



Microsoft Security Portfolio

Get the best out of Microsoft Defender for Endpoint



Innovative technology consulting for business.

Agenda



1

Introduction

- Business → Trust → Security
- Devoteam Security Portfolio

2

IAM = Security Foundation

- IAM Fabric Definition
- Microsoft IAM = Azure AD

3

Microsoft Defender for endpoint

- Endpoint security Maturity Level
- The 6 domains of Endpoint security

4

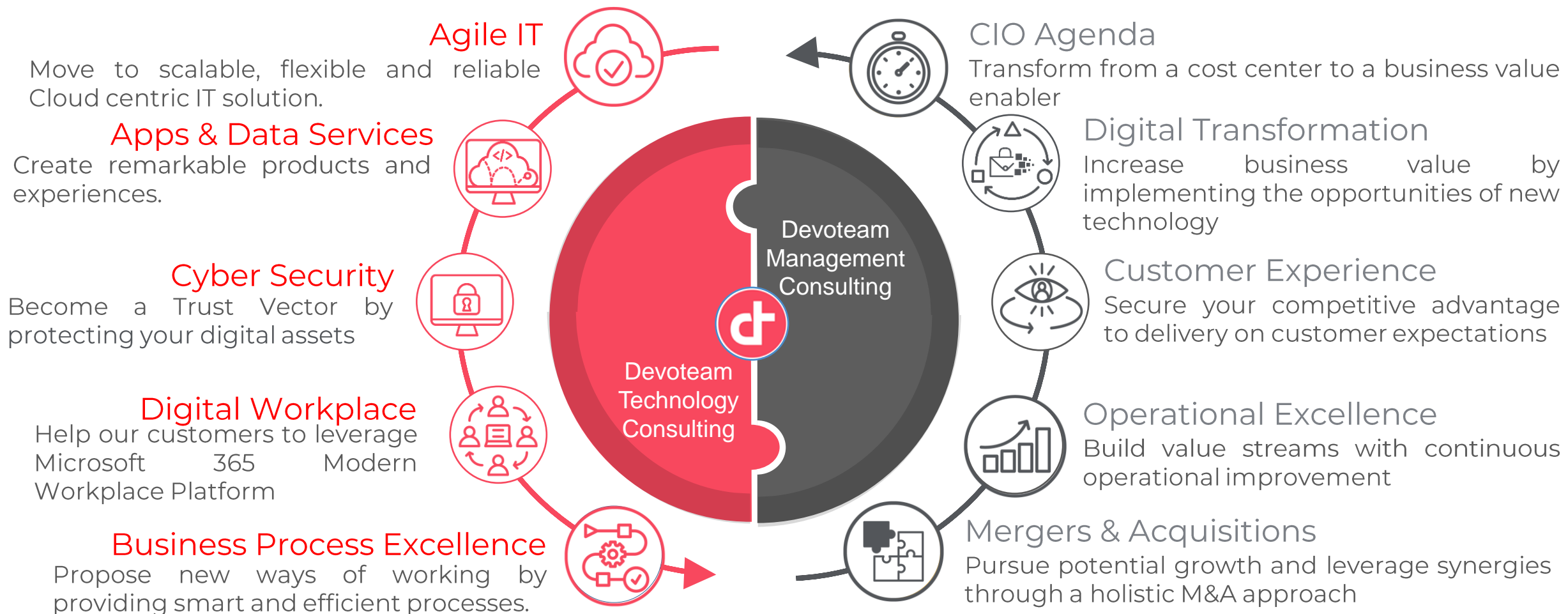
Security Posture Improvement

- Agile Methodology based on continuous improvement
- How to start the initiative?

5

Questions?

