incident Response Planning

07 Streamlines Change and Configuration Management

Best Practices for Least Privilege ?

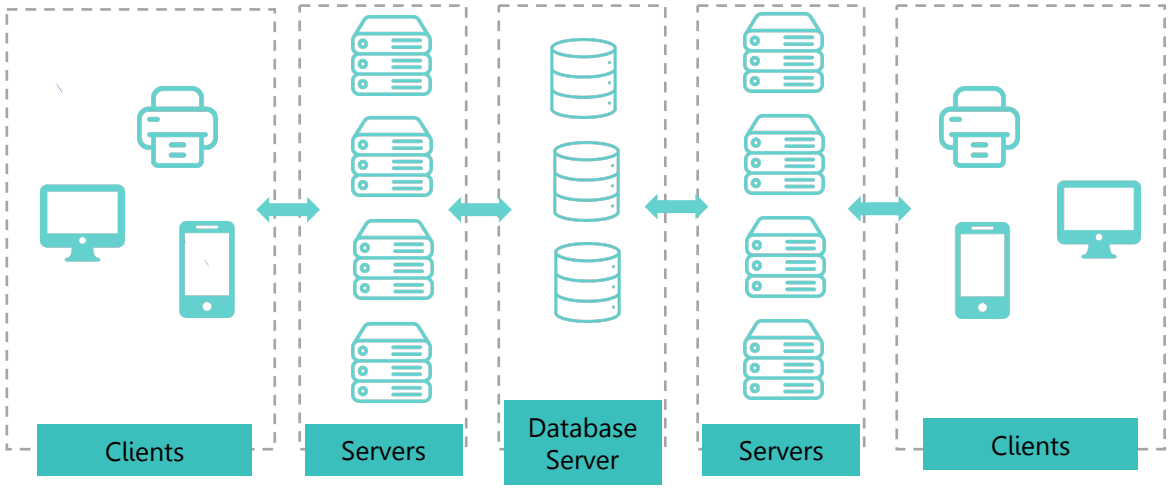
- Limit the number of privileged accounts
- Use time-limited privileges
- Adopt "least privilege as default
- Examine logs regularly
- Disable unneeded components
- Apply relevant security concepts
- Reevaluate accounts and privileges often.

03. Least Common Mechanism

What is Least Common Mechanism ?

Mechanisms used to access resources (e.g. Virtual memory or File systems) should not be shared.

This principle is also restrictive because it limits sharing of resources. Sharing resources provides a channel along which information can be transmitted. Hence, sharing should be minimized as much as possible. If the operating system provides support for virtual machines, the operating system will enforce this privilege automatically to some degree.



The Client-Server Model

04. Principle of Separation of Duties

What is Separation of Duties ?

Principle of Separation of Duties is to prevent conflict of interest (real or apparent), wrongful acts, fraud, abuse and errors. This principle ensures that individuals don't have conflicting responsibilities, and helps detection of control failures like security breaches, information theft and circumvention of security controls.

