CORPORACIÓN FONAFE

Dejando Huella

CORPORACIÓN FONAFE

Dejando Huella

FONAFE TECH

Roberto Munayco

Cybersecurity Practice Leader
Kyndryl

CORPORACIÓN FONAFE

Dejando Huella

FONAFE TECH

Journey de Ciberseguridad en FONAFE

kyndryl

FONAFE Tech Day

Customer Journey

Contenido

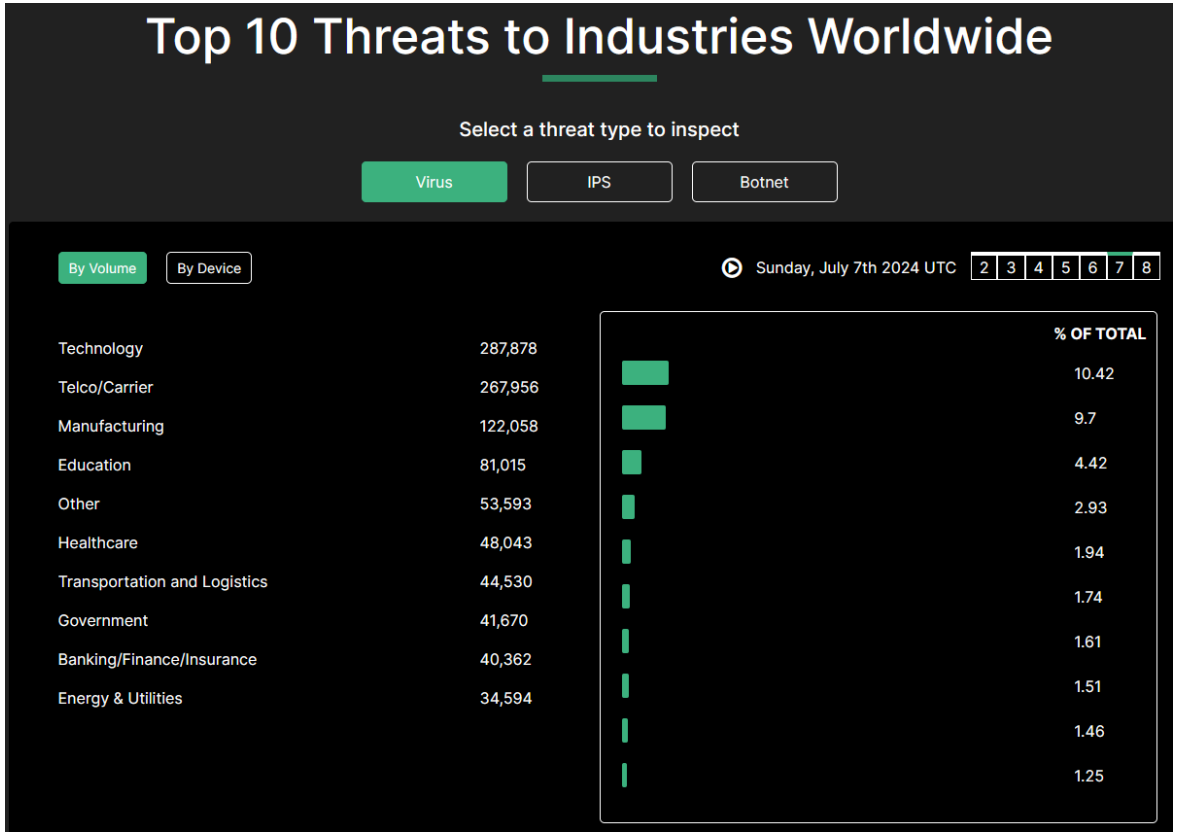
kyndryl

01

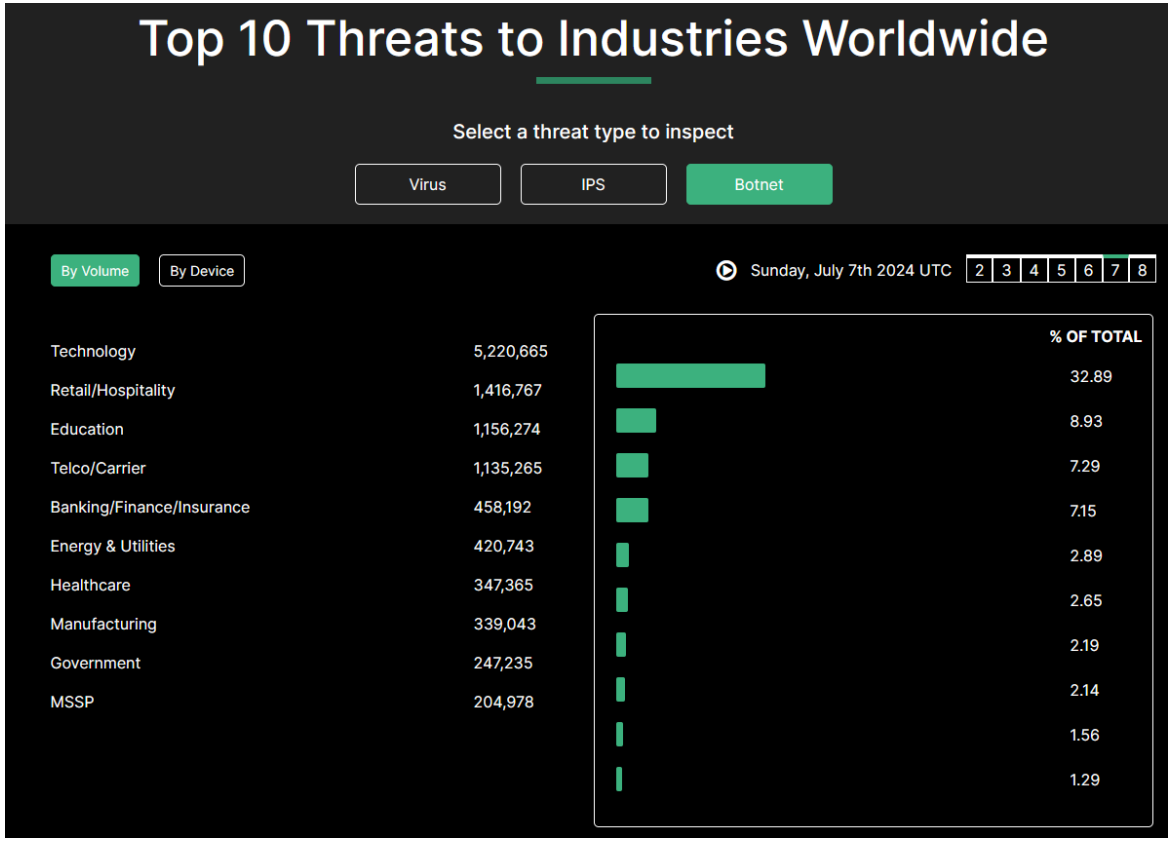
Tendencias de Ciber Ataques en el Mundo

kyndryl

Tendencias de Amenazas en el Mundo por Industria



https://www.fortiguard.com/threat-research



https://www.fortiguard.com/threat-research

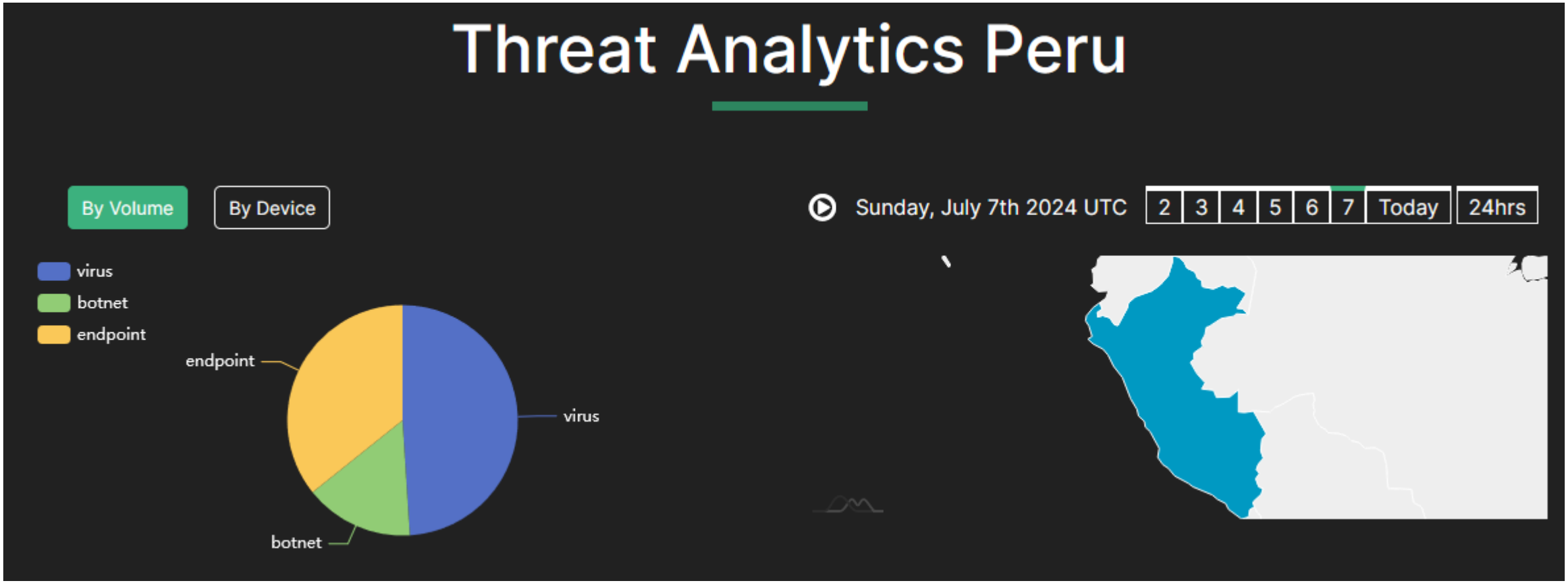
kyndryl

01

Tendencias de Ciber Ataques en el Perú

kyndryl

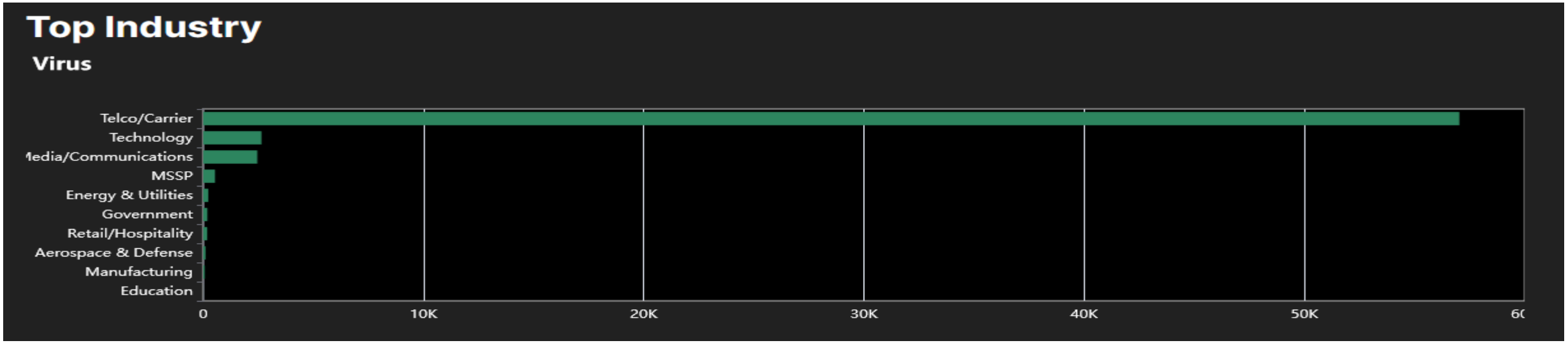
Tendencias de Amenazas en el Perú

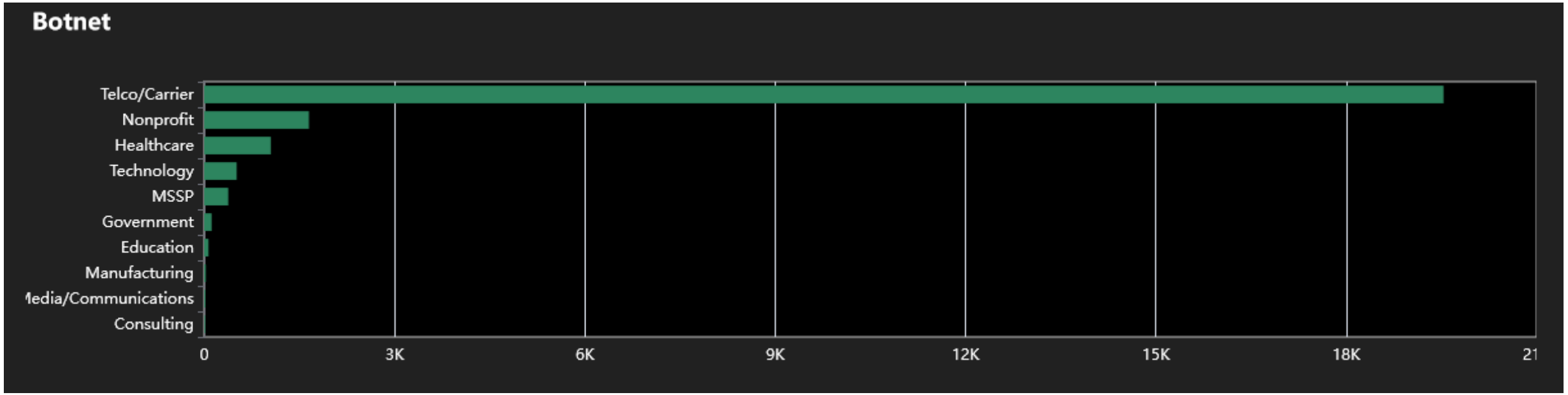


https://www.fortiguard.com/threat-research

kyndryl

Tendencias de Amenazas por la Industria en Perú





kyndryl

03

Casos de Ciber Ataques

kyndryl

Caso 1 – Sector Financiero

¿Quién fue el afectado?

- Banco Santander es una de las principales instituciones financieras globales, conocida por su extensa red de servicios bancarios y financieros, presencia internacional, y compromiso con la innovación y la sostenibilidad.

¿Qué comprometieron?

- Información de clientes.
- Datos de empleados y ex empleados

¿Que comunicó el banco?

Santander

Comunicado

Madrid, 14 de mayo de 2024 - Grupo Santander ha tenido recientemente conocimiento de un acceso no autorizado a una base de datos de la entidad alojada en un proveedor. El banco implementó de inmediato medidas para gestionar el incidente, como el bloqueo del acceso a la base de datos y un refuerzo de la prevención contra el fraude para proteger a los clientes.

