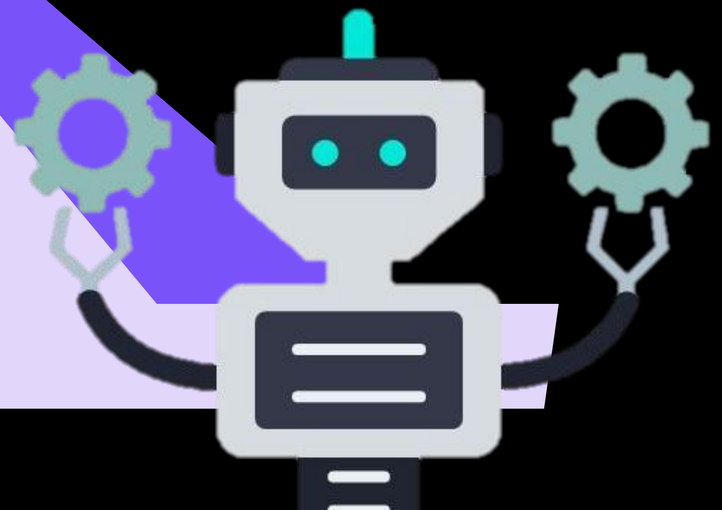
HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Almost Human: How to Protect Machine Identities



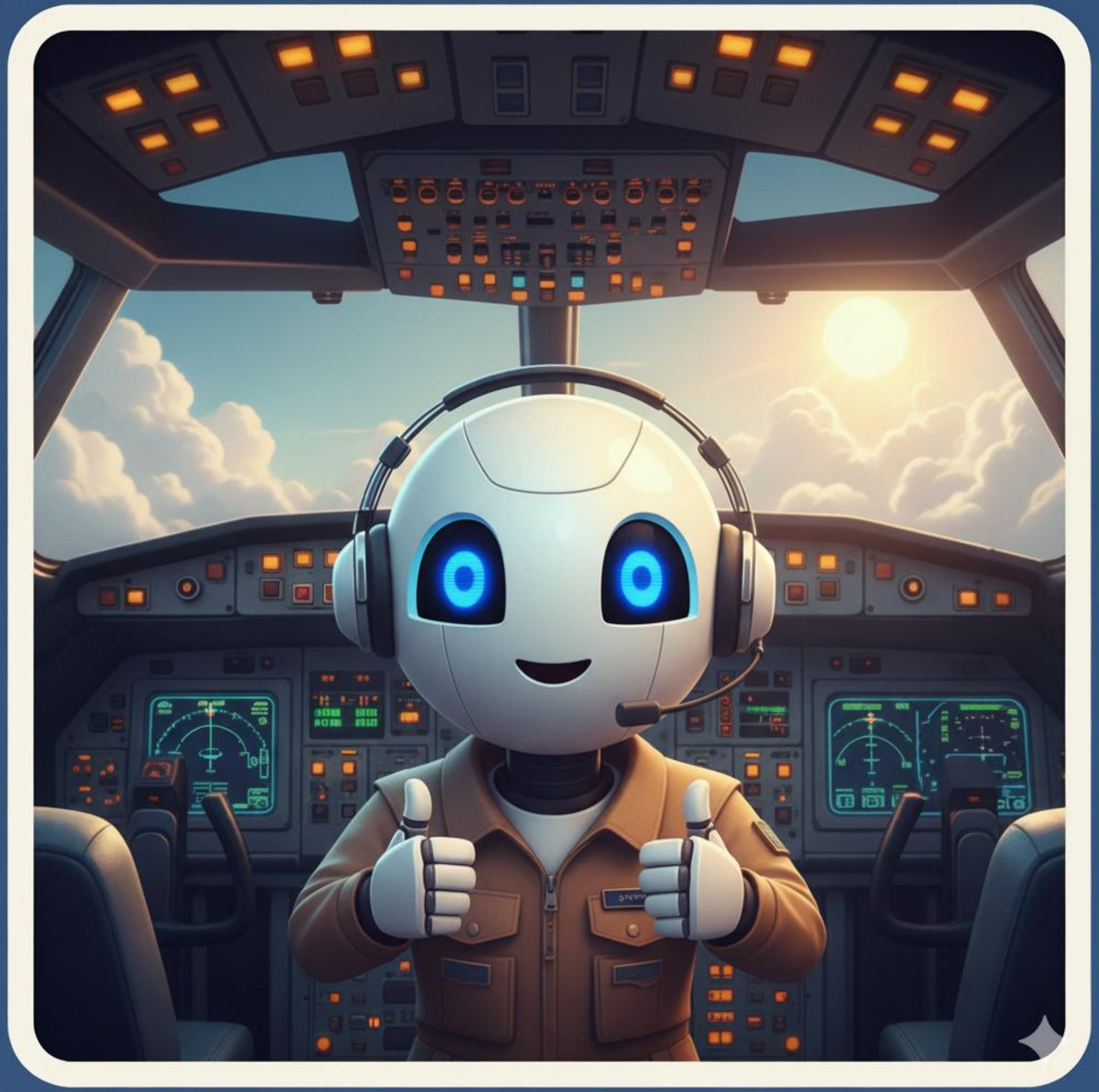
HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Tim Wolf