Access controls

DAC

Discretionary Access Control

Grant right subjects

Ex. Read, Write, Execute

MAC

Mandatory Access Control

Specific permission, and the permission is up to owner

RBAC

Role-based Access Control

Assign based on role and job function

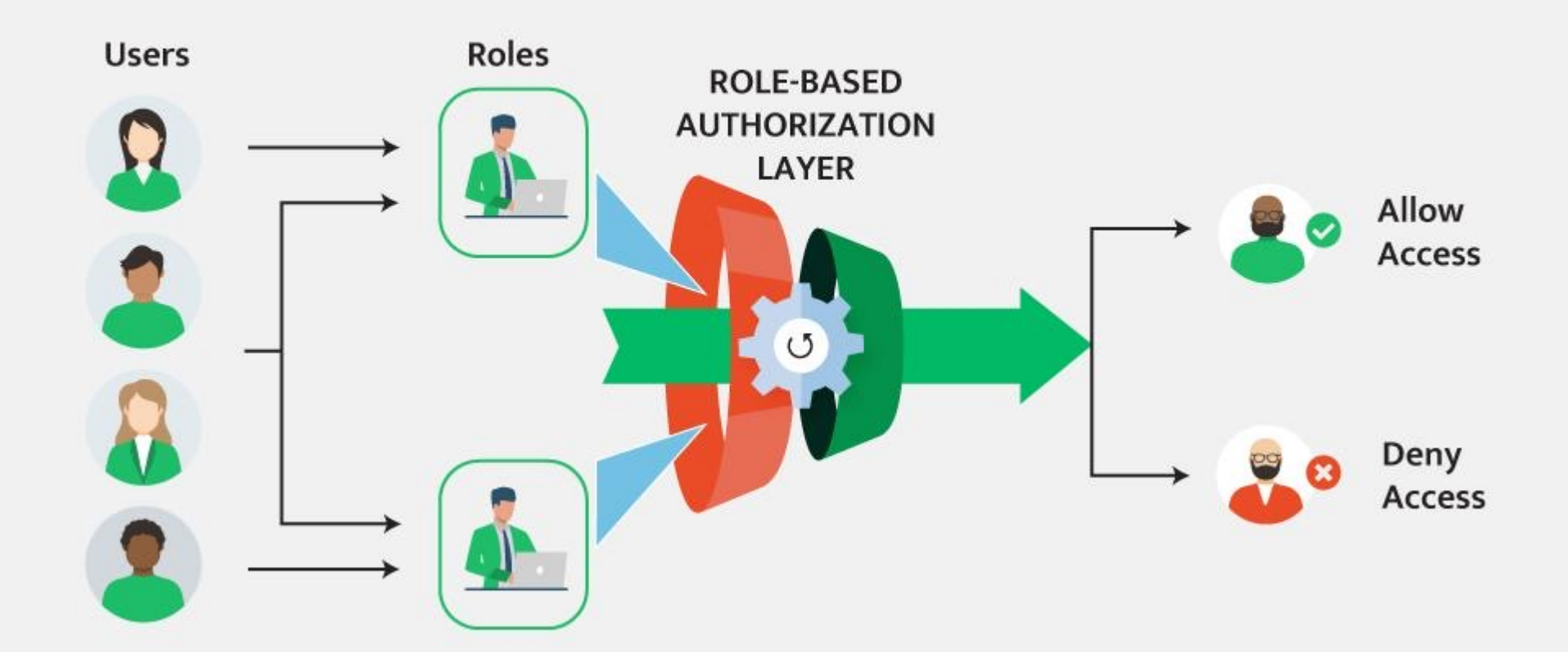
ABAC

Attribute-based Access Control

Require specific attributes (zero trust)

04. Principle of Separation of Duties

Role-based Access controls



https://pathlock.com/learn/segregation-of-duties-in-your-organization/

04. Principle of Separation of Duties

Role-based Access controls - Matrix

Procedure/ Function	User group (role)	Hire employee	Change compensation	Change benefits	Create paycheck
Hire employee	1	√			
Change compensation	2		√	√	
Change benefits	3		√	√	
Create paycheck	4				√

Conflict

Procedure/ Function	User group (role)	Hire employee	Change compensation	Change benefits	Create paycheck
Hire employee	1	√			
Change compensation	2		√		
Change benefits	3			√	
Create paycheck	4				√