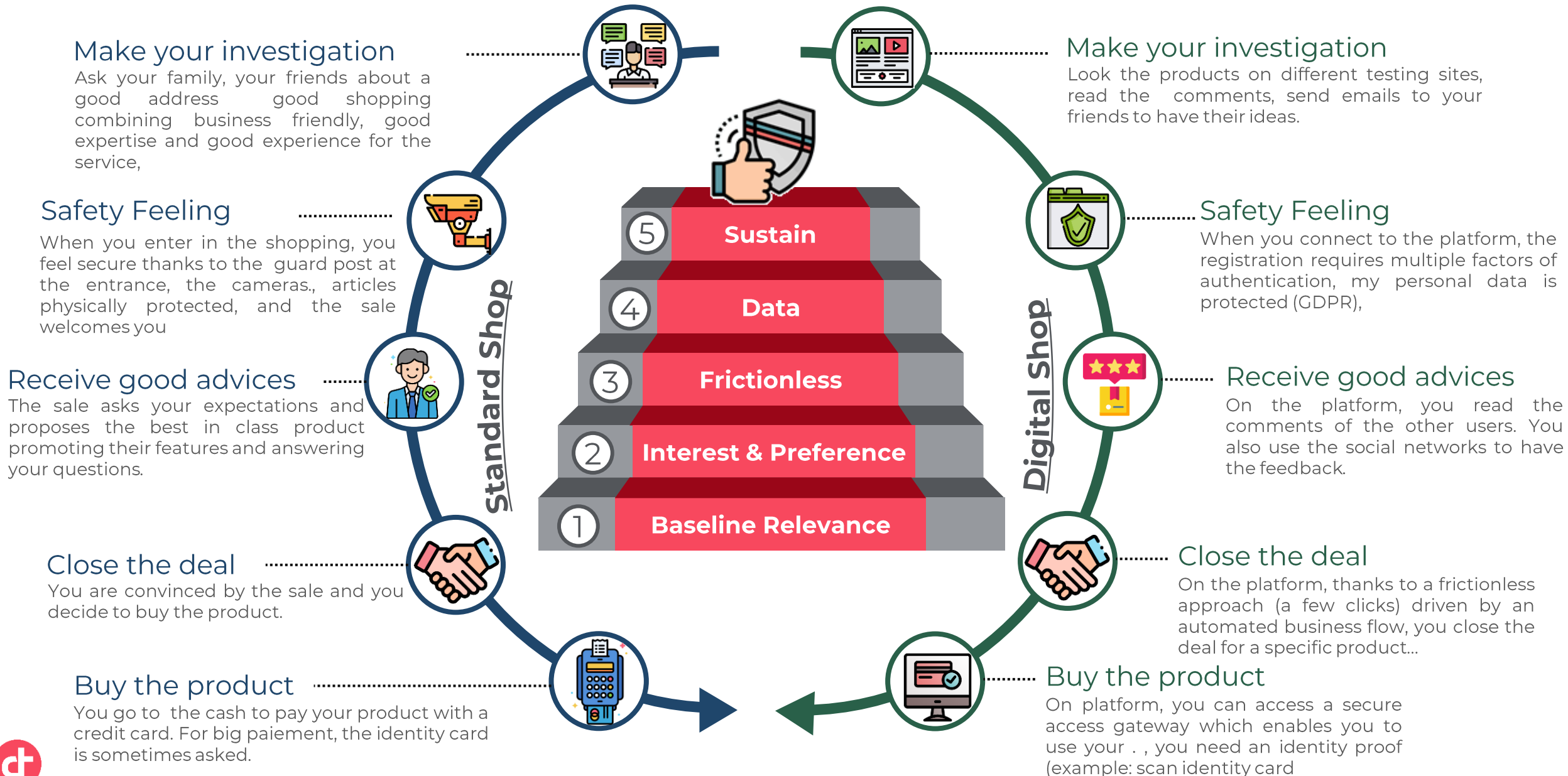
End-2-end Portfolio to shape your digital company...



“We magnify your value by boosting Business & IT collaboration”



Trust : The Business Catalyser



How to create the Trust ?

What are your 3 major expectations to create the Trust, Business Catalyser ?



Experience

Consumers, customers, business partners, and employees all expect great user experiences.

