Cloud Application Security for CCSP®

Cloud Application Development Security

Kevin Henry
CISM CISSP CCSP

kevin@kmhenrymanagement.com

CCSP Certification Examination

Domains	Weights
1. Cloud Concepts, Architecture and Design	17%
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	17%
4. Cloud Application Security	17%
5. Cloud Security Operations	16%
6. Legal, Risk and Compliance	13%

Cloud Application Security

Agenda:

Cloud Application Development Security

Cloud Application Security Testing

The Challenges with Application Security

Applications are built for function

Security can impact performance

Applications are built from many pieces

Developers often have inadequate security training

Rush to production can impact quality

Cloud Application Security

Not all systems can be ‘forklifted’ to the cloud

The CSP may – or may not - be more secure

Integration with legacy systems

Multiple types of end-point devices

Wider attack surface

Key Training Requirements

Security is as essential as function

They are complementary not contradictory

Version control is required

Documentation is not an option

All changes must be tested

Regression

Key Training Requirements

Standards must be followed:

Coding

Documentation

Testing

Change Control

Cloud-based Threats

Threats in the Cloud

Hardware - isolation

Virtualization - misconfigured

Cloud environment – fewer network controls

Communication layer – multiple microservices

Service-application layer

Orchestration layer - scheduling

Common Cloud Vulnerabilities

Multi-tenancy

Lack of Documentation

Insecure APIs

Network Based Attacks

Threat Modeling - STRIDE

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Escalation of Privilege

Threat Modeling - DREAD

Damage

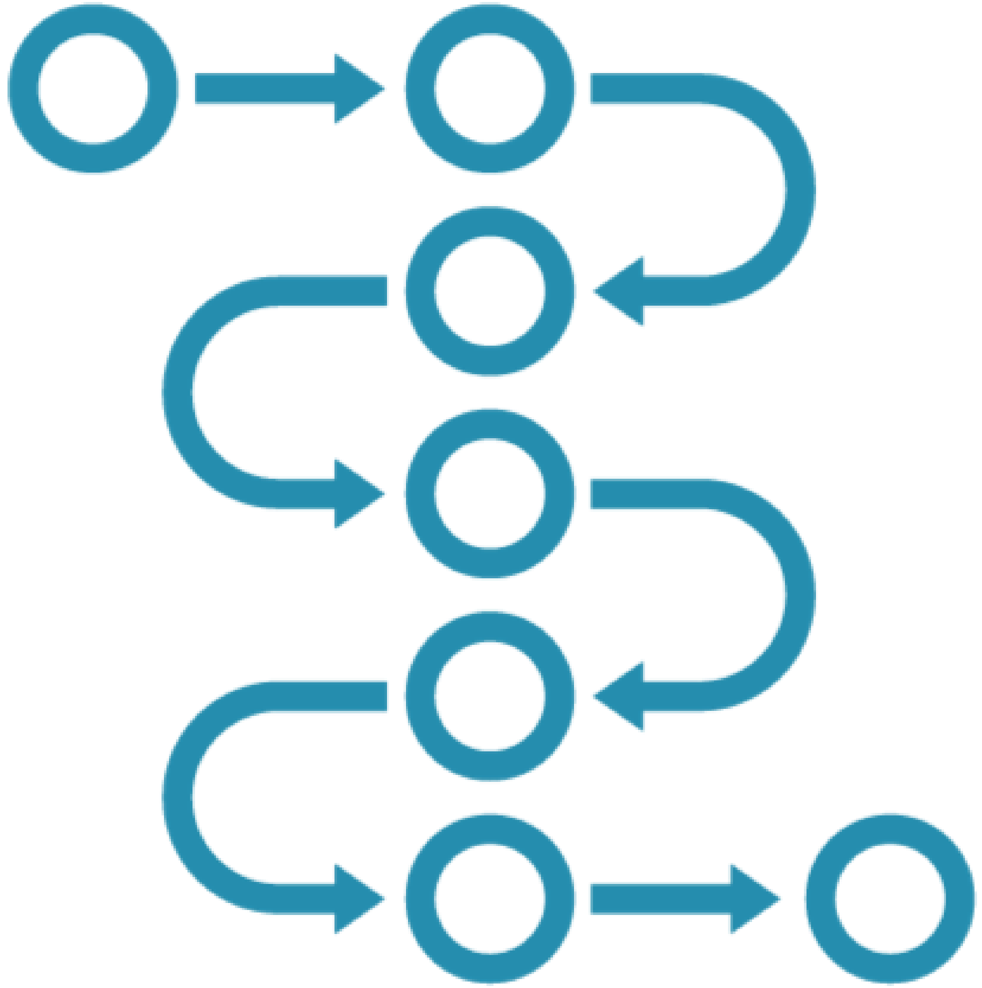
Reproducibility

Exploitability

Affected Users

Discoverability

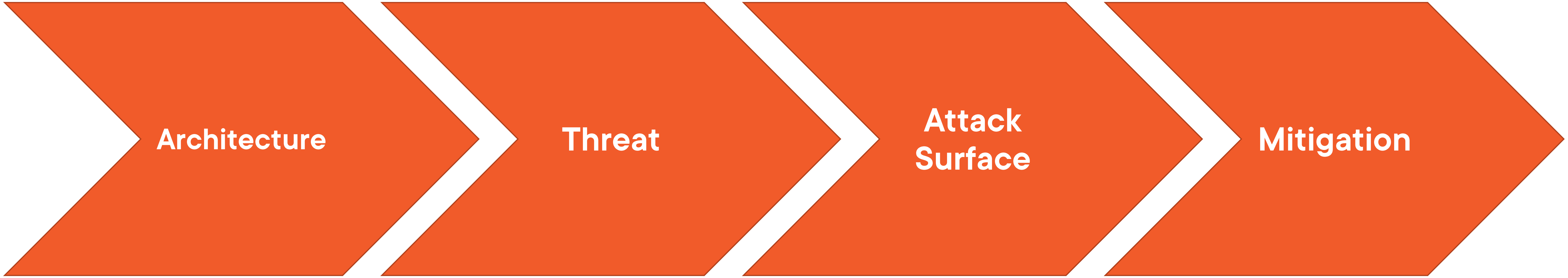
P.A.S.T.A.



Process for Attack Simulation and Threat Analysis:

- Define the Objectives
- Define the Technical Scope
- Decompose the Application
- Analyze the Threats
- Vulnerability Analysis
- Attack Analysis
- Risk and Impact Analysis

ATASM


Architecture

Threat

Attack Surface

Mitigation

Support for Application Security

PA-DSS

OWASP Top Ten

ASVS – Application Security Verification Standard

SAFECode

CWE (Common Weakness Enumeration) Top 25

Most dangerous Software Weaknesses list linked to:

- CVSS (common Vulnerability Scoring System)
- NVD (National Vulnerability Database)
- CVE (Common Vulnerability and Exposure)
- CISA (Cybersecurity and Infrastructure Agency)

