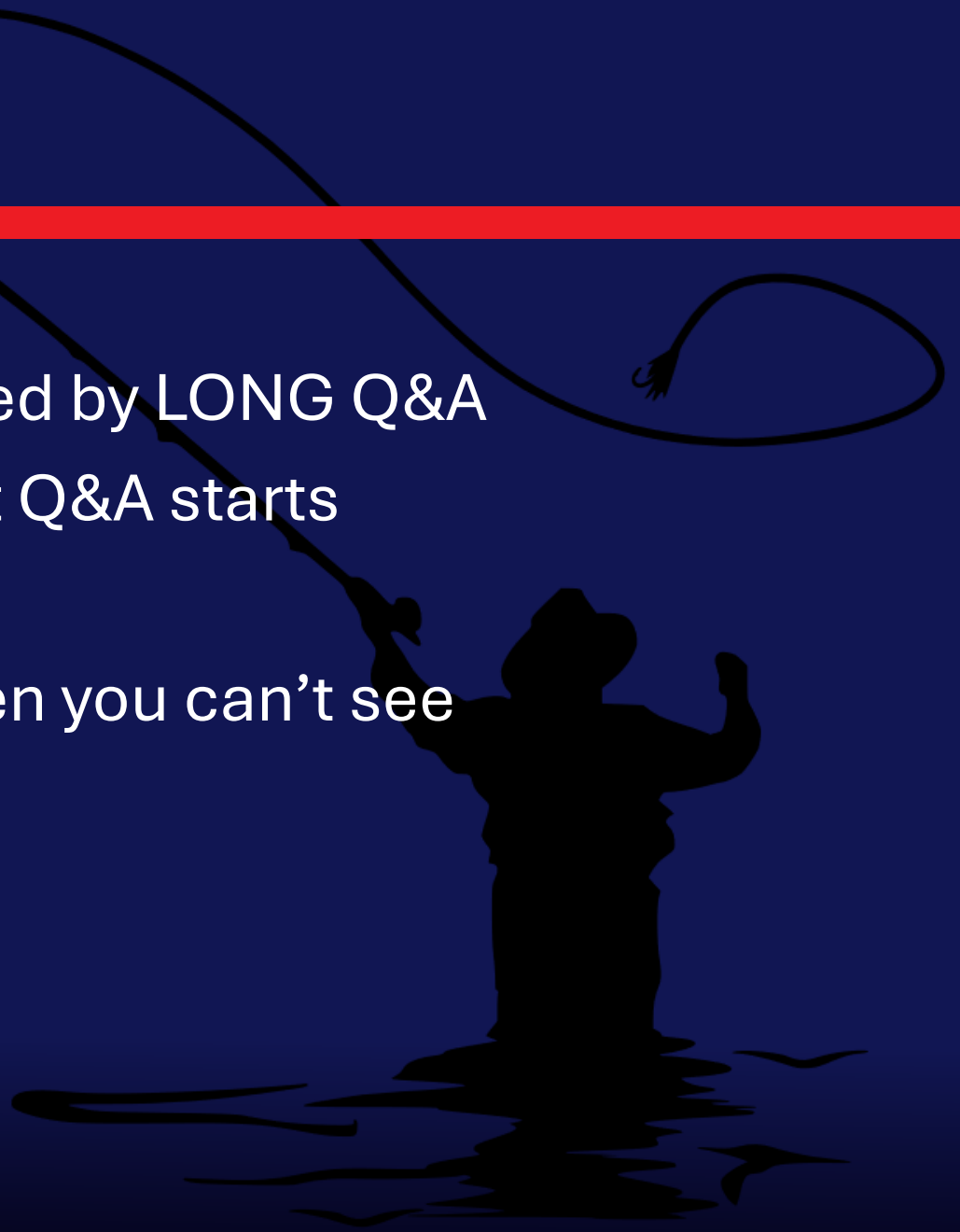
Mastering Entra ID Privileged Identity Management:

Essential Strategies

Attention

- MMS sessions are 60-75 minutes followed by LONG Q&A
- Please hold detailed questions until that Q&A starts
- Feel free to ask clarification questions
- Remind the speakers to use Zoom It when you can’t see



Speakers

Jan Ketil Skanke

Principal Cloud Architect @CloudWay

in/JankeSkanke

Maurice Daly

Used to be my Employee

in/mauricedaly

Can’t see our slides? Can’t hear? Need to repeat the question? Call us out!

