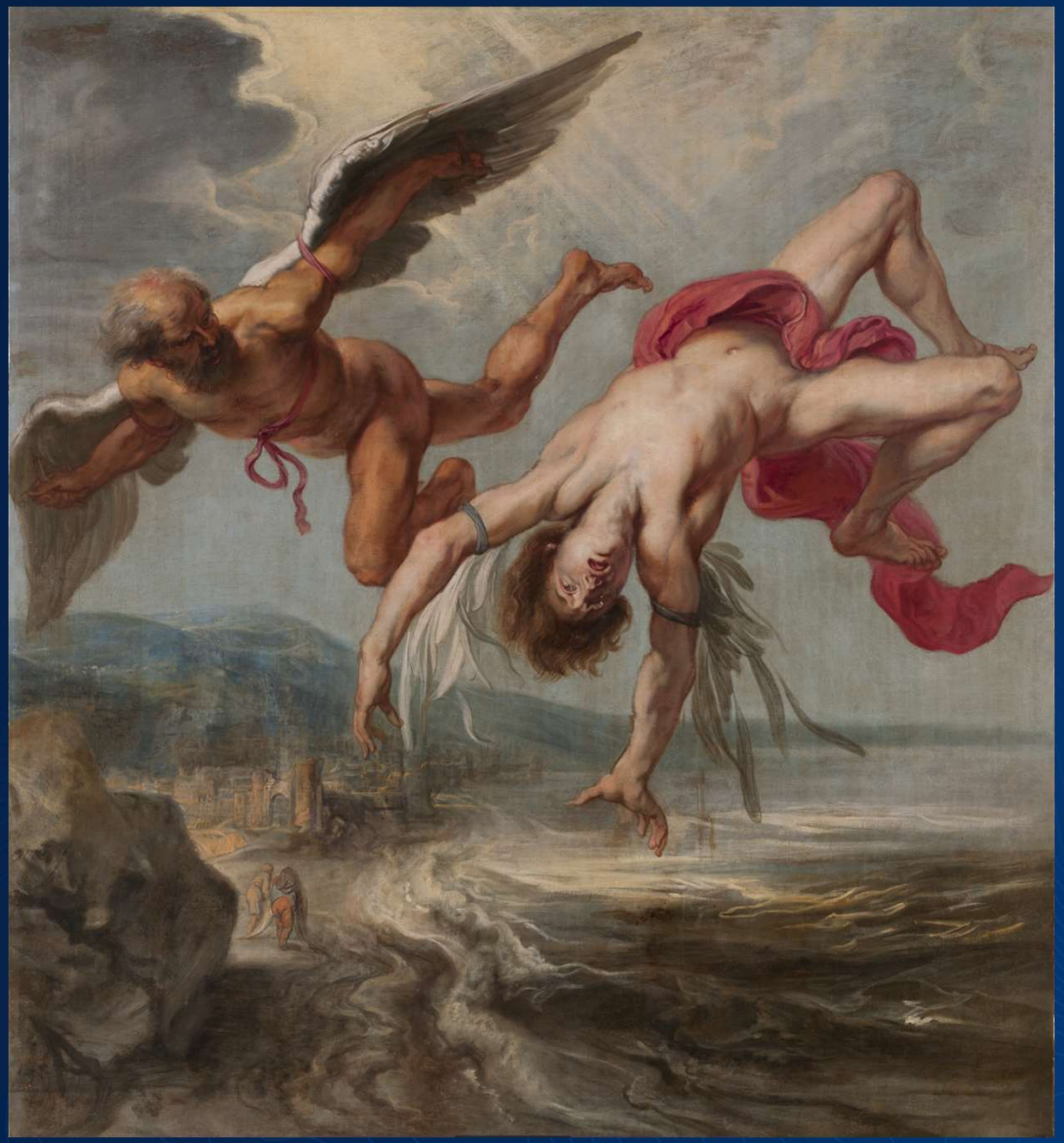
How mature are your current cloud security practices?

SIGS 6th Cloud Security Forum, June 12th, 2024

Rafi Bryl, Senior Director of Product Management,



tenable

About Me

- Senior Director of Product Management
- 2 years at Tenable Cloud Security (joined as Ermetic)
- Responsible for Workload Protection, Container Security, Cloud Identity and Entitlement management (CIEM) and Just in time permissions (JIT)
- Enjoy roasting coffee, baking bread, podcasts and skiing