Building Secure Systems

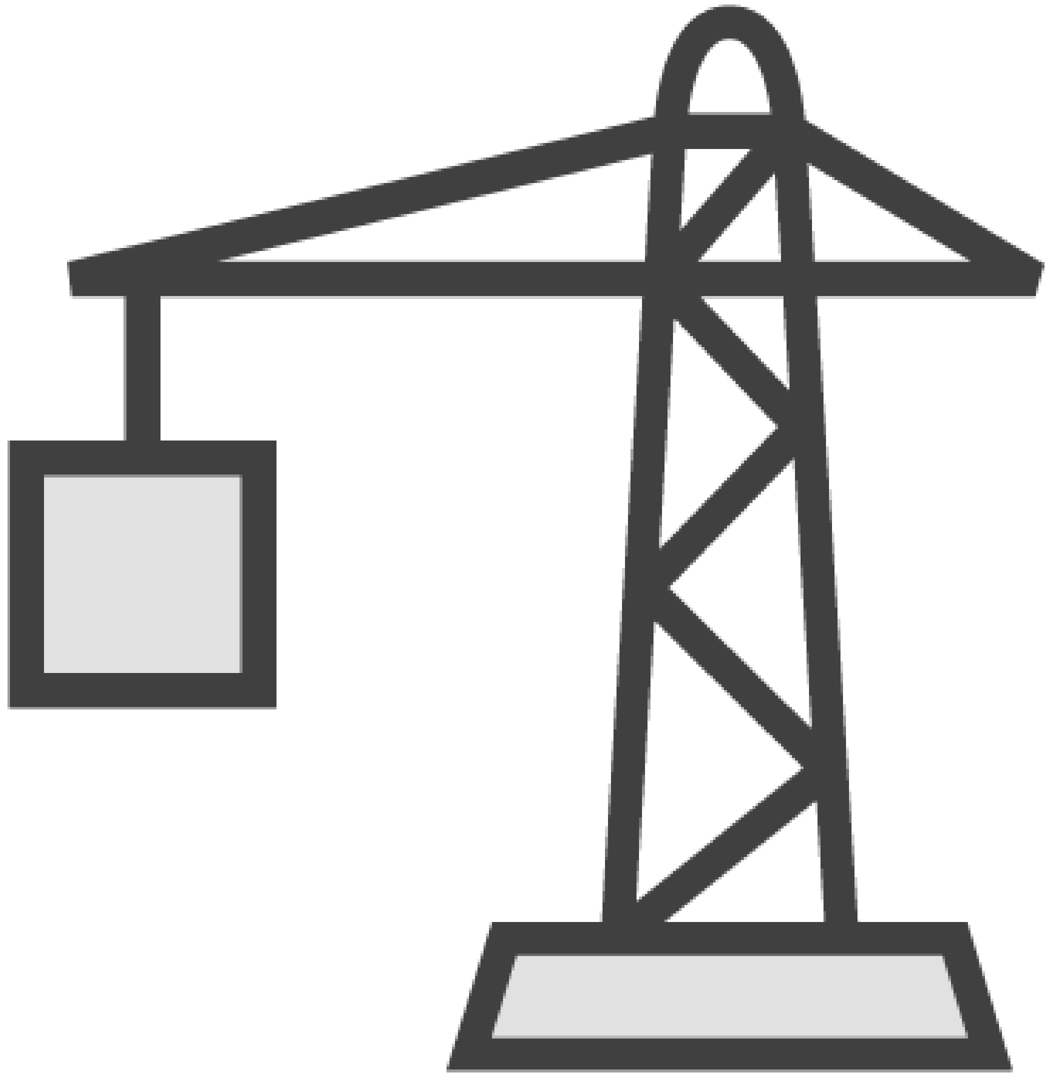
“Providing satisfactory security controls in a computer system is in itself a system design problem. A combination of hardware, software, communications, physical, personnel and administrative-procedural safeguards is required for comprehensive security. In particular; software safeguards alone are not sufficient.”

-- The Ware Report
Defense Science Board Task Force on Computer Security, 1970.