Tras la investigación llevada a cabo, podemos confirmar que se ha accedido a información de clientes de Santander Chile, España y Uruguay, y de todos los empleados y algunos exempleados del grupo. En el resto de mercados y negocios de la entidad no hay datos de clientes afectados.

En la base de datos no hay información transaccional ni credenciales de acceso o contraseñas de banca por internet que permitan operar con el banco. Las operaciones y los sistemas de Santander no están afectados y los clientes pueden seguir operando con seguridad.

- Afectación en 3 paises: Chile, Uruguay, España
- No se afectó la información de credenciales.
- No se afectó información bancaria de sus clientes
- Recomendó estar atentos a posibles phishing.

kyndryl

Caso 2 – Sector Transporte

*!_WHY_FILES_ARE_ENCRYPTED_! - Notepad

File Edit Format View Help

Hello!

First of all it is just a business and the only thing we are interested in is money.

All your data was encrypted.
Please don't try to modify or rename any of encrypted files, because it can result in serious data loss and decryption failure.

Here is your personal link with full information regarding this accident (use Tor browser):
http://rnsm777cdsjrsdlbs4v5qoeppu3px6sb2igmh53jzrx7ipcrbjz5b2ad.onion/<victim_id>/

kyndryl

04

Customer Journey

kyndryl

Customers Journeys

¿Qué es?

Se refiere al **proceso** por el que pasa un cliente cuando interactúa con kyndryl **para modernizar, innovar o transformar su panorama empresarial y tecnológico.**

¿Por qué?

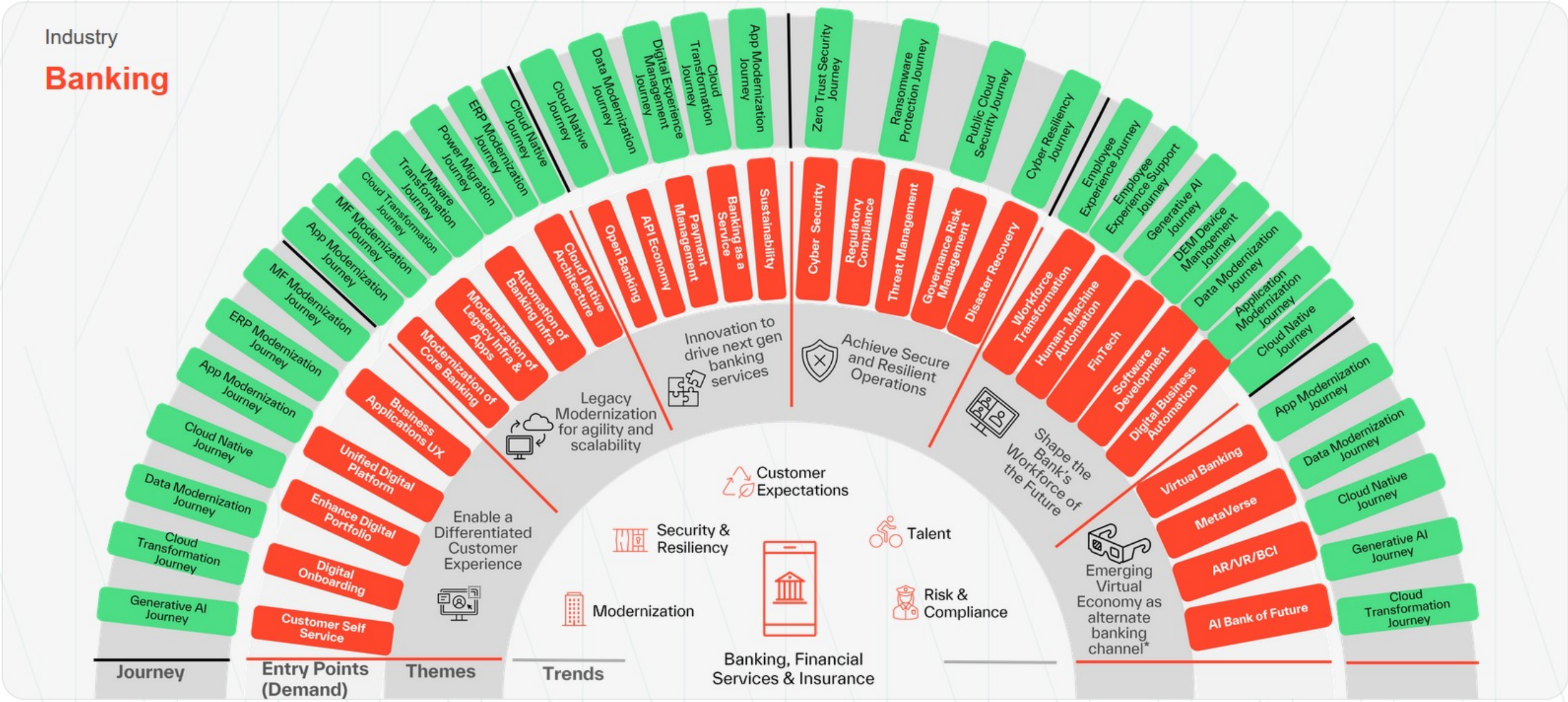
Un Customer Journey bien diseñado ayudará al cliente a **alcanzar sus objetivos comerciales**, que incluyen una **experiencia de usuario mejorada, soluciones modernas, mayor eficiencia, costos optimizados, seguridad mejorada o mayor escalabilidad.**

¿Cómo?