tenable

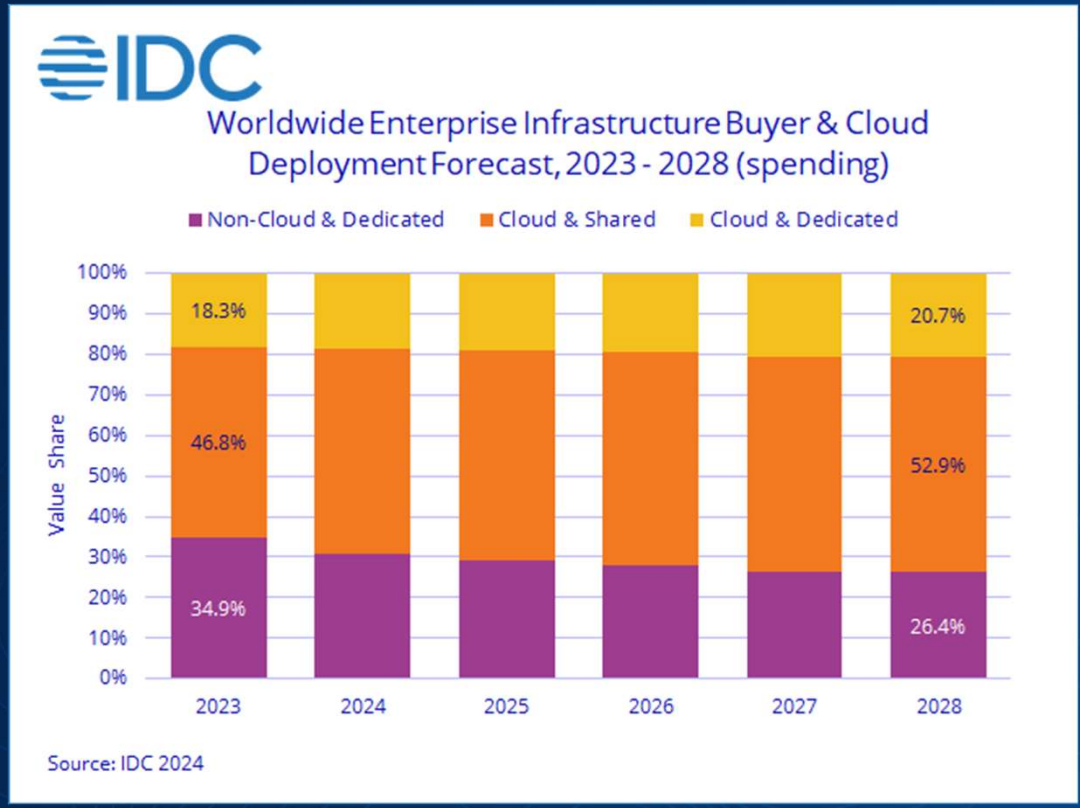
Agenda

- The challenge of cloud security
- Emerging cross-cloud security threats
- Introducing the *Tenable Cloud Security Maturity* Model
- Key takeaways

tenable

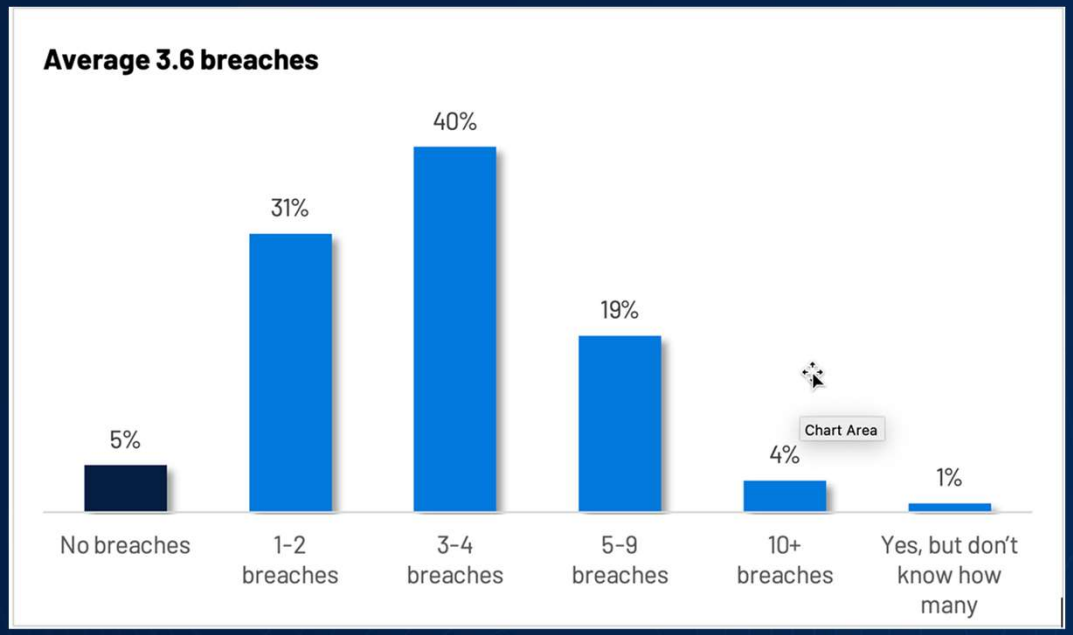
Cloud Spend Trends

Cloud spend continues to grow, whilst the share of non-cloud spend continues to decline



