LAB CYBER
Cybersecurity made easy

# CYBER SECURITY

## ARCHITECTURE FUNDAMENTALS


First let me just say a big thank you for enrolling in this cyber security architecture course.

Security architecture is a relatively new field under cyber security but the demand for security architects is increasing rapidly due to the consistent cyber attacks companies continue to face today.

I developed this hand book to provide you with all the key points of the course and is meant to act as a summary of the entire course. If you ever need to retrieve some information from the course, you can use this book as a quick reference.

I sincerely hope this course will provide you with both the theoretical and practical skills necessary to help you create security architectures from a cyber security perspective.

**Don't forget to follow my company page on LinkedIn-**

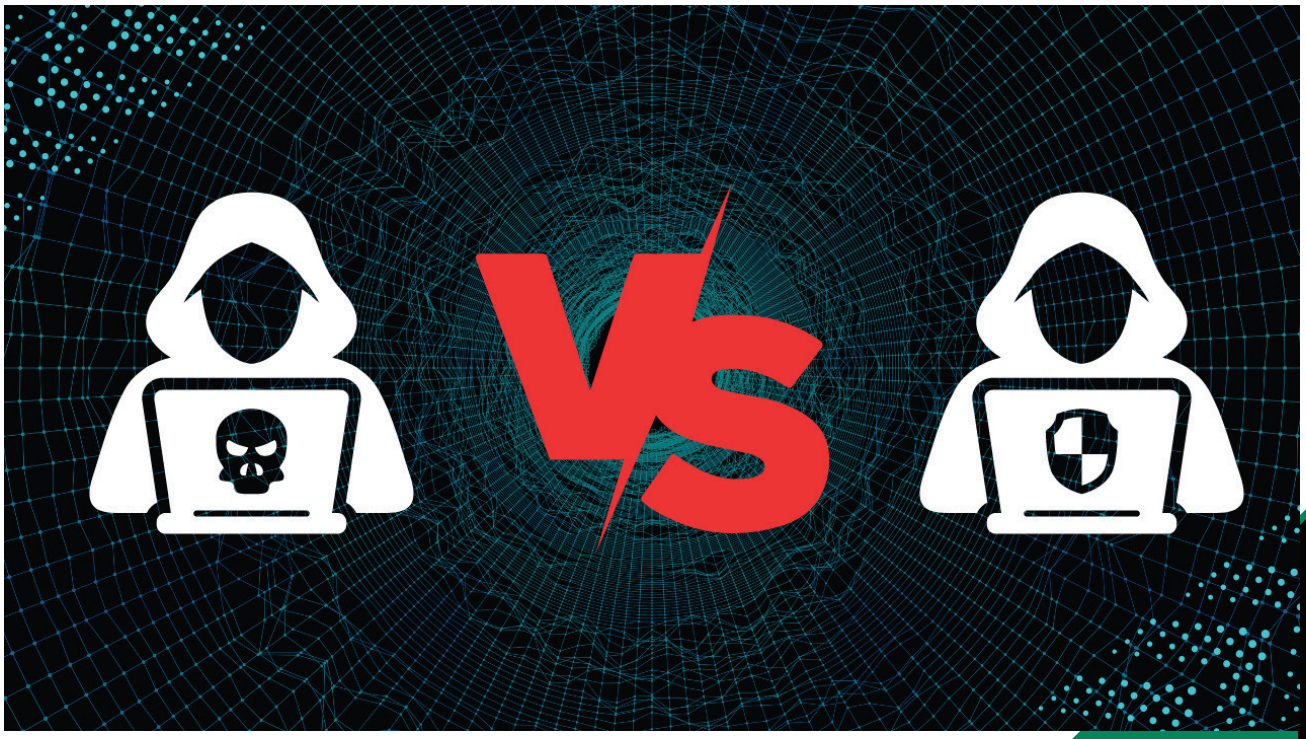
https://www.linkedin.com/company/lab-cyber

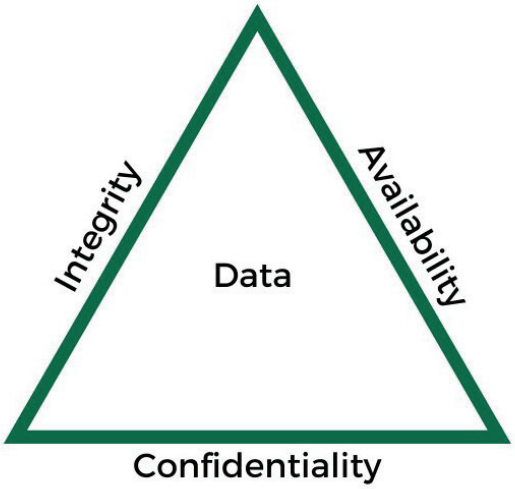
# Table of Contents

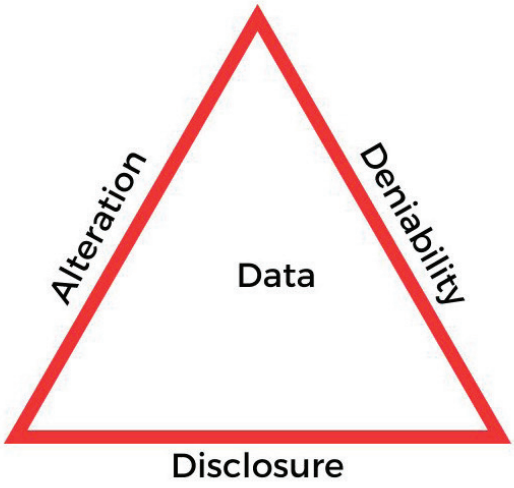
# INTRODUCTION to Cyber Security

Cybersecurity at it's very core can be described with the use of two triads which are the **CIA/DAD** triads.

Cybersecurity professionals strive to ensure the former while cyber criminals go after the latter.






## Confidentiality

Data is accessed by only those with the right permit. Can be achieved through the use of tools like Encryption, Passwords, Biometrics, 2FA, MFA.

## Integrity

Data has not been tampered or altered in any way and can be achieved with the use of Hashing, checksums.

## Availability

Data and resources are available to be accessed or shared and can be achieved with Network access, Server and data availability

## Disclosure

Data is accessed by non-authorized users and can be achieved with Trojans, brute force attacks and theft

## Alteration

Data has been compromised or tampered with and can be attained by using malware, viruses, SQL injection

## Deniability

Access to data and resources are blocked by using Denial of Service attacks, Ransomware etc.

# The Problem with Security Today

Security can be deployed tactically or strategically.

Tactics refer to specific tasks or solutions for a specific problem.

Tactical deployment is typically inferior to strategic deployment and is very often not the best approach.

### Many organisations deploy solutions without consideration for:

- Compatibility and interoperability with other security solutions
- Cost effectiveness
- User experience
- Support for other non-security business requirements

### Why would companies implement security tactically rather than strategically?

- Company culture
- Security objectives are not aligned with business objectives
- Security is not a priority more like an afterthought

### No Business Context:

- Security requirements are not driven by business requirements
- Company's most valuable assets are not identified
- Security goals are too broad - protect all assets with the same amount of resource and priority
- Security goals are too narrow - Real operational risks are not addressed.
- Security requirements are neglected because the project cannot be delayed.

# INTRODUCTION TO SECURITY ARCHITECTURE

## What is Security Architecture?

Security architecture refers to the discipline that defines a set of principles and policies that reduces operational risk to an acceptable level and supports long term business needs.

**Security architectures are driven by business requirements including:**

- Cost vs security benefit
- Usability and operability
- Integration with other business processes

The first step is to understand the business and what gives it its competitive edge or advantage and proprietary information is arguably the most important business asset and must be secured.

## Who is a Security Architect?

### Responsibilities

- Design suitable and cost effective security solutions that enable business objectives
- Develop reusable security patterns and blueprints*
- Keep abreast of emerging threats
- Participate in decision making processes regarding security

It's more of a strategic role than operational and as an architect you are expected to know something about everything.

Architects are NOT responsible for pen testing.

### Key Competencies

- Be able to identify and grade assets
- Understand that the business is the priority **
- Balance security, usability, cost & operability
- Understand and manage operational risk
- Develop threat models to identify all possible threats

# Security Principles & Approaches

## Security Principle

A fundamental statement that serves as the foundation for security design decisions in order to enable the achievement of business objectives and goals.