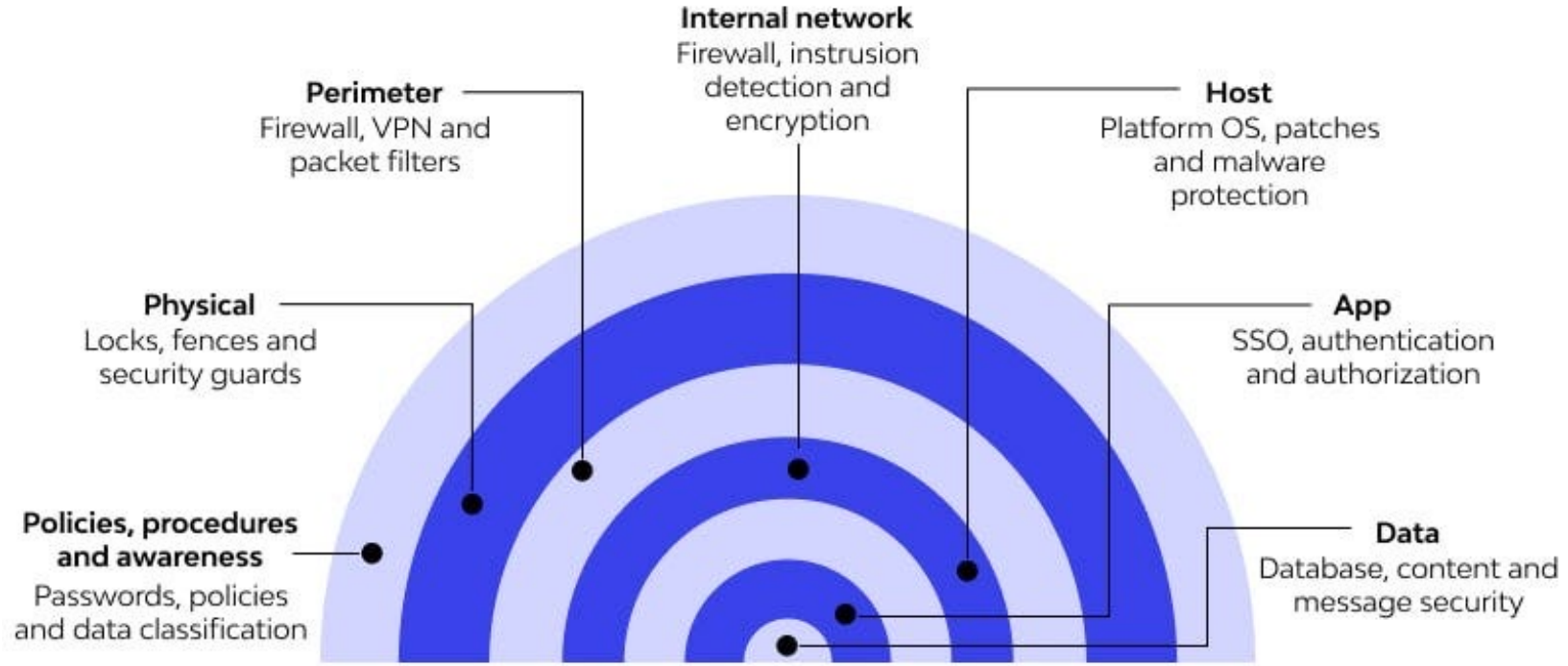
No Conflict

https://pathlock.com/learn/segregation-of-duties-in-your-organization/

05. Principle of Defense in Depth

What is Defense in Depth ?

Defense in Depth is a security strategy that prevents data breaches and slows down unauthenticated attempts to access data by deploying an intense environment with 7 layers of protection and validation. The principles that help define a security posture are confidentiality, integrity, and availability.



https://medium.com/@cyber.ghost/what-is-defense-in-depth-5a8596839f65

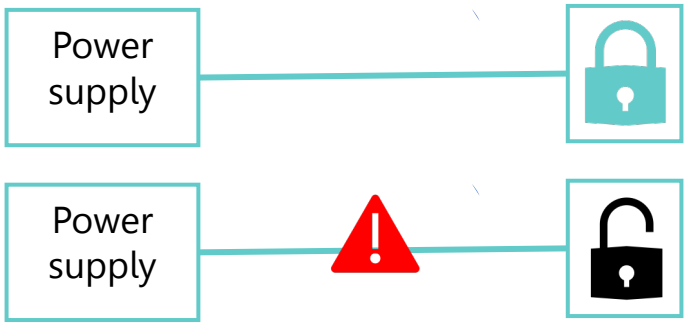
06. Principle of Failing Securely

What is Failing Securely ?

A need to design systems that can fail without leaving systems open to attack. To do this, developers can base access decisions on permission rather than exclusion. The default situation **should block access** until the conditions of a preset protection scheme are met.