tenable

Cloud Security Breaches



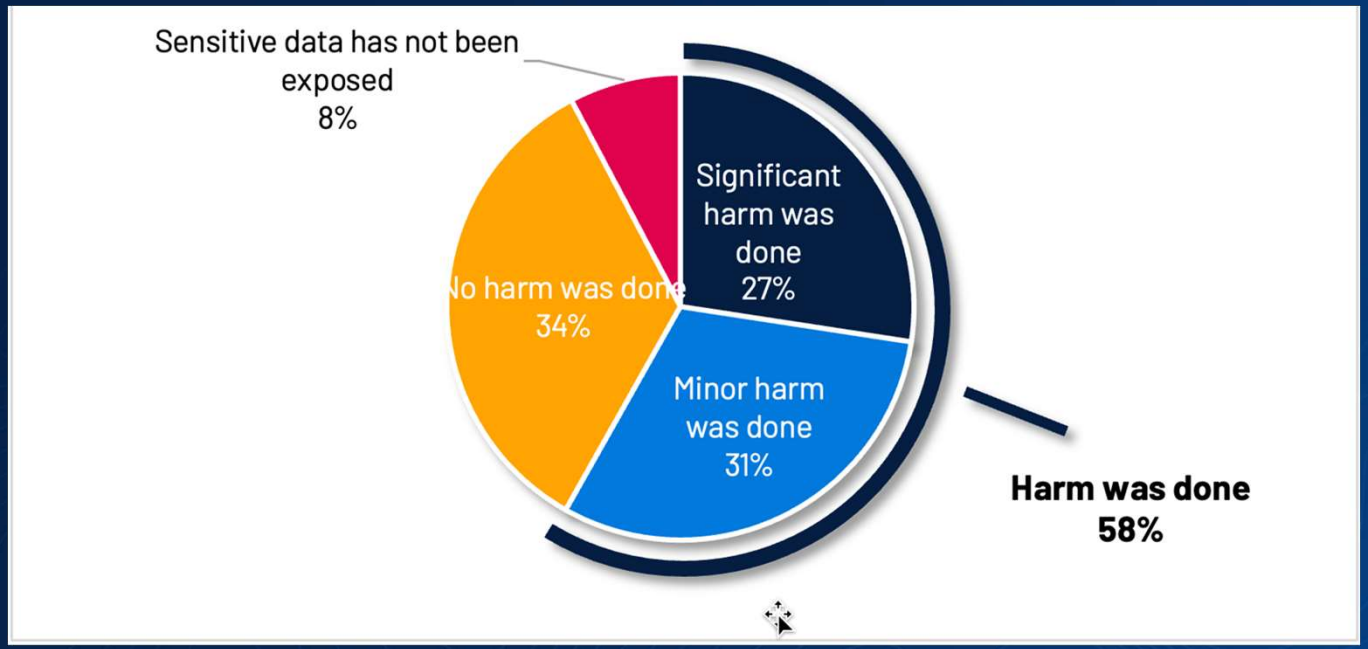
A staggering 95% of respondents acknowledged experiencing a cloud-related breach within the past 18 months, with an average of 3.6 breaches per respondent.

Source : 2024 Cloud Security Outlook. Navigating Barriers and Setting Priorities A global survey of cloud security professionals (Tenable)

tenable

Cloud Security Breaches

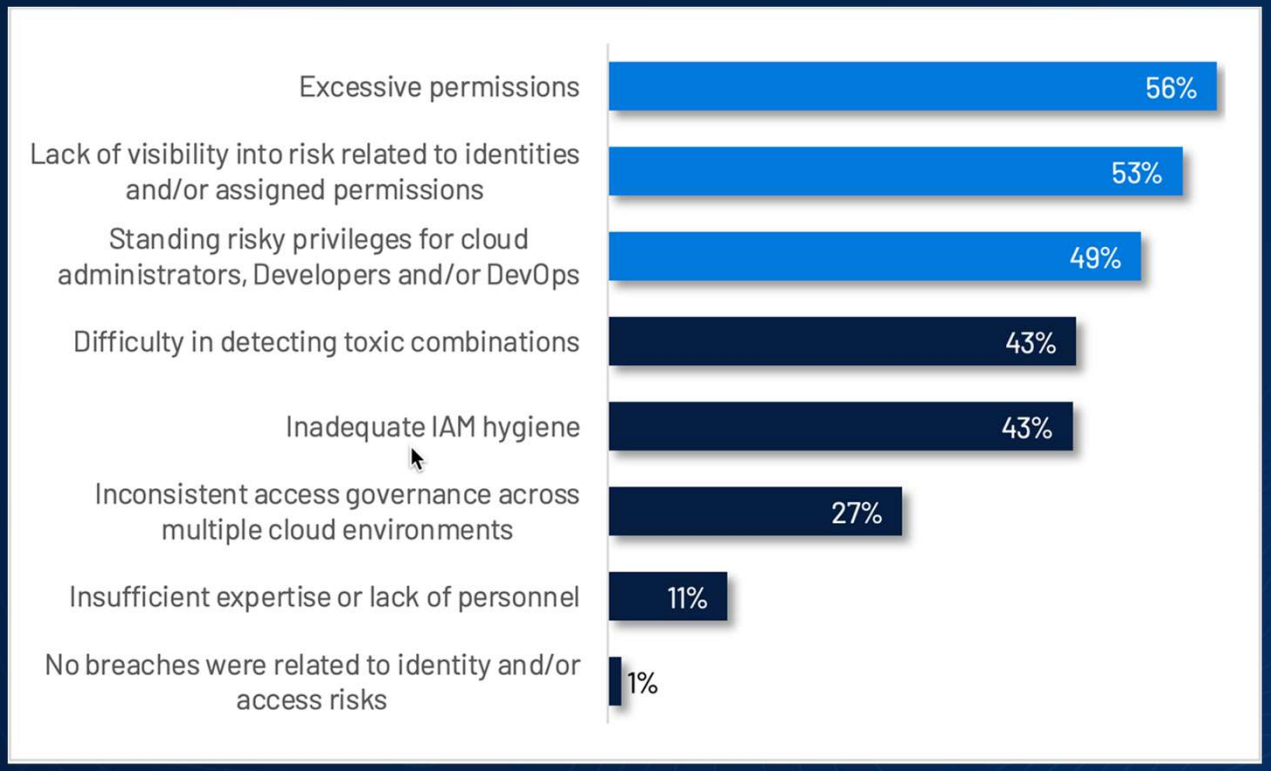
92% of respondents acknowledged situations in which sensitive data was exposed at their organizations. Of those, 58% reported that the incidents resulted in harm.