### Security Design Principles

- OWASP
- Open Group (Jericho Forum Commandments)
- NIST 800-160
- “Ten Guiding Principles of Software Security” - John Viega & Gary McGraw+
- Cyber Security Design Principles
- “High Assurance Design” - Clifford J. Berg

### OWASP

- Minimise the attack surface
- Apply defence-in-depth
- Avoid security by obscurity
- Enforce least privilege
- Secure defaults

### OPEN GROUP

- Fundamentals (level of protection should be appropriate)
- Surviving in a hostile world (devices communicate using
- secure protocols)
- The need for trust (transparency at all levels)
- Identity, management and federation (AAA)
- Access to data (controlled, private and secured at all times)

### NIST

- Least privilege
- Hierarchical trust
- Hierarchical protection
- Minimise sharing
- Reduce complexity

### TTGPSS

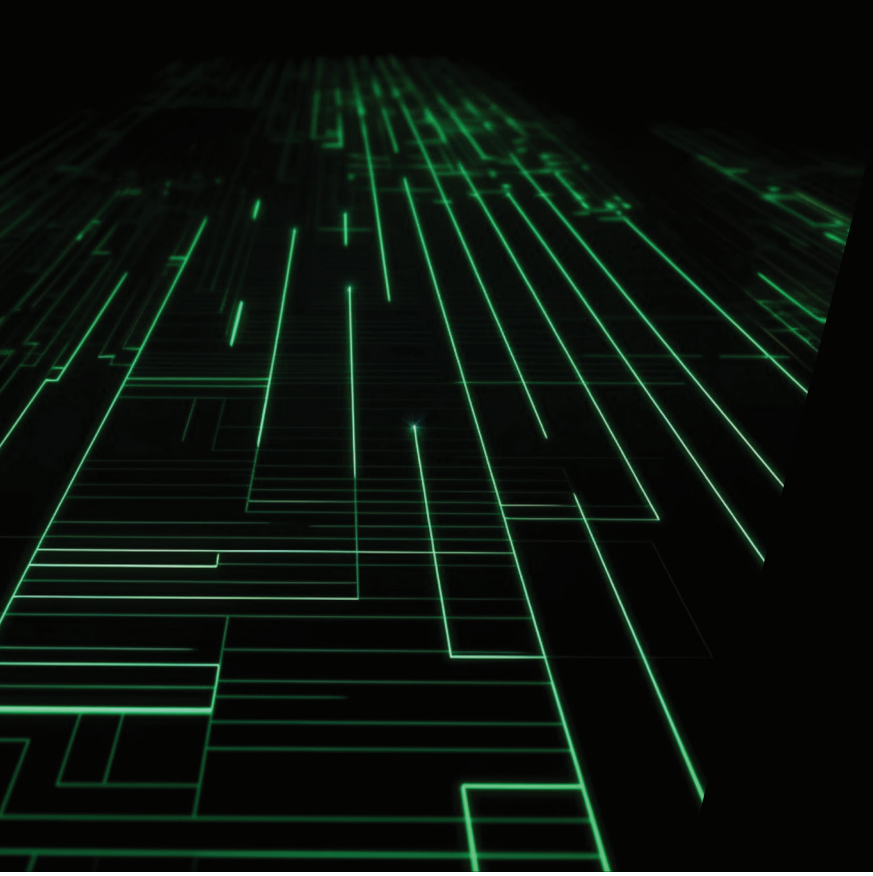
- Secure the weakest link
- Defence-in-depth
- Keep it simple
- Promote privacy
- Be reluctant to trust

### NCSC

- Establish the context before design
- Make compromise difficult
- Make disruption difficult
- Make compromise detection easier
- Reduce the impact of a compromise

### High Assurance Design

- Security design patterns must be verifiable
- Deploy and run securely
- Embed intrusion detection at multiple points
- Logs are secured and reliable
- Segment data and resources according to risk



### Principles of Secure Design

- Least privilege principle
- Strong authentication
- Fail-safe
- Layered Defence / Defence-in-depth
- Simplicity
- Sensitive data is protected at all times (rest, transit and in use)
- Effective incident response

## Approaches to Security

### Security through Obscurity

Keeping a system secure by keeping its very existence or vulnerabilities secret.

### Security through Obsolescence

Using an outdated operating system (windows XP) on a device to prevent hackers from intruding.

### Security through Minority

Using very uncommon software in the hopes that ‘hacker material’ available for such would be limited.

### Security through Diversity

Using a very wide variety of systems and apps to confuse the attacker.

### Security by Design -

Security is considered in every step from requirements to design to deployment.

# CYBER SECURITY PROCESSES

- Incident Response
- Audit & Reporting
- Risk Management

### Incident Response Frameworks

- NIST 800-61
- CERT
- ISACA

## Incident Response

Systems must be designed to support the organisation's ability to respond to security incidents as quickly as possible.

# Risk Management

Risk management involves all processes from assessing the risk to managing it

**The four phases under risk management are**

- Risk Assessment
- Risk Analysis
- Risk Mitigation
- Risk Monitoring

## Risk Assessment

All assets, threats and vulnerabilities are identified

## Risk Analysis

The impact of the risk to the assets

- Risk Mitigation
- Reduce the risk
- Avoid the risk
- Transfer the risk
- Accept the risk
- Reject the risk

## Risk Monitoring

This is an ongoing and never ending process.

## Risk Controls

- Administrative (awareness training, disaster recovery plans, background checks etc )
- Technical (Access control lists, authentication, encryption)
- Physical (trip alarms, security guards, biometrics etc)

## Risk Treatment

- Preventive (system hardening)
- Detective (logs, security audits)
- Corrective (backup restores, self healing system)
- Compensating (use of disaster recovery site, pen & paper)

## Residual Risk

> Those risks that are expected to remain after the planned response of risk has been taken, as well as those that have been deliberately accepted. They are acceptable to the organisation's risk tolerance level. Sometimes a residual risk has no reasonable response either.
>
> **PMBOK DEFINITION**

If an application server blocks traffic from all sources except the web server, the residual risk includes attacks from the compromised web server.

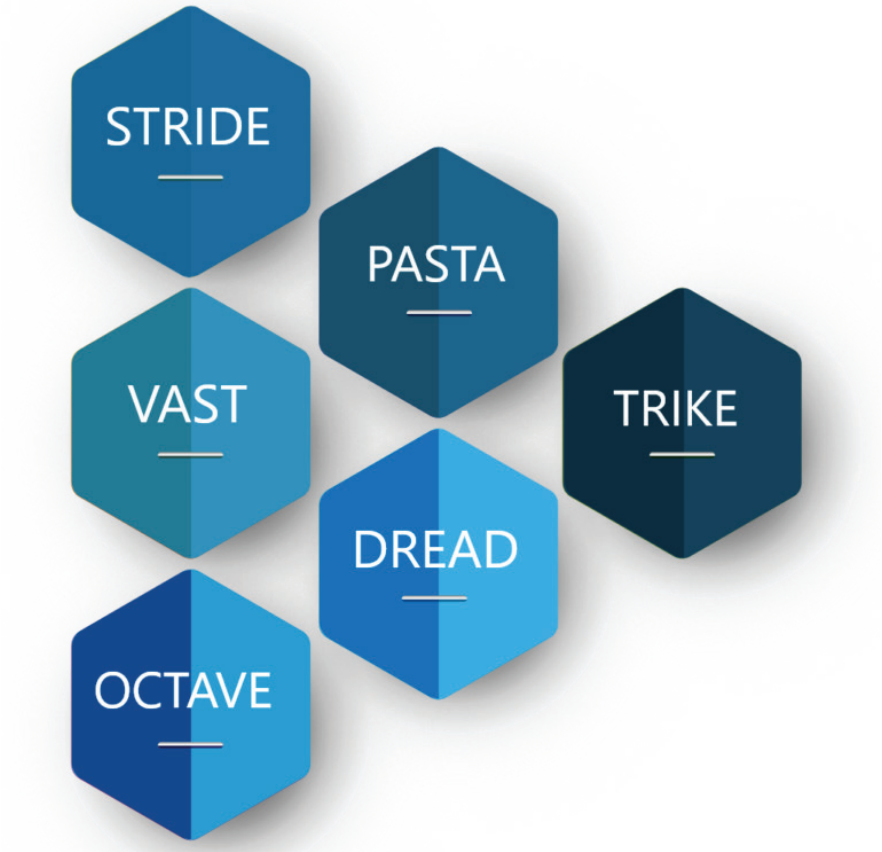
All risks can never be fully covered at an acceptable level of cost or usability. At some point, risk will have to be accepted.

# Threat Modelling

## What is Threat Modelling?

Using a model as an approach for analysing the security of an application and allows the identification and quantification of the security risks associated with the application.

### Threat Modelling Methodologies




### Threat Modelling Perspectives

- Functional
- Process
- Deployment
- Data Flows
- Social
- Environmental

# Threat Modelling vs Risk Assessment

Threat IS NOT a vulnerability because they can exist even when there are no vulnerabilities.

Threats can exist without risks but a risk needs an associated threat to exist.

Risks are often measured based on the probability that an event might occur as well as the impact of the event on the business.

Threat assessment is the combination of a threat actor's intentions to harm combined with an assessment of that actor's capability to carry out those intentions.

To determine the Threat actor's capability, assessments of the actor's training background (skill level) and whether it is a group or individual can be made.

Risk Assessment involves identification of security risks through the analysis of assets, threats and vulnerabilities, including their impacts and likelihood

Threat Modelling primarily focuses on data assets and involves systematically identifying the potential risks and vulnerabilities which are exploitable but from an attackers viewpoint.

Risks are event focused (the database server goes down)

Threats focus on intentions (a hacker wants to take down the database server)

### Threat

Can someone destroy our data?

### Risk

What is the probability our data can be destroyed?