Speakers

Jan Ketil Skanke

Not my boss anymore

in/JankeSkanke

Maurice Daly

Senior Security Architect @Patch My PC

in/mauricedaly

MMS

Can’t see our slides? Can’t hear? Need to repeat the question? Call us out!

Speakers

Jan Ketil Skanke

Principal Cloud Architect @CloudWay

in/JankeSkanke

Maurice Daly

Senior Security Architect @Patch My PC

in/mauricedaly

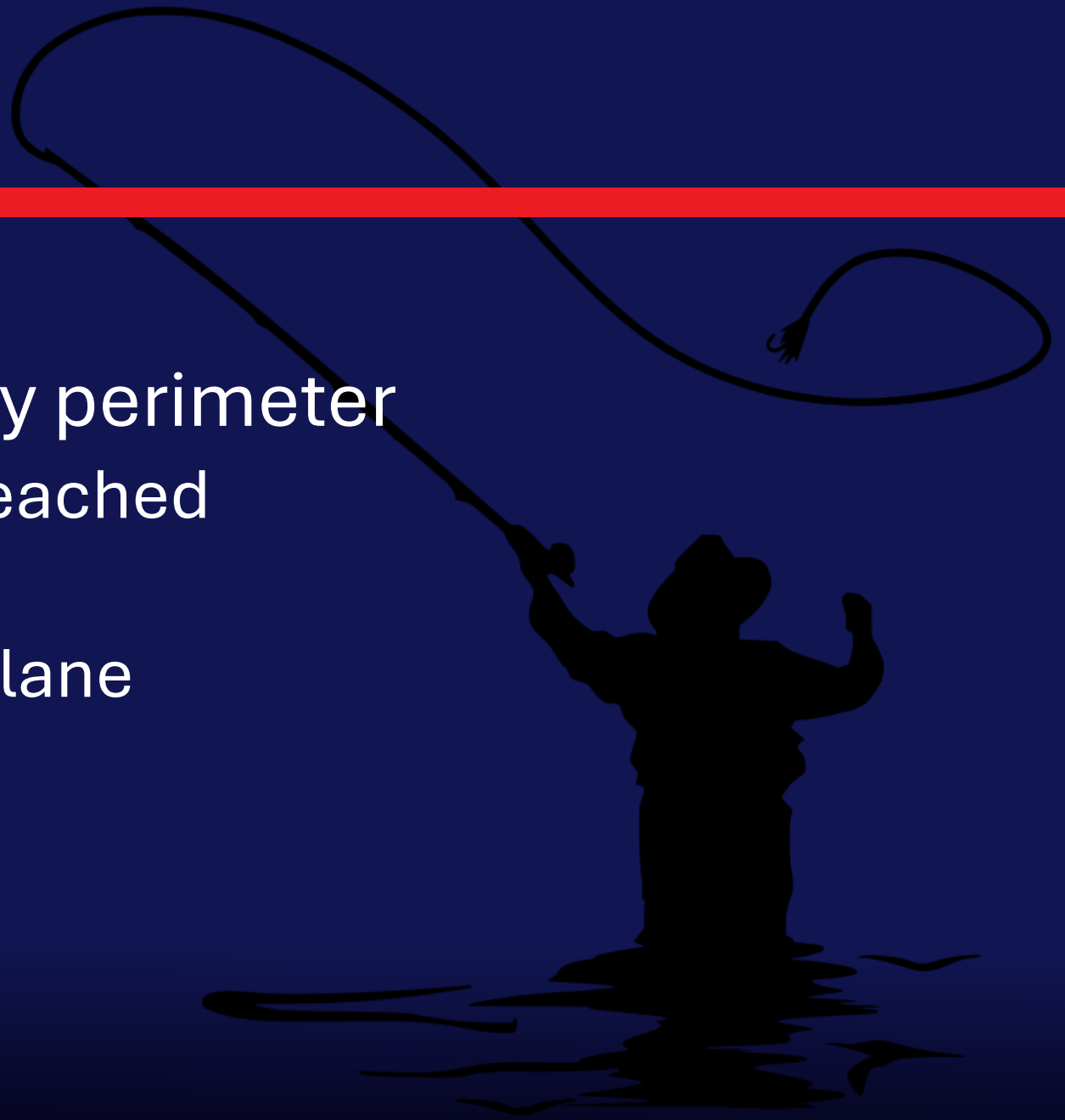
Can’t see our slides? Can’t hear? Need to repeat the question? Call us out!