Semperis

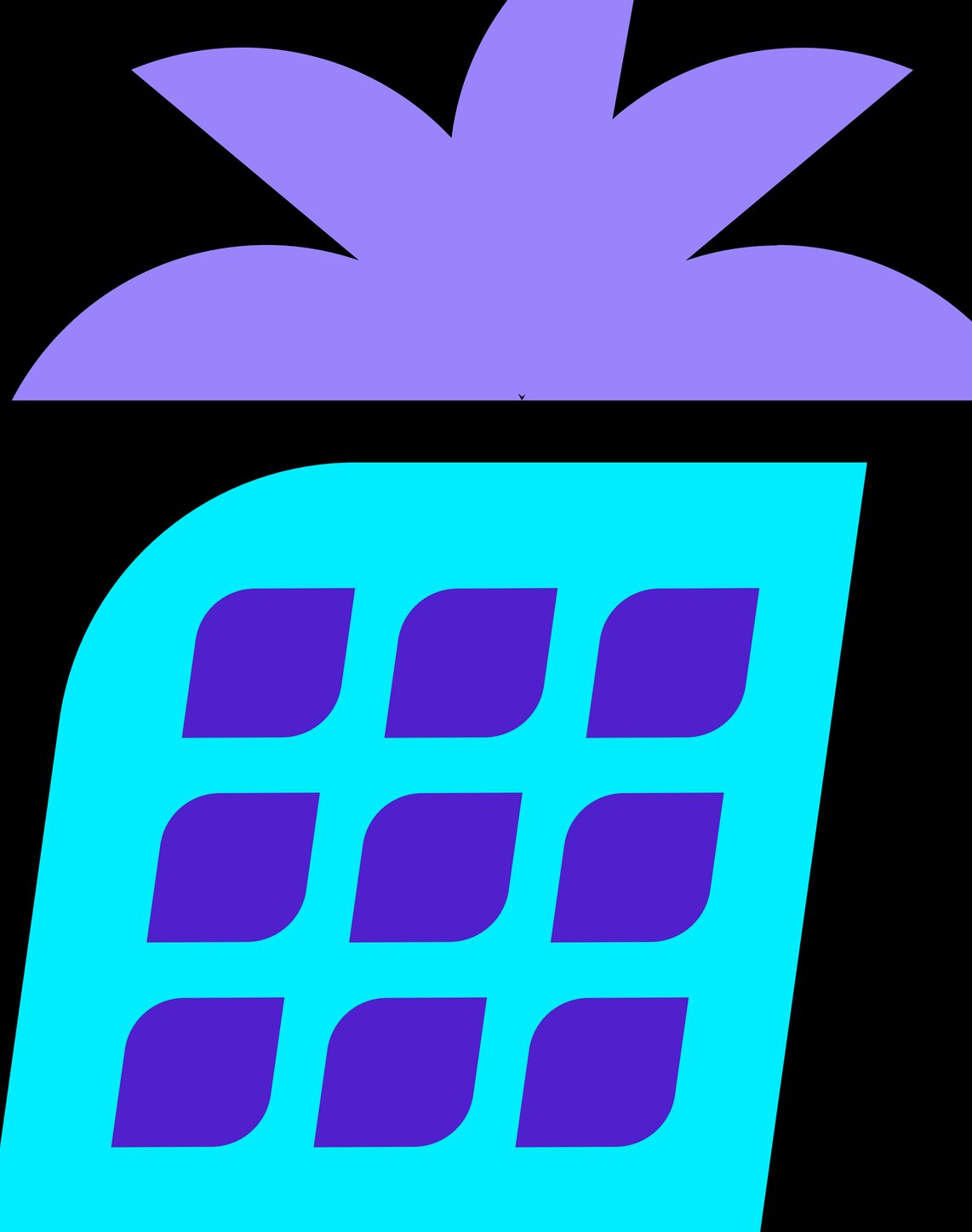
Senior Solution Architect

- Germany
- Ex-MSFT (PFE)
- LinkedIn
- www.azurehero.de



Agenda