# Threat Modelling - Part 2

## Types of Threat Models

- Application threat model
- Operational threat model
- Data Flows threat model

## Application Threat Model

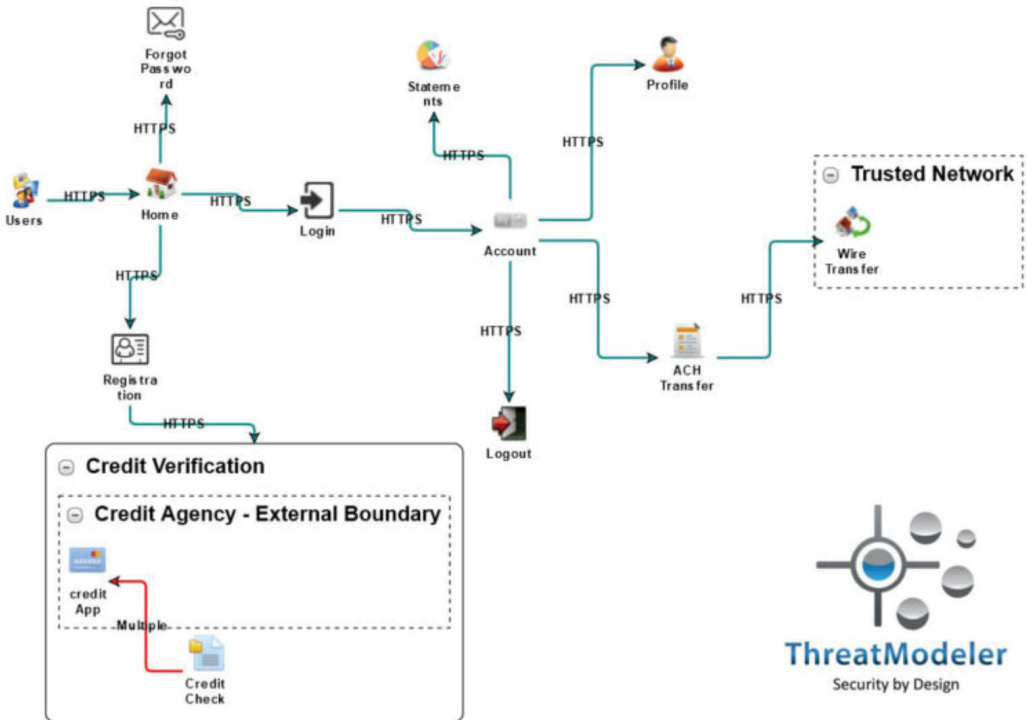
Focuses exclusively on the application the model has been designed for and is used to identify possible threats against  the application.

## Application Threat Model

- First create an architecture design diagram
- Identify the assets in use
- Identify the threats to the assets
- Other team members should participate as well **
- Who are the threat posers?
- Controls to mitigate the threats are developed

## Operational Threat Model

Provides organisations with a general overview of it's infrastructure risk profile in order to better understand the attack surface and develop effective mitigation policies and strategies

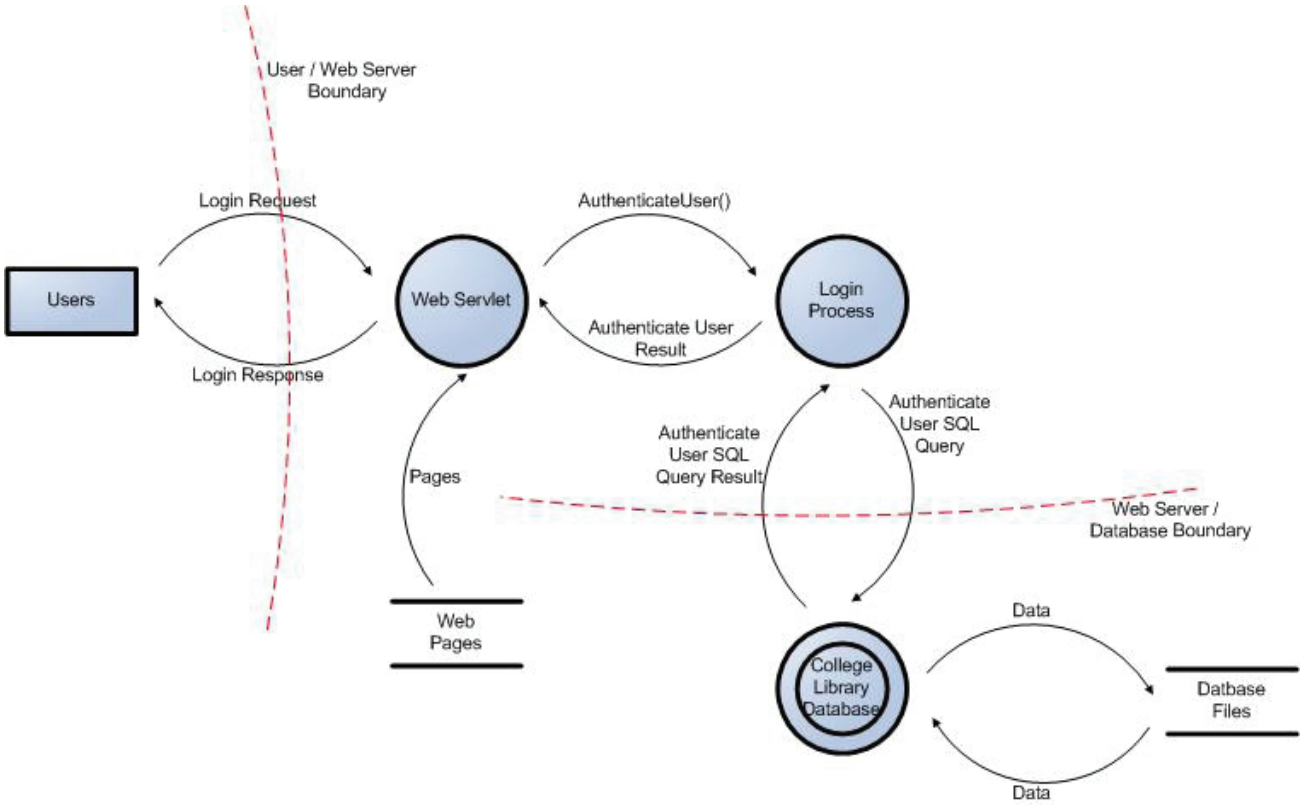



## Operational Threat Model

- First identify the operational environment. This should include shared resources like database or encryption servers
- Every resources attributes are identified e.g a server with unrestricted admin access could have more threats
- Potential threats are identified
- Effective security controls are developed

## Data Flow Model

Data flow diagrams (DFD) are used to accurately model the application through visual representation.




## Data Flow Model

The diagram should identify the affected components through critical points and also highlight the flow of control through these components

# STRIDE

Developed by Microsoft and developers can use this model to spot potential threats during the design phase of an app or system.

A hacker fakes their identity and gains access - **Spoofing**

A disgruntled employee can tamper with company data by changing the software code - **Tampering**

A bad actor performs a malicious operation and then denies their involvement in the attack - **Repudiation**

The application unintentionally reveals data to unauthorised users through insecure coding or error messages - **Information Disclosure**

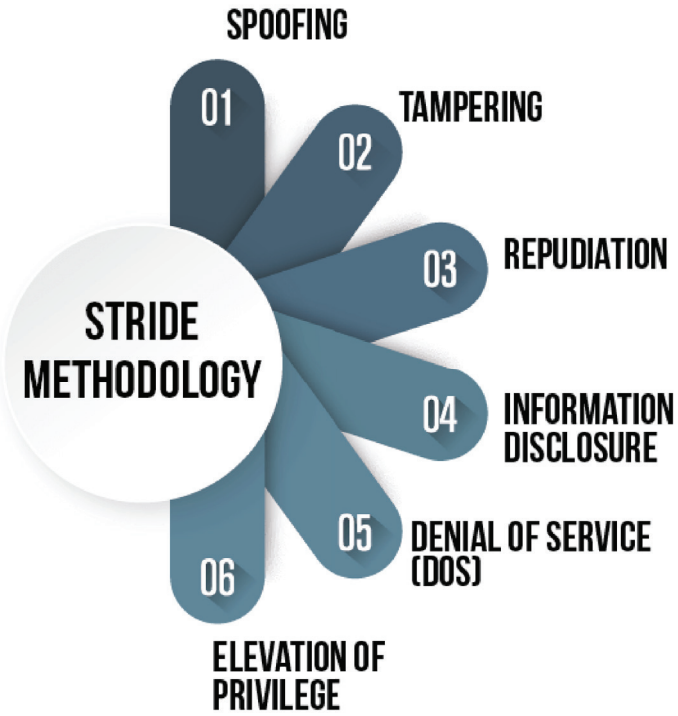
DoS attacks restrict an authorised user from accessing the application - **Denial of Service**

An authorised or unauthorised user in the system can gain access to other information or data that they are not authorised to see or use - **Elevation of Privileges**