Why do we care?

Security

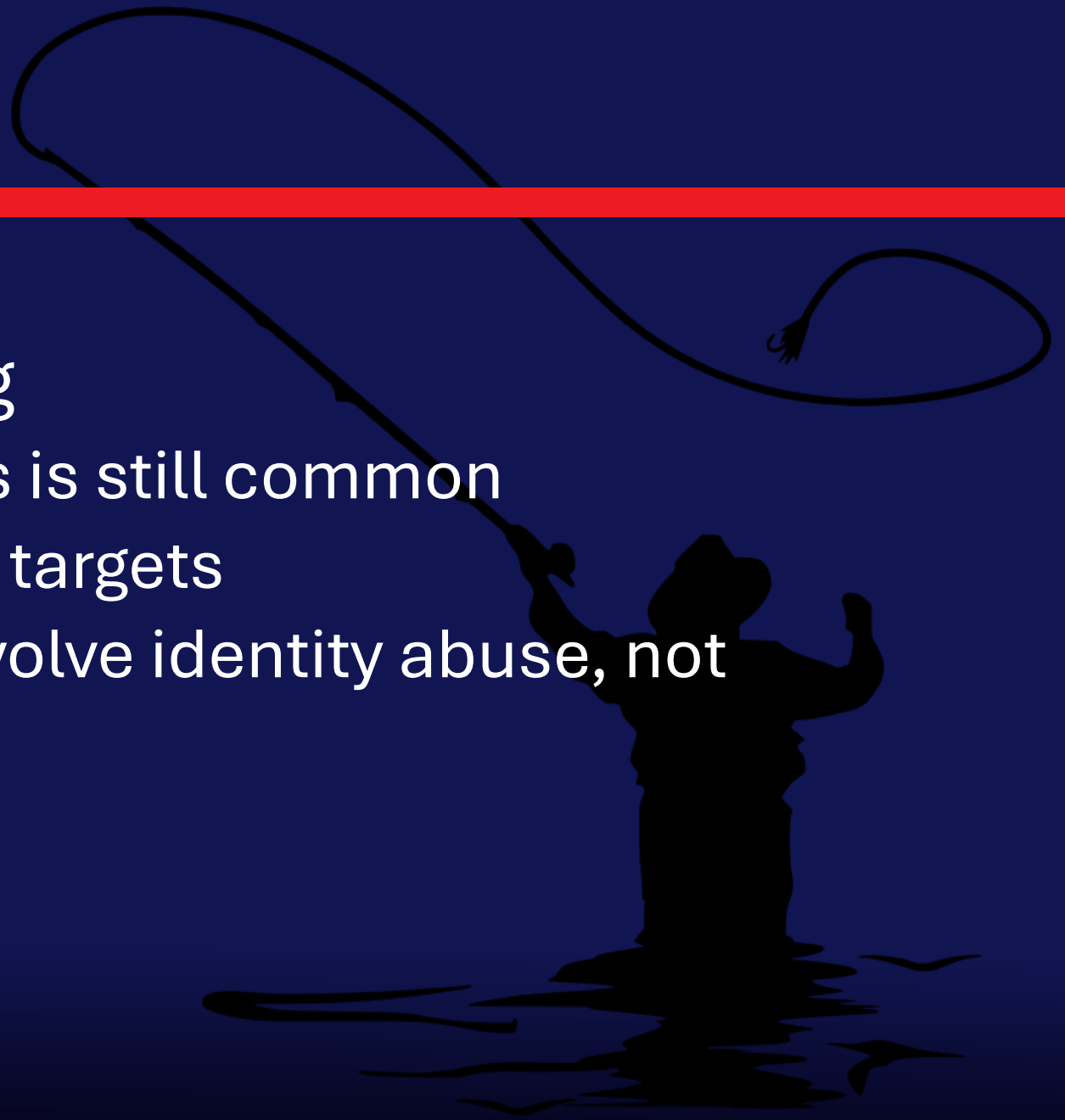
Why this matters

- Identity is the new security perimeter
  - Networks are assumed breached
  - Devices are replaceable
  - Identities are the control plane



Why this matters

- The reality we keep seeing
  - Standing privileged access is still common
  - Those roles are high-value targets
  - Most modern breaches involve identity abuse, not malware.



