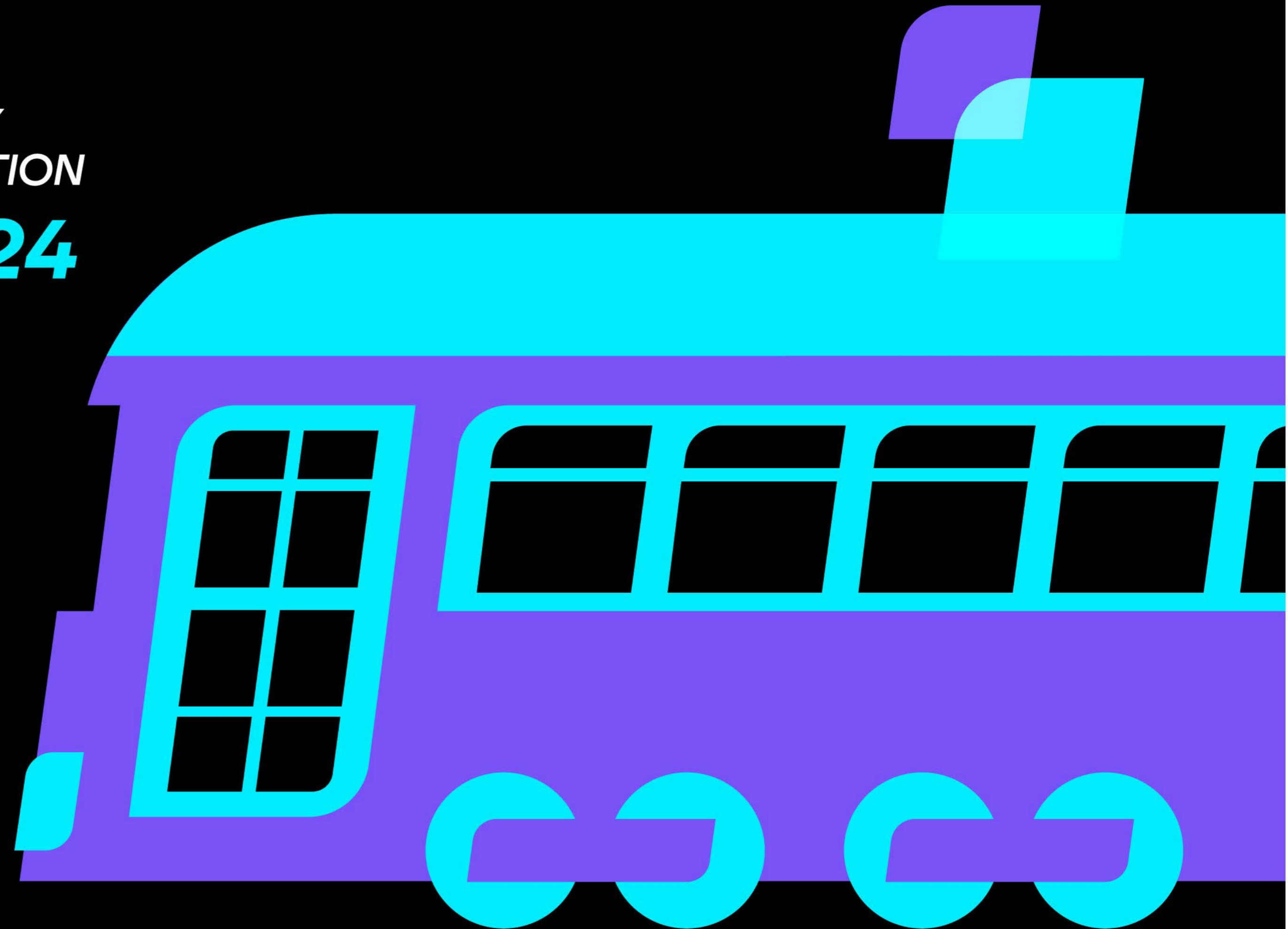


NEW ORLEANS

HYBRID
IDENTITY
PROTECTION
conf24





Benjamin Cauwel

Senior Manager, Accenture



- 2004-2006: Systems Engineer



- 2006-2008: Consultant



- 2008-2010: Senior Consultant



- 2010-2020: Consultant / Senior Consultant / Manager



- 2020-today: Manager / Senior Manager

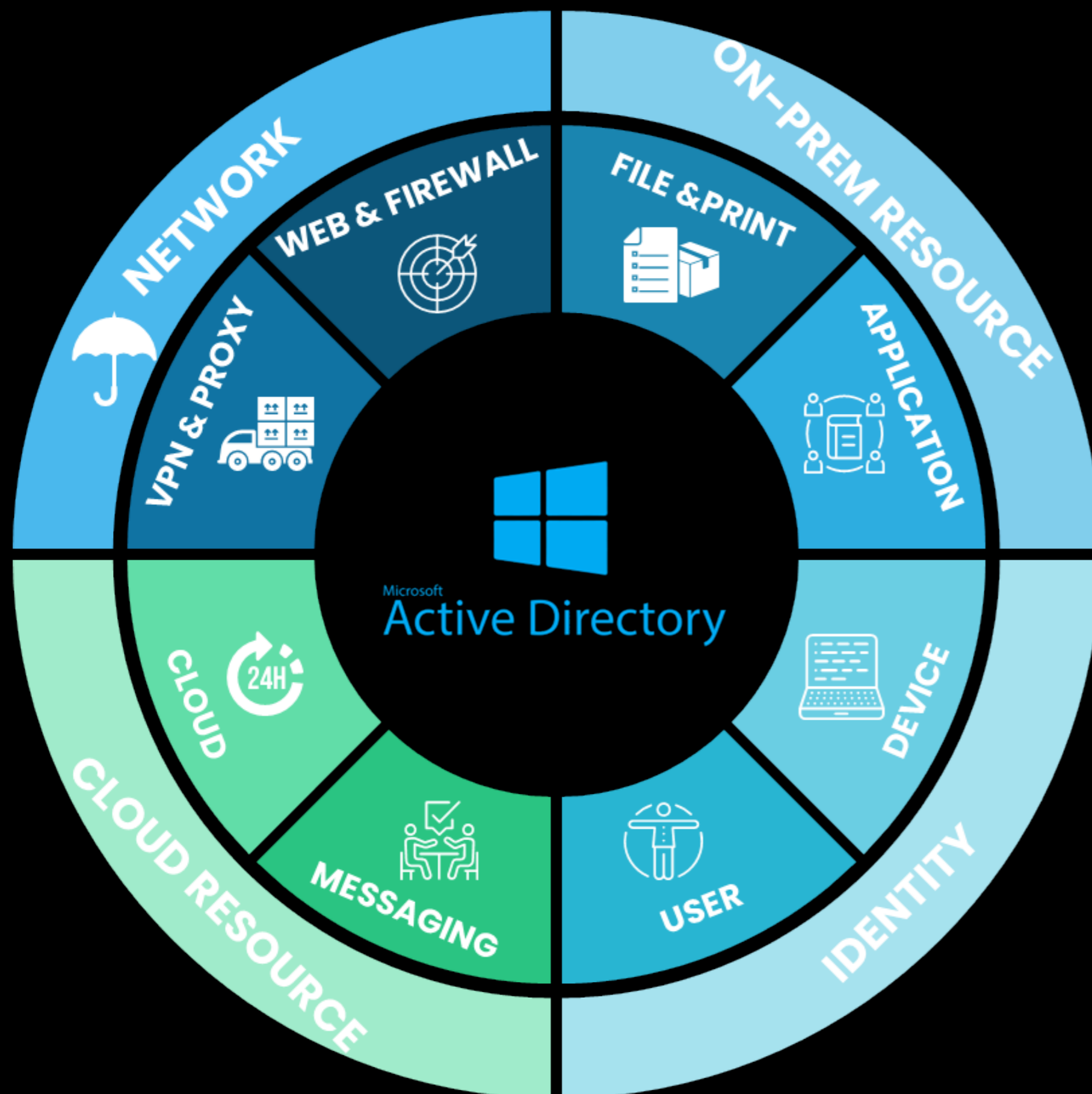
Practical approaches to improving your AD security posture

When did you last invest in improving your Active Directory (AD) and Tier 0 infrastructure?

How about evaluating the best changes to implement rather than the best solutions to purchase?

Reducing the attack surface of your identity system might be a better alternative to stacking on piles of new technology.

Why are we still talking about AD in 2025 ?



Why is everything linked to Active Directory in a company? What happens when...

- A user logs on to a device?
- An identity accesses an application?
- An identity prints or accesses a share?
- An identity wants to access the internet?
- An identity connects remotely to the information system?
- An identity accesses Cloud infrastructure?
- An identity connects to its messaging system?
- An identity accesses SaaS applications?