## All possible threats are enumerated and then addressed by:

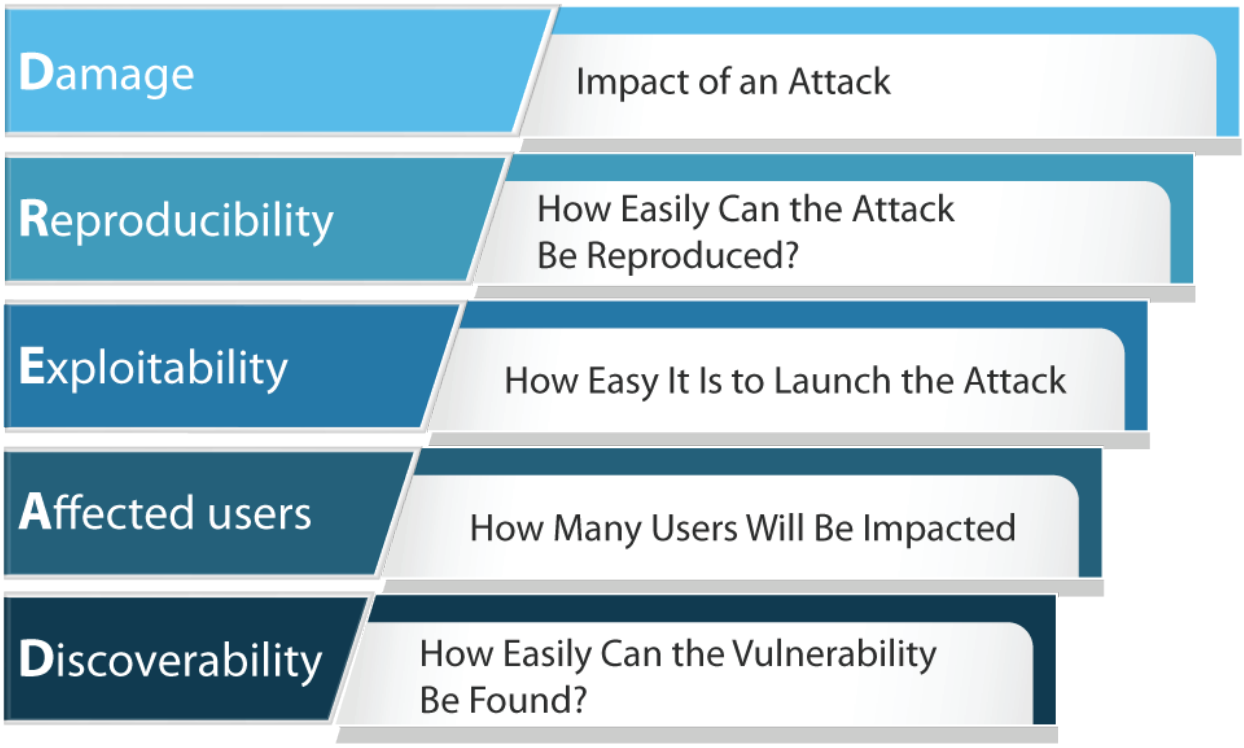
- Mitigation
- Elimination (component is removed)
- Transferred
- Accepted

Final step is to validate the model through testing for completeness, accuracy and effectiveness.



# DREAD

Used to assess, analyse, and find the probability of risk by rating the threats




Each factor is awarded a score but this process can be very subjective and unreliable.

## Let's take a look at an example:

**DAMAGE -** Company reputation can be ruined = 10

**REPRODUCIBILITY -** The attack can be reproduced fairly easily = 6

**EXPLOITABILITY -** Requires access to a secured database = 3

**AFFECTED USERS -** Everyone = 10

**DISCOVERABILITY -** Requires tremendous patience, time and skill = 3

**OVERALL THREAT SCORE -** 10 + 6 + 3 + 10 + 3 / 5 = 6

# PASTA

The Process for Attack Simulation and Threat Analysis and is a seven-step methodology to create a process for simulating attacks to applications, analysing the threats, their origin, the risks they pose to an organisation, and how to mitigate them.


## Define Objectives

Objectives may be internally or externally driven and the purpose of the application must be clearly understood. How does this application make your company money?

Your company won't want an application that is not resilient or an application that can cough up credentials and leave the company liable to be fined.

## Define the Technical Scope

Time to understand the attack surface by defining exactly what you are protecting. Dependencies on third party services should also be defined.

## Attack Surface Component Examples:

- DNS Server
- Network Infrastructure
- Application Framework
- Web Application
- OS Settings
- Certificate Server

## Decompose the Application

The key output of this stage is to understand if you have  implicit trust models and where they are.

## Analyse the Threats

Here potential threats against the application are analysed. The data type and data consumption models are considered as well.

## Vulnerability Analysis

Stage five correlates the application's vulnerabilities to the  application's assets.

**"What is wrong with the application?"**

## Attack Analysis

Here the vulnerabilities discovered in stage 5 are tested to see if they are actually viable.

## Risk & Impact Analysis

Here the vulnerabilities discovered in stage 5 are tested to see if they are actually viable.

# OCTAVE

Operationally Critical Threat, Asset & Vulnerability Evaluation and is a self-directed approach, meaning that people from an organisation assume responsibility for setting the organisation's security strategy

Due to its flexibility, it can be adapted to fit the needs of practically any organisation while only requiring a small team of cybersecurity professionals to collaborate on the endeavour.

## There are three versions of OCATVE:

- **OCTAVE-S** (assumes the entire team already has extensive knowledge about the organization's environment)
- **OCTAVE ALLEGRO -** Best for small teams
- **OCTAVE FORTE -** most adaptable variation

## Phases of Implementation

- Create a profile of all assets and their relevant threats.
- Identify vulnerabilities and policies should be developed to eliminate and manage them.
- Define a security risk management strategy.

System audits, pen testing and risk assessments are common tools that are utilised with **OCTAVE.**

## Benefits

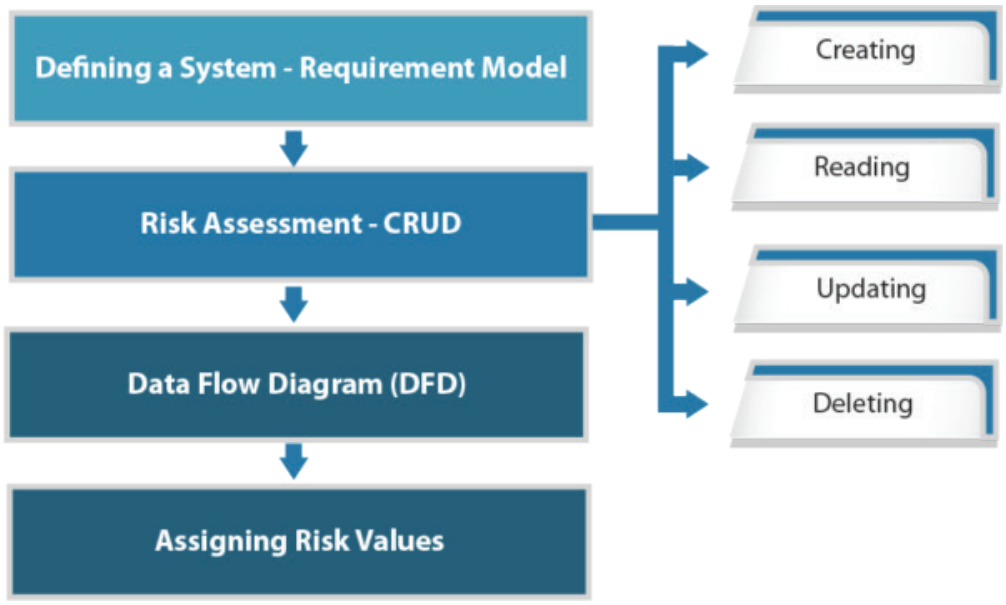
**OCTAVE** is extremely effective as it focuses on the organisation's most critical assets

It's also quite fast at discovering, prioritising and mitigating risks

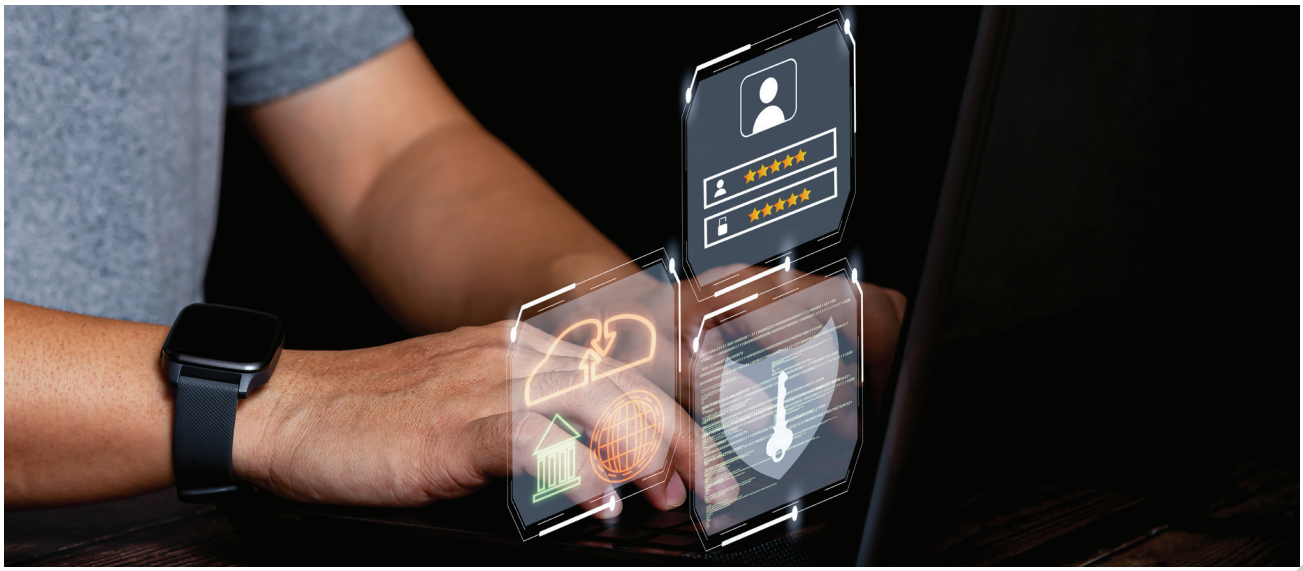
It's also actionable and comprehensive

# TRIKE

Open source framework developed in 2006 and intended for security professionals who run security audits. It is risk driven and focuses on defence rather than offence