Source : 2024 Cloud Security Outlook. Navigating Barriers and Setting Priorities A global survey of cloud security professionals (Tenable)

tenable

Identities and Permissions as contributing factors

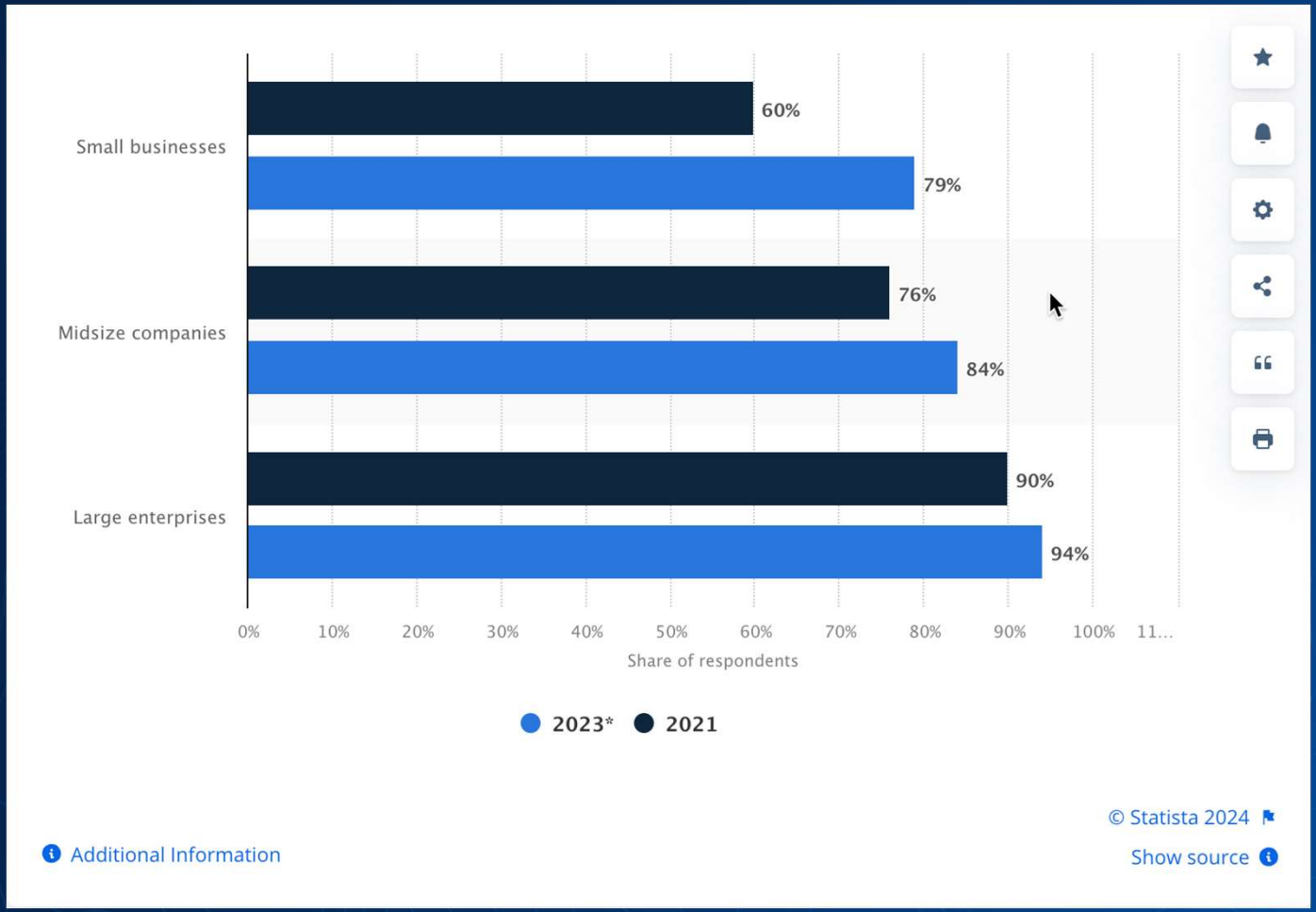


Nearly all survey customers (99%) confirmed that their breaches were related to identities and permissions

tenable

Multi-cloud adoption

As multi and hybrid-cloud adoption continues to grow, **cross-cloud** is emerging as a new attack vector



Workload Identity Cross-Cloud

- A typical use-case is a **workload** or developer endpoint needing access to resources in **another cloud**
- Nothing intrinsically **guarantees segregation** between clouds
- Hardcoding **long-lived credentials** is a bad idea but often unavoidable
- Bad actors can use basic tools such as WinPEAS & LinPEAS to find **privilege escalation paths**
- Even best-of-breed techniques, such as GCP Workload identity federation, can expose **risk** in case of **misconfiguration**