El Journey puede ser complejo y puede involucrar múltiples stakeholders y challenges. Dependiendo de la complejidad, el journey se puede dividir en journeys más pequeños denominados micro journeys y puede abarcar varias etapas, **comenzando con una evaluación, seguida por el diseño, la planificación y la implementación de cambios, la optimización, la gestión y el soporte continuos.**

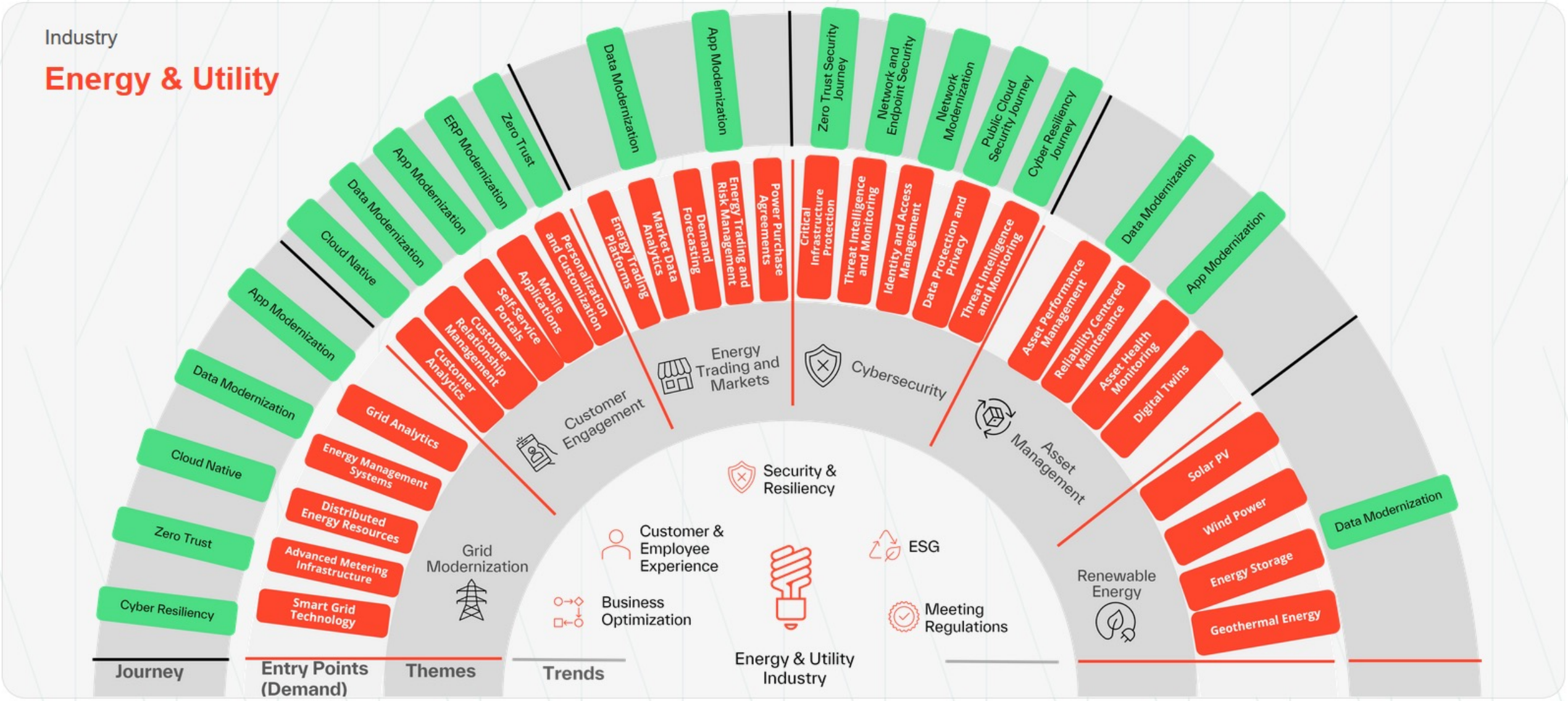
kyndryl

Fields of Plays



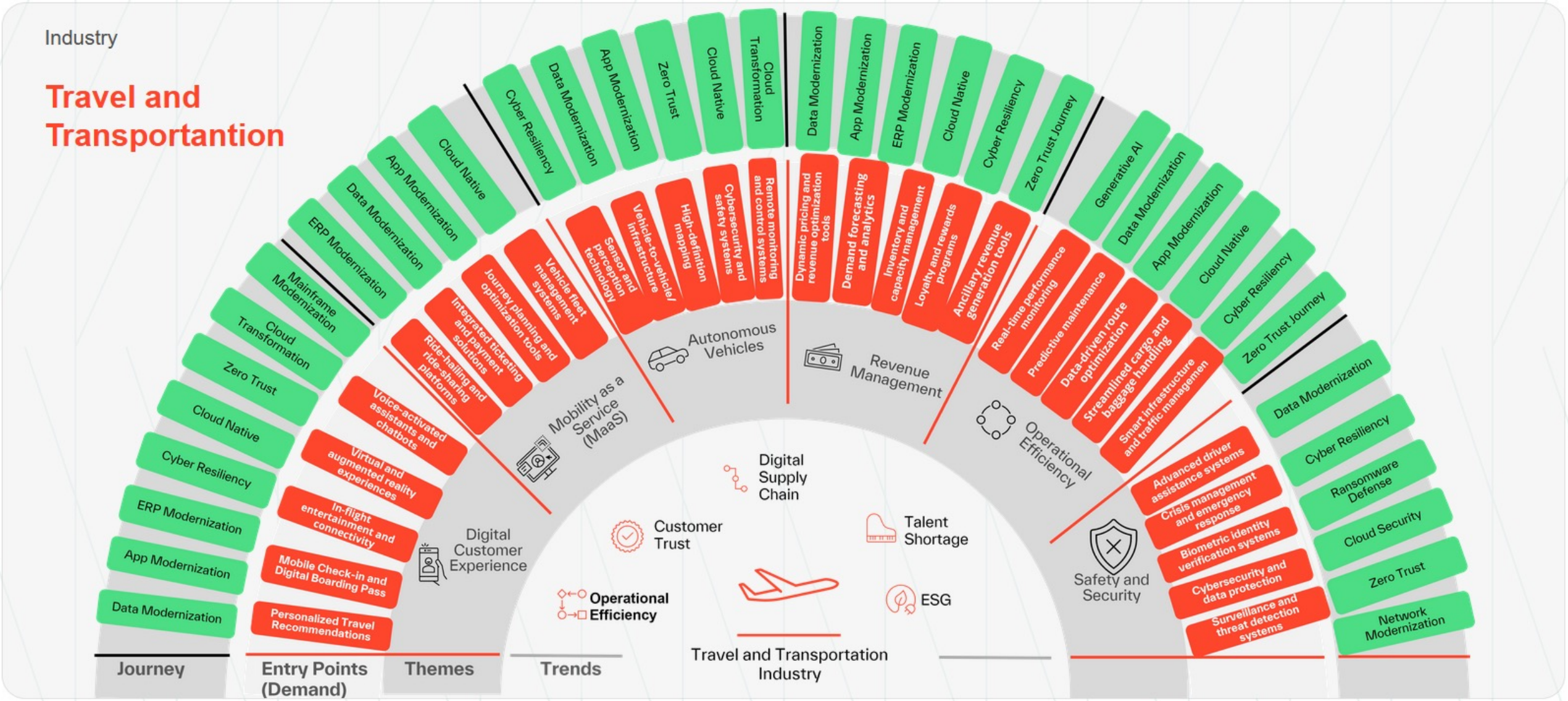
kyndryl

Fields of Plays



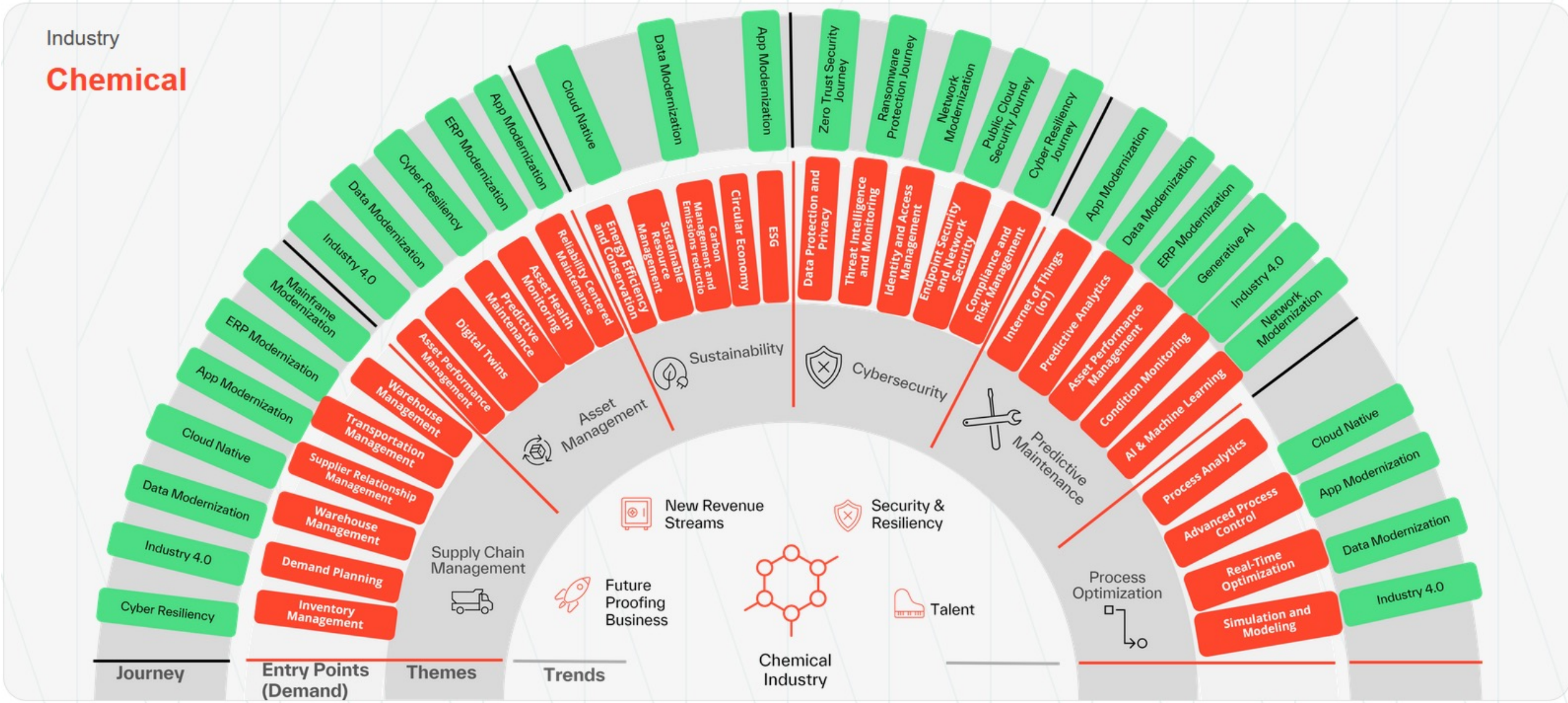
kyndryl

Fields of Plays



kyndryl

Fields of Plays



Security Field Plays

Zero Trust
Secure your digital transformation with end-to-end access control and fine-grained security.

Ransomware Defense