- Determine appropriate risk level for assets
- Document what was done
- Communicate what was done and the impact to stakeholders
- Work with stakeholders to reduce risk



## TRIKE PROCESS 1

- Develop a requirements model
- Actors interacting with the system
- Assets or data elements to be used
- Intended actions performed by the system (CRUD)
- Rules that define when actions can be performed

## TRIKE PROCESS 2

- Develop the implementation model
- Identify the set of supporting operations
- Develop data flow diagrams
- Identify use flows

## TRIKE PROCESS 3

- Build the threat model
- Identify all possible threats
- Identify weaknesses and vulnerabilities
- Identify mitigations that can reduce the risks

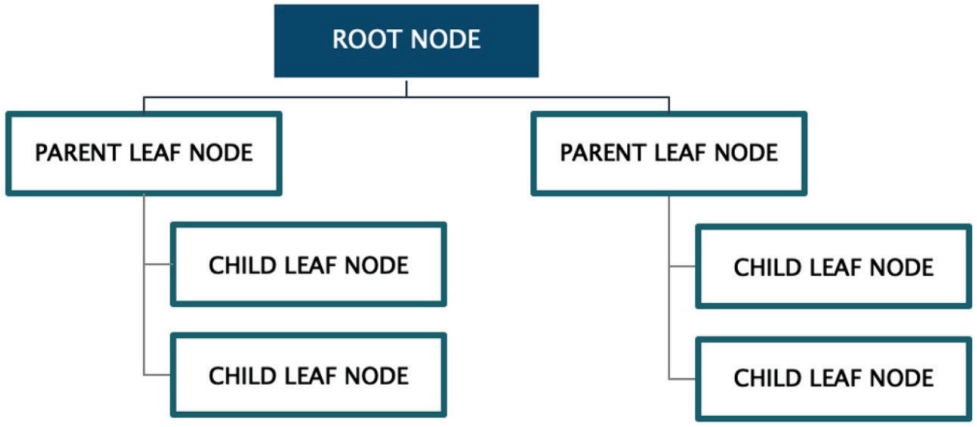
## TRIKE PROCESS 4

- Build the risk model
- Experimental and still under development
- Recommended to use other methodologies NIST

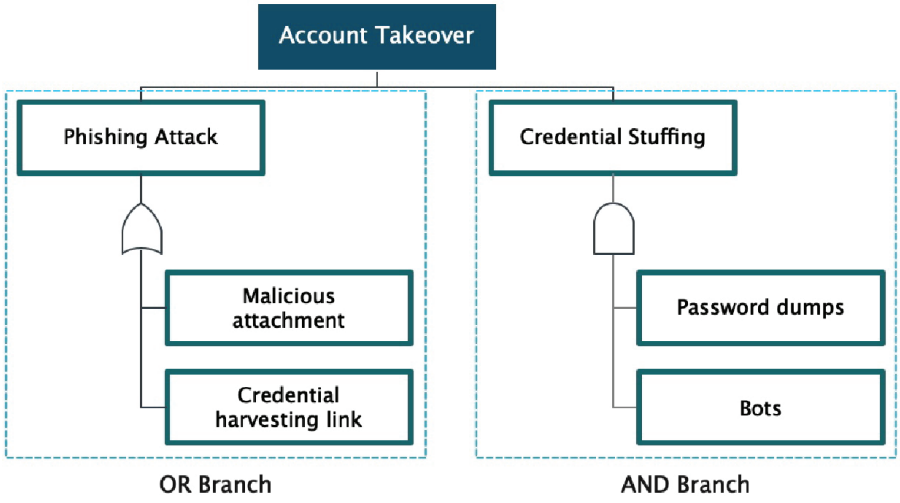
# Attack Trees

## What is an Attack Tree?

This is a graphical representation of attacks against a system/network using a hierarchical tree structure.




- Root node represents an objective of the attacker
- Leaf nodes represent the ways to achieve the objective




- AND trees (when all child leaf nodes must be true)
- OR trees (when any child leaf node can be true)

## Attack Tree Process

- Define the root node - The attacker's core objective
- Is it an AND, OR or a combination of both tree types
- Define the leaf nodes and child leaf nodes if available
- Delete any unlikely/unrealistic leaf nodes
- Check for completeness

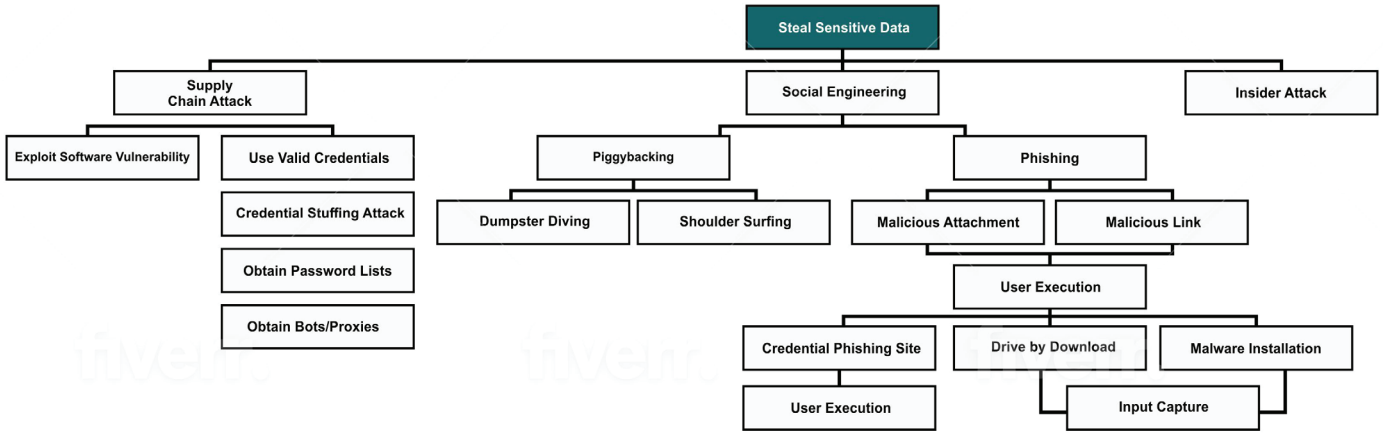
## Attack Tree Example

Your company is on the verge of releasing a revolutionary product and are concerned that the software used to create it will either be stolen and sold to rival companies or could be used to hold the company to ransom.

A third party software development company was also involved in the development of this product

**Your company has so far implemented the following security controls:**

- Awareness training for Phishing attacks
- Strong authentication and authorization tools
- Effective auditing and logging processes



# Enterprise Architecture Frameworks

Enterprise architecture refers to the discipline that ensures business objectives are achieved by aligning business systems with the supporting information systems.

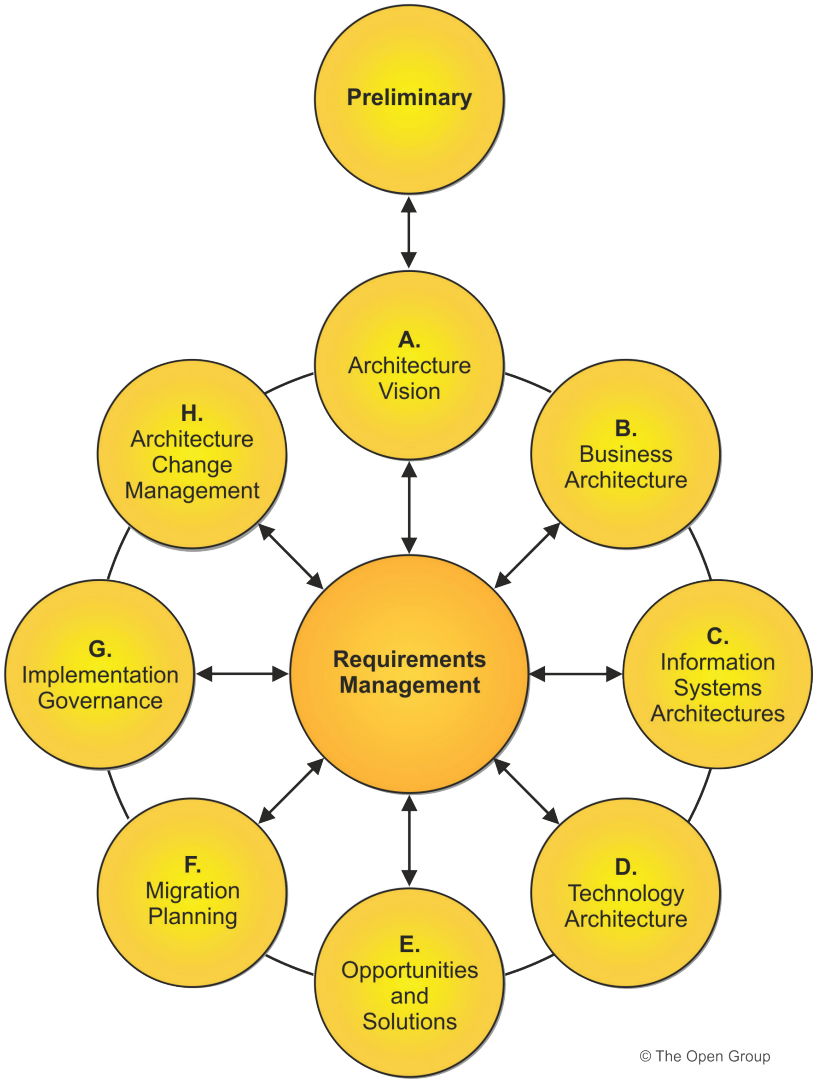
An enterprise architecture framework is the foundational structure upon which different architectures are developed.