Fail Safe

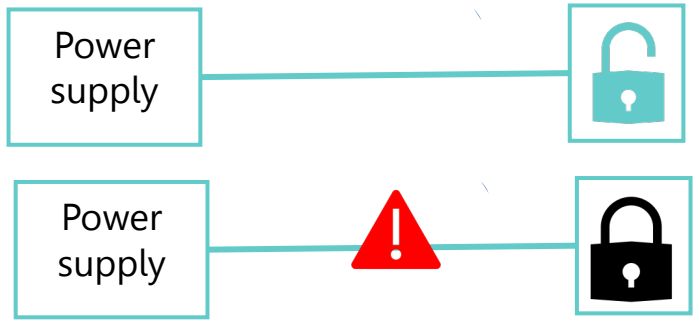
If power goes out, remain unlocked.



Stairwells, Hospitals, Fire Exits, etc.

Fail Secure

If power goes out, remain locked.



Banks, Inner-office, etc.

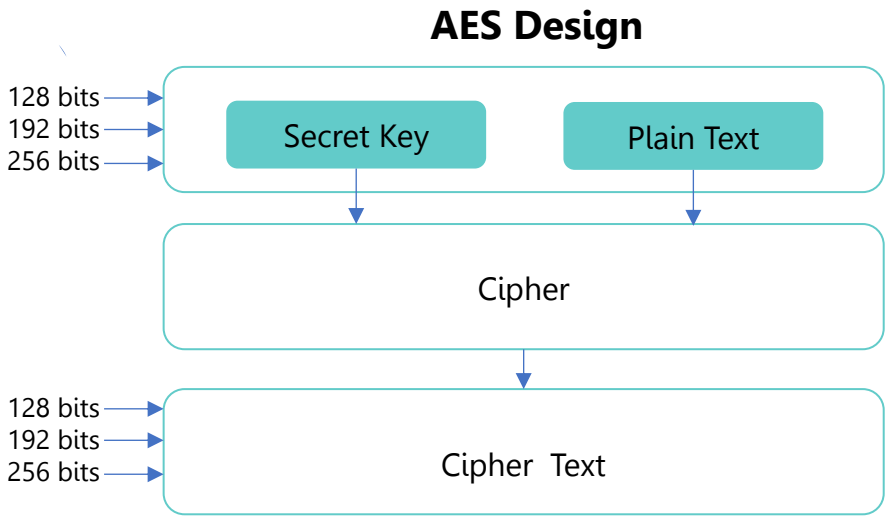
07. Principle of Open Design

What is Open Design ?

The security of a mechanism should not depend on the secrecy of its design or implementation.

Security of a mechanism should not depend upon secrecy of its design or implementation

- Secrecy != security
- Complexity!= security
- Security through obscurity
- Cryptography and openness



10

Hardening Methodology

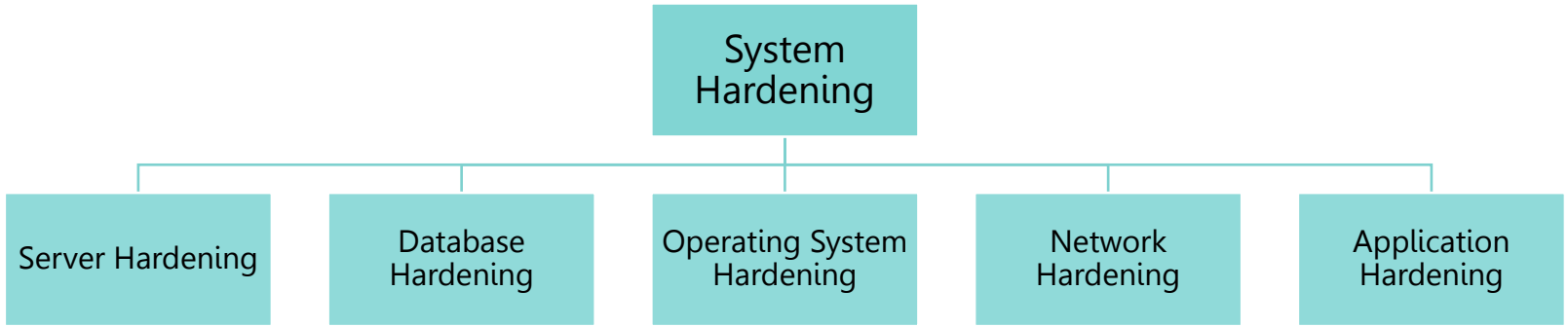
Hardening Methodology

What is Hardening ?