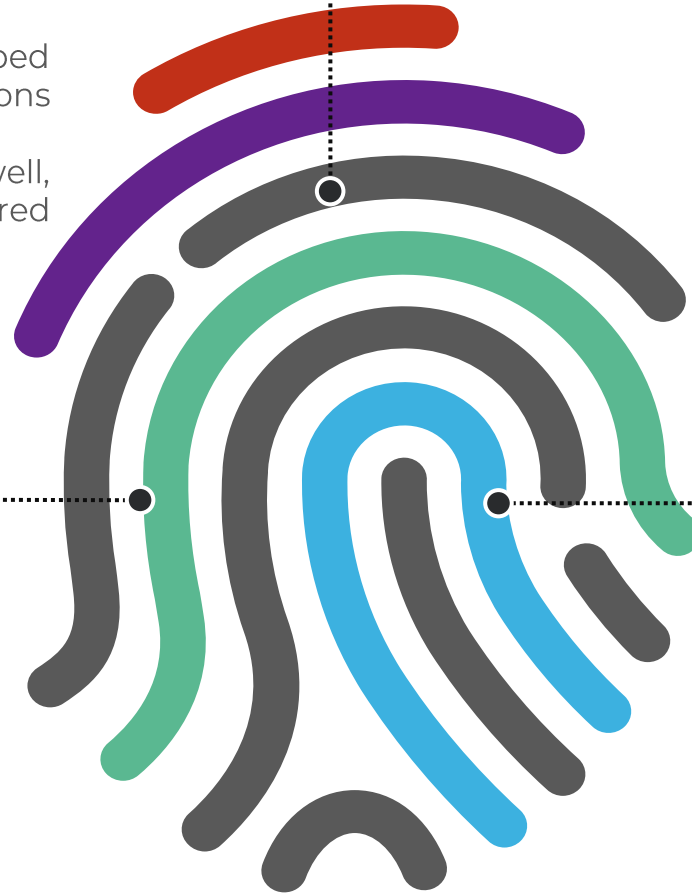
Their loyalty and commitment are shaped by friction less experience of interactions when using new digital services.

Failure to manage digital identities well, threatens the quality of the delivered services.



Consent

Consumers want that the sharing of their personal information is possible if and only if they give the consent. This consent can be easily given and removed thanks to a frictionless application. They also want a complete transparency and tracability about the consents they have.

