Data Security

8th April, 2021

BRITACOM Seminar 3
Tax-related Data Governance and Application

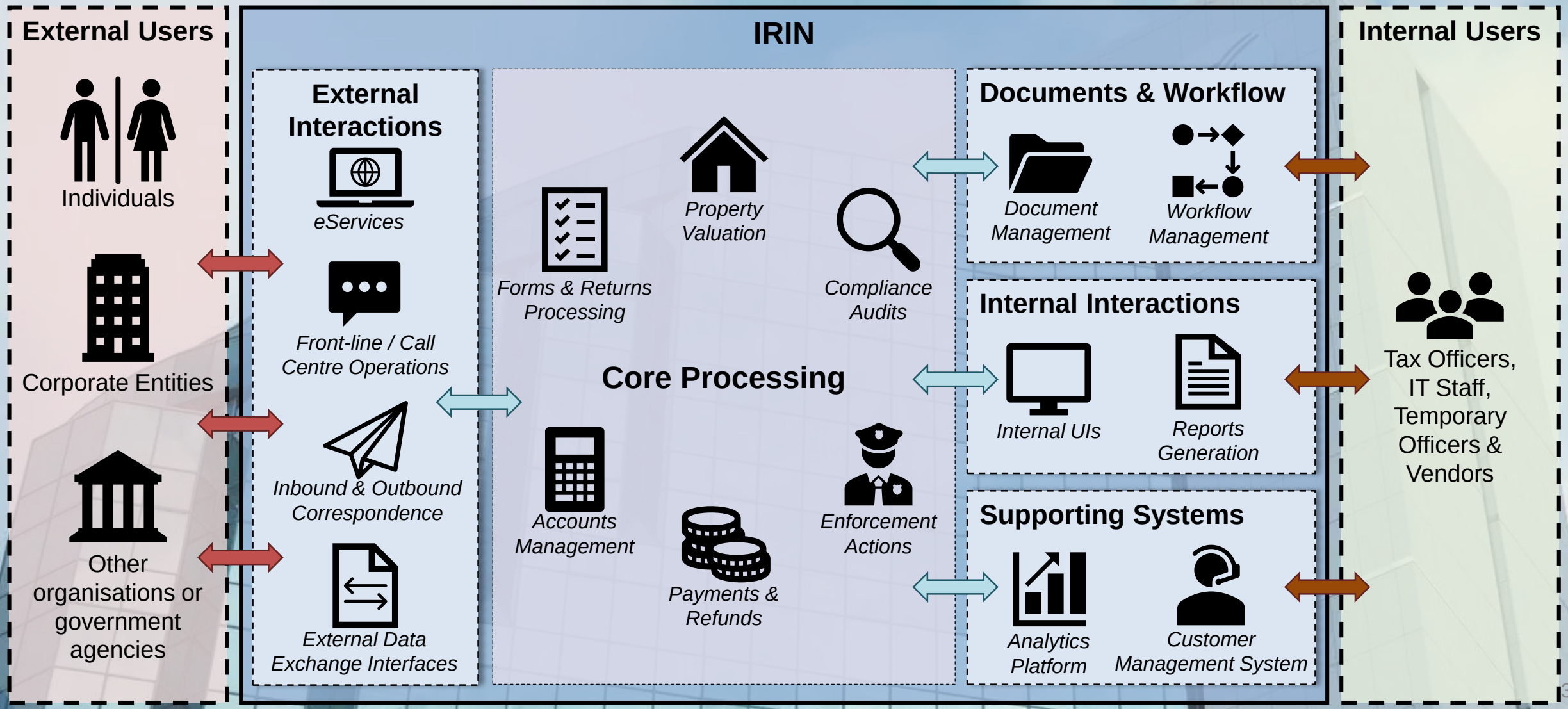
INLAND REVENUE AUTHORITY OF SINGAPORE

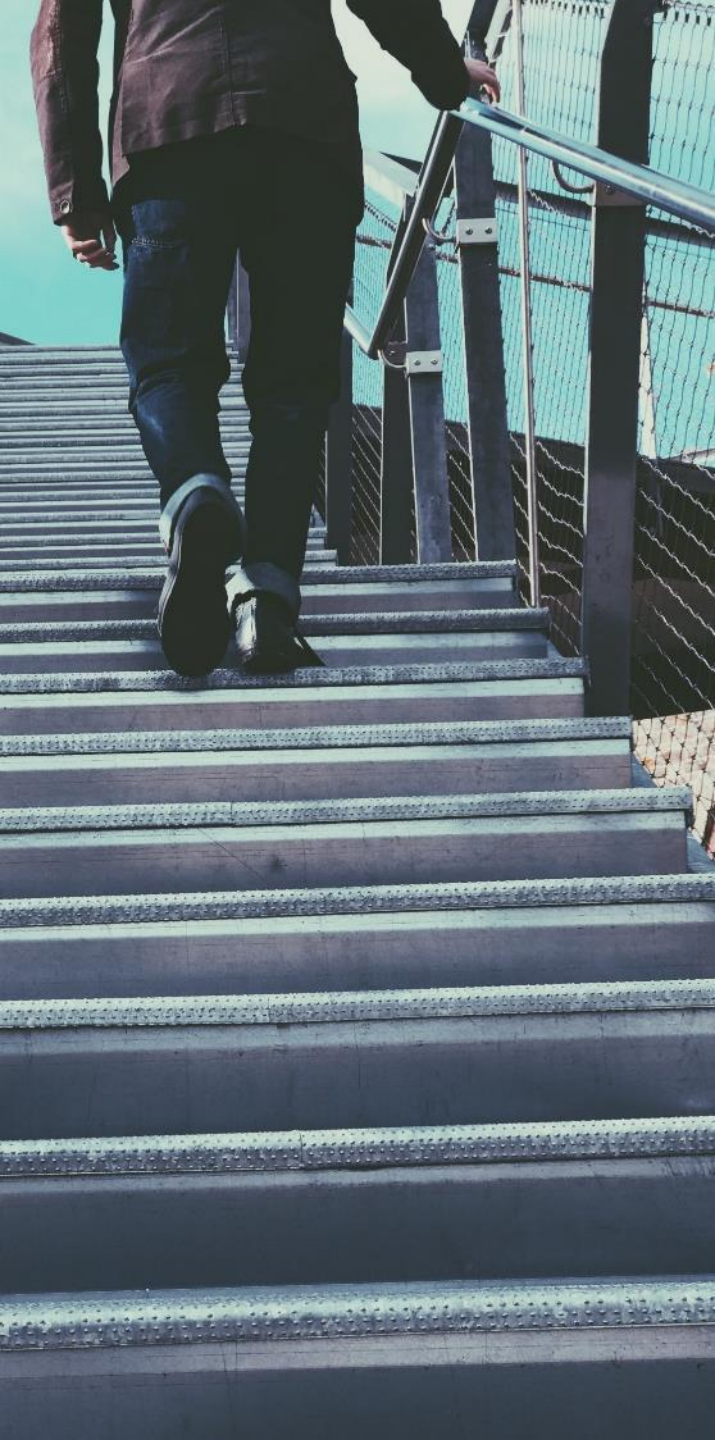
The Next Generation Tax System

An introduction to IRIN 3

IRIN – Inland Revenue Interactive Network

IRAS' Integrated Tax Administration System





Enhancing our Capabilities

Continuously improving our efficiency and abilities to serve our taxpayers

Existing Capabilities

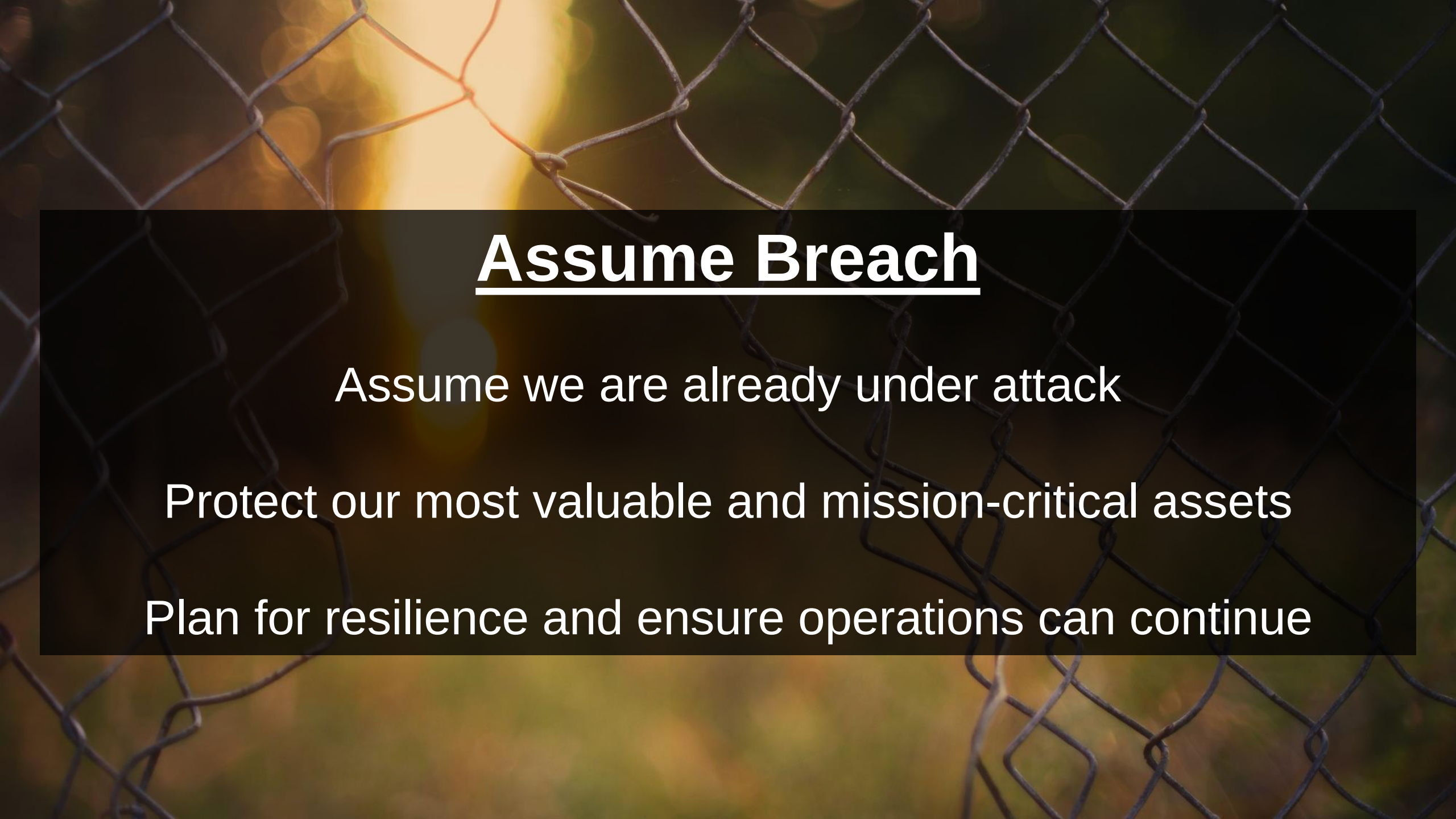
- Taxpayer-Centric Design
- Best-of-breed / Best practices
- Straight Through Processing
- Optimizing resources via virtualisation
- Knowledge Management
- Automated Testing

New Capabilities Being Developed

- Improve **agility and quality** by leveraging on the Government Commerical Cloud and DevSecOps
- **Enhance processing capabilities** with Microservices Architecture