System Alternatives

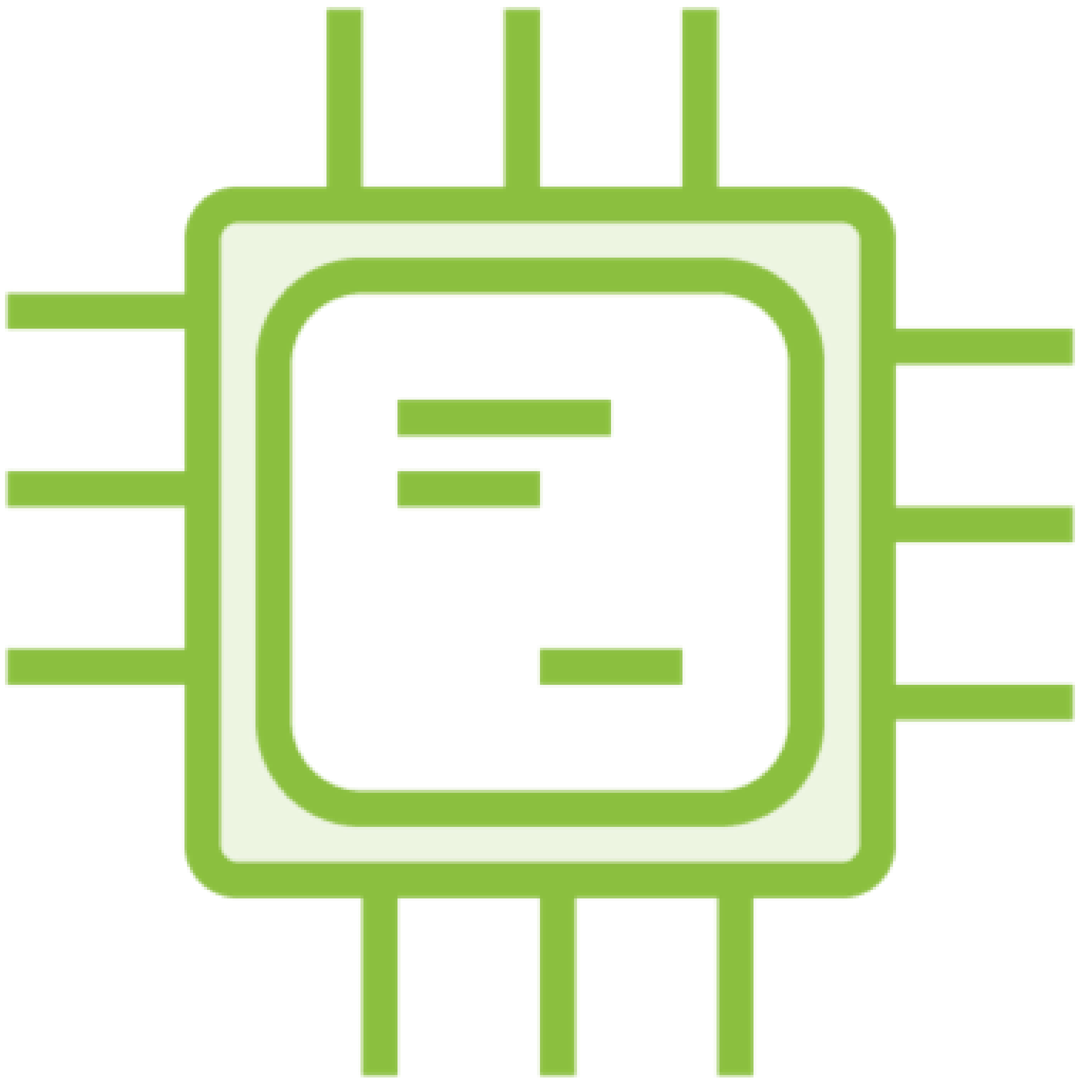
Acquisition

Supply



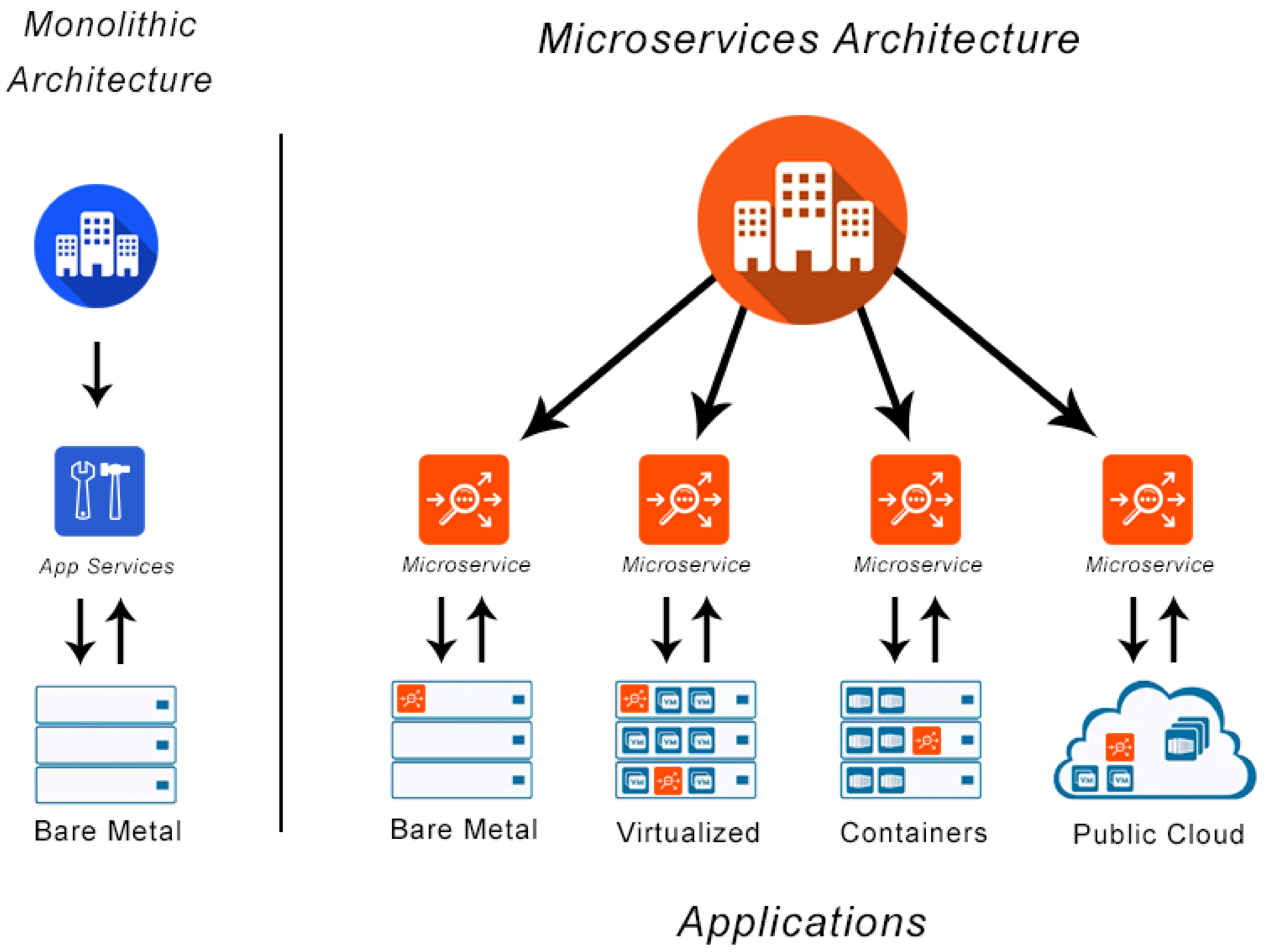
Applications Development

Applications

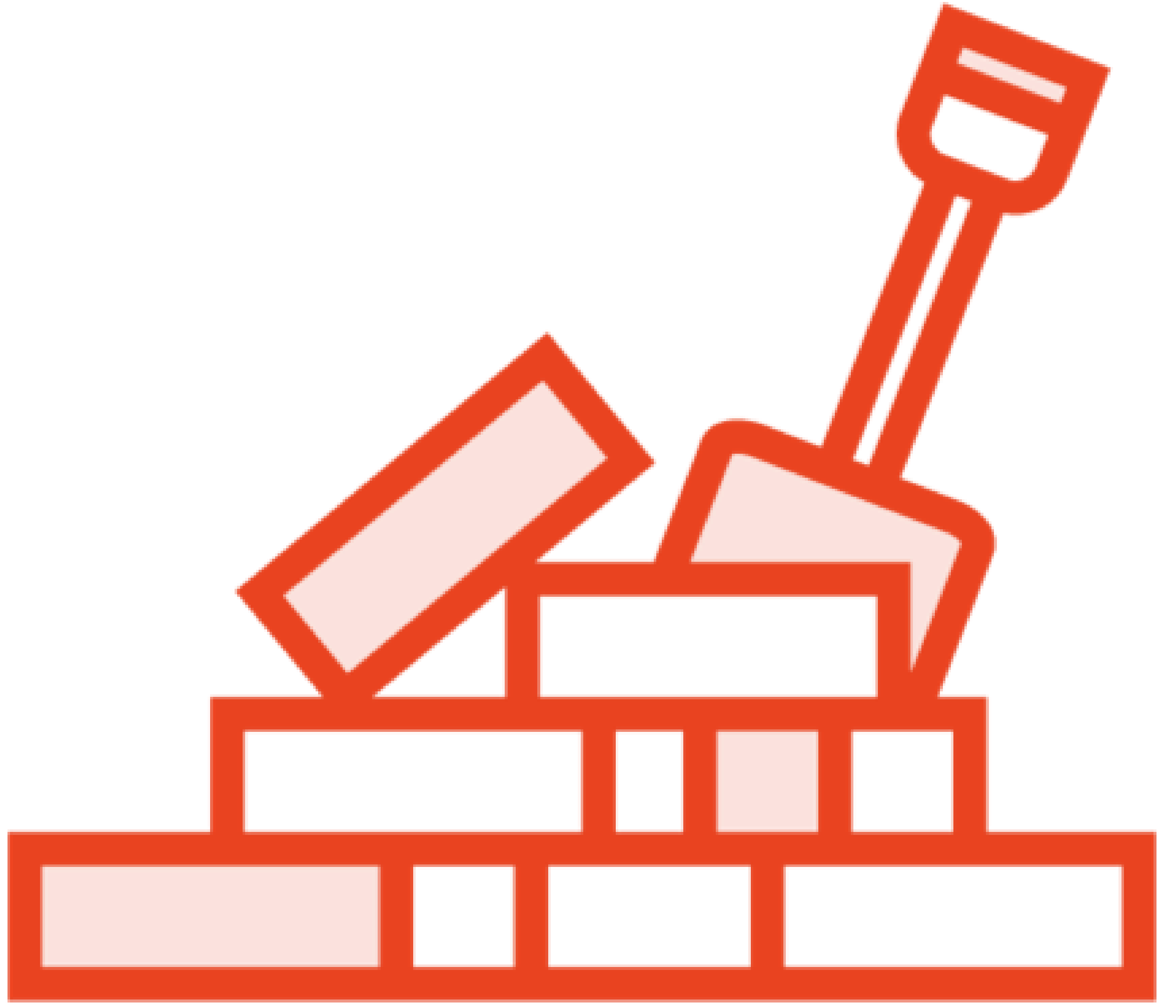


Microservices

Monolithic Versus Microservices Architecture

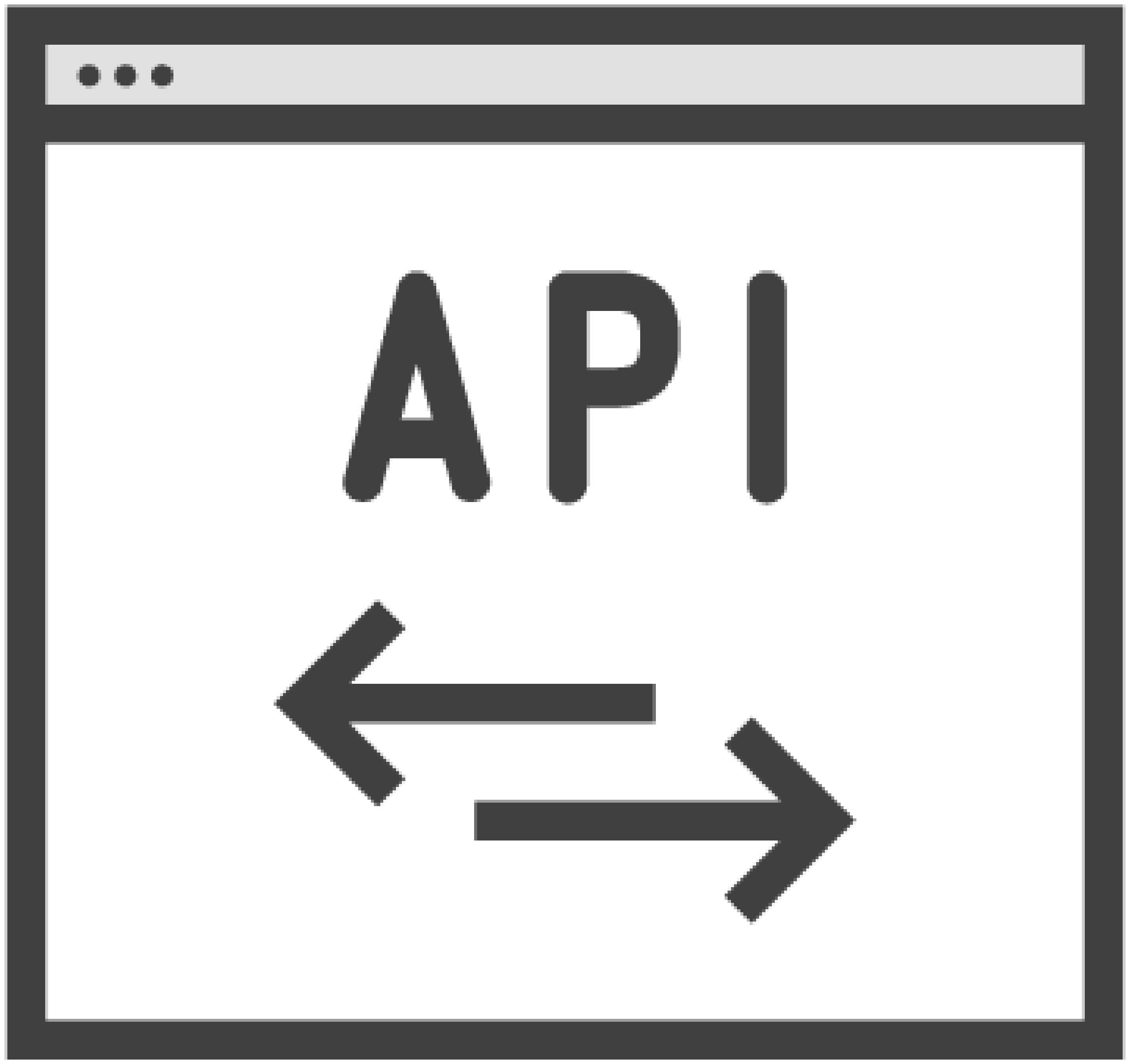


Foundation of Microservices



- Loosely coupled
  - May cause the risk of dependencies
- Lightweight communications protocols
- Granular access controls within microservices