What would happen if Active Directory was unavailable (down or crypto-locked) ?

- Offices?
- Stores?
- Manufacturing?
- Distribution?

AD is the cornerstone of your security posture



“Everybody want a headline, I don't got nothin' to say
'Cept I'm comin' back with the freshness”

Mac Miller - Programs

How many cyberattacks per day?

- According to Security Magazine, there are over **2,200 attacks each day** which breaks down to nearly **1 cyberattack every 39 seconds** or **800,000 attacks each year**

How many times was AD leveraged?

- More than **90% of the time**

AD is the cornerstone of your security posture

- **Worldwide cybercrime costs are estimated to hit \$10.5 trillion annually by 2025**, emphasizing the need for enhanced cybersecurity measures (Cybersecurity Ventures).
- The **average cost of a ransomware attack was \$4.54M** (IBM).
- The **global average cost of a data breach in 2023 was \$4.45 million**, a 15% increase over three years, highlighting the growing financial burden on organizations (IBM).
- **Ransomware is identified as the number one concern of the C-suite** in 62% of surveyed organizations, up 44% from 2022 (CFO).
- **Nearly half (47%) of companies now have a policy to pay ransoms associated with cybersecurity threats**, a 13% increase from the previous year (CFO).
- **Only 8% of businesses that pay ransom to hackers receive all of their data in return** (Sophos).
- Globally, **72.7% of all organizations fell prey to a ransomware attack in 2023** (Statista).
- **Extortion was involved in 27% of attacks**, indicating a growing trend in ransomware tactics (IBM Security X-Force 2023).
- **Backdoors were deployed in 21% of all incidents remediated in 2022**, while ransomware constituted 17% of the incidents (IBM Security X-Force 2023).

Slapping solutions and features as if it were XMas

- Antivirus / antispam
- EDR
- XDR
- SIEM/SOAR
- SASE / Zero Trust
- PAM
- MFA / passwordless / Fido
- Vuln management / CTEM
- Patch management

- External facing applications



- Close to no governance

Time to take a new approach



AD is the core of your identity infrastructure. You cannot build a robust and resilient operational infrastructure on a faulty or neglected Tier0 ecosystem

After you analyze the AD attack surface and identify attack paths and indicators of exposure or compromise, what should your next steps be?



“Precision beats power and timing beats speed” – Conor McGregor

Case study

A company with 12,000 employees / 15,000 computers / 2,500 servers

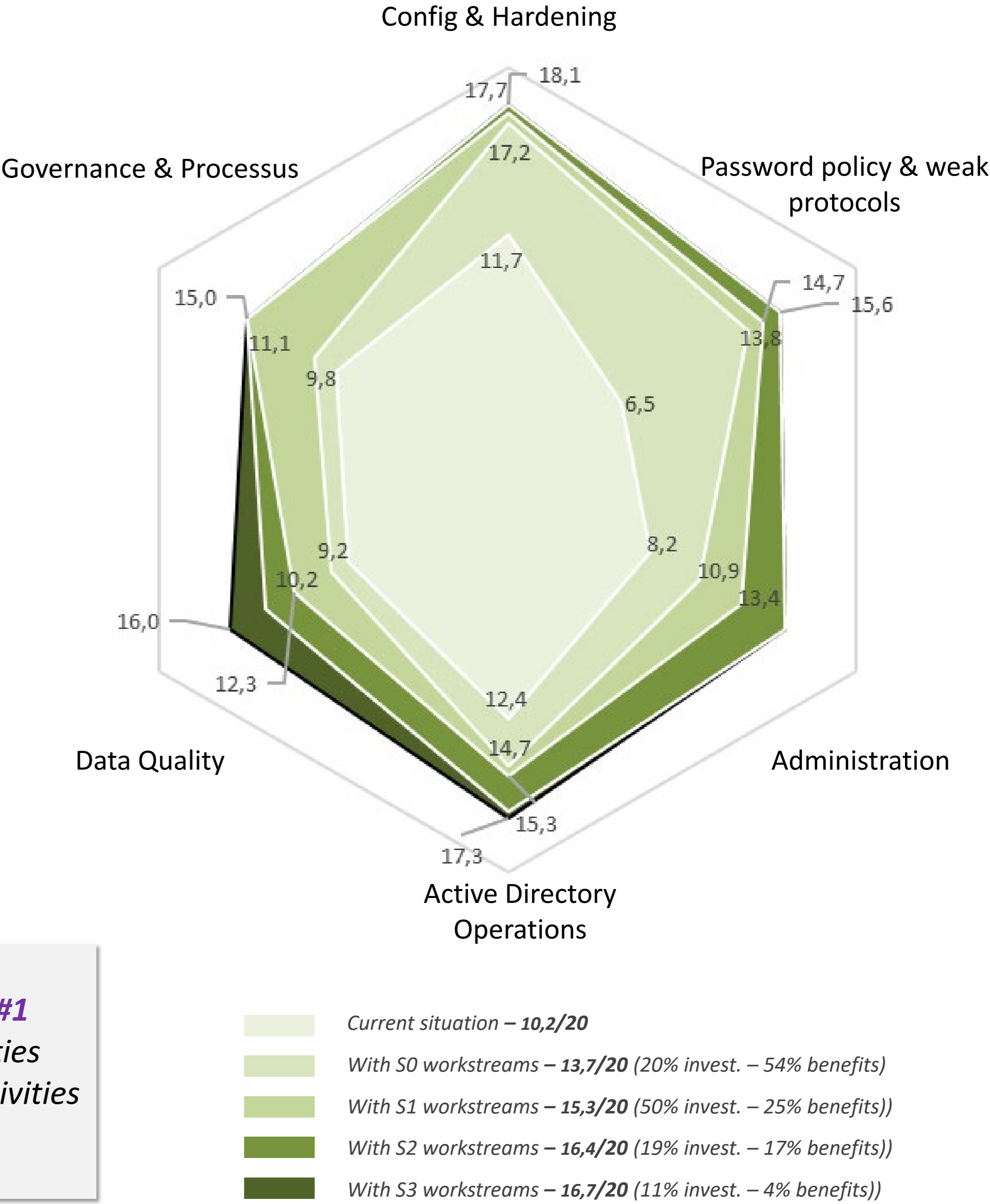
- Case 1 : Assessment + full IOE/IOC remediation + T0 hardening
- Case 2 : Moving to CTEM
- Case 3 : Greenfield

Case 1 : full remediation + evo

We have a total of 62 remediation activities gathered in 6 work packages. For each activity, we have considered 4 levels of stage:

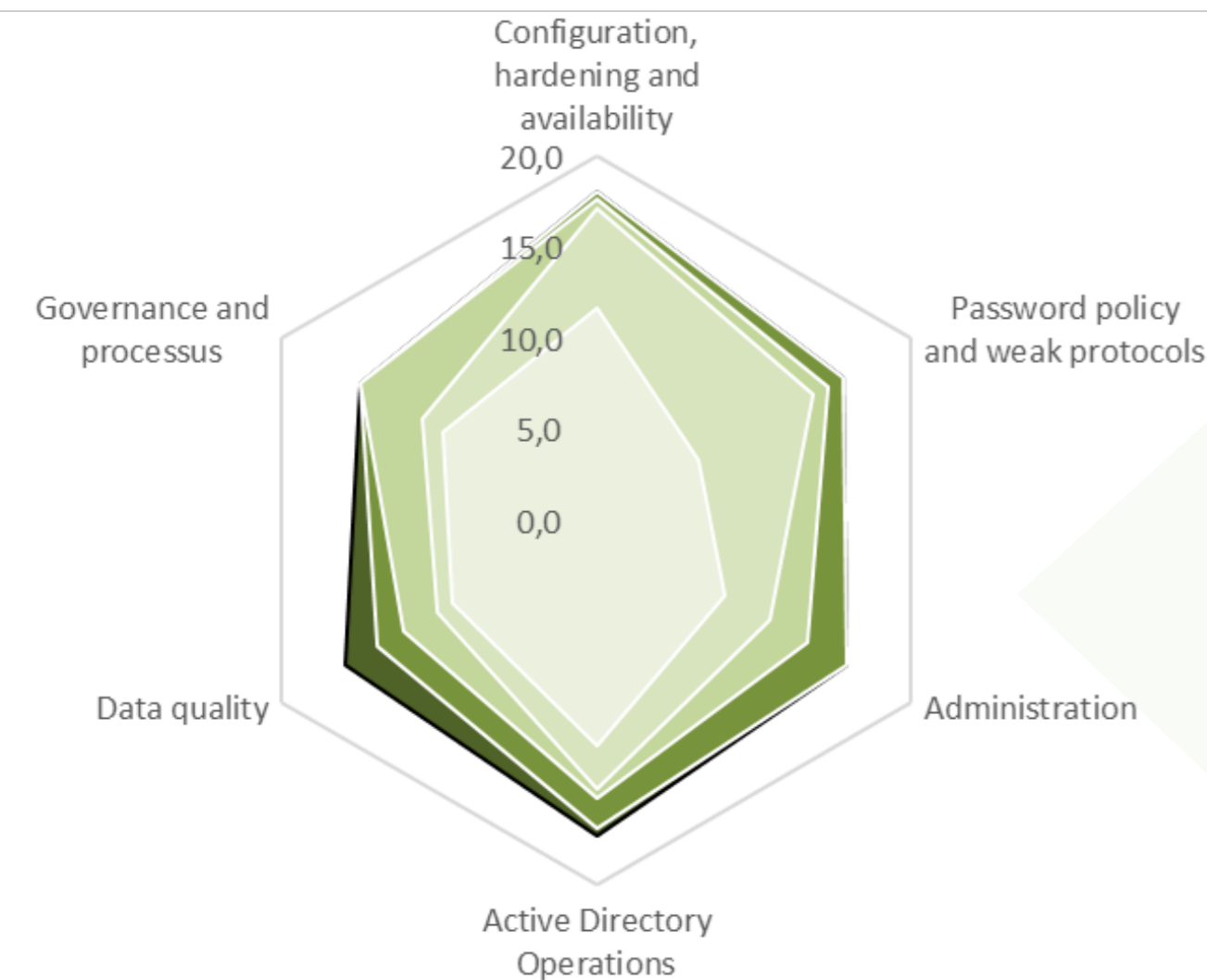
- **Stage 0 activities:** Most urgent remediation tasks that need to start quickly. Achieving them is a no brainer. Caution: not all tasks are quick wins, some of them needs to get started rapidly but will last more than 1 year.
- **Stage 1 activities:** Gather activities that should be started middle term and will bring lot of added value.
- **Stage 2 activities:** Gather the less urgent activities that will bring less benefits.
- **Stage 3 activities:** Gather activities that we do not recommend to run at all, because of huge investment needed and/or low benefits, and also due to the fact that Active Directory in not the future of IT.