System hardening is the collection of steps and processes that increase a system's security by minimizing the exposed attack surface of the infrastructure. This process aims to improve reliability and security to ensure smooth business operations.

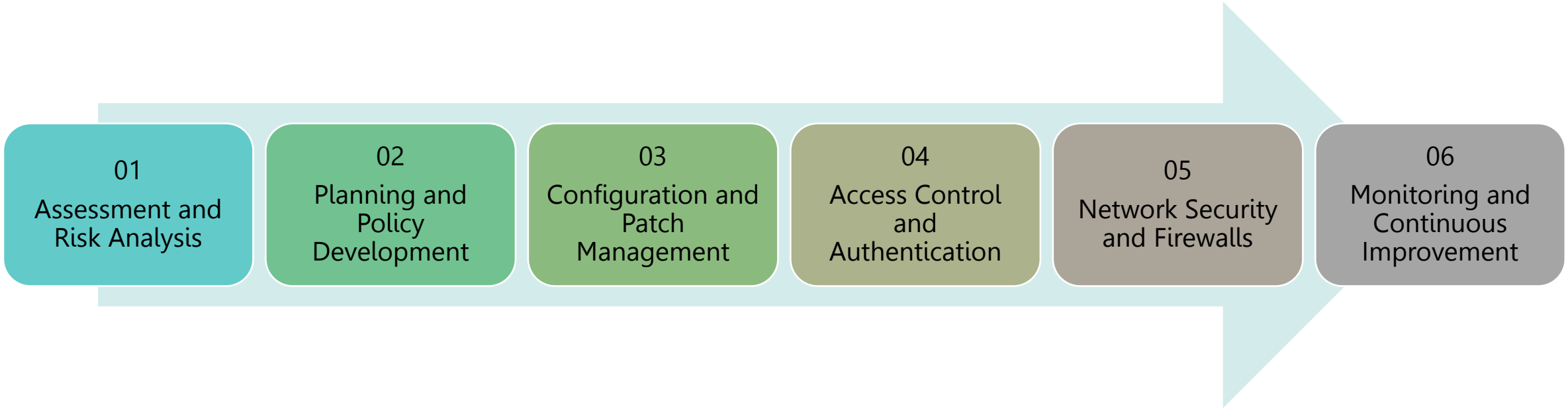
System hardening is a proactive strategy to reduce these risks by minimizing how hackers can access and attack the infrastructure components. In practical terms, system hardening strengthens and supplements other cybersecurity practices, resulting in several layers of defense consisting of firewalls, intrusion detection systems, and antivirus software.

Types of System Hardening



Hardening Methodology

The System Hardening Process



Hardening Methodology

System Hardening Standards

The CIS Benchmarks are recommendations and recommended practices for securely setting up different operating systems, software, and network devices. These benchmarks were created by the Centre for Internet Security and are frequently updated by the community of cybersecurity experts.

CIS Benchmarks

NIST Special Publication 800-53 offers a complete list of security measures and related US federal information systems guidelines. It covers various security measures, including system and communications protection, user and process identification and authentication, audit and accountability, and access control.

NIST SP 800-53

DISA STIGs ((Defense Information Systems Agency Security Technical Implementation Guides) are security recommendations created by the Defense Information Systems Agency for protecting software and computer systems.

DISA STIGs

Hardening Methodology

Benefits of Following System Hardening Standards

01 Smaller Attack Surface
System hardening standards focus on securing or disabling unused services, ports, and configurations. These steps directly reduce the possible points of entry/execution for cyber attacks

02 Increased Security Posture
System hardening techniques result in a measurable improvement in an organization's overall security posture. When applied properly, you can be sure that all systems are set up securely, and the infrastructure becomes resilient to possible attacks.