Defend against ransomware attacks and protect critical assets with comprehensive security measures.

Security Operations
Strengthen your cybersecurity posture with proactive threat identification and response.

Cyber Security Incident Response & Forensics (CSIRF)
Manage and mitigate security incidents with a systematic response approach.

Cyber Resilience
Anticipate, withstand, and recover from cyber threats with a resilient cybersecurity framework.

Public Cloud Security
Ensure data sovereignty and minimize cyber threats in public cloud environments.

DORA Awareness and Preparation
Prepare for and comply with DORA regulations to ensure operational resilience.

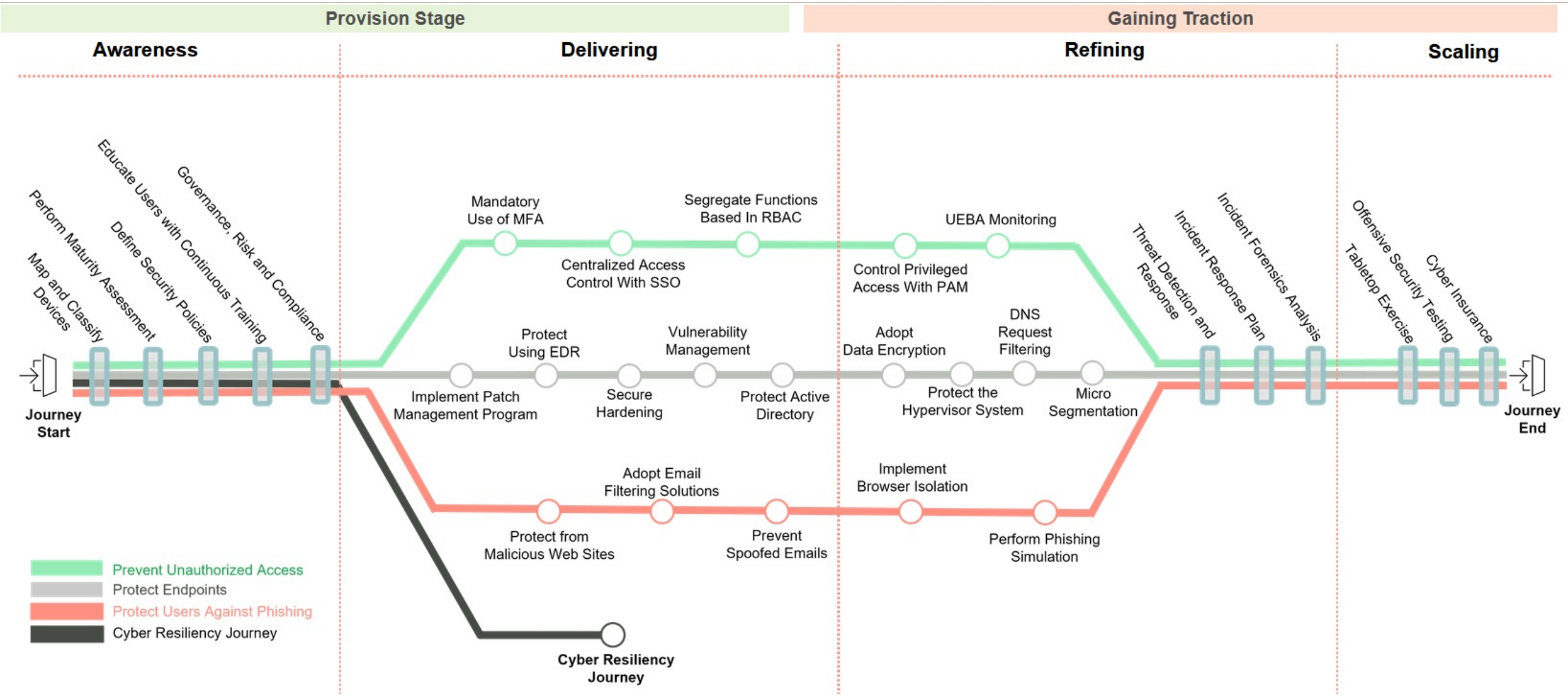
IAM Maturity
Building a shield of trust, aligning with Zero Trust principles to safeguard the digital realm from unauthorized challenges.