Stage #0 Activities represent **20%** of investment and will bring **54%** of the benefits, **Stage #1** activities represent **50%** of investments and will bring **25%** of the benefits, **Stage #2** activities represent **19%** of the investments and will bring **17%** of the benefits whereas **Stage #3** activities would represent **11%** of investment for only **4%** of the benefits.



Case 1 : full remediation + evo

Average : **10,2** /20
Objective : **16**/20 mid term



Configuration, hardening

11,7 Obj. **18** /20

Stage 0 activities will bring a significant enhancements already, mainly due to DC hardening (new master) and Active Directory hardening activities – places in Stage 0

Password & protocols

6,5 Obj. **15** /20

Password enforcement and weak protocols removal are Stage 0 activities. Additional Stage 1 and Stage 2 workstreams will not bring significant improvement.

Administration

8,2 Obj. **16** /20

Administration will be enhanced progressively through the different workstreams, essentially due to Tiering and delegation model implementation in the beginning, then data clean-up, and lastly with dedicated administration improvement workstreams.

Operations

12,4 Obj. **17** /20

Stage 0 workstreams will permit to enhance this part of AD Security.

Data Quality

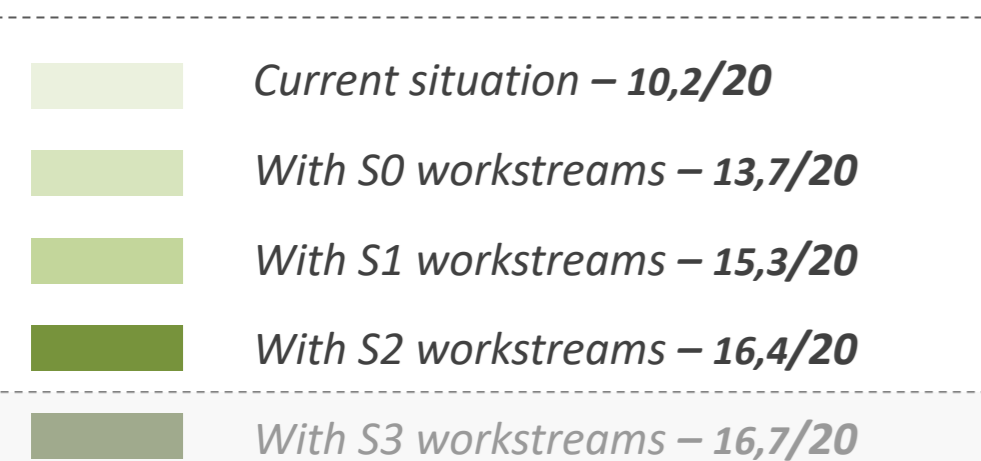
9,2 Obj. **14** /20

Data clean-up workstreams are those who will mainly bring improvement to this part of AD Security. They have been placed with Priority 1 degree

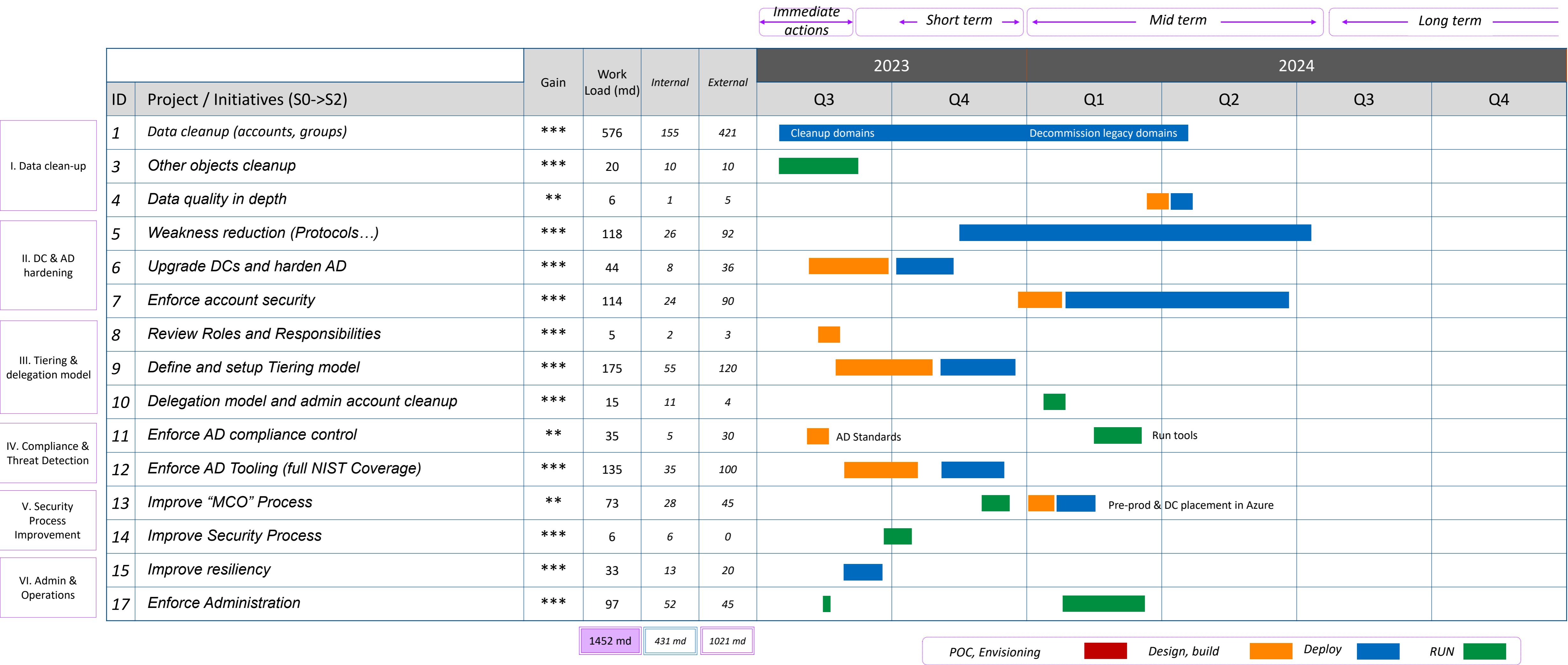
Governance, processus

9,8 Obj. **15** /20

Majority of process improvement workstreams have been placed with Stage 1 degree



Case 1 : full remediation + evo



Case 2 : Shift to CTEM

01

Think Exposures, Not CVEs

- Not all CVEs and misconfigurations result an exploitable exposure
- Identity and credential issues have far greater impact on exposure than CVEs
- **Attack Path Analysis** demonstrates true exposure potential
- Knowledge of adversary behaviours and (critical) business assets is key
- Exposure Management is not a one-off or periodic activity, rather a continuous cycle