## TOGAF

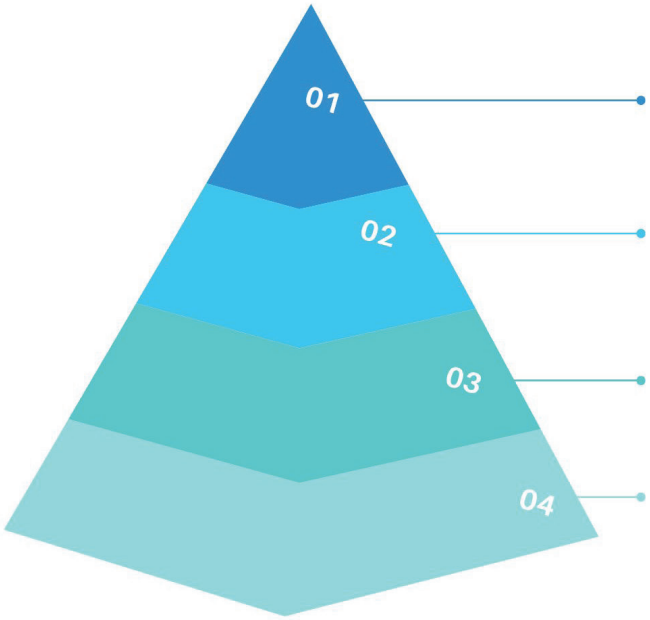
The Open Group Architecture Framework and are the tools and methodologies for assisting in the acceptance, production, use and maintenance of enterprise architectures.

### TOGAF: Architecture Development Method

Repeatable process for developing enterprise Architectures



## ARCHITECTURE DOMAINS




**BUSINESS**
Business strategy, governance, organization and key business processes

**DATA**
Logical and physical data assets and data management processes

**APPLICATION**
Individual applications and their relationships with core business processes they intend to support

**TECHNOLOGY**
Hardware and software capabilities needed to support the business, data and applications.

## TOGAF Security?

Often considered to be part of the model but a separate discipline that is present across all domains.

## TOGAF Security Processes

- Information Security Management (ISM) (ISO/IEC 27001:2103)
- Enterprise Risk Management (ERM) (ISO 31000:2009 Risk
- Management principles and guidelines)

## ISM

This is the process through which security objectives are established, risk ownership is assigned, security controls are implemented and reported on to reduce information risk and security incidents are handled effectively.

**TOGAF** uses a risk-based approach for maintaining the security of information systems and managing risks.

## ERM

Risk is defined as the effect that uncertainty has on the achievement of business objectives and can either be positive (beneficial outcome) or negative (threats and losses).

# Zachman Framework

A logical structure for classifying and organising the descriptive representations of an Enterprise that are significant to the management of the Enterprise as well as the development of the Enterprise's systems, manual systems as well as automated systems.

Based on principles found in older disciplines of architecture, engineering and manufacturing.

It is an ontology - a theory of the existence of a structured set of essential components of an object (enterprise, value chain, project, building, plane etc) for which explicit expressions are necessary for creating, operating or changing the object.

The zachman framework is not a methodology but the framework for describing the enterprise

Framework (ontology) is a structure whereas methodology is a process. A structure establishes definition whereas a process provides transformation.

Processes based on ontological structure will be predictable and produce repeatable results (chemistry periodic table).

Processes without ontological structures are dependent on the practitioner skills (software development)

## Zachman Communication Interrogatives

**An issue or topic is broken down to 6 logical questions**

- What (things) - What components are involved?
- How (process) - How do they work?
- Where (location) - Where are they located?
- Who (responsibility) - Who is responsible for what?
- When (timing) - When do things happen?
- Why (motivation) - Why are we doing this?

## Zachman Security

**Based on three principles**

- Role-based access
- Positive identification of a person accessing the enterprise
- Confidentiality of data transmitted outside of the enterprise

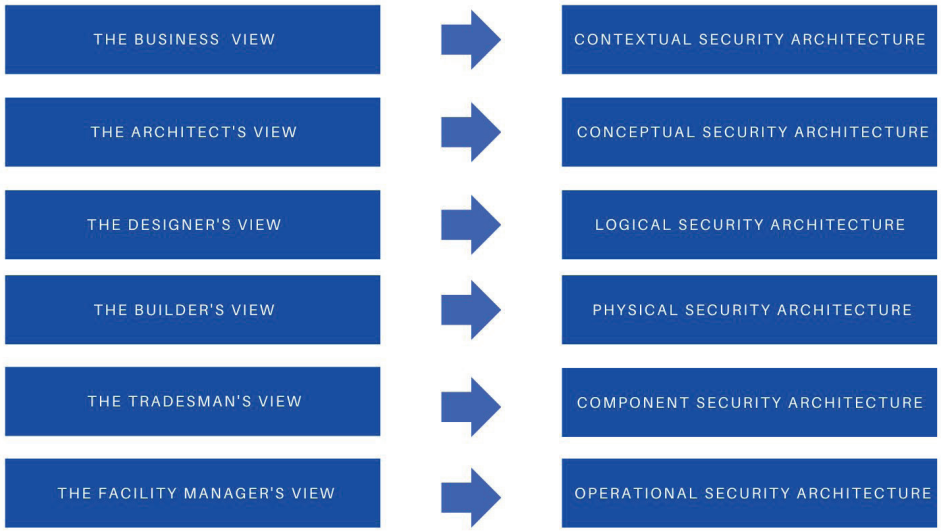
# SABSA

Sherwood Applied Business Security Architecture and is a framework and methodology for developing and documenting business and risk driven enterprise security and security solutions architectures.

First released in October 1996 and adopted in over 50 countries to meet diverse needs under

- Risk Management
- Information Assurance
- Governance
- Continuity Management

## SABSA Structure




## SABSA: Six Questions

**Each layer is analysed by asking the following questions at each layer:**

- What assets need to be protected?
- Why is protection needed?
- How will protection be achieved?
- Who will ensure the protection of the assets?
- Where is protection needed?
- When is protection needed?

## SABSA: Business View

Developing security architectures must always begin from a business perspective

- **WHAT:** Business drivers for securing the system being built
- **WHY:** Business risks that need to be addressed
- **HOW:** Business processes that need security
- **WHO:** Business organisations that will take part in security
- **WHERE:** Business locations where security is needed
- **WHEN:** Time dependencies of business processes

The answers will enable the development of the contextual security architecture

## SABSA: Architect's View

Conceptualising solutions that will meet the security needs of the business

- **WHAT:** Desired protection in terms of business attribute profile
- **WHY:** Rationale behind the desired protection in terms of control objectives
- **HOW:** Method for achieving desired protection in terms of high-level security strategies
- **WHO:** Players involved in security management
- **WHERE:** Relevant security domains where protection must be achieved
- **WHEN:** Time-related aspects of security

The answers will enable the development of the conceptual security architecture.

## SABSA: Designer's View

Translating the architect's conceptual design into a logical system design.

- **WHAT:** Business information that needs to be protected
- **WHY:** Security policy requirements
- **HOW:** Logical security services needed to protect the business information
- **WHO:** Users that will interact with business information
- **WHERE:** Relevant security domains where protection must be achieved
- **WHEN:** Security processing life cycle

These answers will enable the development of the logical security architecture.

## SABSA: Builder's View

Translating the designer's logical design into an actual physical system design

- **WHAT:** Business information that needs to be protected
- **WHY:** Rules, practices and procedures
- **HOW:** Security mechanisms and controls needed to protect business data
- **WHO:** Users, applications and interfaces
- **WHERE:** Security technology infrastructure, platforms and networks
- **WHEN:** Time-related dependencies

The answers will enable the development of the physical security architecture

## SABSA: Tradesman's View

Turning the builder's physical design into an actual implementation

- **WHAT:** Detailed data structures that need to be protected
- **WHY:** Relevant security standards
- **HOW:** Vendor products are tools needed to protect data structures
- **WHO:** Users, their privileges, roles and access controls
- **WHERE:** Servers, computers, appliances, protocols, etc
- **WHEN:** Security step timing and sequencing

The answers will enable the development of the component security architecture.

## SABSA: The Facility Manager's View

Operating, maintaining and monitoring the system and the services it provides

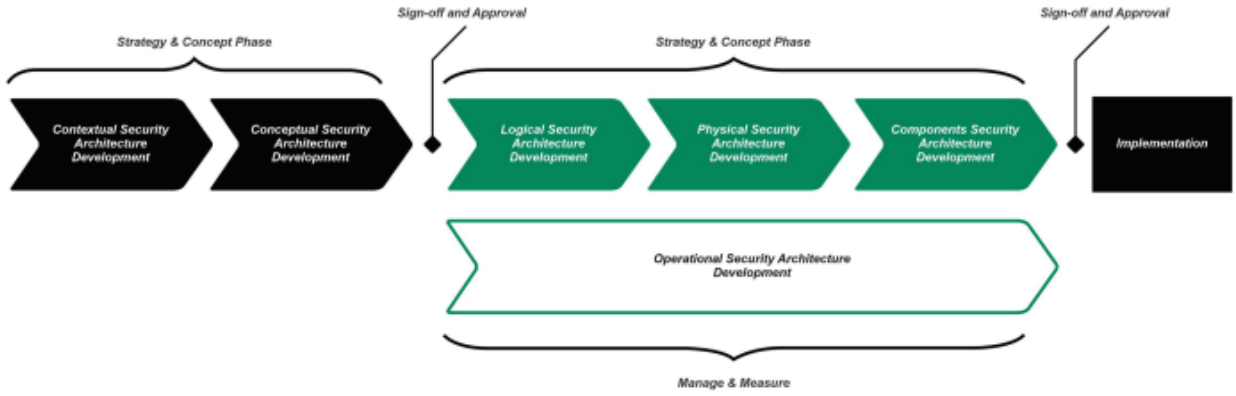
- **WHAT:** System performance and security maintenance
- **WHY:** Reduce operational failure and security incidents
- **HOW:** Security-related operations
- **WHO:** Users involved in providing security-related operational support
- **WHERE:** All system components, platforms and networks
- **WHEN:** Scheduling and executing security-related operations

The answers will enable the development of the operational security architecture.