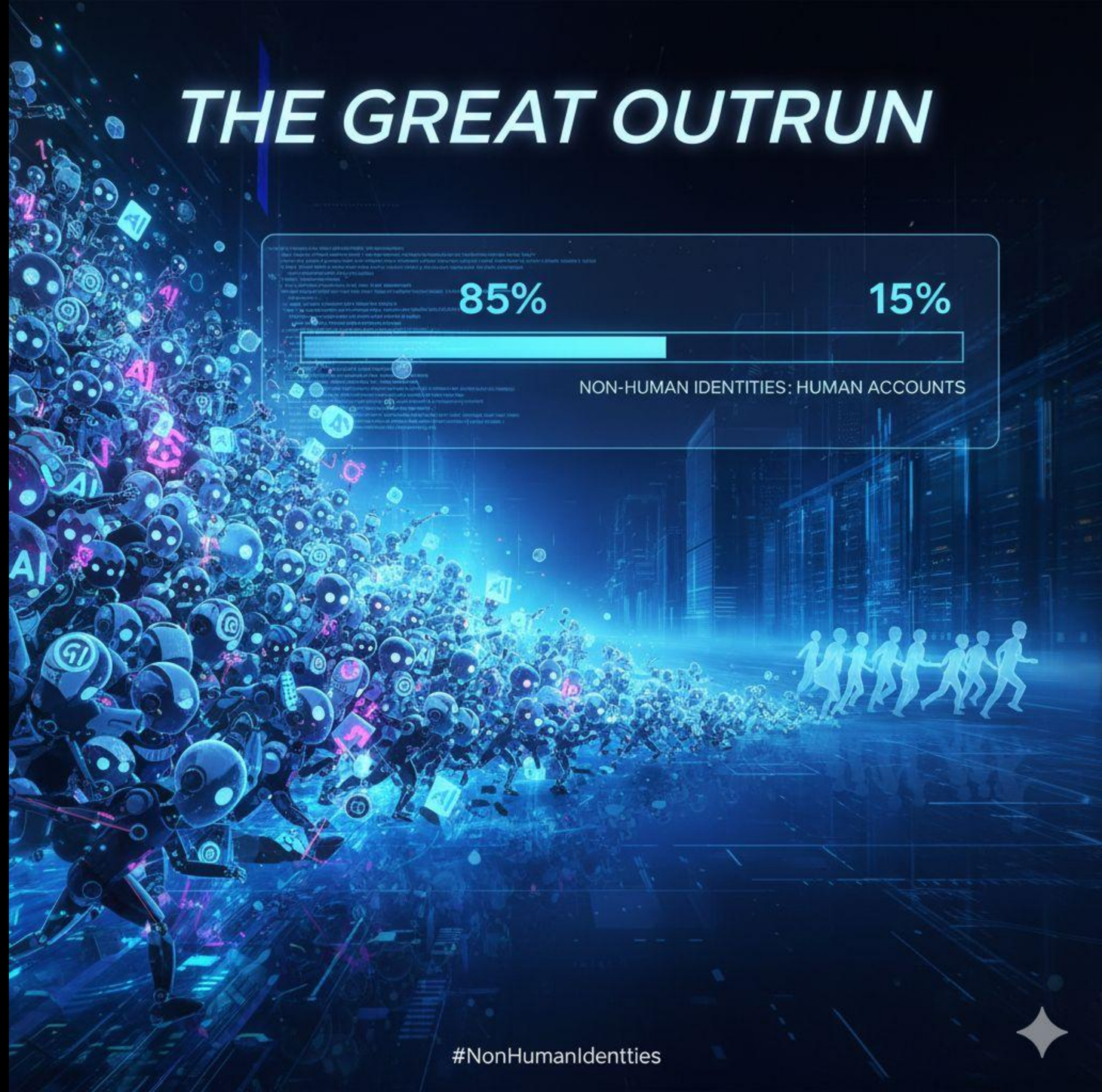
- AI is outrunning us
- What is a non-human identity?
- How they attack
- How to detect them
- Takeaway