02

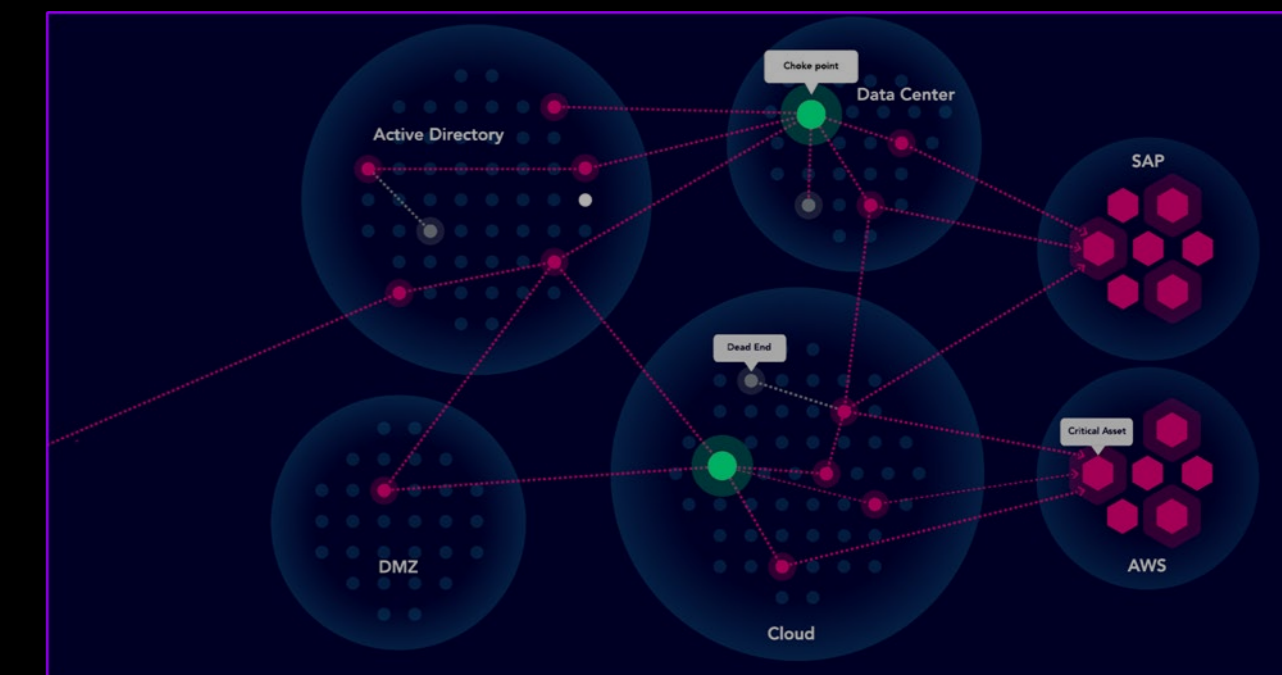
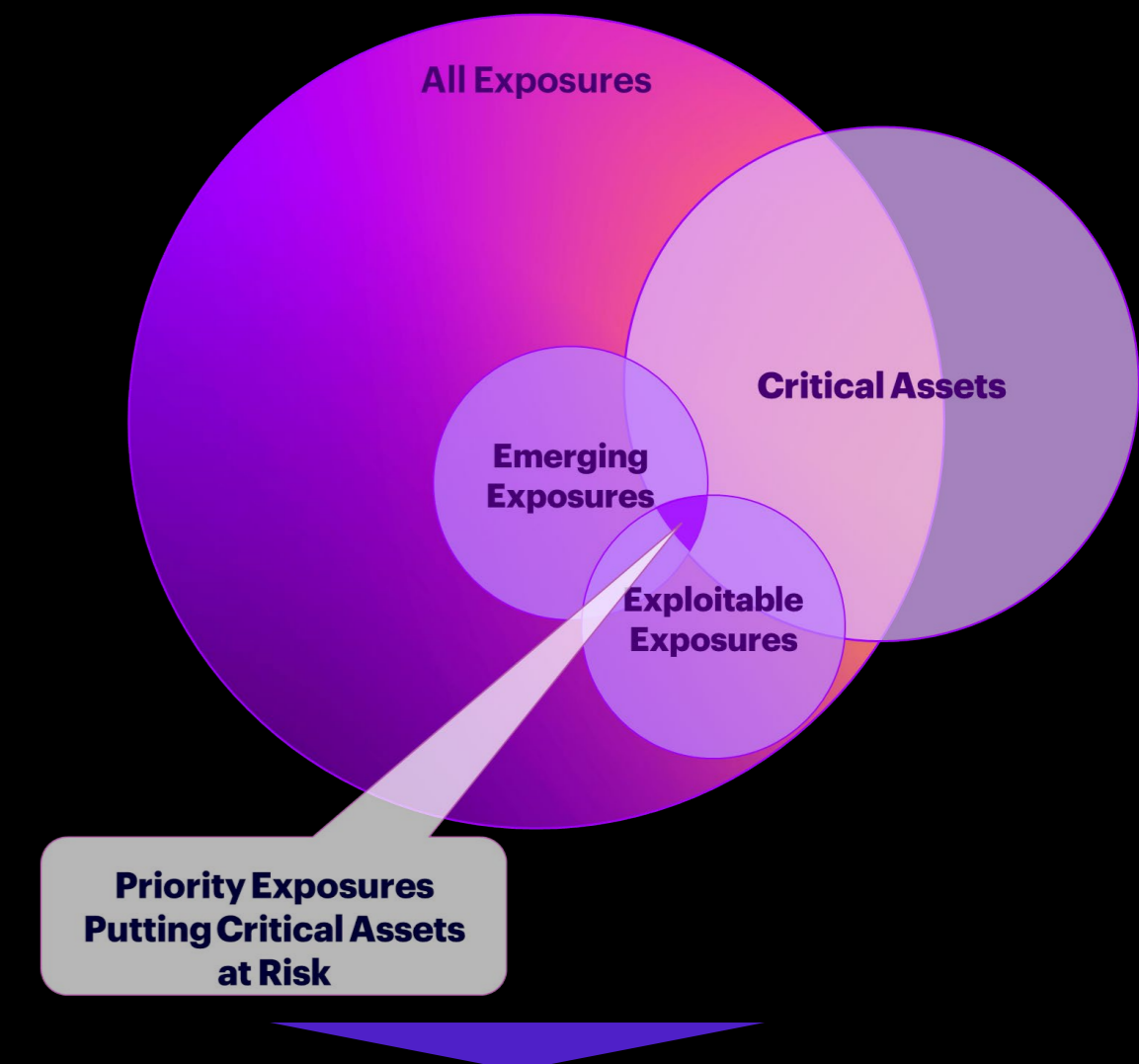
Drive Down Business Risk, Not Scan Results

- Not all exposures represent equal risk to the business
- Overlay individual attack paths to identify converge points
- **Prioritise Exposures** that affect critical assets and those where multiple attack paths converge
- Integrate with Enterprise and Security Risk Management practices
- Exposure Management must provide an anytime risk-based view on exposure posture