- Leverage **Data** and **Design Driven** approaches to **Redefine Experiences**
- Deploy up-to-date security measures such as the **Zero-Trust Model** and appropriate **Security Risk Management Measures**

Protecting our Data

Our thought process and steps taken



Assume Breach

Assume we are already under attack

Protect our most valuable and mission-critical assets

Plan for resilience and ensure operations can continue

Developing our Security Strategy

Evolving from preventive security to “assume-breach”

Identify Threats

A rising number of security controls being bypassed by sophisticated threat groups or insiders. Perform **Threat Modelling** to identify the different types of threats and potential scenarios where we may be attacked

Enhance Capabilities

Enhancing detection and response strategies while continuing preventive efforts. Aim to slow down attackers, increasing our window of opportunity to detect attackers and allow quick response to attacks

Develop Solutions

Require verification and authentication at multiple points in the network, more granular security across various layers and extensive monitoring to develop a **zero trust model**

Zero Trust

Infrastructure

Data

Identity

Data Encryption at storage or in transition

Data Tokenisation of sensitive fields

Database Activity and query monitoring

Governance and Risk Management

Hub and Spoke Architecture

SOC, Logging and Monitoring

Fine-grained access policies for control

Tracking end-to-end user activities

Authentication and authorization

Setting Up The Overall Strategy

Defining Threats and Controls

Governance and Risk Management

Risk Management and Governance Frameworks are developed to model potential risks (threat vs impact) and govern the development of security controls to address those risks.