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

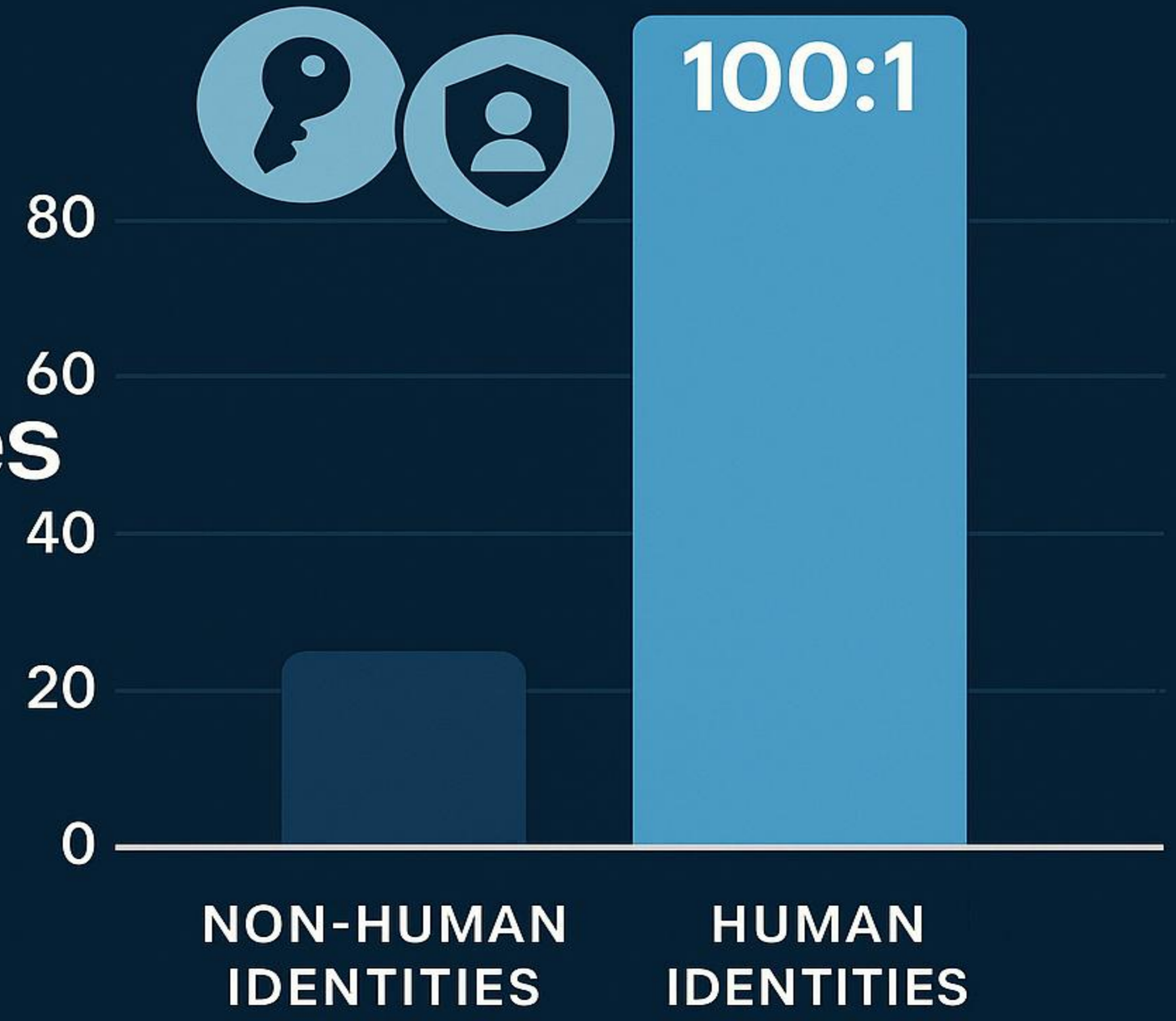
HYBRID IDENTITY PROTECTION conf25
CHARLESTON