03

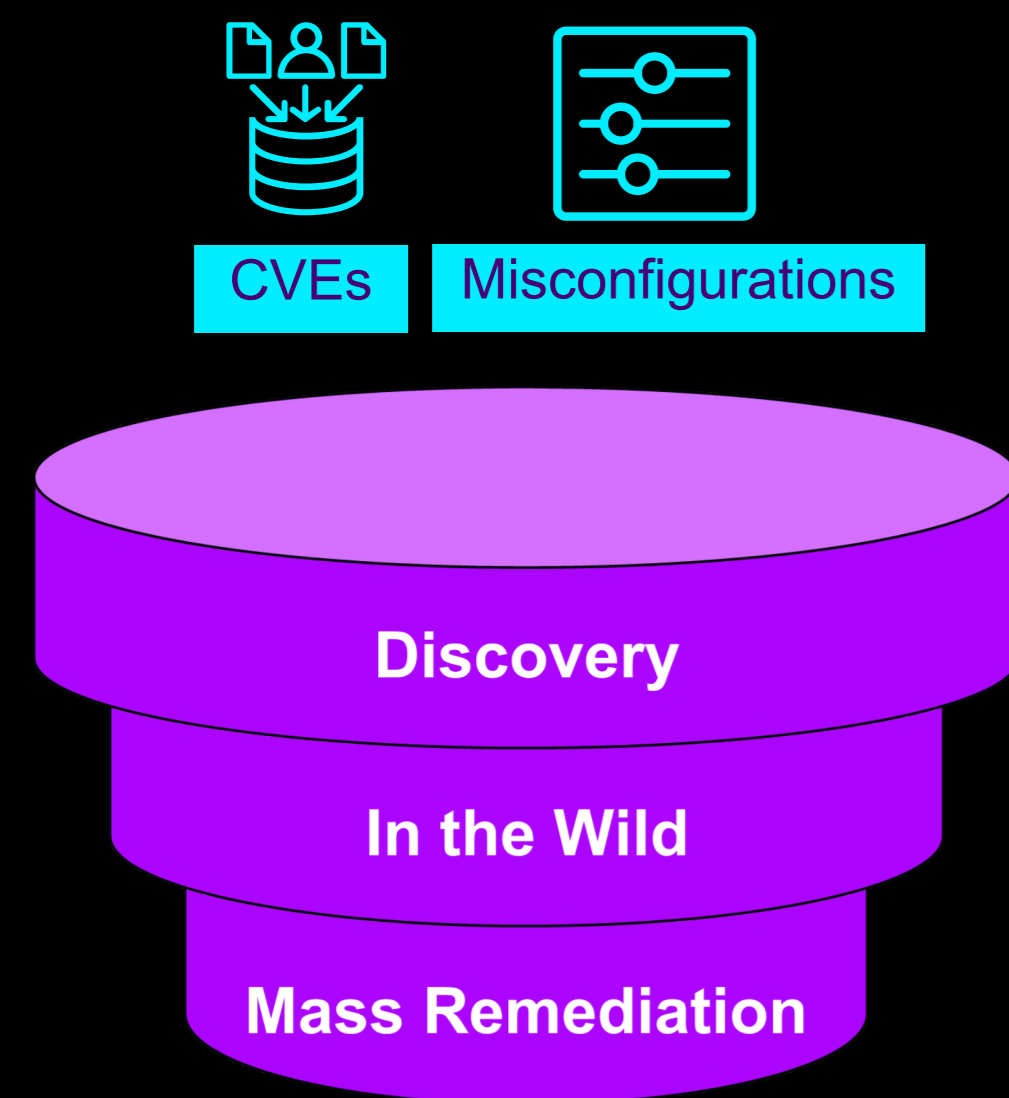
Focus on Collaboration, Not Dissemination

- Establish clear workflows for remediation mobilisation and closure
- Feed into existing IT and business workflows where possible
- **Align Metrics** for exposure remediation across teams
- Embed security into dev and ops practices across the organisation
- Exposure Management must offer guidance and (strategic) advisory to drive targeted remediation



To most efficiently mobilise vulnerability remediation, attack paths should be overlayed to identify “choke points” where multiple attack paths come together. Taking away just those vulnerabilities has the largest individual impact in terms of business risk reduction.