API Characteristics



Act as an interface between system elements

Aggregate data from several microservices into one service

May be insecure – need to be tested for data leakage

Systems Development Methodologies

Life Cycle Stages

Concept

Development

Production

Utilization

Support

Retirement

As depicted in ISO/IEC/IEEE 15288-2015

Concept Phase

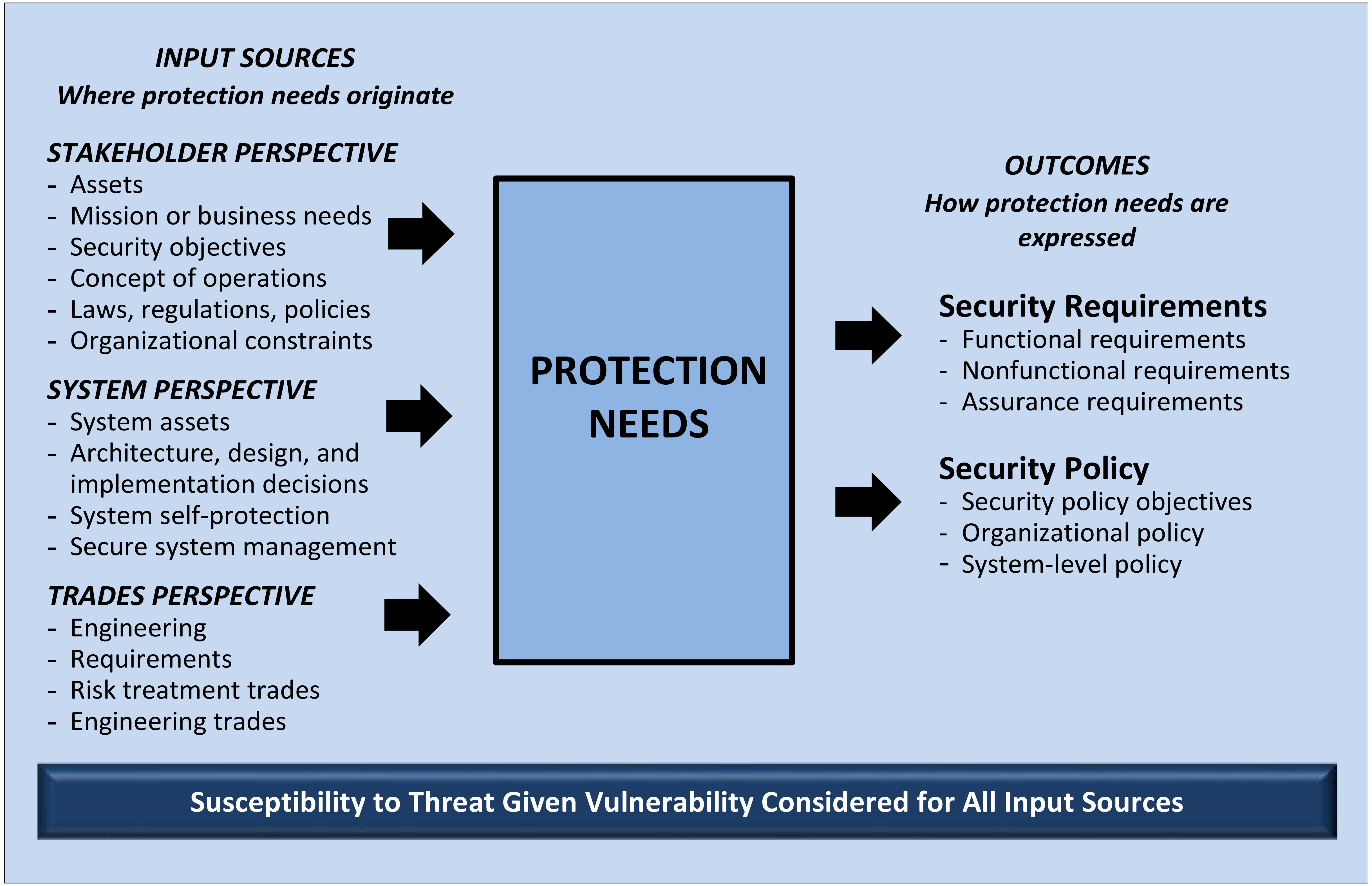
Define business functions to be provided by system

- Problem Space
  - Non-technical

Define Security requirements based on data processed by the application

- Intellectual Property, PII, financial, investigative

Gathering Requirements



INPUT SOURCES
Where protection needs originate

STAKEHOLDER PERSPECTIVE
- Assets
- Mission or business needs
- Security objectives
- Concept of operations
- Laws, regulations, policies
- Organizational constraints

SYSTEM PERSPECTIVE
- System assets
- Architecture, design, and implementation decisions
- System self-protection
- Secure system management

TRADES PERSPECTIVE
- Engineering
- Requirements
- Risk treatment trades
- Engineering trades

PROTECTION NEEDS

OUTCOMES
How protection needs are expressed

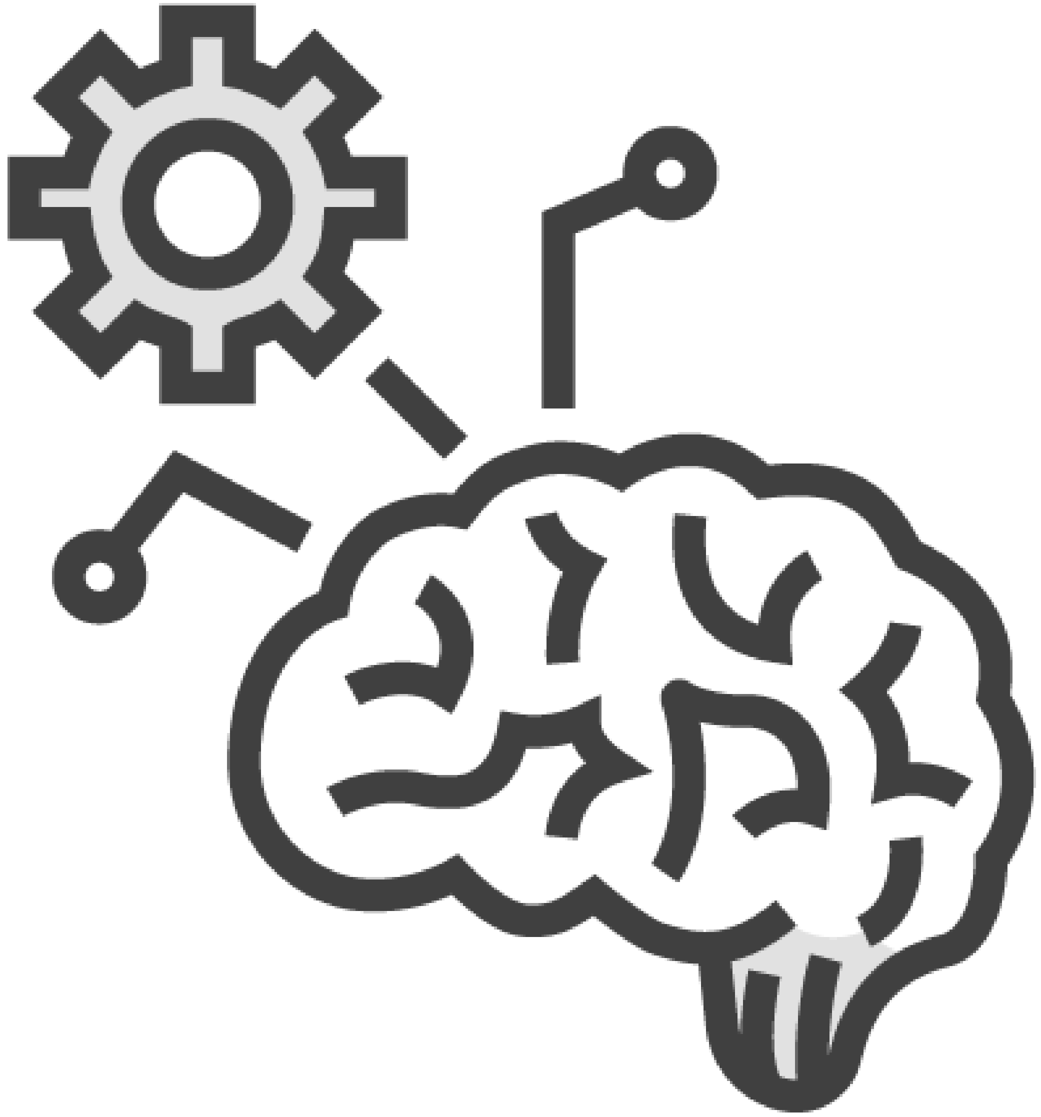
Security Requirements
- Functional requirements
- Nonfunctional requirements
- Assurance requirements