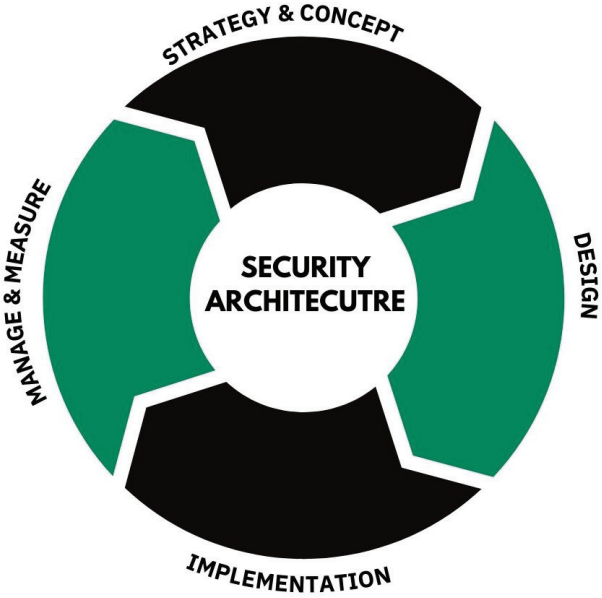
## SABSA: The Inspector's View

Will provide security architecture assurance and will ensure that the security architecture is complete and meets the security needs of the business.

## SABSA: Development Process




## SABSA: LIFE CYCLE



# Cyber Architecture for Enterprise Security

## Network Security

By far the most important security area and isn't just about having a firewall

Proper network security should also consist of security policies and practices designed to prevent and monitor unauthorised access.

### Common issues include

- Wifi
- Wireless protocols like Bluetooth, NFC
- Weak protocols like Telnet & HTTP
- MAC Address Spoofing

### Passive Threats

- Wiretapping
- Port Scanning
- Information Gathering

### Active Threats

- Malware
- DDoS
- DNS Spoofing
- Man-in-the-middle attacks

# Network Security Tools

## Can be categorised into the following

- Blocking
- Inspecting
- Monitoring
- Policy

## Tools for Blocking Threats

- Firewalls
- Network Access Control
- IPS & IDS

## Tools for Inspecting Threats

- Packet Capture
- Netflow Capture (network protocol developed by Cisco for collecting IP traffic information and monitoring network flow)

## Tools for Monitoring Threats

- Logs
- Network Visibility Tools e.g Wireshark

## Tools for Policy Enforcement

- Non Technical Compliance Checking (Human Auditing)
- Contractual Compliance Checking (Employee Network Use)
- Real-time Technology Enforcement (Firewalls)
- Passive Technology Enforcement (IDS)

# Application Security

Refers to the hardening of an application to prevent it from being misused or exploited and is not limited to just code scanning

## Application Security Threats

### Passive Threats

- Weak key management
- Information disclosure
- Storage of credentials in plain text

### Application Security Threats

- SQL Injection
- XSS Attacks
- Brute force attacks
- Man-in-the-middle attacks

### Application Security Tools

Can be categorised into

- Code
- System
- Availability
- Databases
- Containers

### Application Security Tools

- White box scan (tester has access to all network and system information)
- Peer review
- Tracing function to requirements
- Black box scan (no info is provided to the tester)
- Penetration testing
- Application firewalls

### Tools for Availability

- Load Testing
- Performance Testing
- Dependent system

### Tools for Database

- Activity Monitoring
- Limit access channels
- Configuration Management

### Tools for Containers

- Isolation (Namespaces)
- Cgroups
- Seccomp (used in Linux to restrict the actions available within the container)

# Endpoint Security

This focuses on the end devices of a network like servers & computers and is also the most difficult area to control. It is often seen as the frontline for cyber security.

Any device connected to a network is referred to as an endpoint and can quickly grow especially in companies with a BYOD policy.

## Endpoint Security Threats

- Malware
- Ransomware
- Keyloggers
- Phishing
- Social Engineering


## Endpoints

- Tablets
- Mobile Devices
- Smart watches
- Printers
- Servers
- ATM Machines

## Endpoint Security Tools

- Anti-malware
- Application Whitelisting
- Device Whitelisting
- Data loss prevention
- Machine learning
- Endpoint Detection & Response (EDR)

# Identity & Access Management

Covers the authentication & authorization aspects of a system and how privileged users are managed.

## FOUR PHASES

**Identity** - Supply identification information

**Authenticate** - Identity information is verified

**Authorise** - Allows actions based on verified identification

**Audit** - Keeps track of actions performed with the identification

### Identity Threats

- Spoofing
- Identity theft
- Keylogging

### Access Threats

- Escalation of privilege
- Information leakage

### IM Tools & Techniques

- Identity Manager
- Fraud Analytics
- Multi Factor Authentication

### AM Tools & Techniques

- Single Sign On
- Behaviour Analytics
- Role Based Approach

## Data Protection

This handles the collection, storage and provision of data

Data should be available at all times and can be accessed only by those authorised to do so.

Laws and regulations governing the use of data need to be considered as well to avoid legal issues.

### Data Laws

- General Data Protection Regulation (GDPR)
- Data Residency Laws
- Right to Erasure
- Data Portability

### Data Protection Tools

- Encryption
- Anonymizer (tokenization)
- Multi-Party Trust Computation
- Database monitoring

## Vulnerability, Patch & Availability Management

This refers to the cyclical practice of identifying, categorising and mitigating vulnerabilities.

This covers the lifecycle of reviewing and applying  patches to systems.

### Vulnerability Management Threats

- Zero day vulnerabilities
- Workarounds (temporary fixes)

### Patch Management Threats

- Patch failure
- Poor patch testing (time pressure)

## Vulnerability Management Tools

- Intel from external sources
- Good communication plan

## Patch Management Tools

- Multiple environments for testing
- Effective roll back procedures
- Virtual patching

## Availability Management

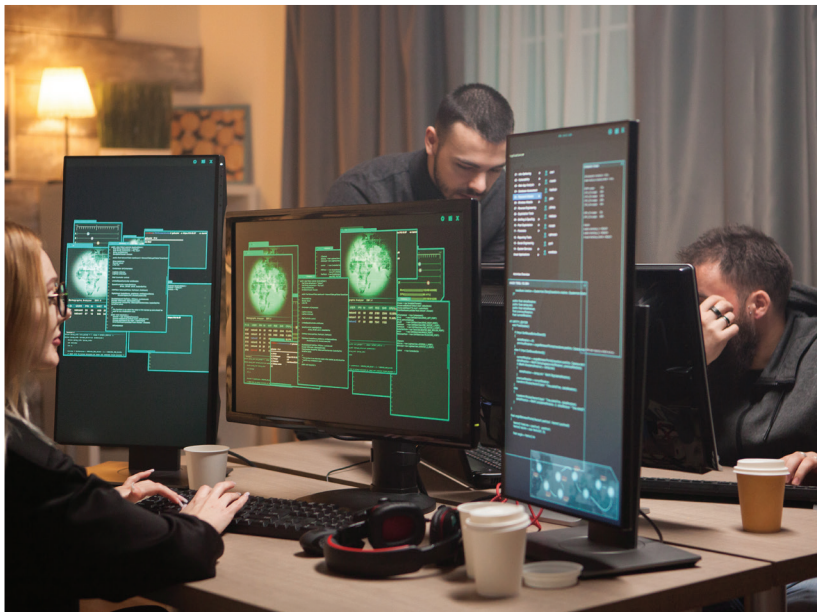
Concerned primarily with uptime and also disaster recovery procedures.

## Availability Management Threats

- Application failure
- DDoS attacks
- Misconfiguration
- Power failure
- Natural disasters

## Availability Management Tools

- Load balancing
- Redundancy
- Backups
- Backup sites



# Supply Chain Security

Covers the upstream and downstream of components in a system

## SCS Threats

- Open Source Libraries (OpenSSL)
- Shared library
- Hardware components (Meltdown/Spectre)

## SCS Tools

- Alternative sources
- Updates from suppliers
- Intel feeds
- Effective incident response plans

# Designing for Security

## Security Design Patterns

This refers to a proven and repeatable solution to solving specific recurring information security problems.

- Should be based on security best practices
- Should solve a specific issue in terms of the CIA triad
- Should be adaptable

Security patterns have their origin from physical architecture and construction and are attributed to Christopher Alexander who developed a pattern based approach to architecture.