Case 2 : Shift to CTEM

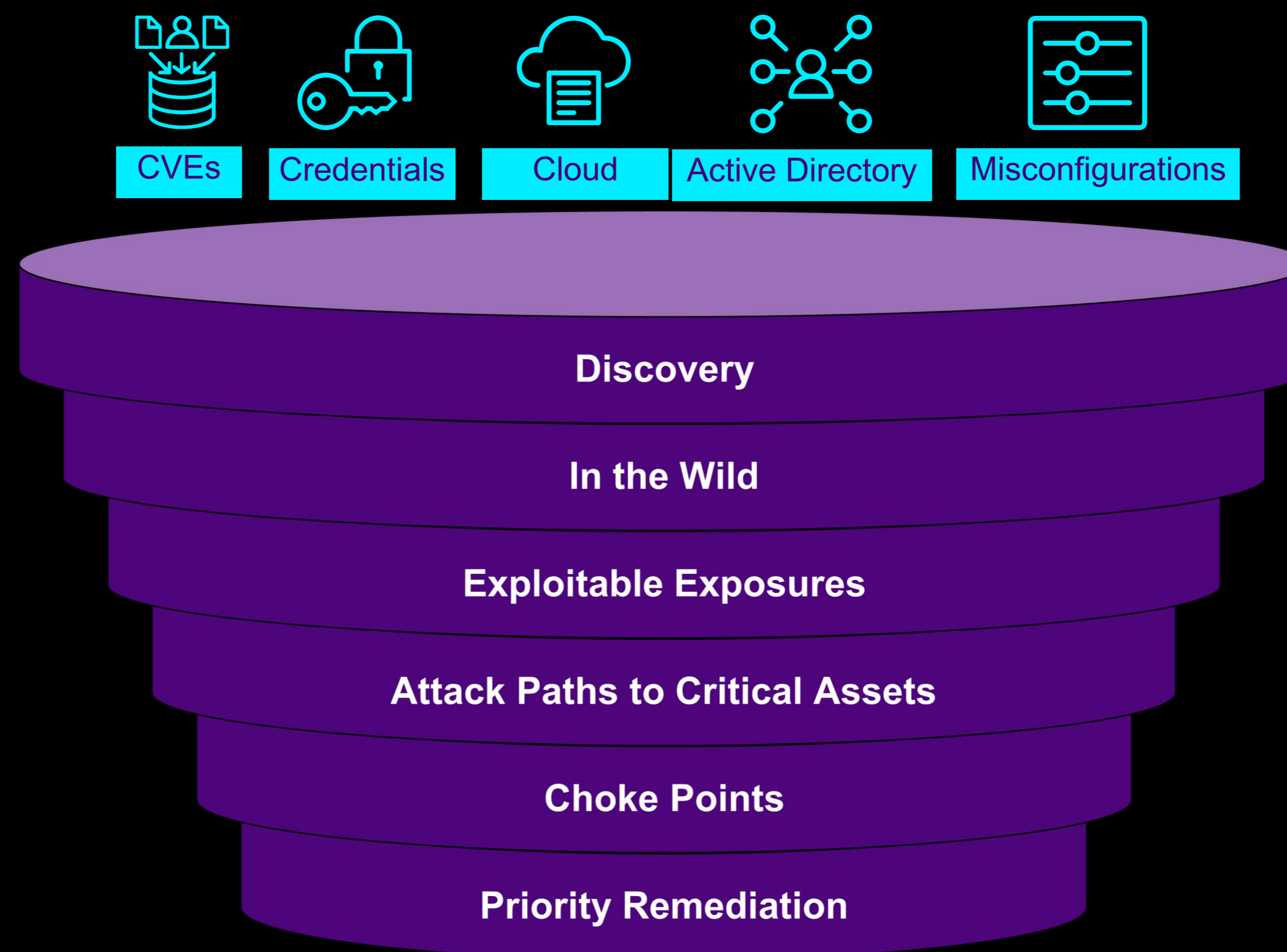


Traditional Vulnerability Scanner

No Business criticality context

Long lists of only CVEs

No attack path insight

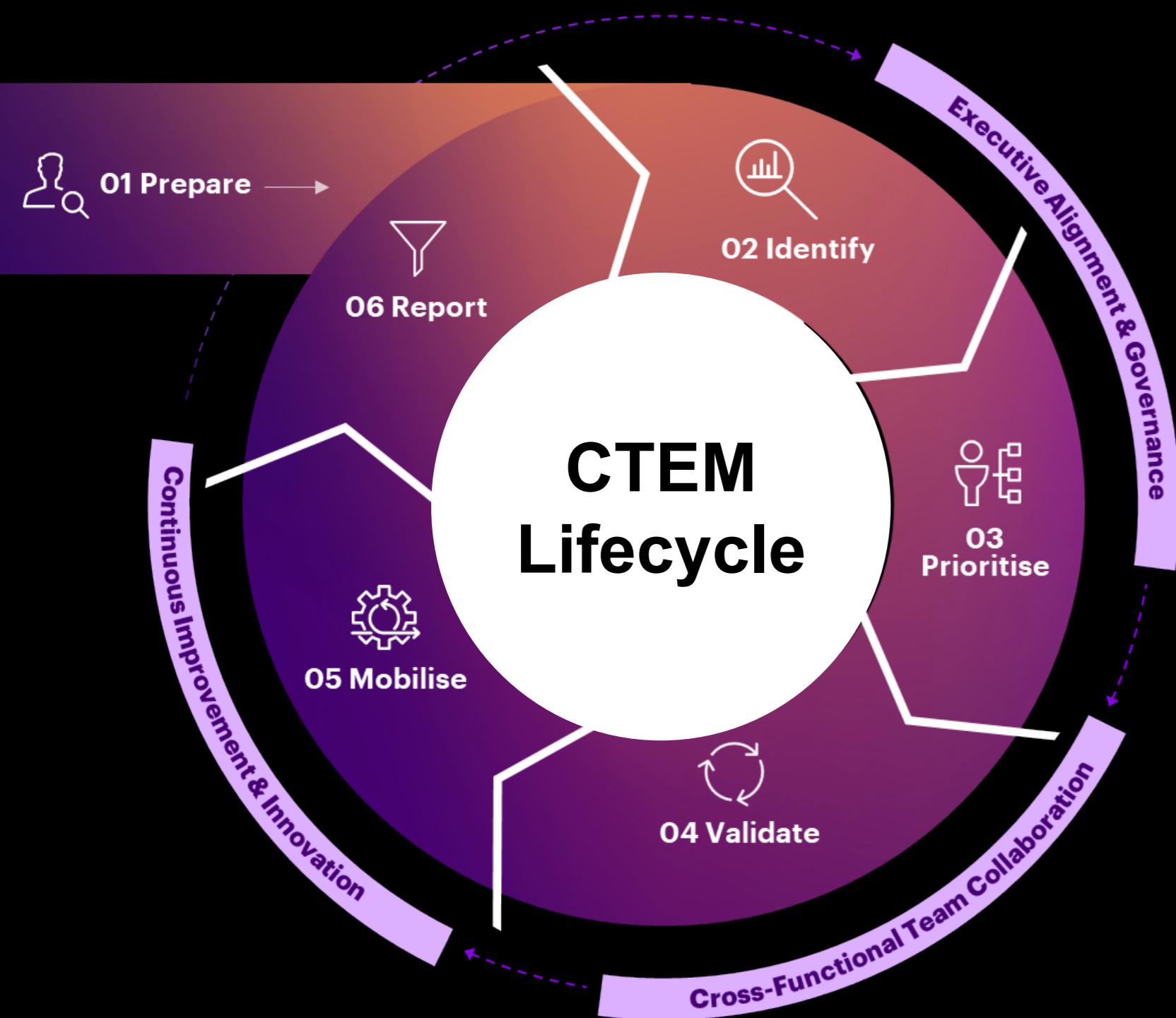


CTEM Platform

Use Cases


-  Vulnerability Prioritization
-  Ransomware Readiness
-  Zero-Day Vulnerabilities
-  OT Security
-  Digital Transformation & Cloud
-  Cyber Risk Reporting
-  Supply Chain & 3rd Party Risk
-  Mergers & Acquisitions

Case 2 : Shift to CTEM

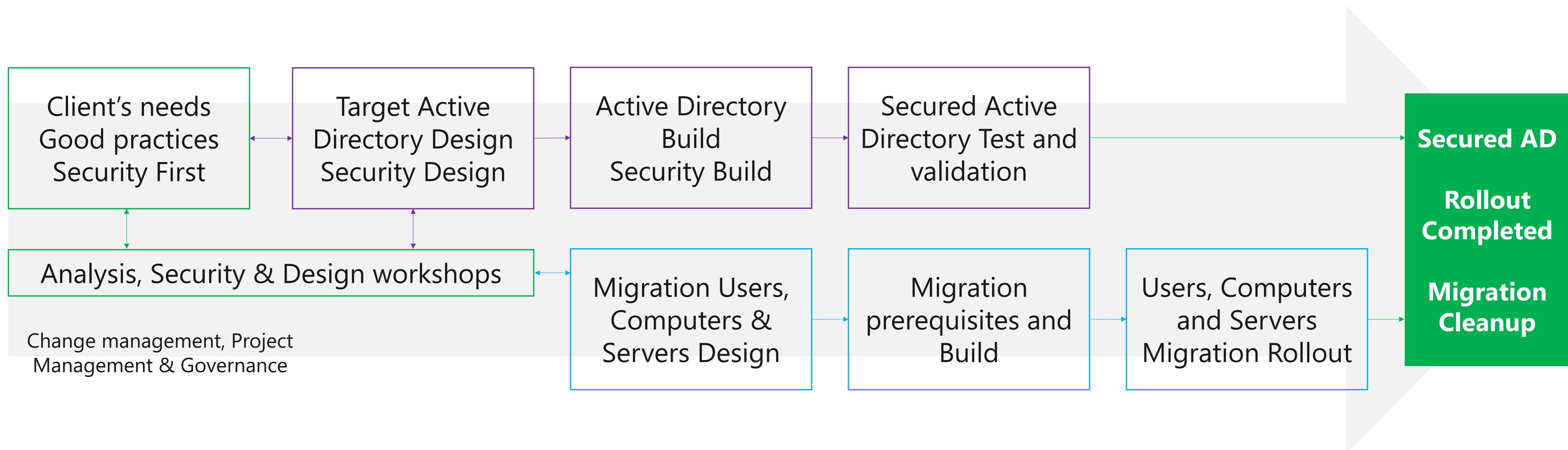


The **CTEM Lifecycle** and **CTEM Operating Model** define the fundamental capabilities derived from Gartner’s CTEM concept supplemented with a practical approach by Accenture.

Executive Alignment & Governance															
01 Prepare		02 Identify		03 Prioritise		04 Validate		05 Mobilise		06 Report					
Scoping		CVE-Vulnerabilities		Attack Path Analysis		Validation		Notification		Executive Reporting					
Governance		Misconfigurations		Correlation & Consolidation		Root Cause Analysis		Tracking & Follow-up		Operational Reporting					
Policy & Procedure		Identity Vulnerabilities		Asset Context		False Positive Handling		Verification		Service Performance Reporting					
Blueprint Definition		Application, API & Platform Vulnerabilities		Threat Context				Remediation Support		Strategic Advisory					
		Security Testing & Responsible Disclosure						Risk Acceptance Handling							
		Dark Web Exposure & External Reputation						Escalation Handling							
Continuous Improvement & Innovation															
Cross Functional Team Collaboration															
Asset & Configuration Management		Patch Management		Release Management		Change Management		Problem Management		Identity & Access Management		Threat Detection & Response		Risk & Compliance	