Mapping Threats to Governance Controls

	Reconnaisance		Delivery		Attacks	
Threat:	Social Engineering	Reconnaissance Scans	Malware	Exploiting User Interfaces	Lateral Movement	Data Theft
Control:	User Education	Patching & Regular reviews	Anti-Malware & Containment Measures	Code Scanning & Penetration Testing	Network Compartments & Traffic Control	Data Protection & Monitoring

Identifying Users, Controlling Access

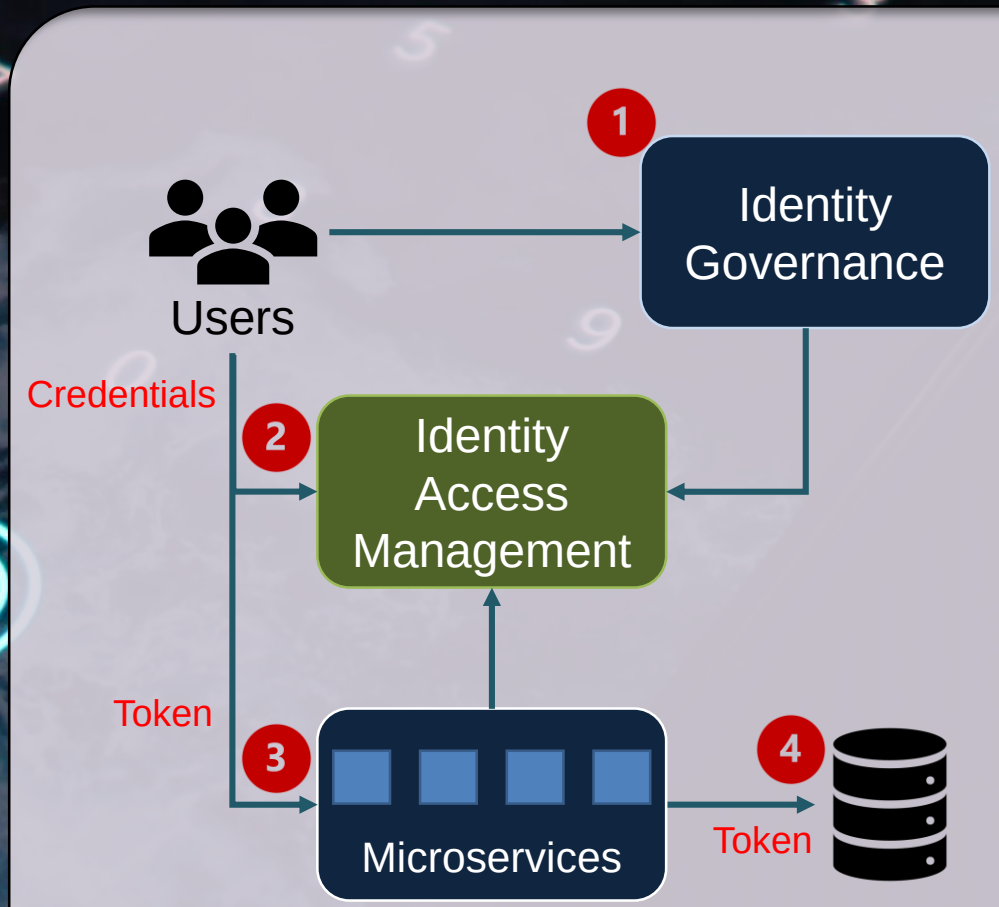
Understanding who is accessing data and what can they access

Authentication and authorization

Develop a range of services that provide end-to-end management of a user's credentials, from provisioning to disposal. Use identity governance workflows to standardize access requests to data, and the authority to grant access to data.