05

Metro Map

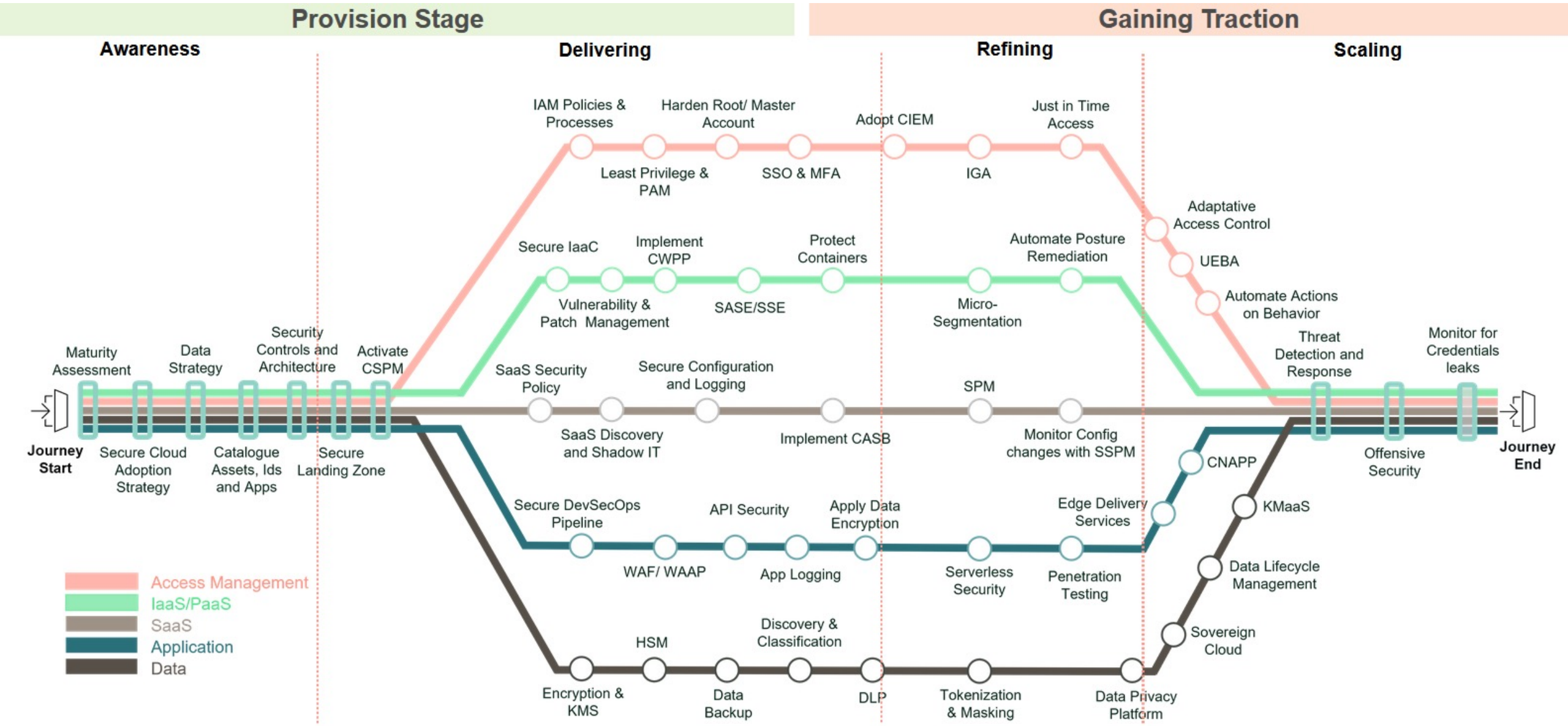
kyndryl

Ransomware Defense



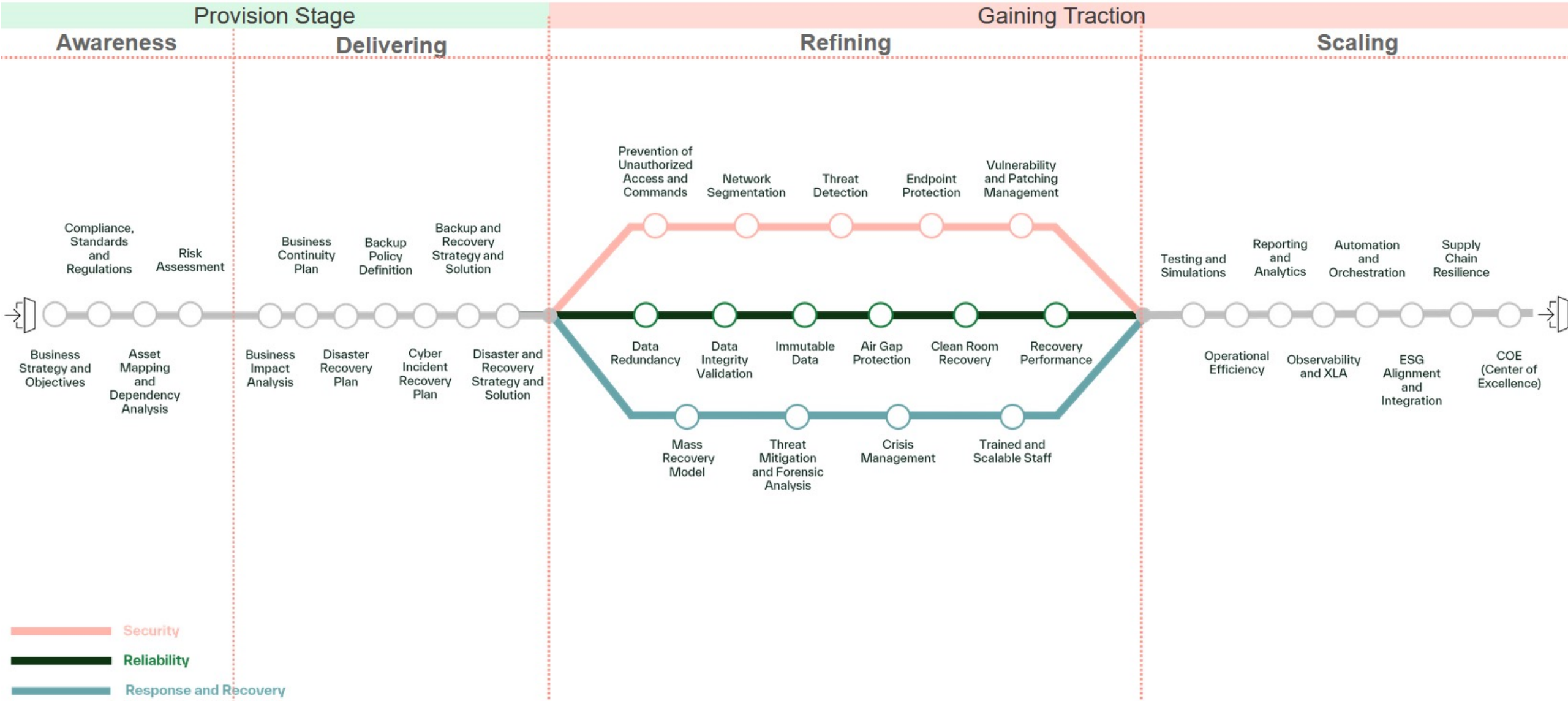
kyndryl

Public Cloud Security



kyndryl

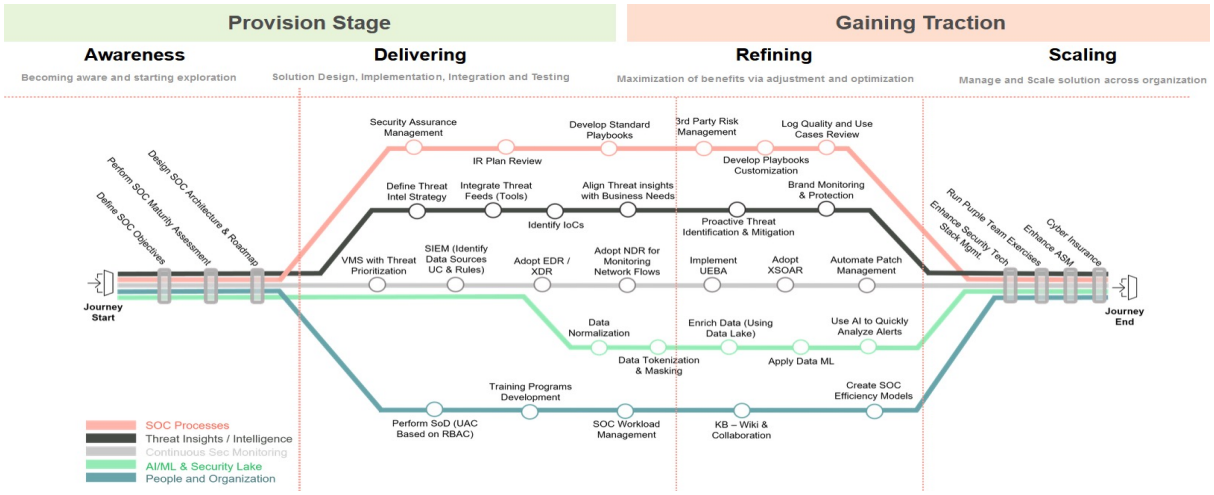
Cyber Resilience