 capability is key in transformation from VM to CTEM

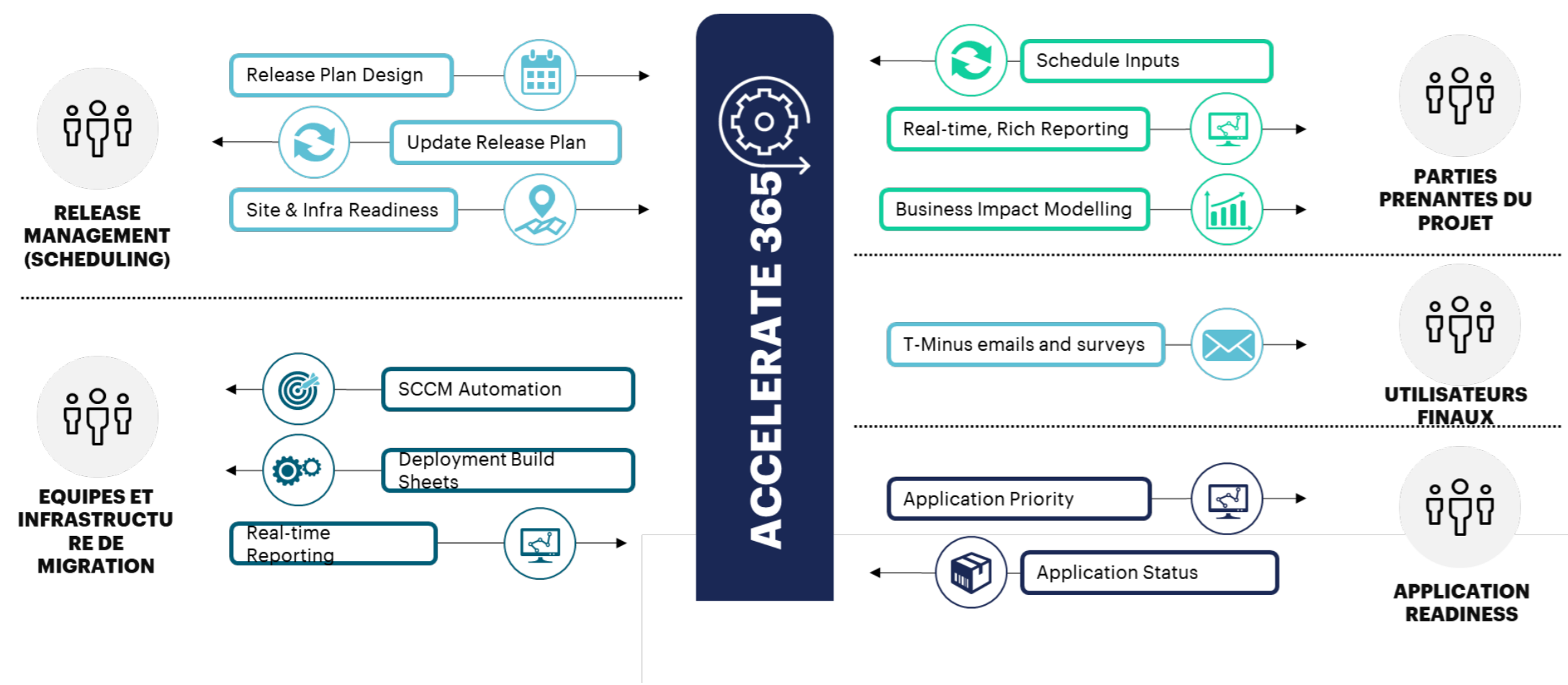
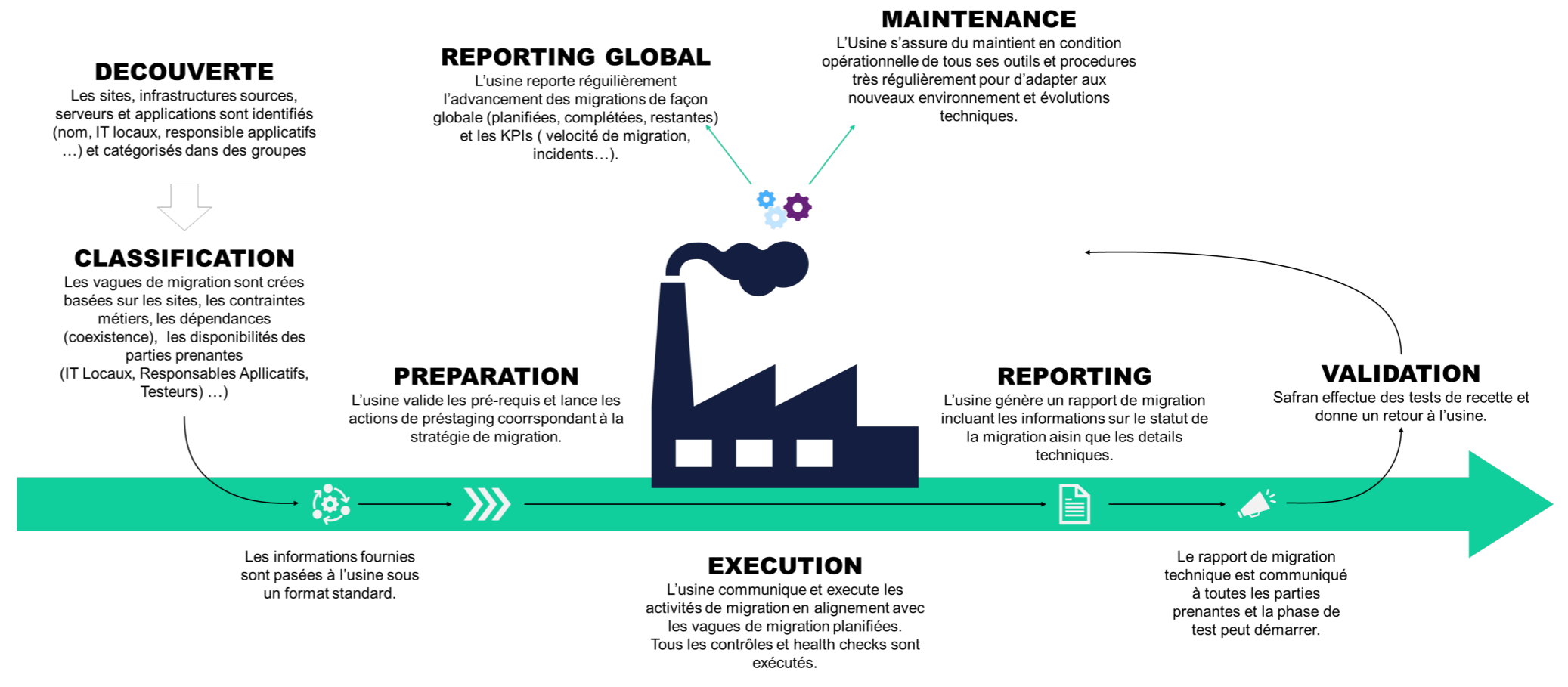
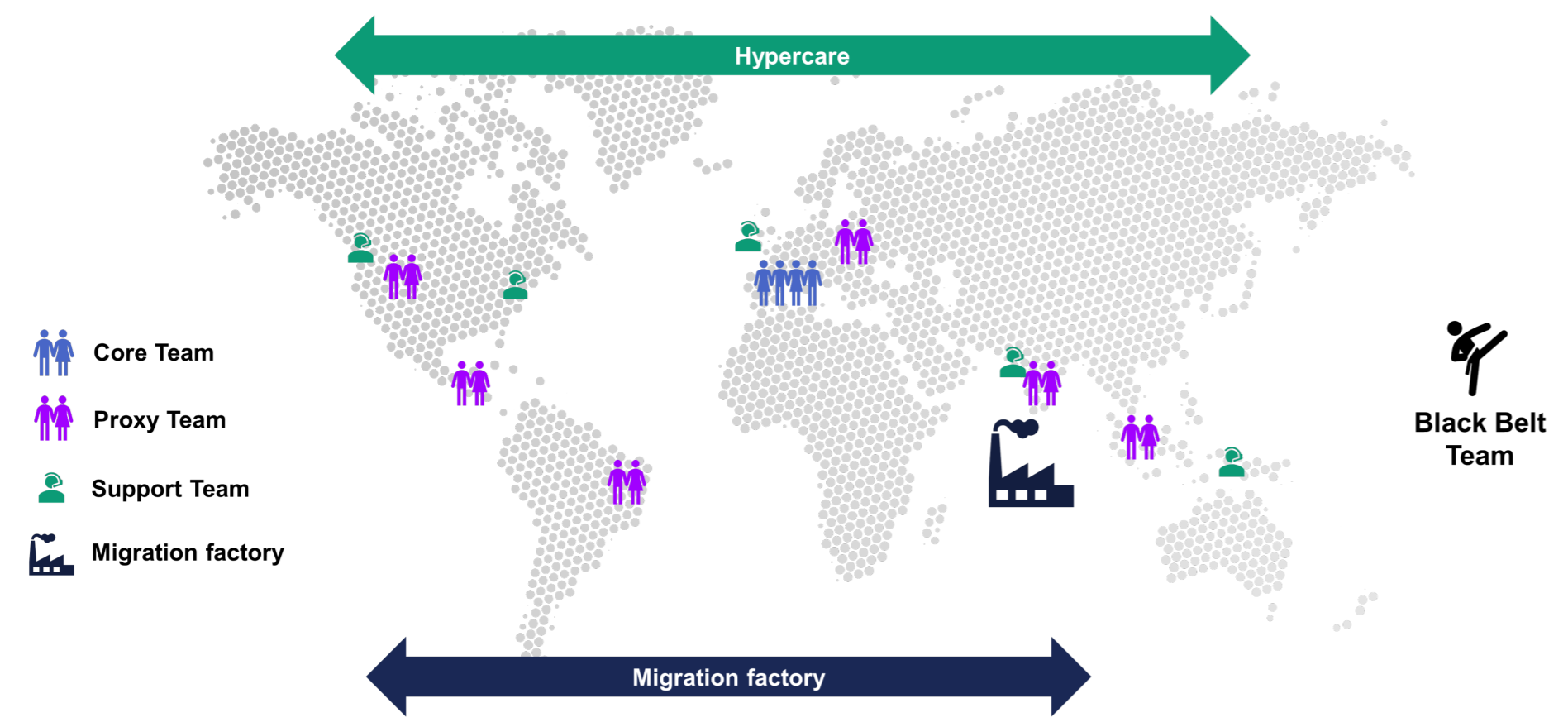
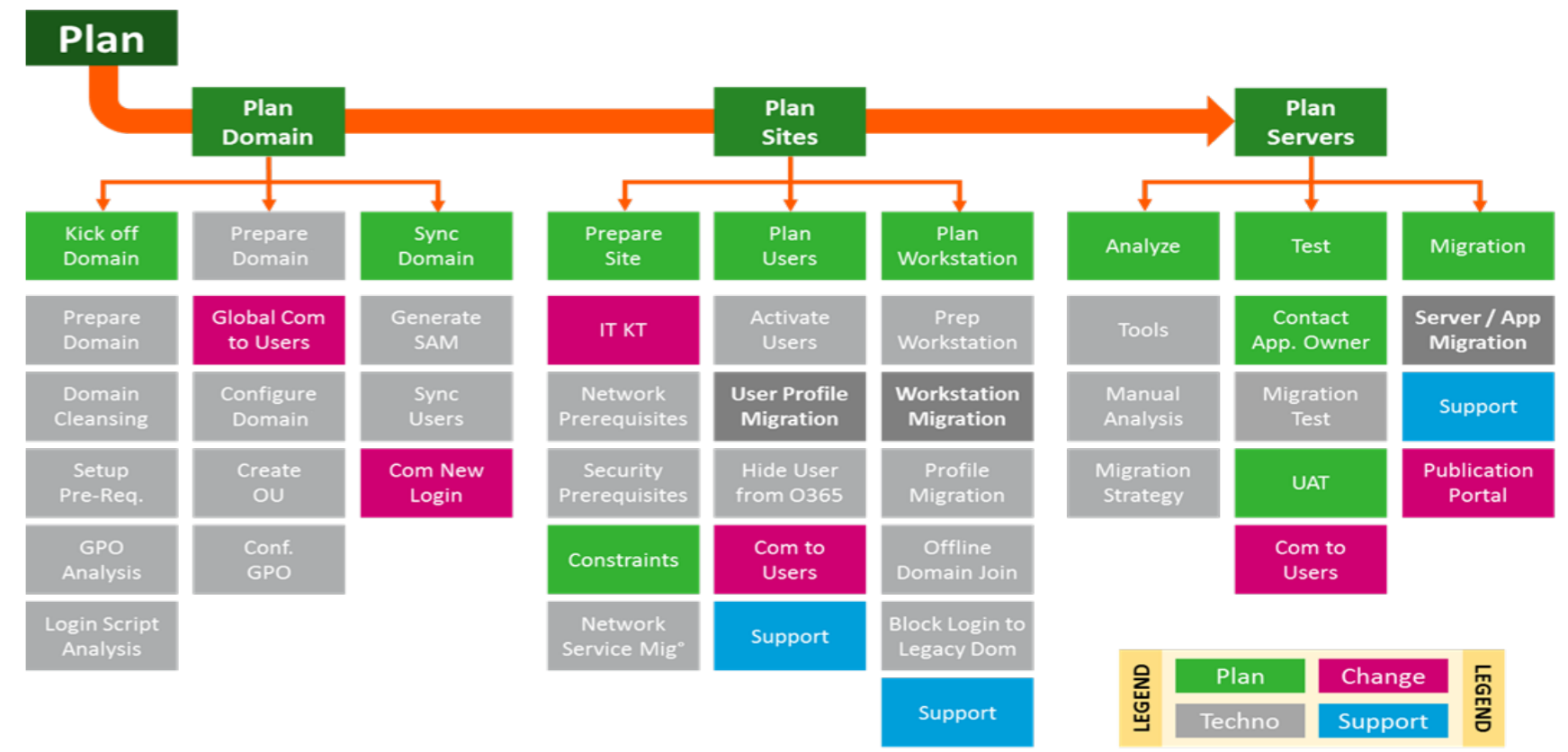
Case 3 : Greenfield