Security Policy
- Security policy objectives
- Organizational policy
- System-level policy

Susceptibility to Threat Given Vulnerability Considered for All Input Sources

NIST SP800-160

Development Phase



Development may be done by a disparate team

- May be managed by CSP or internal or external developer teams
- Coding and documentation standards
- Project management
- Build in the ability to test and audit
- May be a very dynamic process
  - Agile
  - DevOps or DevSecOps

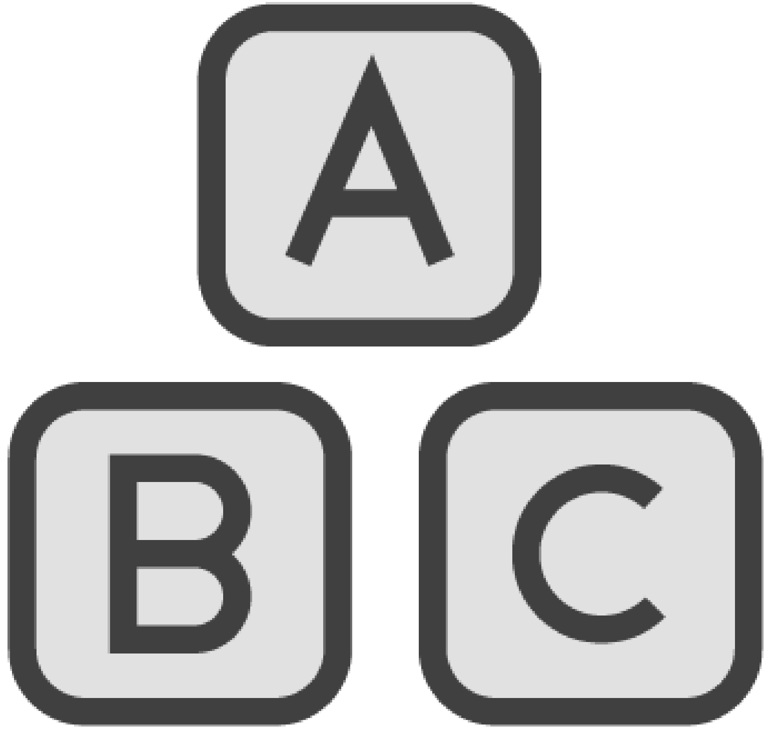
Quality Assurance

A QA pipeline is essential to ensure integrity of production systems

- Test all changes
- Even Agile development must follow change management process

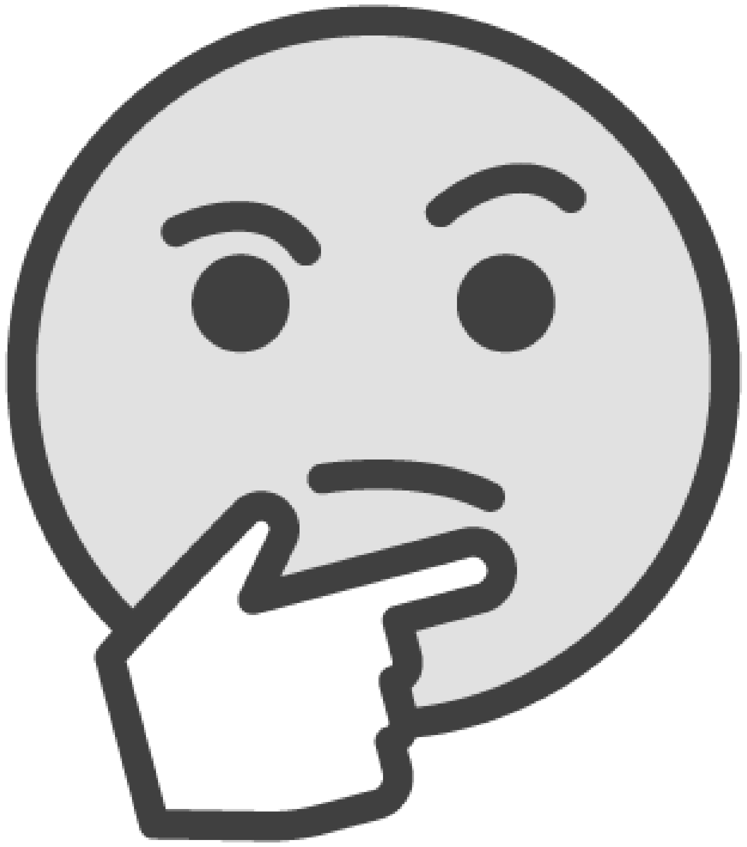
Production

Patching



Version control

Review of logs



Addressing user issues

Key Points Review

The Cloud provides unique security challenges to Application development and operation

The security professional should ensure that security is designed into, implemented and maintained in cloud-based applications

Identity Basics

Identity Management

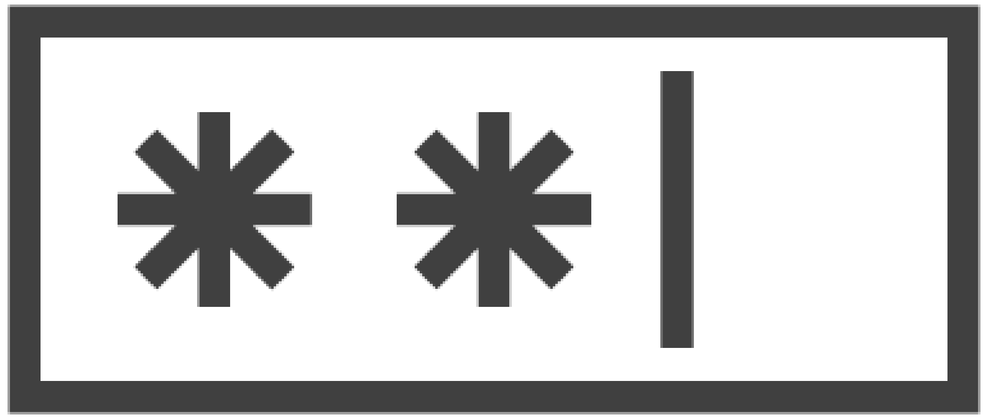
Identification

Authentication

Authorization

Accounting / Auditing

Identity Management



Identity

- Unique – secure registration process
  - Not shared
  - Individuals and process IDs