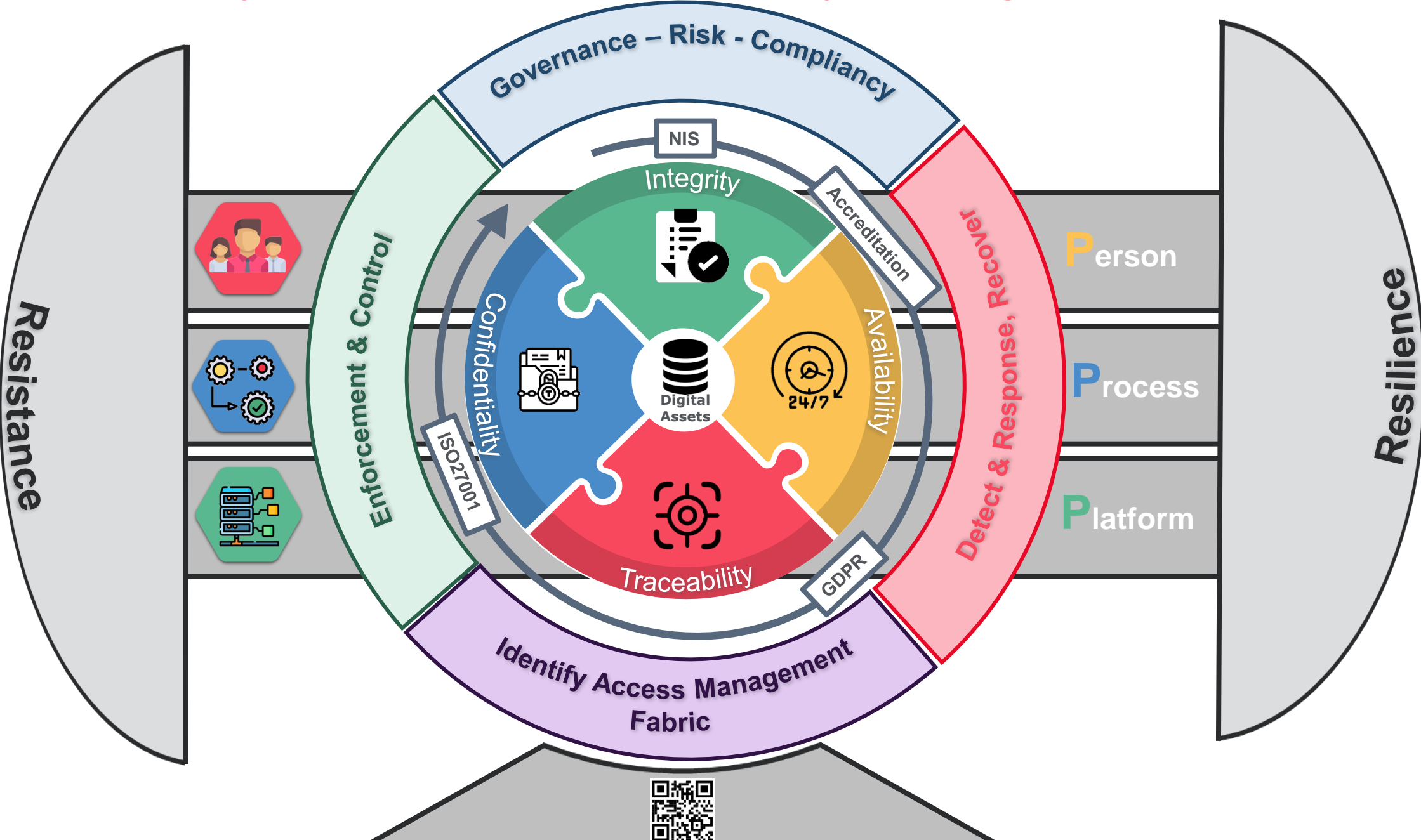


Accountability

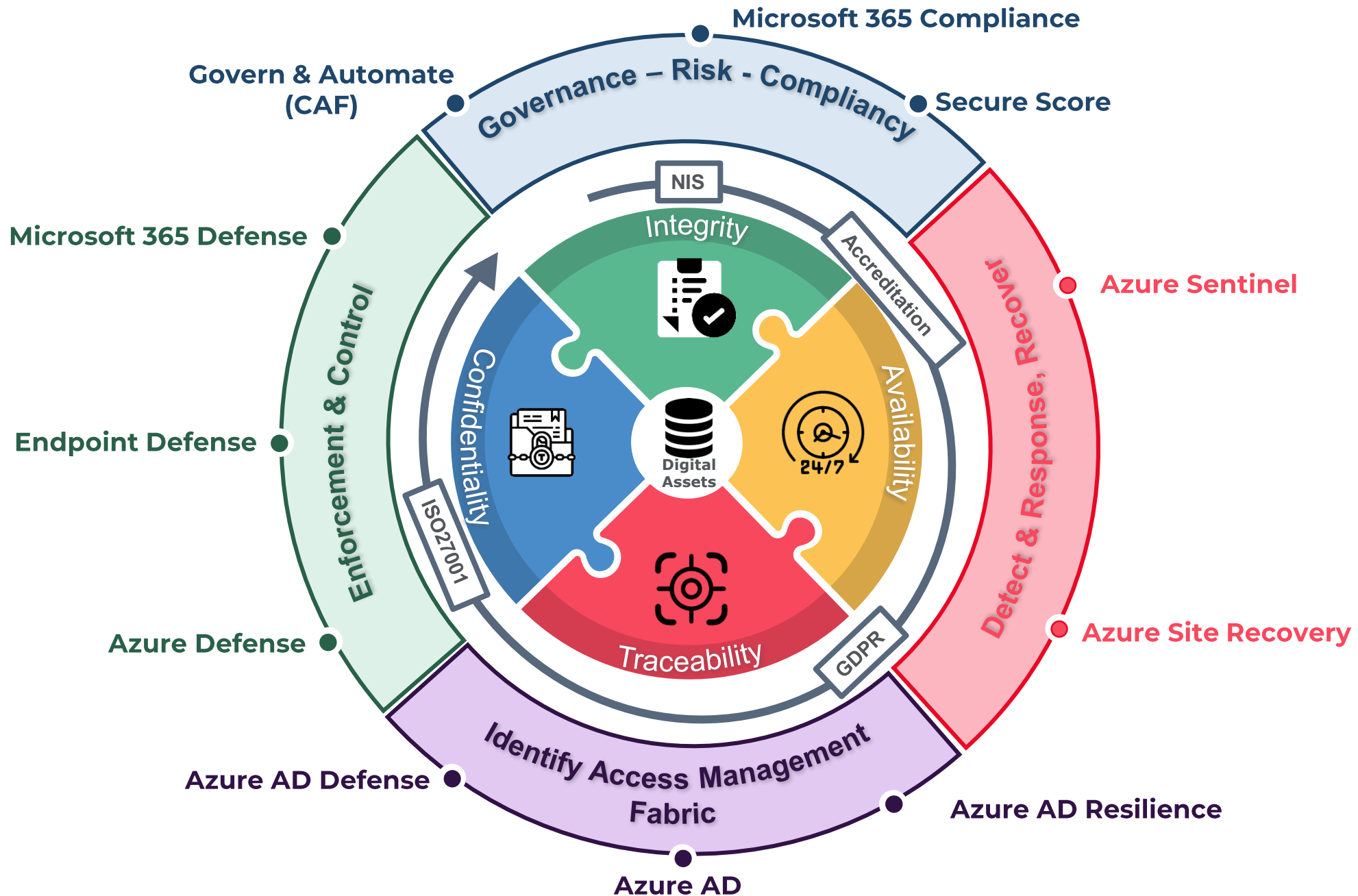


The majority of the consumers is not aware of the amount of information they shared about themselves online. Their knowledge of their rights regarding the use and the protection of their personal data is really limited