AI is outrunning us



Non-Human Identities Increasing as 2026 Approaches

API keys, service accounts, and cloud tokens expected to surpass human identities by a ratio of 100 to 1 in businesses

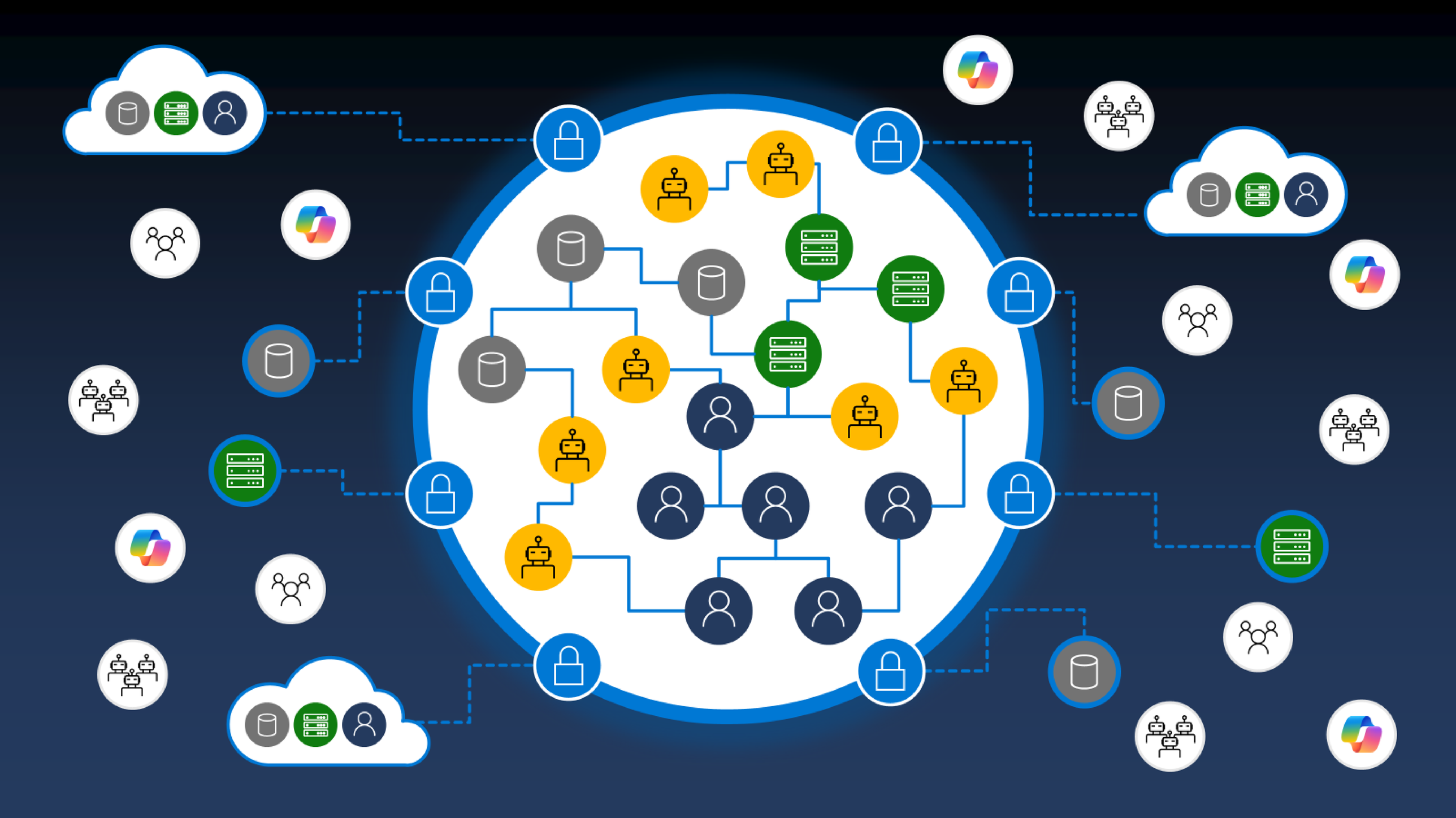


CyberArc Security Report 2025

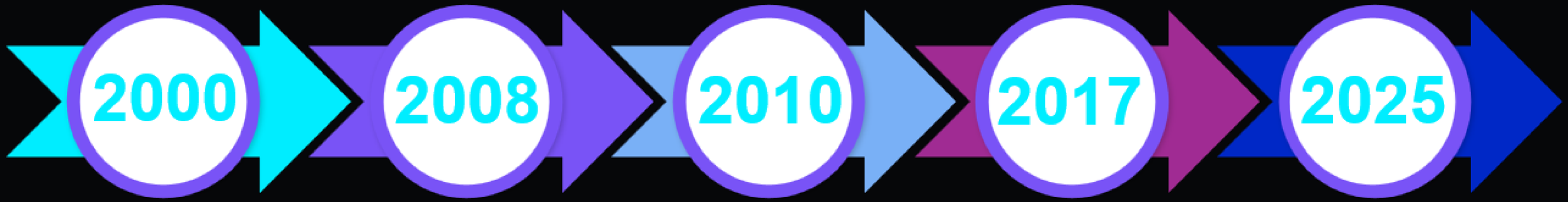
HYBRID IDENTITY PROTECTION conf25

CHARLESTON

What is a Non-Human Identity



Different Types of Non-Human Identities



Tech User

MSA / gMSA

Enterprise Apps
App Registrations

Managed Identity

dMSA

User	NHI
MFA	Maybe a Trust Relationship?
Lifecycle	Maybe Exist Forever?
Least-Privilege	Maybe Directory.ReadWrite.ALL?
Governance	Maybe an Owner?

User	NHI
MFA	No Credentials
Lifecycle	Lifecycle
Least-Privilege	Least-Privilege
Governance	Governance

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

How They Attack

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Attack 1: App Registration

Demo

Demo

```
# Through App
Connect-MgGraph –ClientId ”b9f849de-5fb2-49ca-9f57-42a13bd762c5”

#VIP User
Remove-MgUser -UserId $UserID
 #ERROR: 403 UNFORBIDDEN
-----------------------------------------------------------
# AS App
Connect-MgGraph –ClientId ”b9f849de-5fb2-49ca-9f57-42a13bd762c5”
–ClientSecret <XXXXX>

#VIP User Delete
Remove-MgUser -UserId $UserID
 # SUCESSFUL
```

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Attack 2: Service Account Lateral Movement

Demo

Demo

Adding WhiteBoard after Session with new Upload

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Attack 3: And AI?