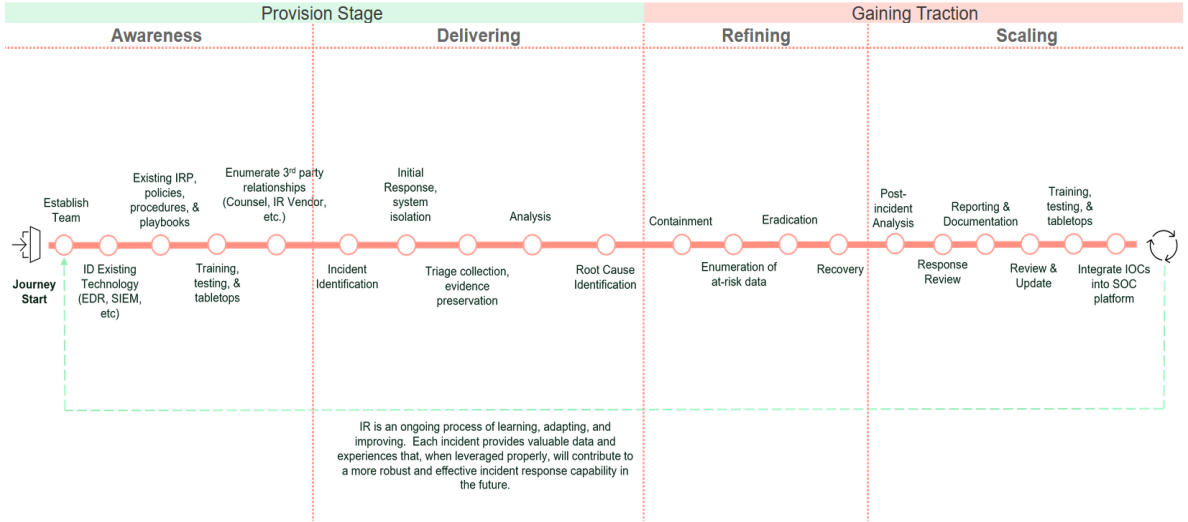
kyndryl

Cyber Resilience

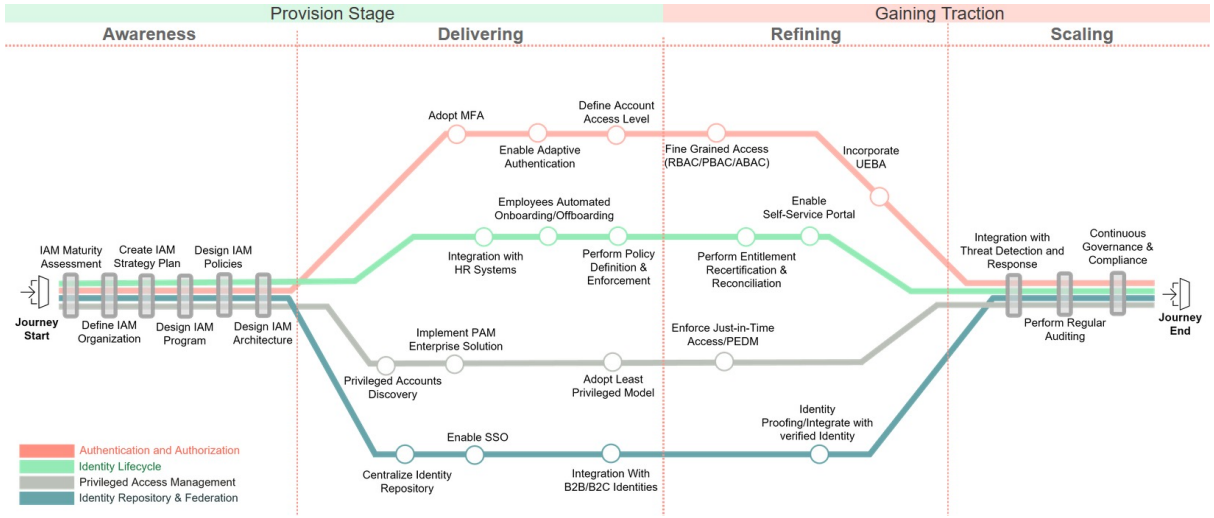
Security Operations Center



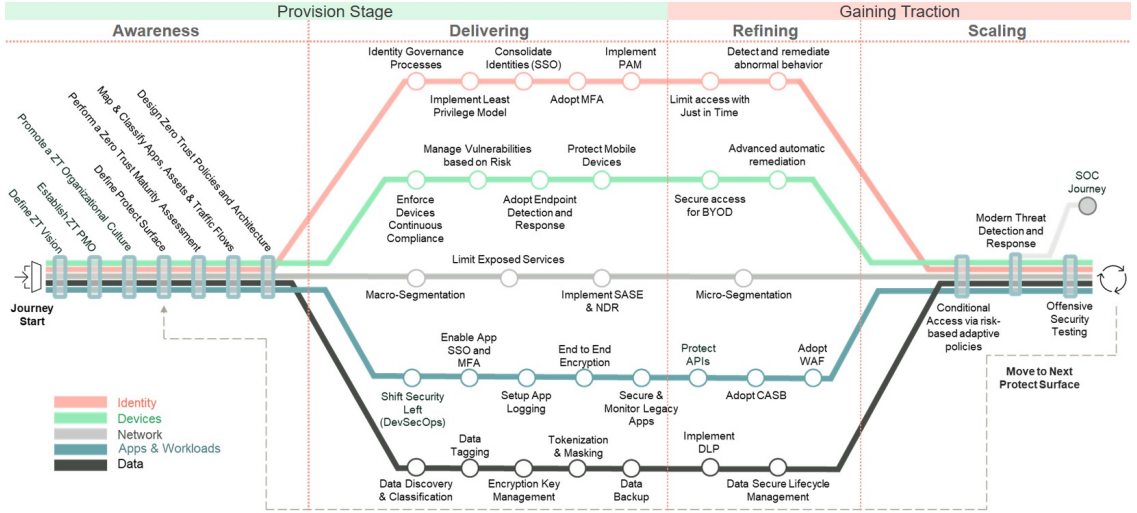
Cyber Security Incident Response & Forensics