More details here

tenable

IDP Takeover is emerging as an attack vector

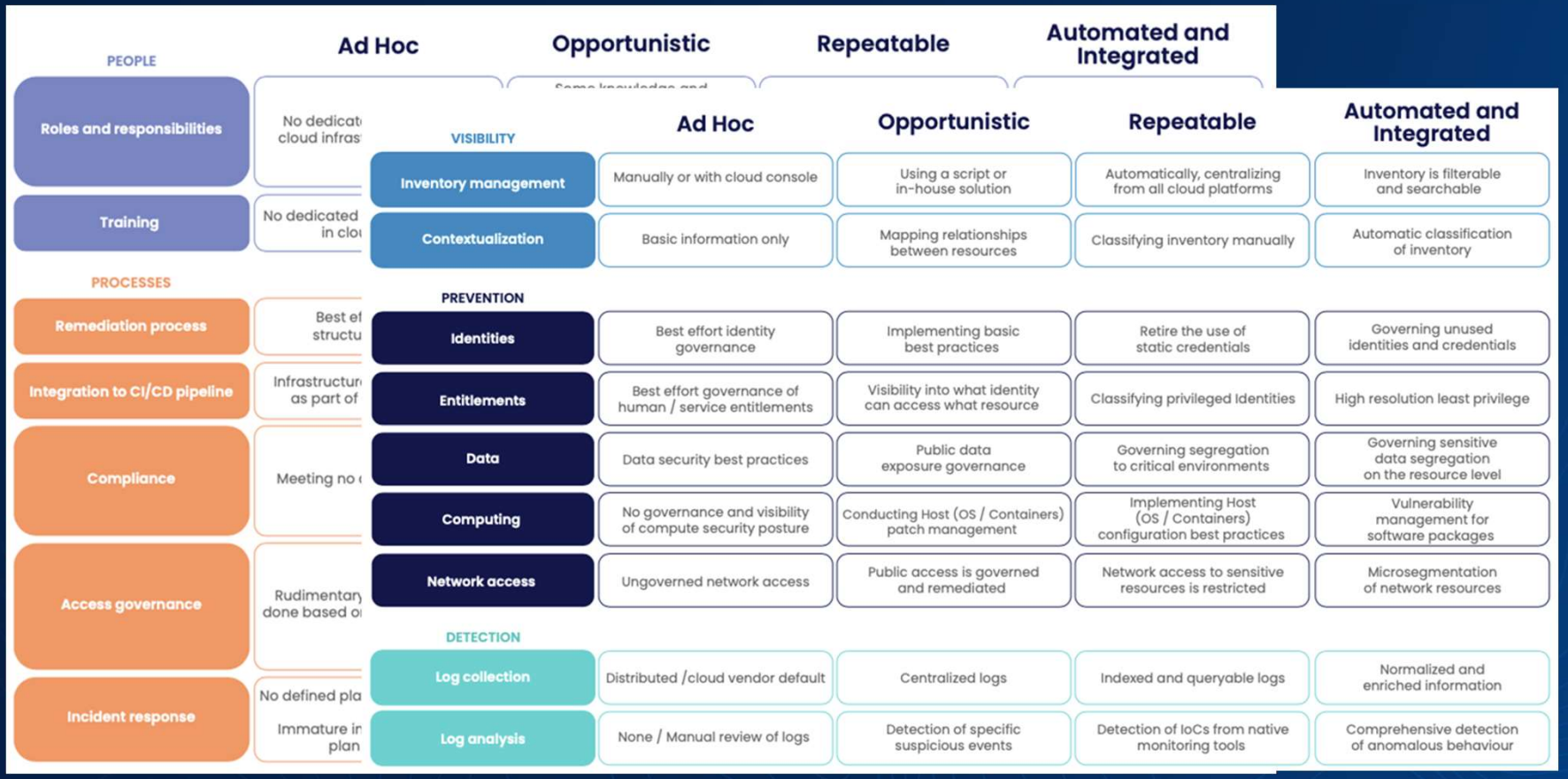
- The Identity provider is emerging as a point of weakness
- IDP takeover cloud allow an attacker to pivot and laterally move to other services and between cloud providers
- Even MFA can be bypassed by a sophisticated attacker
- More details here

Casino giant MGM expects $100 million hit from hack that led to data breach

Reuters

2 minute read · Published 9:40 PM EDT, Thu October 5, 2023

Introducing the Tenable “Cloud Security Maturity Model”



	Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
PEOPLE				
Roles and responsibilities	No dedicat cloud infras			
Training	No dedicated in clo			
PROCESSES				
Remediation process	Best ef structu			
Integration to CI/CD pipeline	Infrastructur as part of			
Compliance	Meeting no			
Access governance	Rudimentar done based o			
Incident response	No defined pla			
	Immature ir plan			

	Ad Hoc	Opportunistic	Repeatable	Automated and Integrated
VISIBILITY				
Inventory management	Manually or with cloud console	Using a script or in-house solution	Automatically, centralizing from all cloud platforms	Inventory is filterable and searchable
Contextualization	Basic information only	Mapping relationships between resources	Classifying inventory manually	Automatic classification of inventory
PREVENTION				
Identities	Best effort identity governance	Implementing basic best practices	Retire the use of static credentials	Governing unused identities and credentials
Entitlements	Best effort governance of human / service entitlements	Visibility into what identity can access what resource	Classifying privileged identities	High resolution least privilege
Data	Data security best practices	Public data exposure governance	Governing segregation to critical environments	Governing sensitive data segregation on the resource level
Computing	No governance and visibility of compute security posture	Conducting Host (OS / Containers) patch management	Implementing Host (OS / Containers) configuration best practices	Vulnerability management for software packages
Network access	Ungoverned network access	Public access is governed and remediated	Network access to sensitive resources is restricted	Microsegmentation of network resources
DETECTION				
Log collection	Distributed /cloud vendor default	Centralized logs	Indexed and queryable logs	Normalized and enriched information
Log analysis	None / Manual review of logs	Detection of specific suspicious events	Detection of IoCs from native monitoring tools	Comprehensive detection of anomalous behaviour