His approach was later adopted by the software developers

**A security pattern structure consists of:**

- Title
- Purpose/Intent
- Abstract
- Motivation (in relation to the business)
- Specific problem statement
- Solution to the problem
- Structure/Diagram
- Risks

### Categories

- Availability & resiliency patterns (predictable and reliable access problems)
- Protection patterns (CIA) (unauthorised access and disclosure, tampering and authenticity problems)

### Design Methodology

- Define the problem
- Identify all resources, users and possible threats
- Identify realistic ways the resources can be compromised
- Define the protection goals
- Create relational diagram

# Security Design Pattern Example

**Objective** - Develop a secure security pattern for corporate emails

Problem Definition - Emails are sent and received on a daily basis containing sensitive data. As such, the confidentiality , integrity, authenticity and accountability of these emails must be achieved.

RUTs - Email Servers, Communication channel (emails), Email Users (senders & receivers) , Threat actors (internal & external)

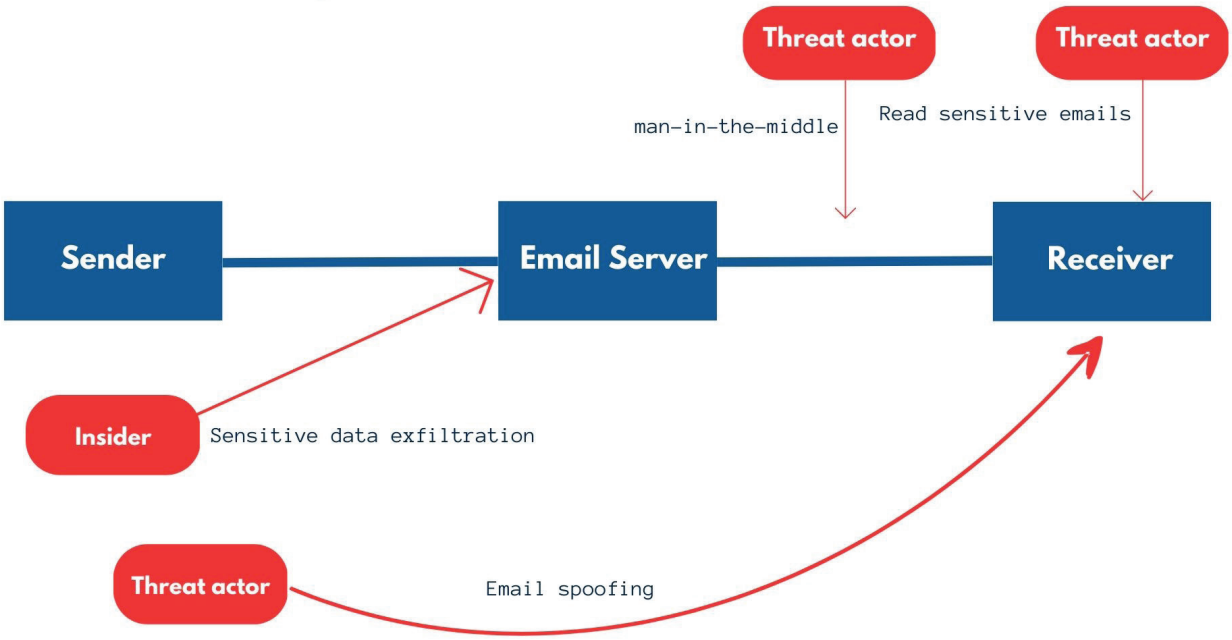
## Attack Paths

- Insider can send sensitive documents to their personal account
- Insider can download sensitive documents from an email account to a USB device
- Man in the middle attacks can be used to intercept the exchange of emails
- Employee can deny sending an email
- Threat actors can send spoofed emails using the company's email domain

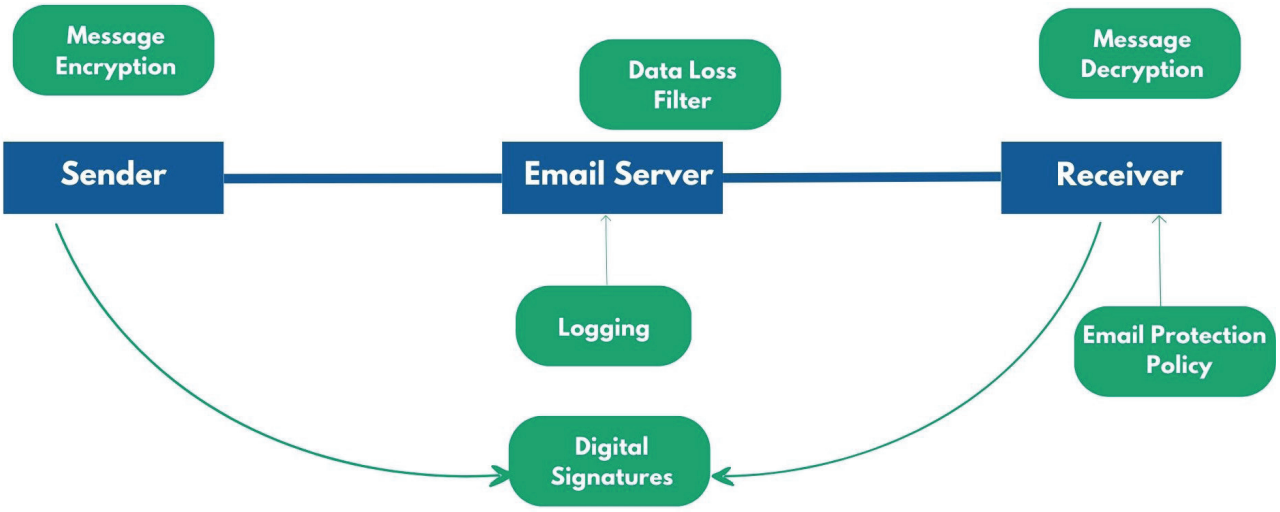
## Protection Goals

- Ensure the confidentiality of the email communications
- Ensure the integrity of the email communications
- Ensure the authenticity of the email communications
- Ensure non-repudiation
- Prevent the incoming and outgoing of malicious emails and SPAM
- Prevent the unauthorised transmission of sensitive data

## Threat Actors Diagram




## Protection Diagram

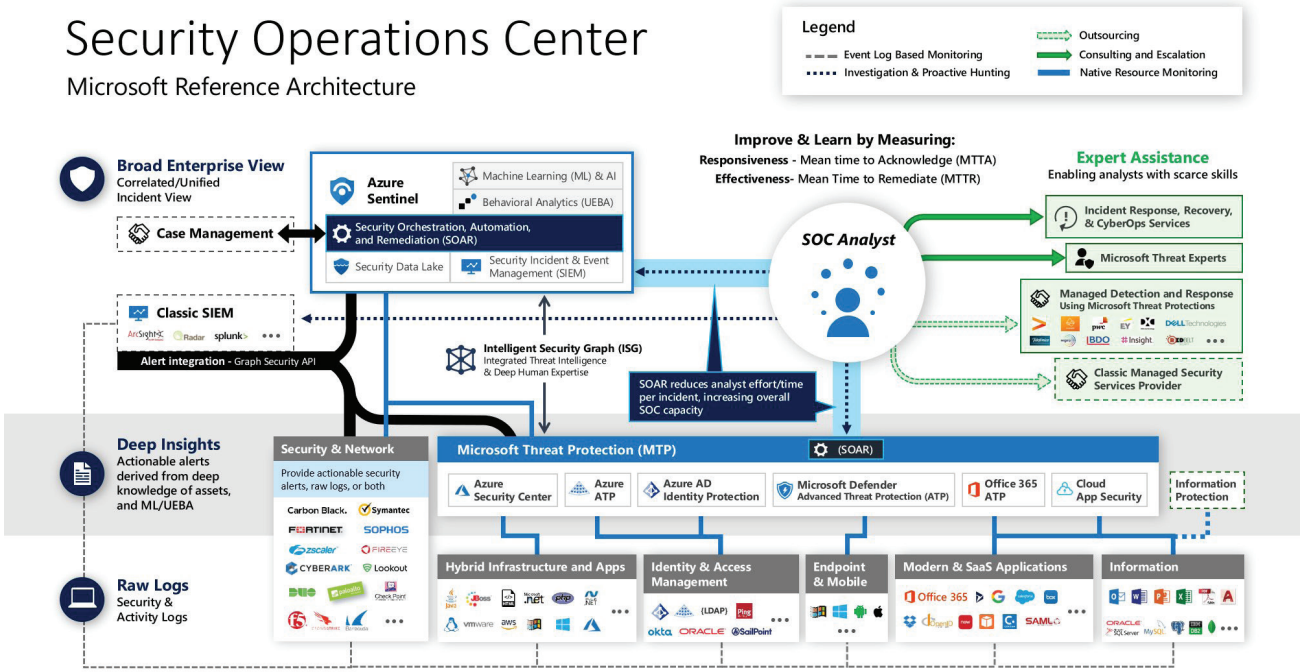


# Reference Security Architectures

These are templatized and reusable security solutions for an architecture in a particular domain.

Rather than focusing on a single problem like security patterns, they focus on a particular security domain and can contain multiple related security patterns.

Companies can benefit from decreased development costs.




## Additional Reading and Links to follow:

- https://securitypatterns.io/docs/how-to-write-a-security-pattern/
- https://owasp.org/www-community/Threat_Modeling_Process
- https://sabsa.org/
- https://www.opengroup.org/togaf
- https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/
- https://pecb.com/whitepaper/risk-assessment-with-octave