03 Security from Known Vulnerabilities
System hardening standards call for quick application of security upgrades and fixes. This lessens the chance of hackers exploiting known vulnerabilities in operating systems, applications, and devices.

04 Regulation and Framework Compliance
Numerous system hardening guidelines help increase compliance with industrial regulations and cybersecurity frameworks. This increased compliance with these standards helps organizations avoid legal issues stemming from regulatory violations.

05 Protection Against Emerging Threats
Organizations can better protect themselves against emerging cyber threats and attack vectors by updating their security standards. This significantly reduces the risk of emerging attack vectors using existing vulnerabilities to compromise your system.

Key Takeaway – 03 Principles

Key Takeaway for 03 Principles

Threat Modeling

Threat modeling techniques help identify potential threats and prioritize security controls and countermeasures.

Secure Design

Secure design principles emphasize integrating security into the design phase of software and systems development to mitigate vulnerabilities.

Hardening

System hardening involves strengthening configurations and implementing security measures to minimize risks and protect against cyber threats effectively.

C.

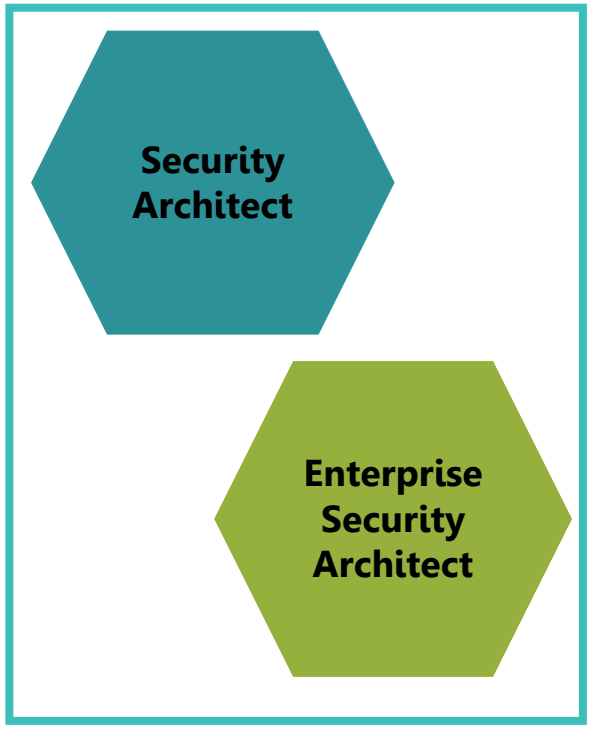
Summary

C.

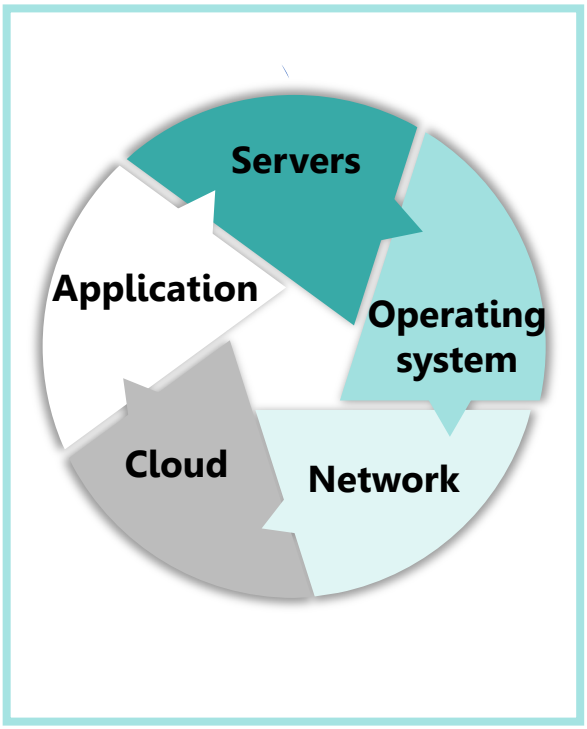
Summary of Security Architect and Design

Summary of this topic

Security Architect



System Architect



Principles