https://www.tenable.com/whitepapers/cloud-security-maturity-model-vision-path-execution

tenable

Levels of Maturity

Repeatable

- Easy execution
- Adaptable to changes

Ad-hoc

- No structure
- Cloud security as an afterthought
- Mainly Putting out fires

Automated and Integrated

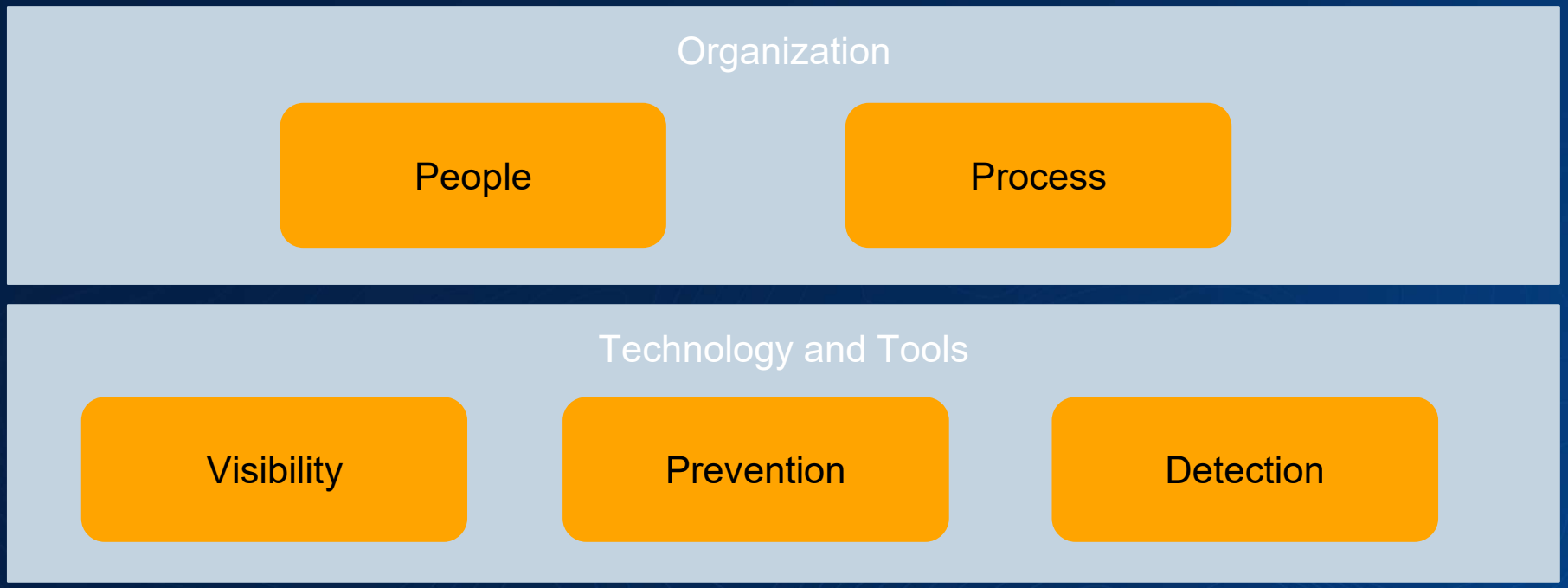
- Seamless
- Fully integrated into infrastructure
- Enforcement applied automatically