Case 3 : Greenfield

WORKSTREAMS	Plan	Analyze	Design	Build	Test	Deploy	Run
RELEASE PLANNING		Identify Dependencies and Constraints		Construct/Manage Release Sets			
	Workplace Discovery		User/Department Profiling		User Scheduling/Countdowns		
MIGRATION PLANNING	Develop Migration Approach		Detailed Migration Design	Build Migration Plan/Runbooks		Migration Support	
	Develop Toolset Approach			Build/Test Migration			
APPLICATIONS	Identify Apps	App Dependencies	Develop Approach (Kerberos, WIA, NTLM, etc.)			Application Support	
	App Roadmap			App/Server Coexistence & Migration		Transition to BAU	
IDENTITY MANAGEMENT	Provisioning Requirements		IdM Design			IdM Support	
	Develop Policies & Procedures			Build/Config/Test IdM		Transition to BAU	
INFRASTRUCTURE	Network Assessments	Logical Infrastructure		Build/Config/Test Servers, Storage, Directory Svcs, Networks		Deployment Support	
	Conceptual Infrastructure		Detailed Design			Transition to BAU	
MIGRATION EXECUTION				Pilot Migrations	Mass Migrations		
				Pilot Feedback	Transition to BAU		
ORGANIZATION CHANGE MANAGEMENT	Develop Comm Plan	Develop Support Plan	Design Adoption, Comms., and Training Materials	Develop/Test IT/End User Training		Deliver IT/End User Training	Support by BAU team
		Develop Training Plan		Launching communication campaign		T – Minus Comms	
GOVERNANCE		Governance Model	Detailed Program Plan	Build/Review Key Stakeholder Reports		Monitor & Manage	
	Milestone Plan	Program Plan	Metrics/ Measures				

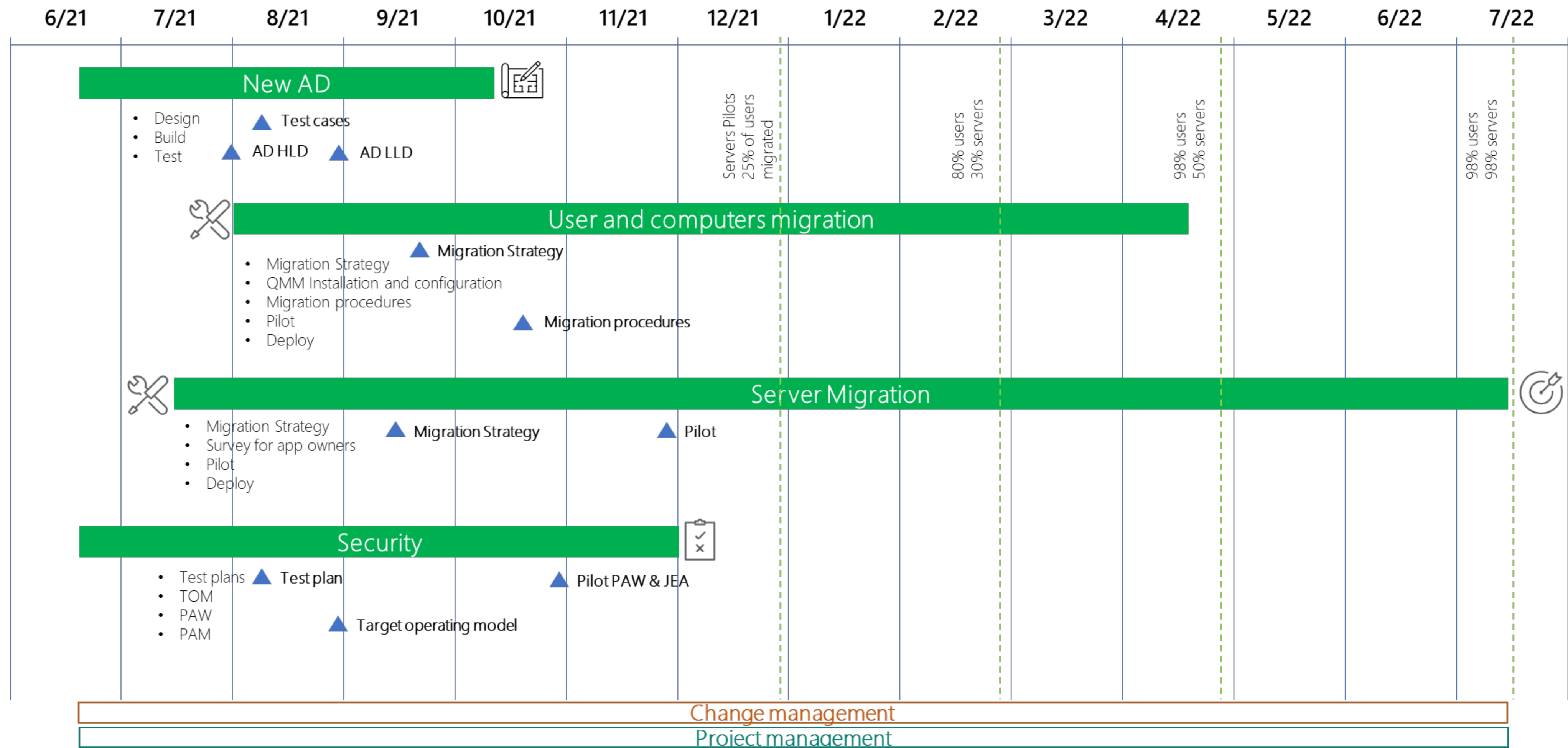
Case 3 : Greenfield



Edit Deployment Scenario - Mailbox

Details	T-	T0	T+	All
Tasks	<div>Copy Update Sequence Show Migration Pattern</div>			
All Versions	Offset Days	Sequence	Name	Type Group
Notes	-30	1	T-30: Validate User is Scheduled	Manual --
	-30	2	T-30: General Announcement Mailbox	Email --
	-15	3	T-15: License Exchange Online	PowerShell --
	-14	4	T-14: Batch Mailbox Sync	PowerShell --
	-14	5	T-14: General Comms Mailbox - ScheduleDate	Email --
	-7	6	T-07: General Comms Mailbox	Email --
	0	1	T-0: General Comms Mailbox - Migration	Email --
	0	2	T-0: Batch Migration Cutover	PowerShell --
	1	1	T+1 Success Comms Mailbox	Email --

Case 3 : Greenfield





“If you don’t know me
by now, I doubt you’ll
ever know me”

KRS-One – MC’s act like they don’t know

 [linkedin.com/in/bencau](https://www.linkedin.com/in/bencau)

 benjamin.cauwel@accenture.com

Questions?