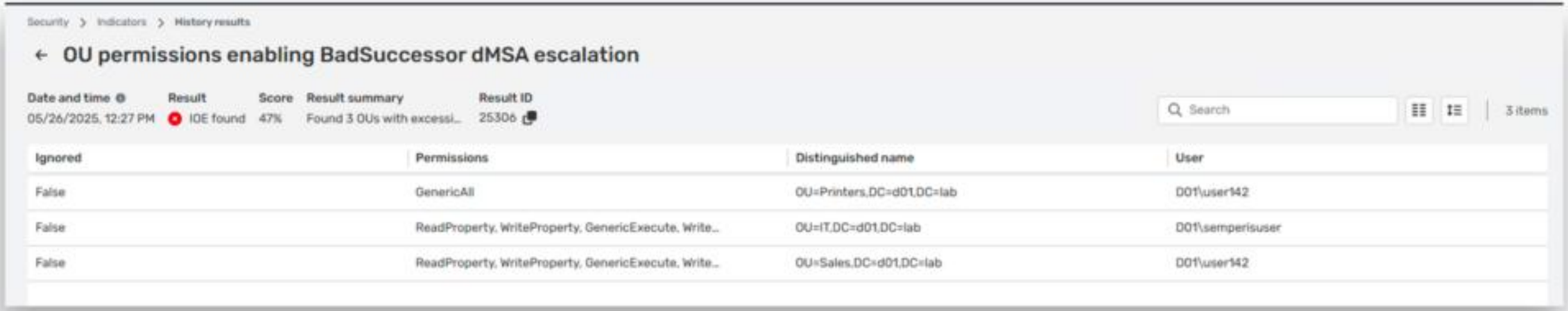
Demo

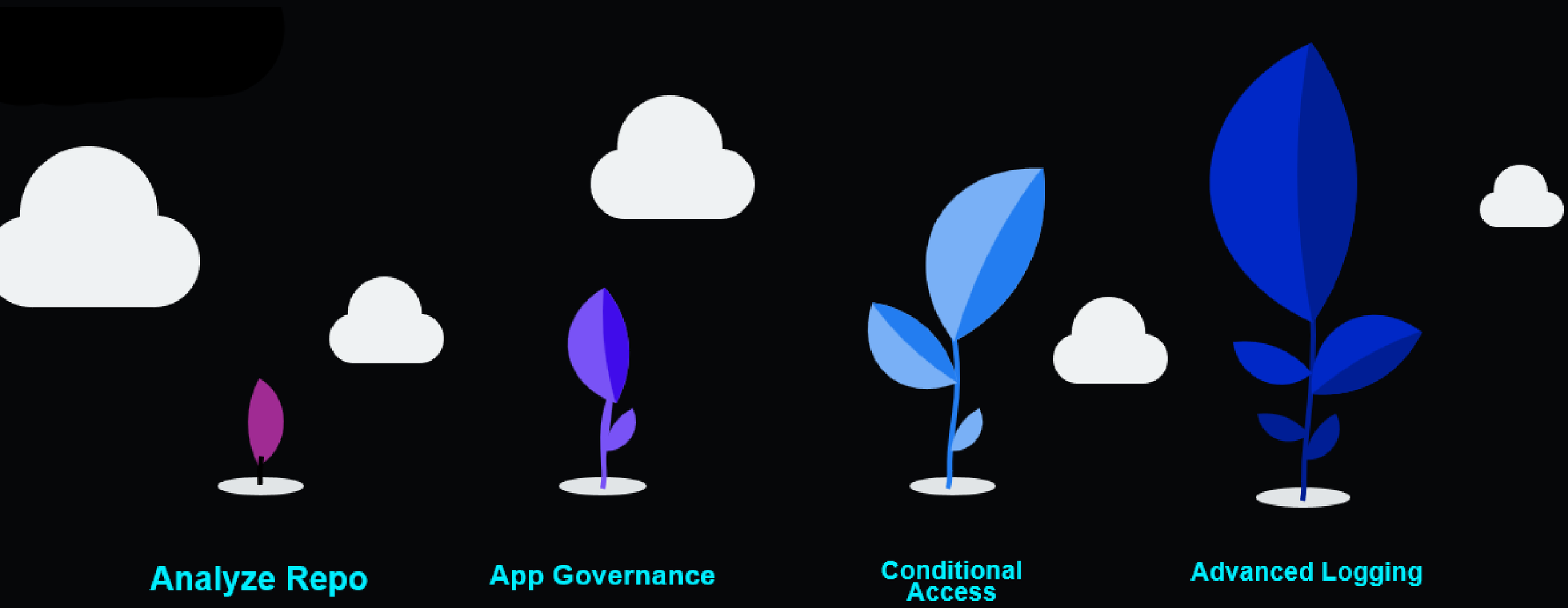
Demo

Adding WhiteBoard after Session with new Upload

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

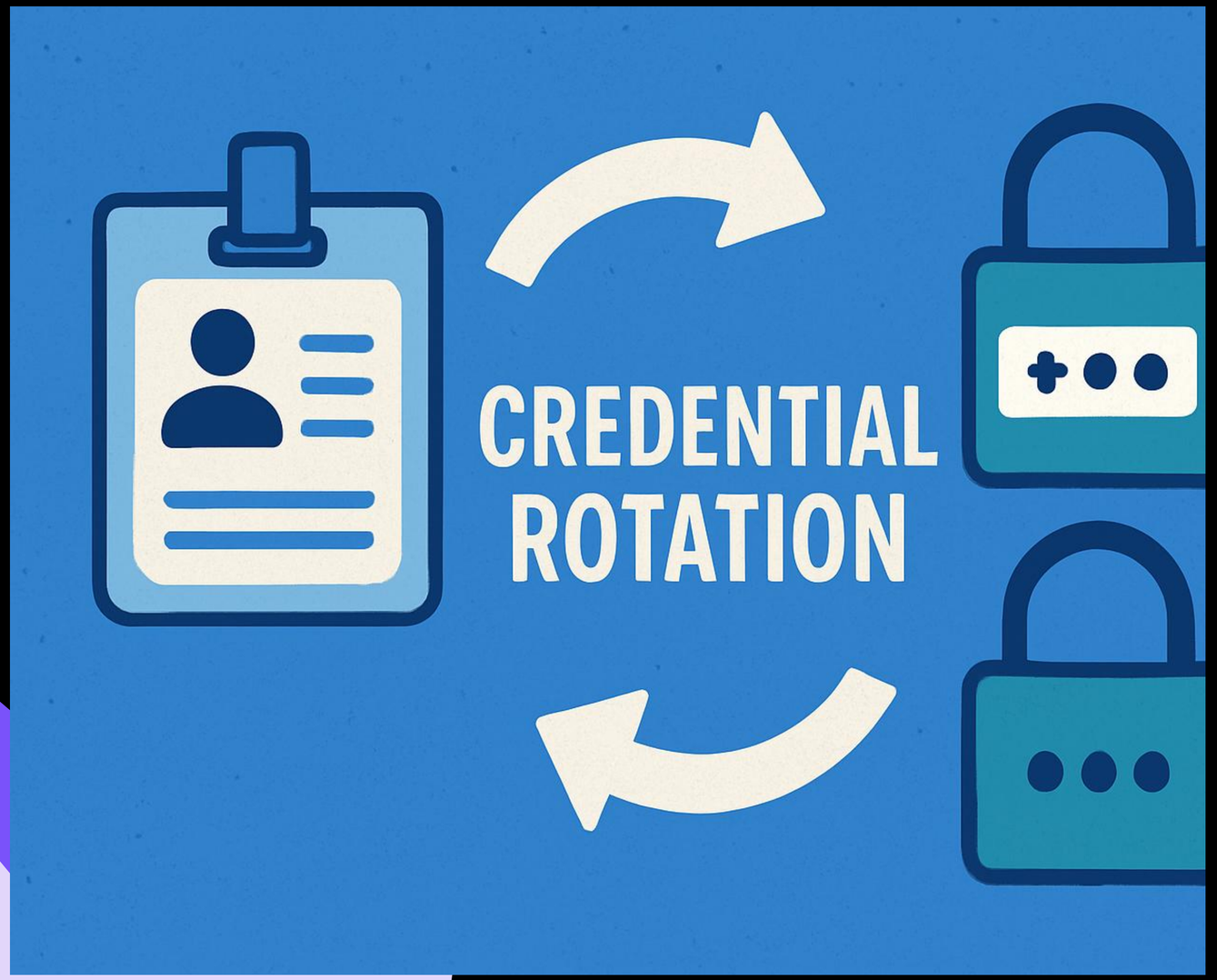
How to Detect Them


Security > Indicators > History results
OU permissions enabling BadSuccessor dMSA escalation
Date and time
05/26/2025, 12:27 PM
Result
IOE found
Score
47%
Result summary
Found 3 OUs with excessi...
Result ID
25306
Search
3 items
Ignored
Permissions
Distinguished name
User
False
GenericAll
OU=Printers,DC=d01,DC=lab
D01\user142
False
ReadProperty, WriteProperty, GenericExecute, Write...
OU=IT,DC=d01,DC=lab
D01\semperisuser
False
ReadProperty, WriteProperty, GenericExecute, Write...
OU=Sales,DC=d01,DC=lab
D01\user142


Analyze Repo
App Governance
Conditional Access
Advanced Logging

HYBRID IDENTITY PROTECTION conf25

CHARLESTON



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Takeaway

No Secrets

Knowledge

Conditions

Ownership

Developer

Governance

Detection

Logging

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Thanks!

Enjoy HIP and happy to connect with you!

HYBRID
IDENTITY
PROTECTION

conf25

CHARLESTON