Opportunistic

- Basic structure
- Some strategy and roadmap

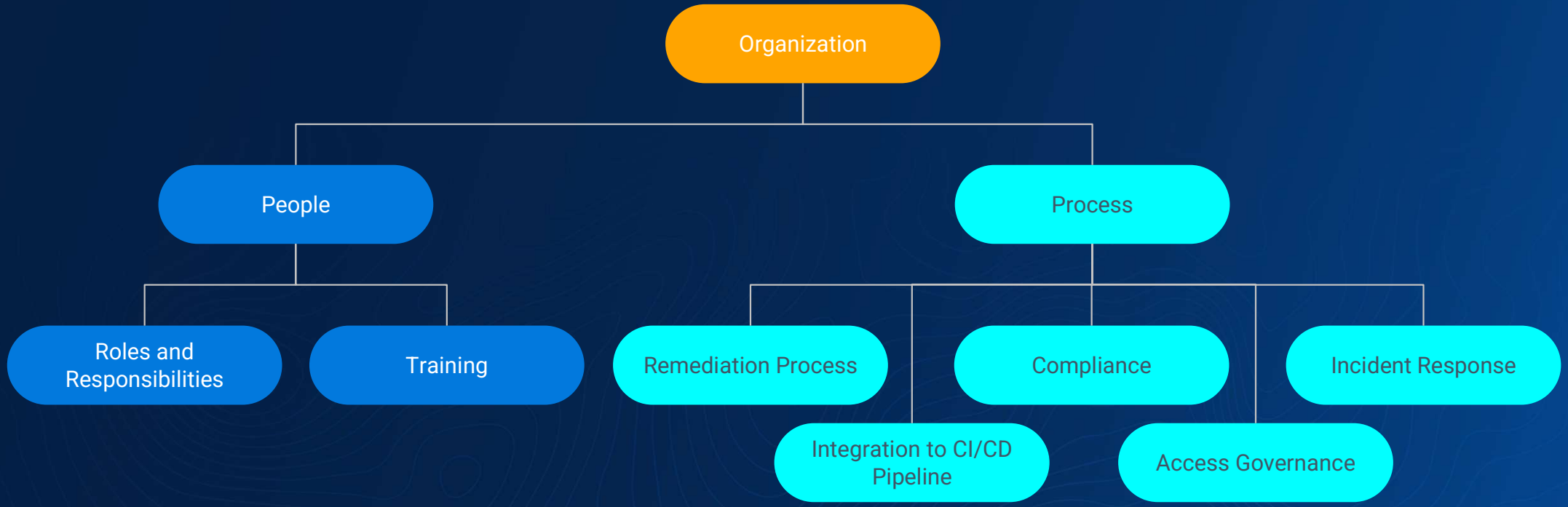
tenable

Scope



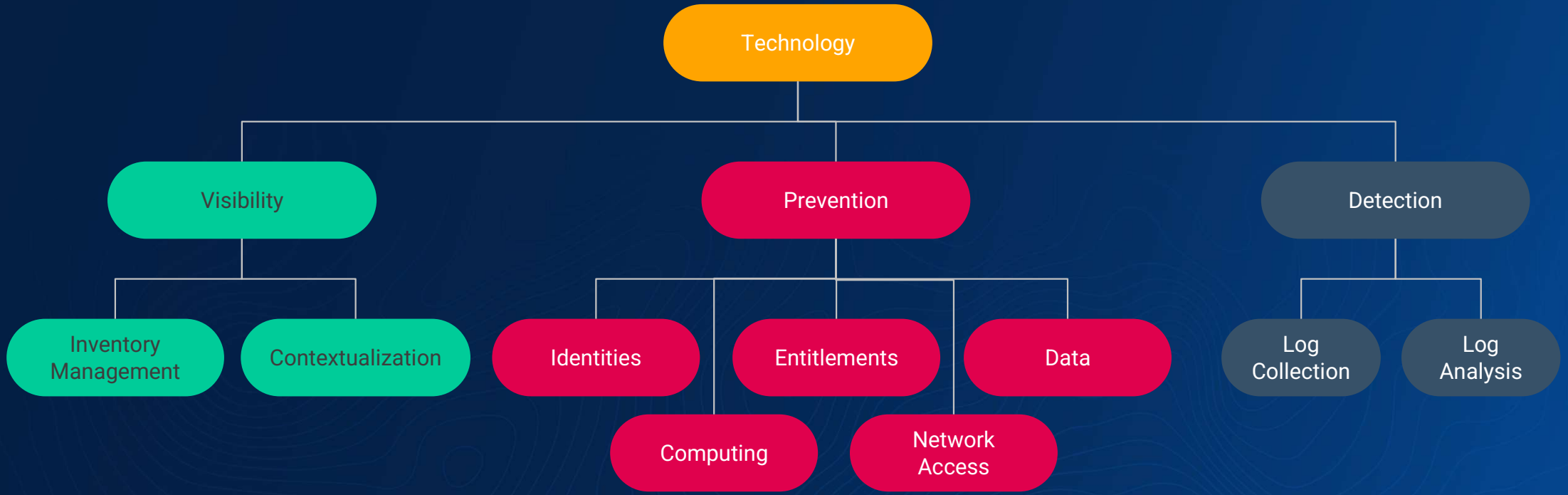
tenable

Organization



tenable

Technology



tenable

Key Attributes

MATURITY MODEL: TECHNOLOGY

VISIBILITY

	Adhoc	Opportunistic	Repeatable	Automated & Integrated
Inventory management	Manually or with cloud console	Using a script or in-house solution	Automatically, centralizing from all cloud platforms	Inventory is filterable and searchable
Contextualization	Basic information only	Mapping relationships between resources	Classifying inventory manually	Automatic classification of inventory

PREVENTION

Identities	Best effort identity governance	Implementing basic best practices	Retire the use of static credentials	Governing unused identities and credentials
Entitlements	Best effort governance of human / service entitlements	Visibility into what identity can access what resource	Classifying privileged Identities	High resolution least privilege
Data	Data security best practices	Public data exposure governance	Governing segregation to critical environments	Governing sensitive data segregation at the resource level
Computing	No governance and visibility of compute security posture	Conducting Host (OS / Containers) patch management	Implementing Host (OS / Containers) configuration best practices	Vulnerability management for software packages
Network access	Ungoverned network access	Public access is governed and remediated	Network access to sensitive resources is restricted	Microsegmentation of network resources

DETECTION

Log collection	Distributed /cloud vendor default	Centralized logs	Indexed and queryable logs	Normalized and enriched information
Log analysis	None / Manual review of logs	Detection of specific suspicious events	Detection of IoCs from native monitoring tools	Comprehensive detection of anomalous behaviour

MATURITY MODEL: ORGANIZATION

PEOPLE

	Adhoc	Opportunistic	Repeatable	Automated & Integrated
Roles and Responsibilities	No dedicated personnel for cloud infrastructure security	Some knowledge and responsibility within the security team Executive sponsor for cloud security program	Dedicated person / team with relevant training and expertise	Additional expert delegates within R&D
Training	No dedicated training / expertise in cloud security	Some members of security team undergo cloud security	Cloud security team undergoes formal cloud security training and certification	Cloud security awareness training program for R&D