Cyber Security Portfolio calibrated for your Digital Transformation



The Microsoft Roadmap for a best-in-class security posture

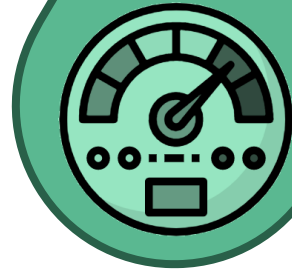


What's your Endpoint security maturity level ?

Two approaches

Endpoint Maturity Audit

Assessment providing an overview of the secure posture of the endpoints according to the 3P (**P**eople – **P**rocess – **P**latform)



Endpoint Secure Score

The endpoint secure score is a number that functions as an indicator for how aligned you are with Microsoft's best practice recommendations for security.

What's your endpoint level of maturity ?

Driven by an assessment covering six dimensions

Threat & Vulnerability Management

- Do you know which vulnerable softwares are running?
- Do you quickly understand the real risk associated with vulnerabilities?
- Do you take your unique business context to evaluate the risk?
- Do you remediate the vulnerabilities timely?
- Can you justify to internal audit why exceptions have been granted?

Protection

- Does your protection agent leverage machine learning?
- Can you quickly adapt to new indications of compromise?
- Do you protect credentials properly?
- Do you use the endpoint risk score to control access to assets?

Attack Surface Reduction

- Do you have control on malicious network destinations access?
- Do you block productivity applications from behaving out of the normal?
- Do you allow applications to run from removable storage?

Security Posture Management

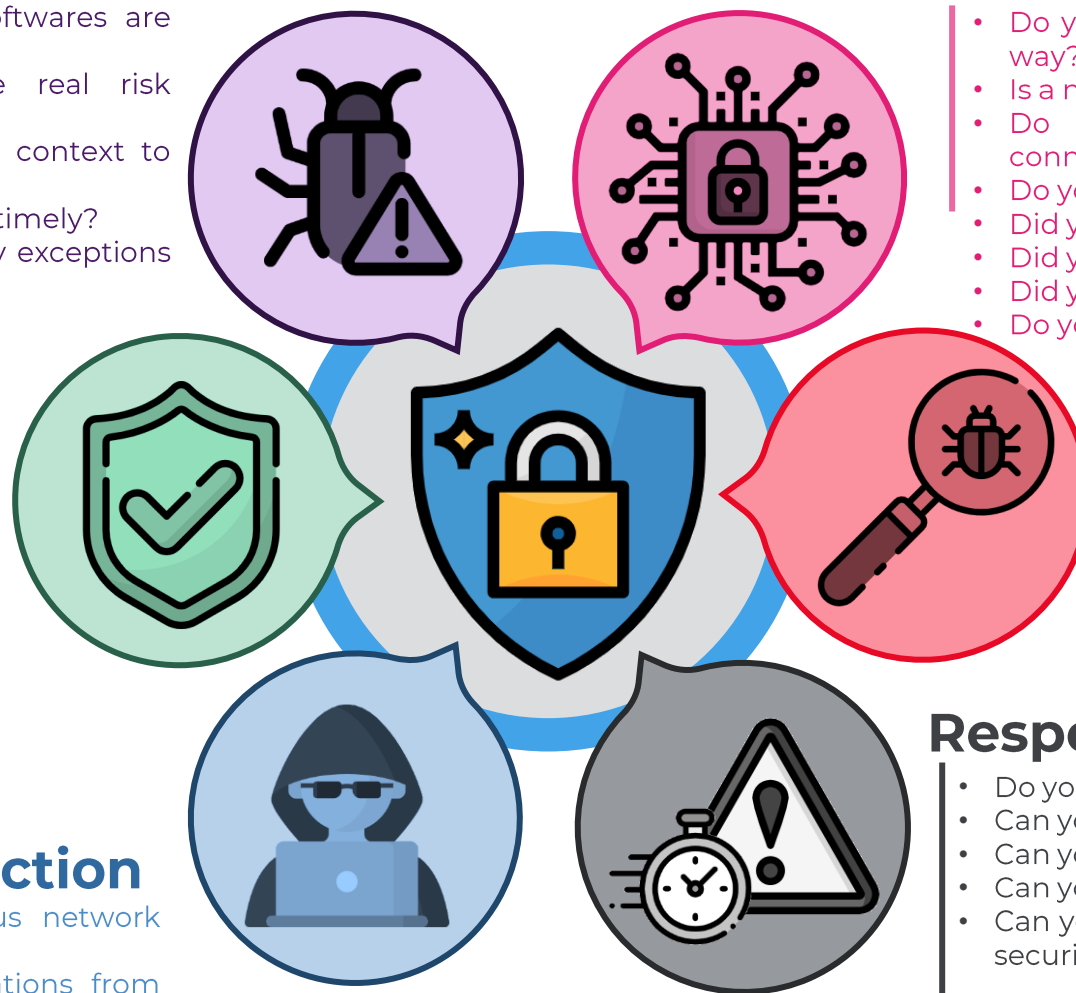
- Do you bootstrap your devices in a consistent way?
- Is a newly delivered device secure by default?
- Do you rely on enterprise network connectivity?
- Do you have a complete inventory available?
- Did you adopt modern management?
- Did you define acceptable use policies?
- Did you define device policies?
- Do you prevent secure configuration drift?