Identity Management

Authentication

Verification of the right to use the stated identity

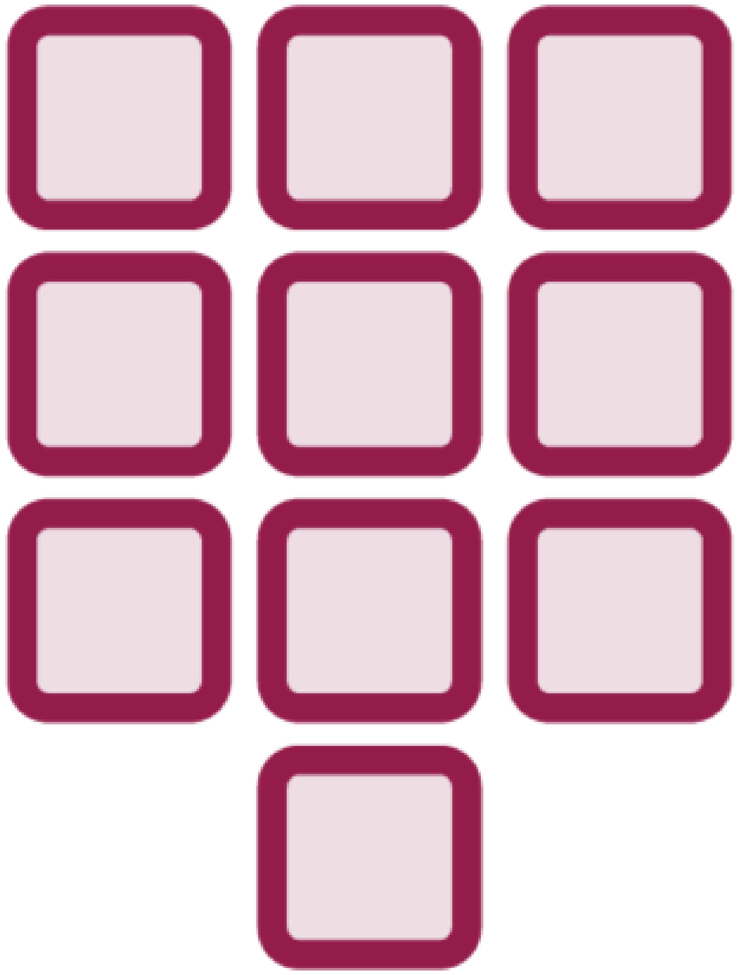
Three factors:

What you know

What you have

What you are

Identity Management



Multifactor Authentication (MFA)

- Using a combination of two or more authentication factors to increase the reliability of the authentication process
- Sometimes known as ‘strong authentication’

Identity Management

Least privilege

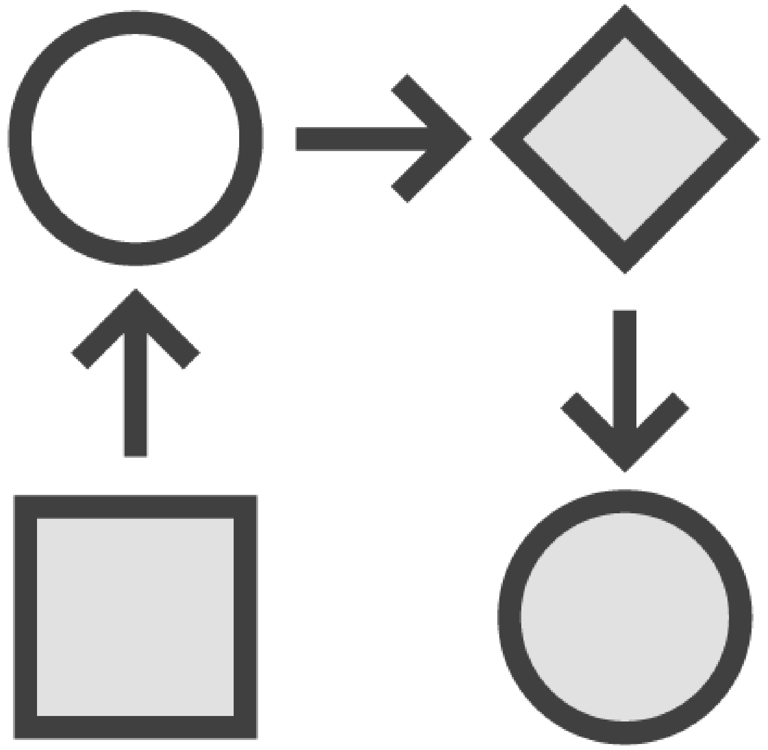
Need to know

Separation of duties

- Dual control
- Mutual exclusivity

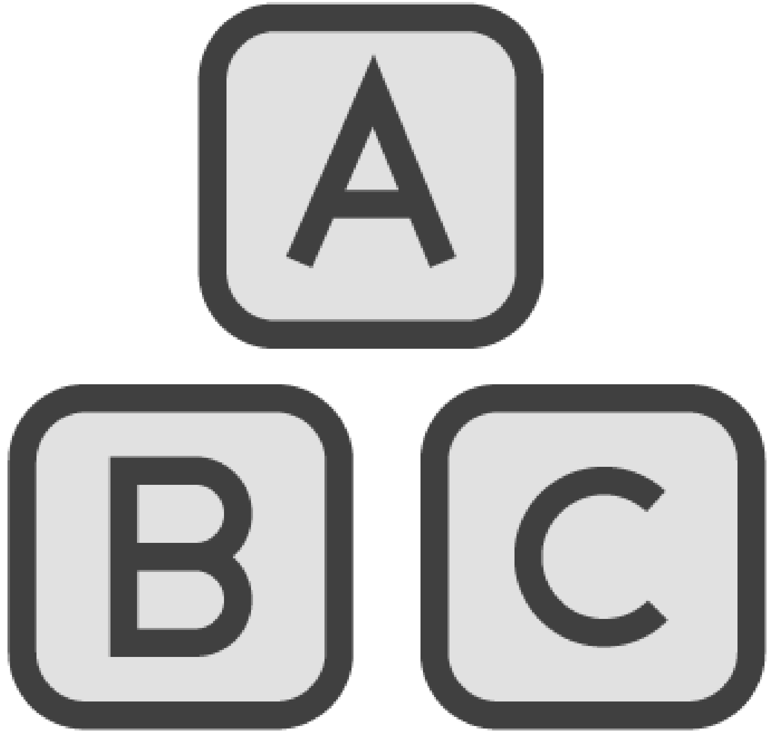
Identity Management

Authorization:



Rule-based access control

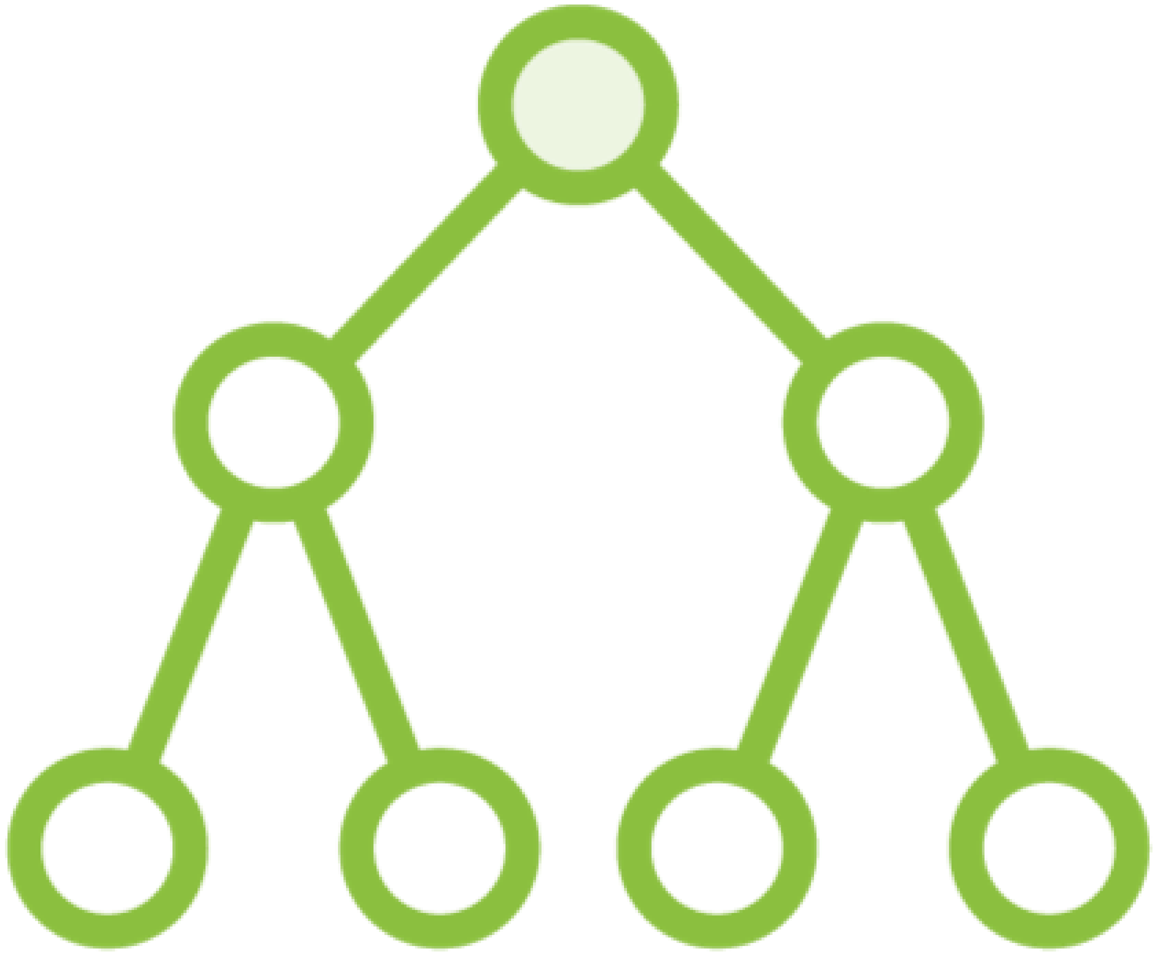
Role based access control (RBAC)