IAM Maturity



Zero Trust



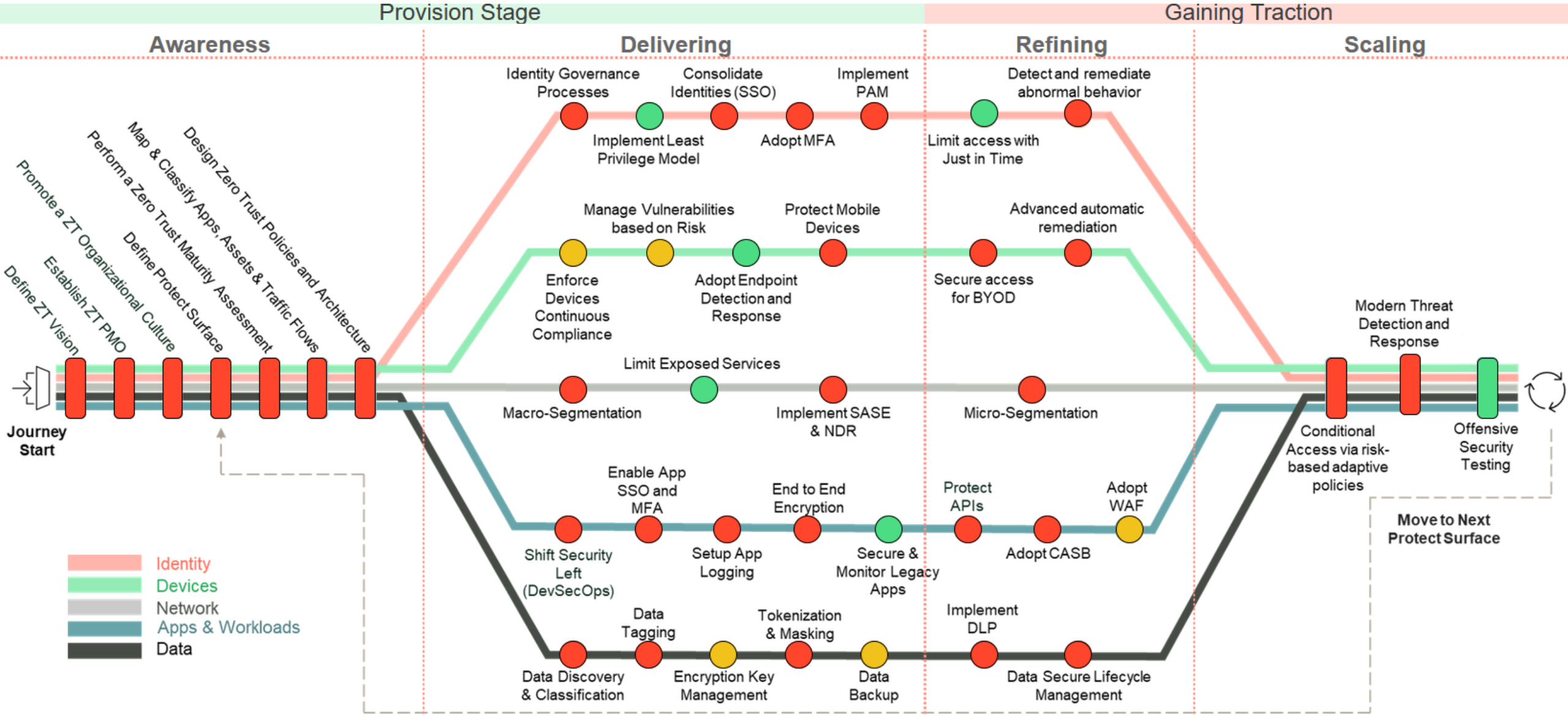
kyndryl

06

Resultados Customer Journey

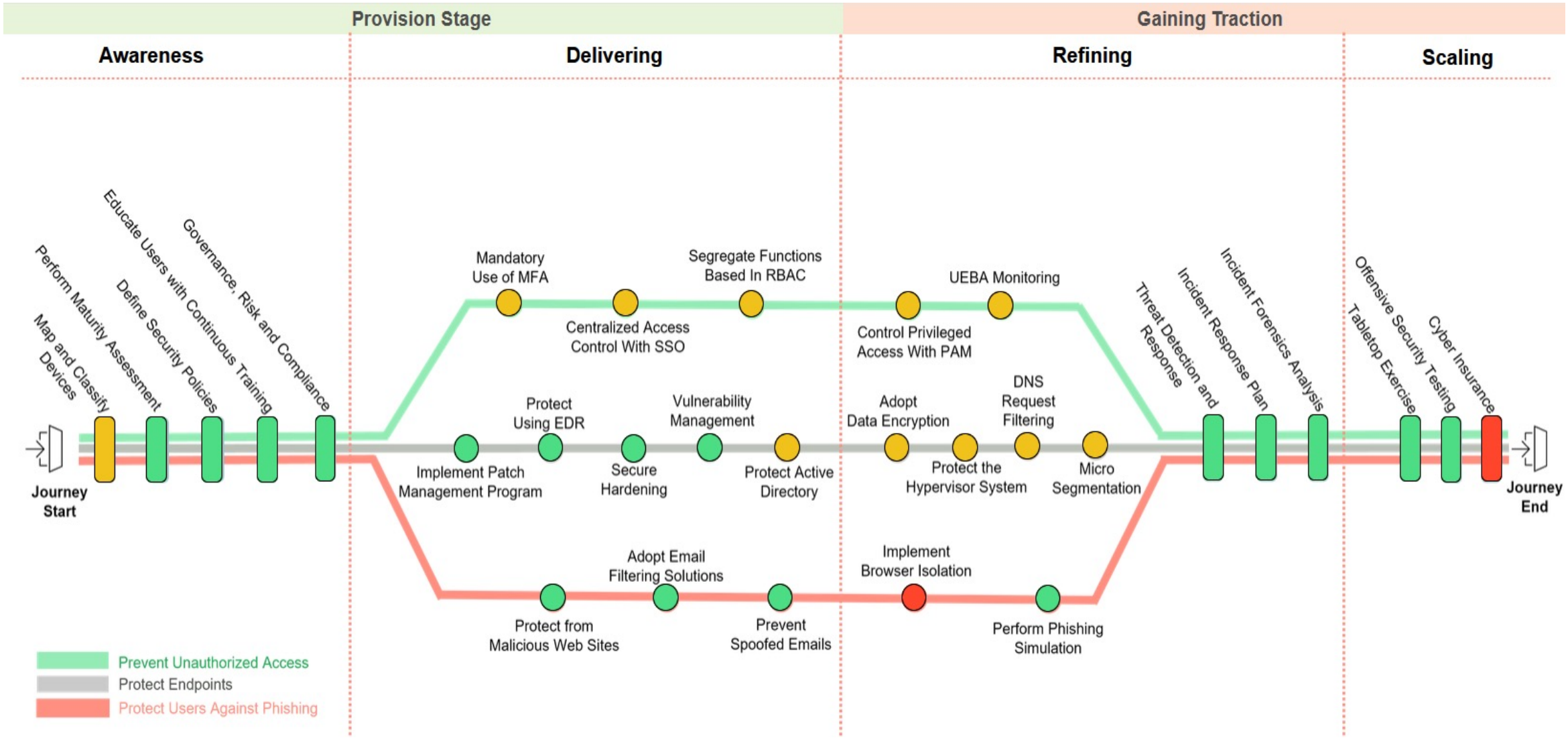
kyndryl

Resultado – Zero Trust



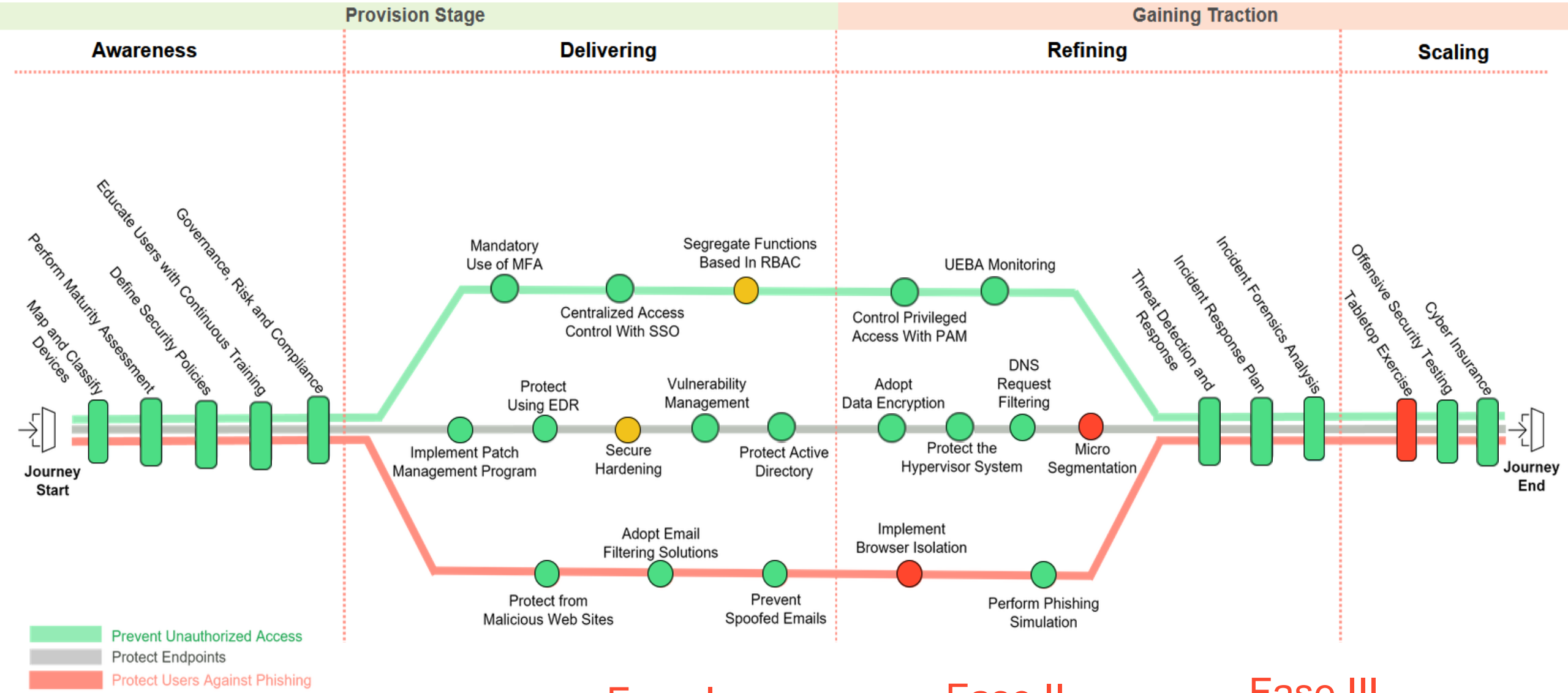
kyndryl

Resultado 1 – Ransomware Defense



kyndryl

Resultado 2 – Ransomware Defense



Fase I

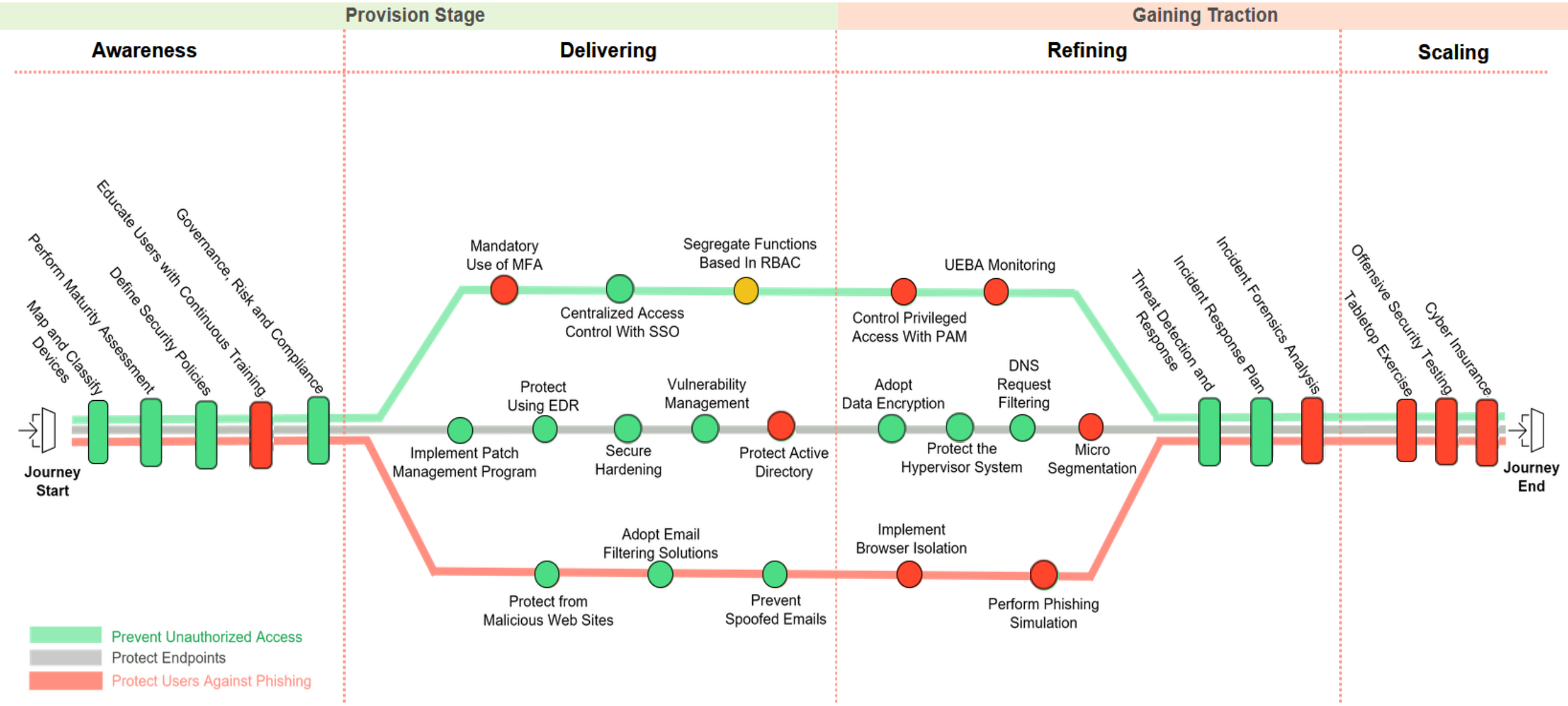
Fase II

Fase III

kyndryl

Línea de Tiempo

Ransomware Defense – Centro de Datos FONAFE



kyndryl

Informe de Resultado

Assessment Results

Introduction

In this section you will find the results of the Customer Journey Assessment, which is composed by a set of questions designed to map your organization level of implementation and adoption of key journey requirements.

The Kyndryl Customer journeys are organized in four main stages (Awareness, Delivering, Refining and Scaling) and within each stage, there are stations, which are where the requirements are defined and action takes place.

For each station, you may have one or more questions, which can be answered as Yes (Implemented), Partially (Partially Implemented) and No (Not Implemented).