PROCESSES

Remediation process	Best effort with no structured process	Security team owns and prioritizes security findings	Prioritized findings automatically shared with stakeholders	Full ownership of R&D teams for resolution of issues
Integration to CI/CD pipeline	Infrastructure is not managed as part of CI/CD pipeline	Proper process for governing change management	Managing Infrastructure as Code	Embedding infrastructure security in the CI/CD pipeline
Compliance	Meeting no defined standard	Mandatory compliance standards are met	External best practice(s) implemented and audited Governance principles documented and tracked Screen reader support enabled	Custom compliance rule enforced
Access governance	Rudimentary access review is done based on best effort, if at all	Groups / labels / organizational-structure based level access review Consistent access and governance Screen reader suppport enabled	Risk-based access review for sensitive resources and privileged identities	Risk-based access review for all resources and identities
Incident response	No defined playbook for incidents Immature incident response	Well defined manual playbook for responding to incidents	Organization wide incident response program in place and tested periodically	Automation of playbook based on pervious experince

Example - Remediation

Remediation process

The process of remediating findings of security gaps / misconfigurations in the cloud environment leads one to ask who owns the process of responding to findings arising from governance, and how is it done?

	Adhoc	Opportunistic	Repeatable	Automated & Integrated
Remediation process	Best effort with no structured process	Security team owns and prioritizes security findings	Prioritized findings automatically shared with stakeholders	Full ownership of R&D teams for resolution of issues

tenable

Example - Permissions Management

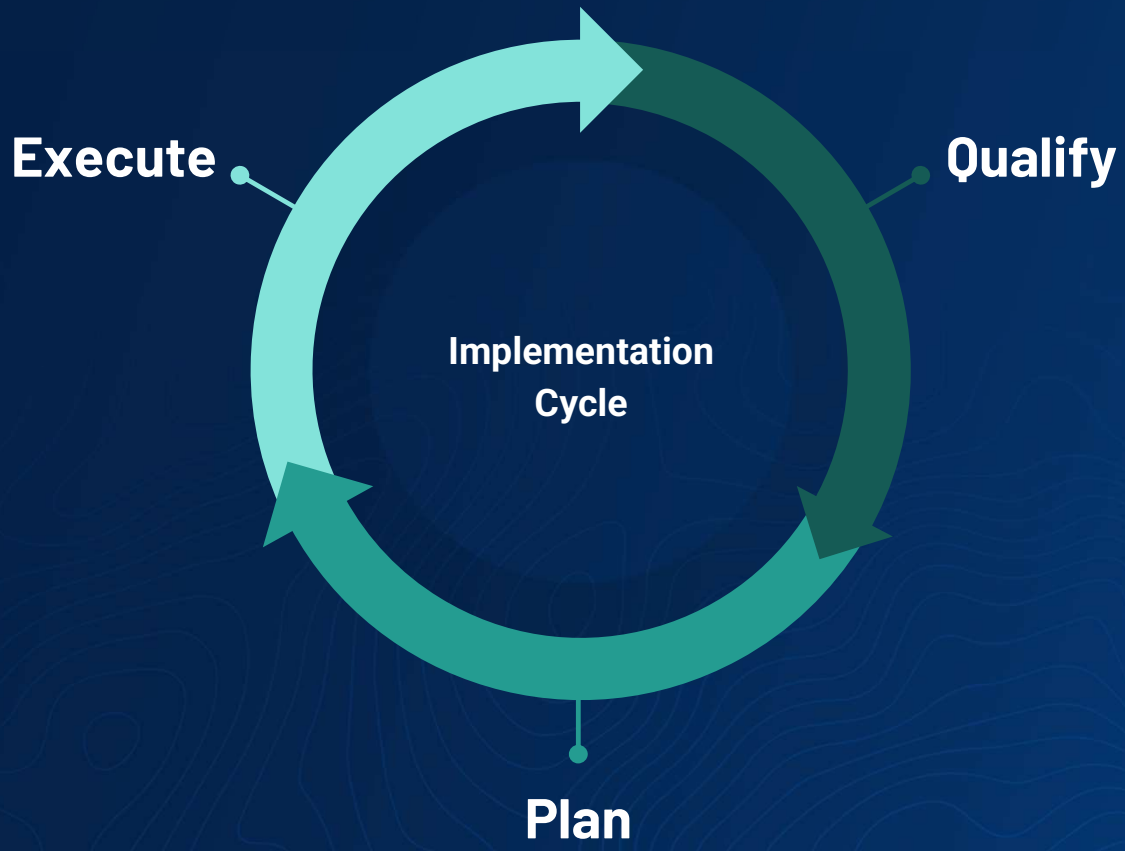
Entitlements

What kind of visibility and enforcement are required for the principle of least privilege?

	Adhoc	Opportunistic	Repeatable	Automated & Integrated
Entitlements	Best effort governance of human / service entitlements	Visibility into what identity can access what resource	Classifying privileged Identities	High resolution least privilege

tenable

Implementation



tenable

What this is not !!

A Silver Bullet

A step-by-step guide

A vendor recommendation

tenable

Takeaways

- Understand your **cloud security risks**
- Seek a **cloud security tool** which provides full **visibility**, **prevention** and **detection**, ideally with a strong **identity focus**
- Consider implementing a **structured program** to improve your cloud security **maturity level**

tenable

tenable