Attribute based access control (ABAC)

- Temporal
- Location

Implementations of Authorization



Directory

- LDAP
- Microsoft Active Directory
    - Schema
    - Replication
- X500
- Various other vendor products

Identity Management

Accounting / Auditing

Recording all activity on a system

Ability to associate actions with a known identity

Log retention, management, analysis

- Compliance
- Investigations

Identity Management

Is almost always the responsibility of the Cloud Consumer

- Manages access rights of their users
- CSP manages access to the equipment or components that they manage

Identity Management

IDaaS

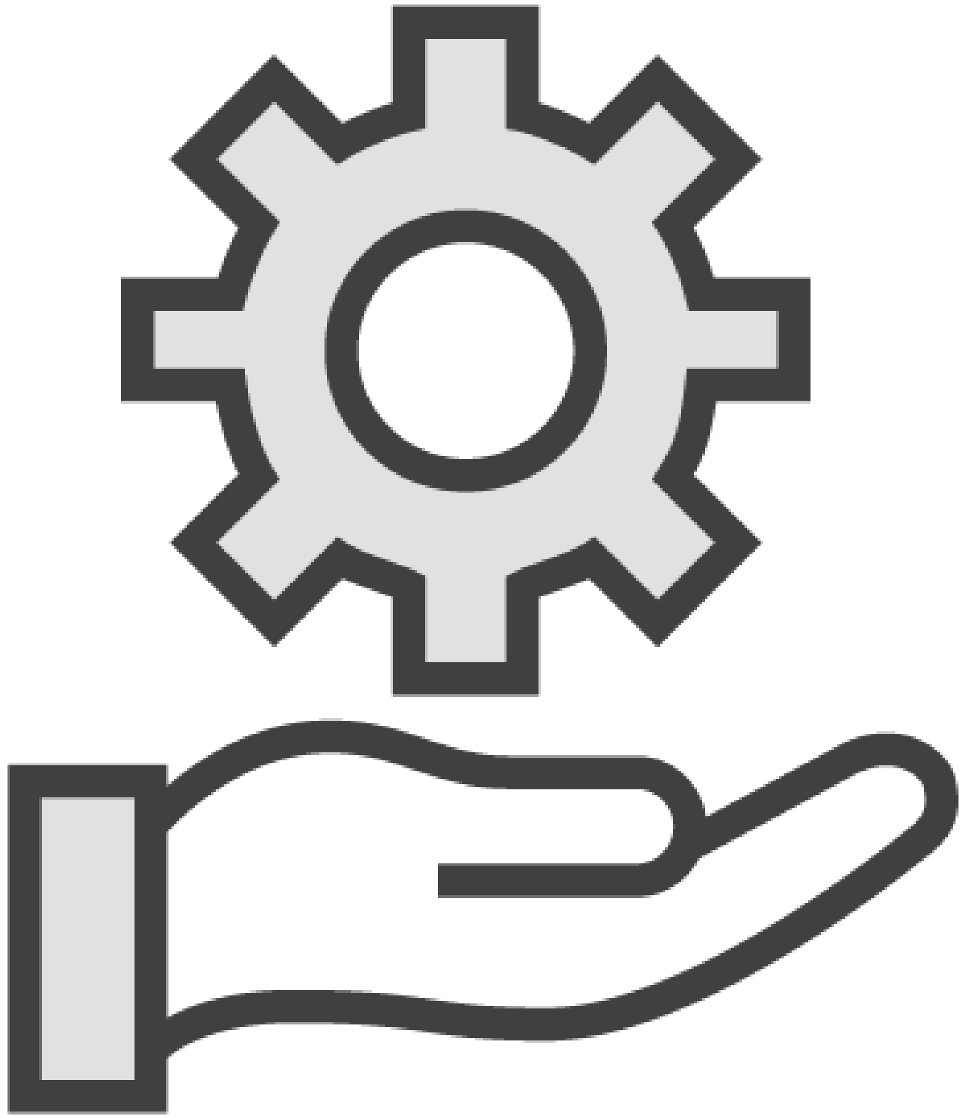
SaaS based IAM offering

Cloud Service that supports SSO

Provides

- Access of users to cloud applications
- Supports federation standards
- Provides access log monitoring and reporting

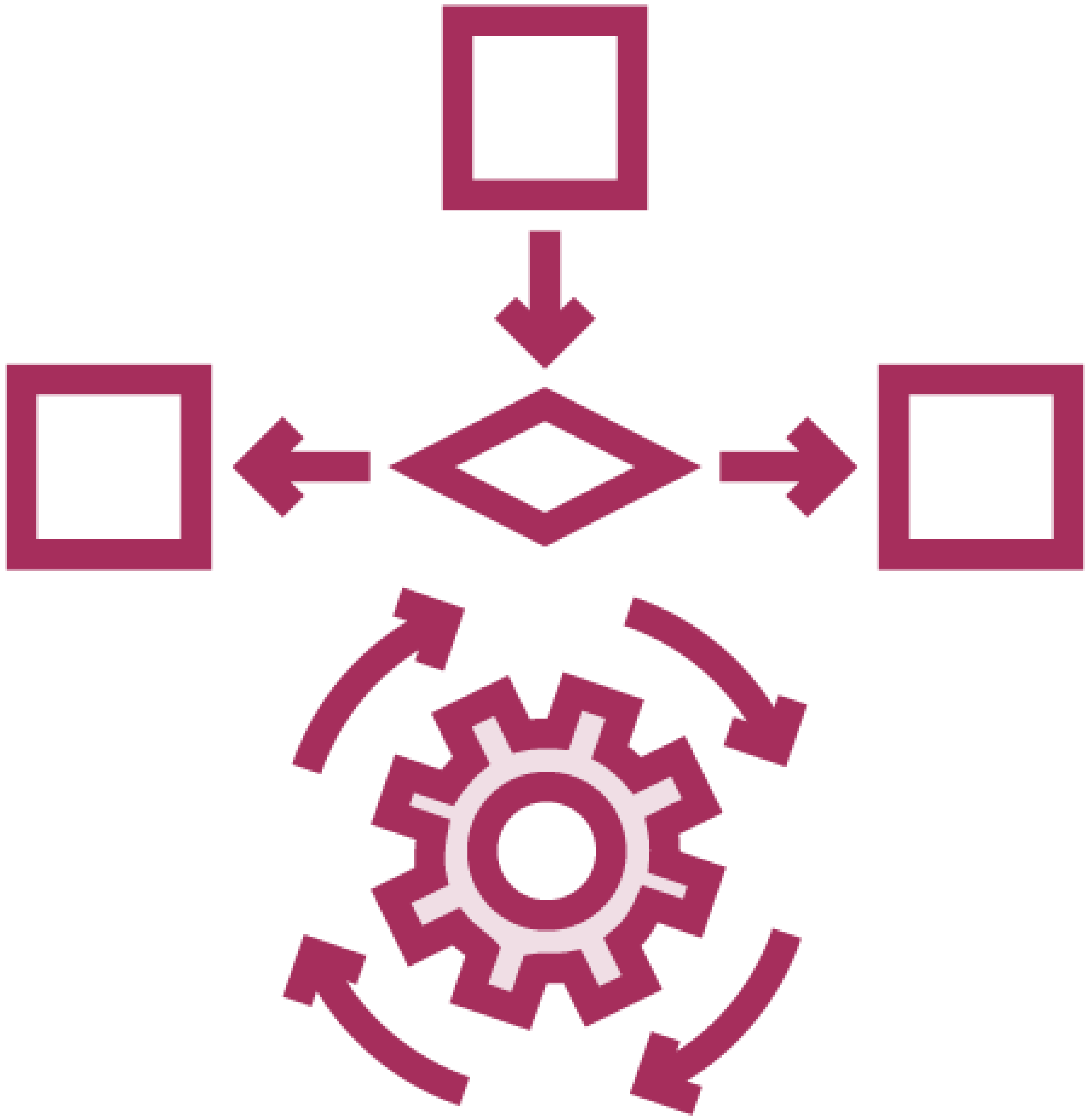
Identity Management



CASB – Cloud Access Security Broker

- May manage access rights as a third party
- Manage access across multiple platforms or cloud implementations