Detection

- Do you capture process execution trees?
- Do you capture command-line parameters?
- Do you capture changes to critical configuration items?
- Do you enrich the endpoint telemetry with other sources?

Response

- Do you auto-remediate with high confidence level?
- Can you connect to endpoints for deeper investigation?
- Can you quickly isolate a compromised endpoint?
- Can you find the initial vector of compromise?
- Can you make an accurate assessment on how critical a security incident is?



What's your endpoint level of maturity ?

Driven by an assessment covering six dimensions

Threat & Vulnerability Management



Protection



Surface Attack Reduction



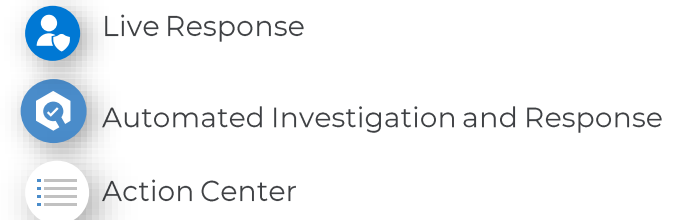
Security Posture Management



Detection

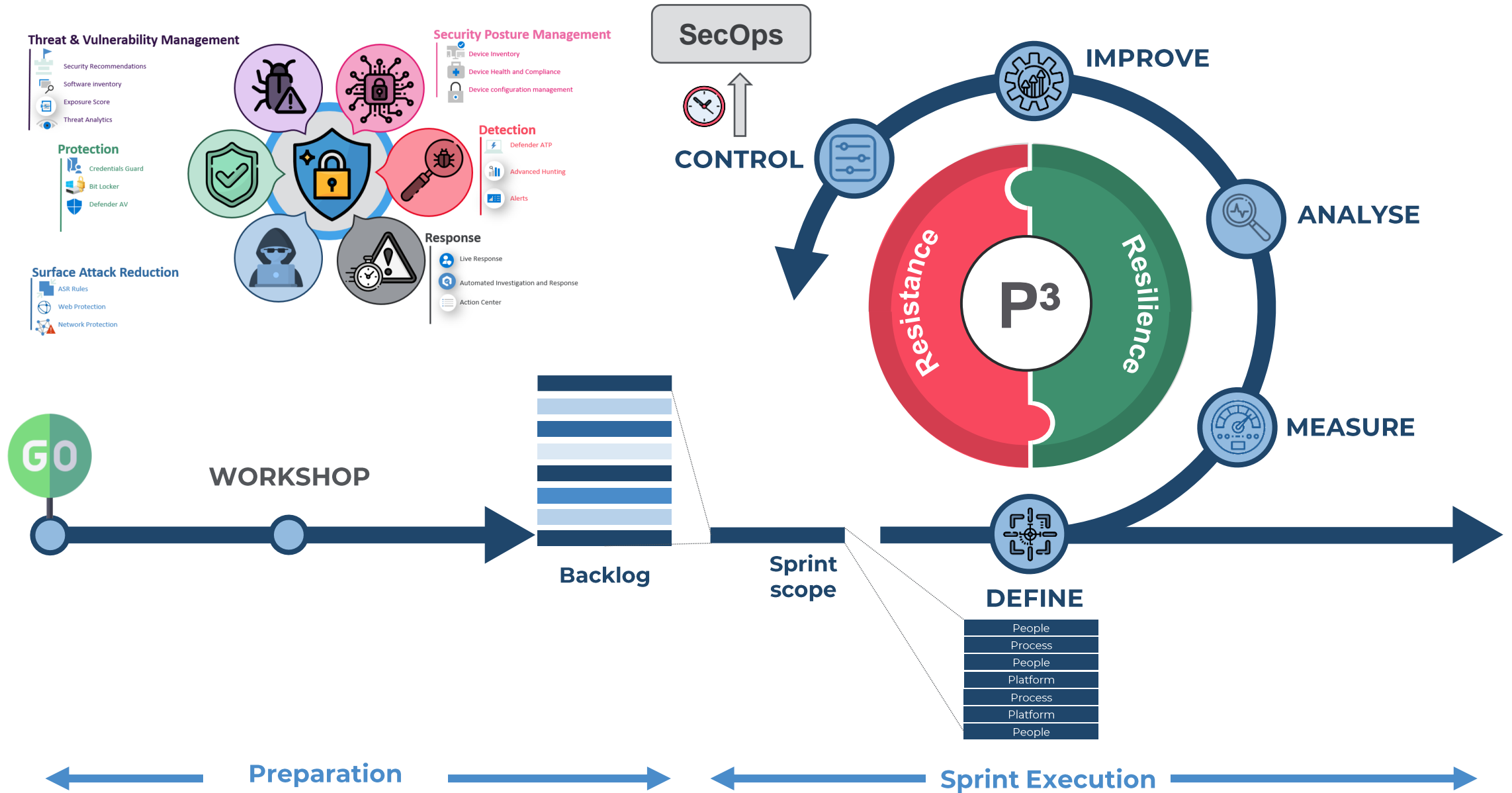


Response



How to improve your Security Posture ?

An Agile Methodology focused on Continuous Improvement



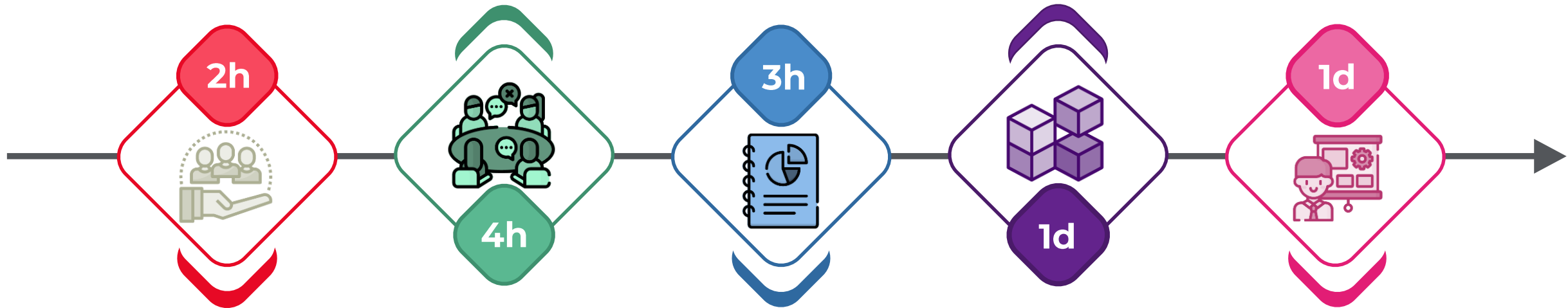
How to improve your Security Posture ?

The Workshop

Engagement Setup

- Kick-Off Meeting
- Secure Score Overview & Security Posture

Design & Planning



Pre-Engagement

- Pre-Engagement Call
- Endpoint Security Workshop Questionnaire

Reporting

- Application Discovery Reporting & Discussion

Workshop

- Customer Value Conversation
- Discovery Session
- Demos
- Key Results, recommendations & next steps

How to improve your Security Posture ?

Iteration loop for the Threat and Vulnerability management activity