Recommendations are provided for stations where the answer was Partially or No

Journey Name	Journey Stage	Journey Station	Question	Response
Network Modernization V2	Awareness	Data & Apps consumption assessment	Have you conducted a thorough assessment of applications' network flows? Have you leveraged any tool to identify unknown traffic flows?	Partiallly
Network Modernization V2	Awareness	Network and Security Operations Assessment	Do you have centrally managed network operations in place that meets the business needs? Have you performed operations assessment for NOC and SOC?	Yes
Network Modernization V2	Awareness	Define Network Technology Stack	Do you have a forward looking enterprise architecture document that identifies technology vendors for all aspects in your network environment? Do you have a process in place to continuously evaluate this document?	No
Network Modernization V2	Awareness	Security and Compliance GAPS Assessment	Have you performed a targeted security and compliance assessment of your network environment? Are you confident in saying your network devices are fully hardened and secured from any external threats?	Partiallly

kyndryl Customer Journey Explorer

Network Modernization V2	Awareness	Comprehensive Roadmap and Execution Strategy	Have you defined a roadmap along with timelines for modernizing your network? Have you created the execution plan?	Partiallly
Network Modernization V2	Delivering	Cloud Strategy Plan	Do you have a comprehensive cloud strategy that aligns with your business goals. Consider factors such as cost, scalability, security, and compliance when choosing the right cloud model (public, private, or hybrid). (Yes/No/Partially)	Yes
Network Modernization V2	Delivering	Hybrd Multi-Cloud Connectivity design & Build	Have you defined Software Enterprise connectivity framework	Partiallly
Network Modernization V2	Delivering	Hybrd Multi-Cloud Connectivity design & Build	Have you implemented your Multi-Hybrid Cloud networking architecture? Do you have automation in place for Cloud network brokerage services?	Partiallly
Network Modernization V2	Delivering	App/Data Migration	Have you planned and executed the deployment of applications in the cloud using the 7Rs (Rehost, Refactor, Revise, Rebuild, Replace) approach? (Yes/No/Partially)	Partiallly
Network Modernization V2	Delivering	DC Network Assessment & Planning	Do you have target Data Center Operating Model or Blueprint defined to meet modernized software defined DC architecture of the future?	Yes
Network Modernization V2	Delivering	DC - Network Design	Is Software Defined Network the targeted network architecture and its design has been developed and ready for its implementation?	Yes
Network Modernization V2	Delivering	DC- Security Design	Do you have the updated network security design defined and developed that is to be integrated with the target DC Network architecture?	Yes
Network Modernization V2	Delivering	DC- Infra Prep	Is the data center setup ready to support and accommodate the physical and environmental specifications	Yes

Recomendaciones

Recommendation: Depending on business requirements it is advisable to have a tactical as well as 5 year roadmap of Network services that meets the business requirements of future. Its highly recommended such exercise is performed on a periodic basis

Additional notes: Por revisar con el equipo de arquitectura.

Priority: High Priority

Journey Stage: Delivering

Assessment Question: Do you have governance framework in place for defining, executing, auditing and tracking network device compliance and risk management?

Selected Context: Client does not have a framework for Device compliance and risk management.

Recommendation: A robust and matured framework is highly recommended which can developed with help of appropriate partner. While organization can always develop such a framework on its own, however partner's industry and peer knowledge will be extremely useful to ensure organization framework can be in line with Industry standards.

Additional notes: Kyndryl gestiona la red, se revisará al interno.

Priority: High Priority

Journey Stage: Delivering

Assessment Question: Have you started implementation of the new target WAN and Access networks in all your sites - corporate, regional and remote sites?

Selected Context: Client may be half way through their project for deployment of the network modernization/transformation on the WAN and/or Access Network for sites.

Recommendation: Organization has started on the path to standardize the LAN sites, It is recommended that the client creates a repeatable plan in place with a methodology. It could be based on refresh cycle or based on sites criticality.

Additional notes: Tienen definido el clear pass de aruba

Priority: High Priority

Journey Stage: Delivering

Assessment Question: Are the sites WAN and Access networks migrated to the new network,

kyndryl Customer Journey Explorer

integrated seamlessly and are functioning in expected performance?

Selected Context: Client may be half way through their project in migrating the users and workloads to the new WAN and/or Access Network for sites.

Recommendation: Have a repeatable plan in place and ensure the migration plan and its success criteria validation is performed every time a new site is transformed.

Additional notes: si ha sido evaluada, se esta evaluando con ZTNA

Priority: High Priority

Journey Stage: Refining

Assessment Question: Do you leverage AI based insights on top of standard observability stack (Performance, capacity monitors) ? Have you developed UI to grant role based access with targeted views for NOC engineers, NOC managers and for executives?

Selected Context: This client lacks the latest observability stack for governing their network services. Client does not have foundation in place to take advantage of enhancements in artificial intelligence.

Client is not in a positioned to leverage insights into NOC operations using AI.

Recommendation: Modernization of network services also demand modernizing the way an organization operate their SOC and NOC. That involves enhancement of operating model to facto in dev-sec-ops framework, Without which it is impossible to exploit true potential of your network infrastructure to meet Business demands, Network services can be agile with modern NOC and integrating NOC and SOC operations. Recommendation for this domain can be in four sub domains

Client needs to urgently start work in Implementation of latest observability stack that is not only SNMP based but it has AP based collectors for Metadata that will indicate performance and capacity of Software defined networking technologies.
If Client needs to evaluate tools or look for a partner which can bring these latest tools for their Network operations. Client needs to look at adopting those API based tools for all segments of network and define architecture to bring data in a central Data lake.

Client also needs to look at leveraging AI based operational insights not he central data lake which can possibly look beyond just Network metadata. This will enhance Clients ability to seamlessly integrate NOC and SOC operations and even System operations.

Additional notes: Existen tareas automatizadas, para alertamiento.

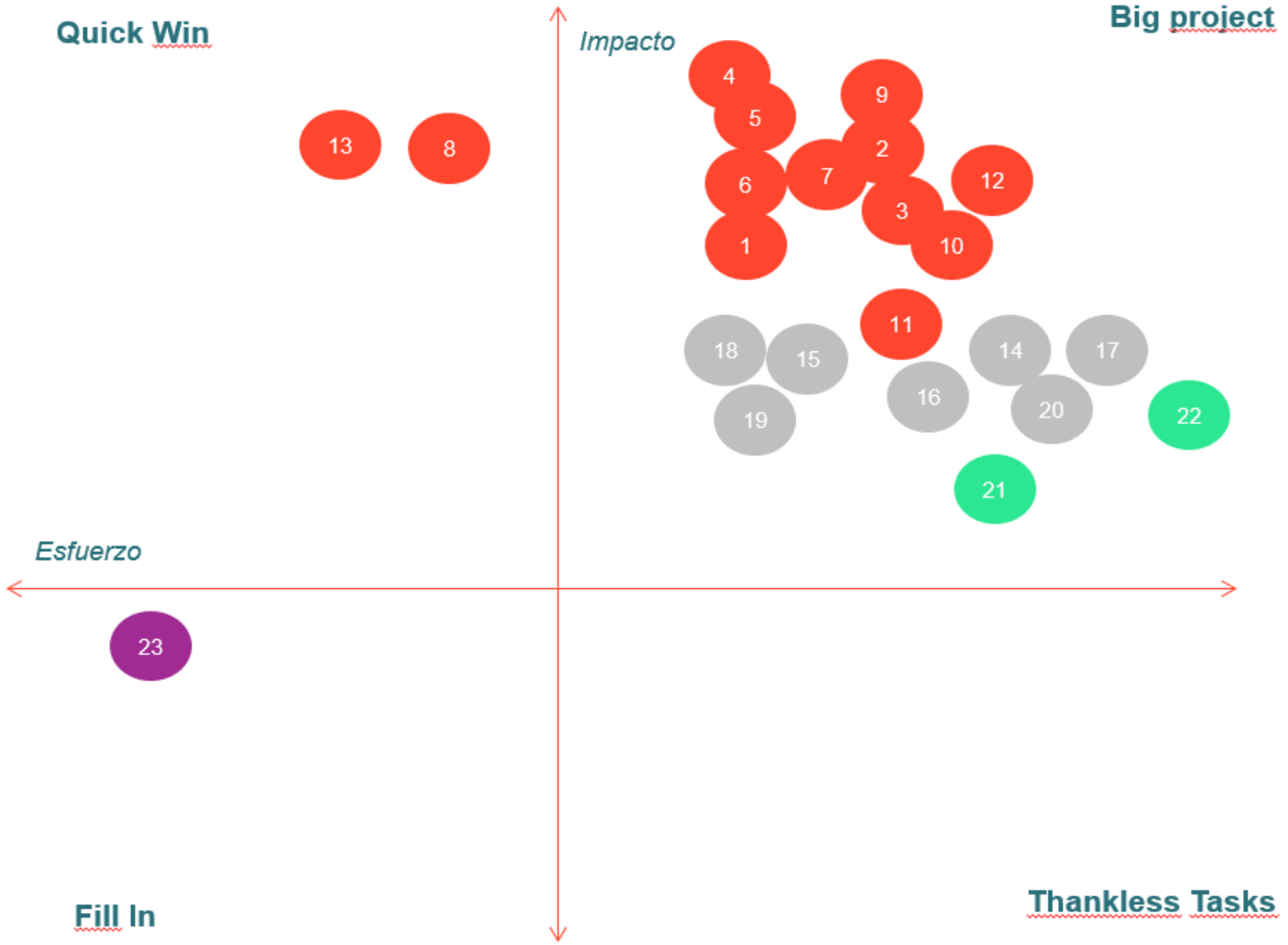
Priority: Medium Priority

Informe Ejecutivo – Priorización de Proyectos

1. Mapear y clasificar dispositivos
2. Definir políticas de seguridad
3. Gobernanza, Riesgo y Cumplimiento
4. Realizar evaluación de madurez
5. Uso obligatorio de MFA
6. Implementar el programa de gestión de parches
7. Implementación de Hardening
8. Gestión de vulnerabilidades
9. Detección y respuesta a amenazas
10. Plan de respuesta a incidentes
11. Realizar simulación de phishing
12. Análisis forense de incidentes
13. Pruebas de seguridad ofensivas

14. Educar a las usuarias con formación continua
15. Funciones segregadas basadas en RBAC
16. Control de acceso privilegiado con PAM
17. Monitoreo UEBA
18. Adopte el cifrado de datos
19. Proteger el sistema hypervisor
20. Ejercicios de Tabletop

21. Micro Segmentation
22. Seguro cibernético
23. Implementar el aislamiento del navegador



kyndryl

Thank You

Notices and disclaimers

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

kyndryl

Thank You