Fine-grained access control policies

Granularity of access is important. Fine-grained access control can refer to which field in a dataset is granted to which group or individual. Through the use of such granular access control, we can track exactly what data a user has accessed



Data Encryption & Tokenisation

What is it, and what should it do

Data Encryption at storage or in transition

Data encryption requires control of the methods of encryption and the keys used to encrypt. Encryption keys should be generated by the organization (BYOK) and stored in a secure area such as a Hardware Security Module (HSM).

Data Encryption may be performed either on the data, the database file or on the underlying disk used to hold the data.

Data Tokenisation of sensitive fields

Tokenisation of sensitive fields involves replacing data such as PIIs with a string of randomized characters of a similar length and content. For example a credit card number can be replaced by other digits but still in the same format.

Tokenisation helps keep such data secure as it passes through different systems.

Pro-Active and Reactive Controls

What is it, and what should it do

Database Access and query monitoring

Database activity monitoring (DAM) is a database security technology for monitoring and analyzing database activity.

DAMs may combine data from network-based monitoring and database audit information to provide a comprehensive picture of database activity.

Data Loss Prevention

Data Loss Prevention (DLP) is a network or endpoint monitoring solution that detects for sensitive data being extracted or misused by unauthorized users.

DLP software will scan network traffic or files at rest on a user's machine to identify key contents, such as PII information and raise alerts or block access to such data

Endpoint Detection and Response

Endpoint Detection and Response (EDR) software is installed on endpoints to provide continuous monitoring on the computer, to identify any activities or patterns that may pose a threat.

An example of a threat could be programs being launched by external sources. The EDR will raise alerts and block the threat from escalating.

Monitoring & Tracking

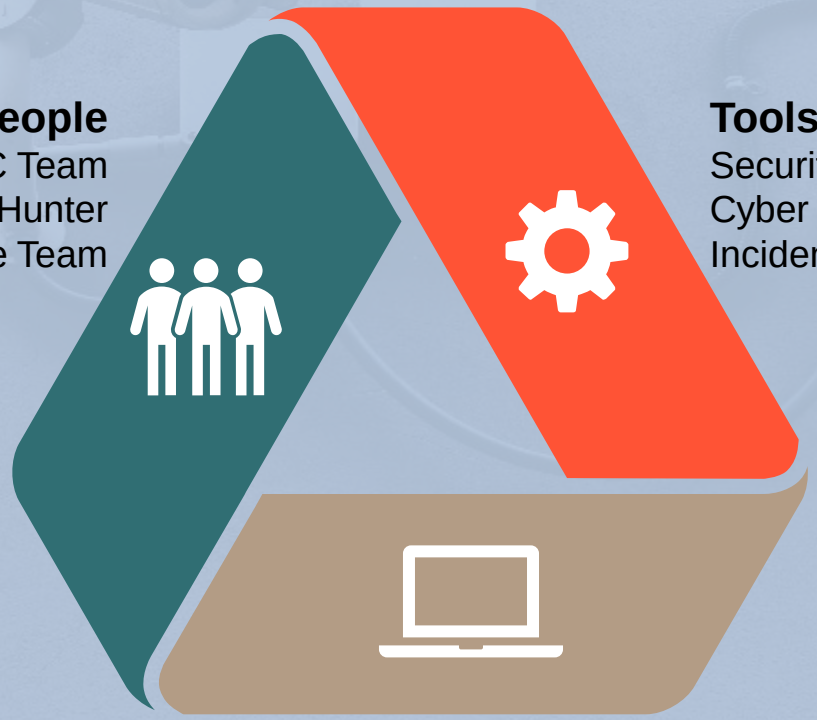
Post-Activity Tracking and Pro-Active Anomaly Detection

SOC, Logging and Monitoring

Tracking end-to-end user activities

Logging & Monitoring and tracking of end-to-end user activities depend on a comprehensive Security Operations Centre (SOC) to collate, investigate and raise alerts when anomalies are detected. A pro-active SOC requires a well thought out set of events handling and containment processes

People
SOC Team
Cyber Threat Hunter
Incident Response Team



Tools
Security Monitoring
Cyber Threat Hunting
Incident Response

Technology
Security Information & Event Management (SIEM)
User and Entity Behaviour Analytics (UEBA)
Security Orchestration Automation and Response (SOAR)

Thank You