Access Control



Requirement to manage access permissions throughout the identity lifecycle

- Access expansion
- Provisioning
- Maintenance
- De-provisioning

Single Sign On

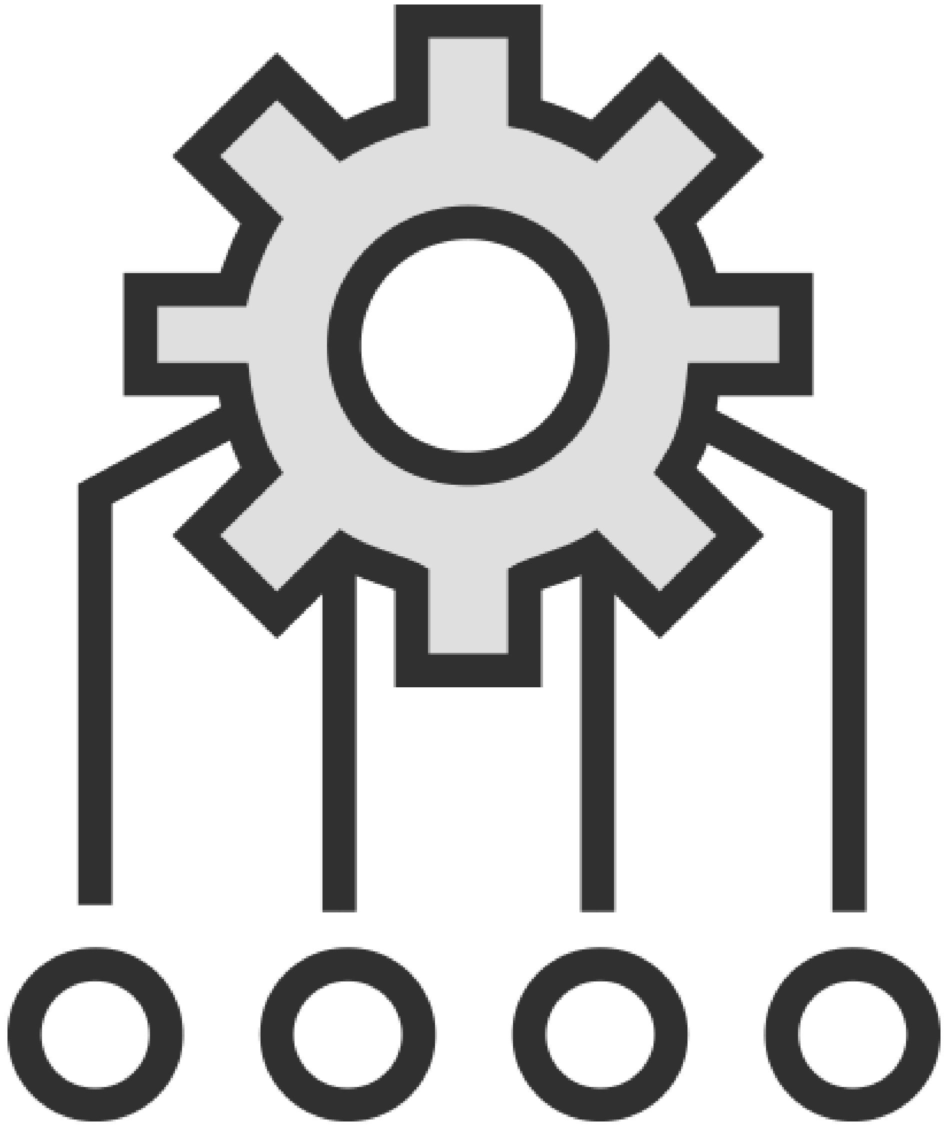
Reduce sign in requirements for a user accessing multiple systems

- Single access control point
  - Single userID, single password
  - Single point of compromise or failure

Better ability to ensure compliance and consistency

- **Centrally managed**

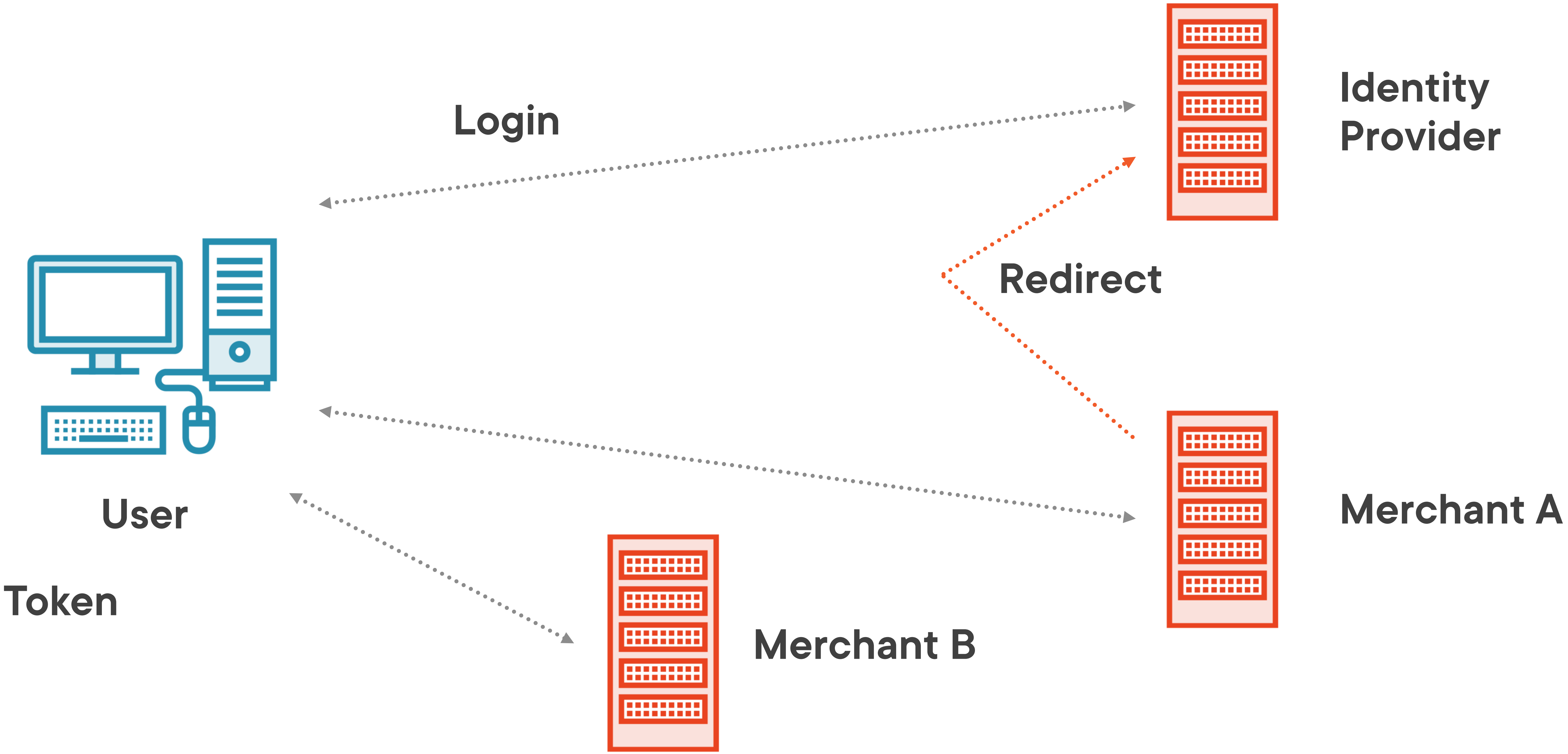
Federated Identity Management



Single sign on for the Internet

- Different companies that use a common identity management system
  - Use of a third party to manage access

Federated Identity Management



Login

Identity Provider

Redirect

User

Merchant A

Token

Merchant B

Federated Identity Management

Standards:

- SAML
- OpenID
- OAuth

Summary

This course addressed the importance of designing and implementing security controls into Cloud-based applications

Applications sit at the front edge of an organization’s network and are subject to attacks leading to compromise of the organization’s data or business processes