Bottom line

Privileged Identity Management is no longer nice-to-have

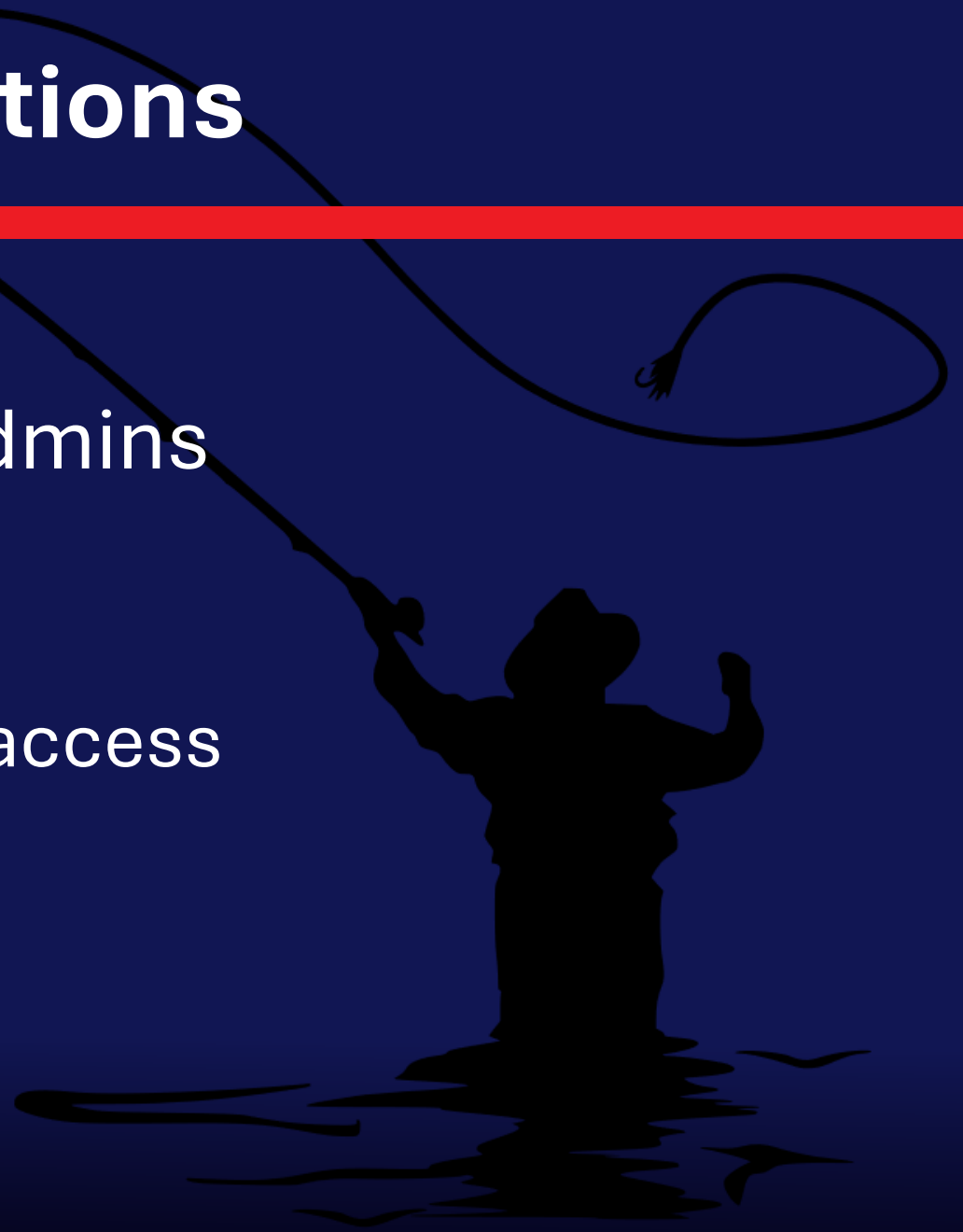
It’s table stakes for Zero Trust

Let’s reset some assumptions

- Privileged access != Global Admin
  - Exchange, SharePoint, Security Reader
  - Custom roles, app permissions, Azure RBAC
  - Privilege sprawl is the real risk

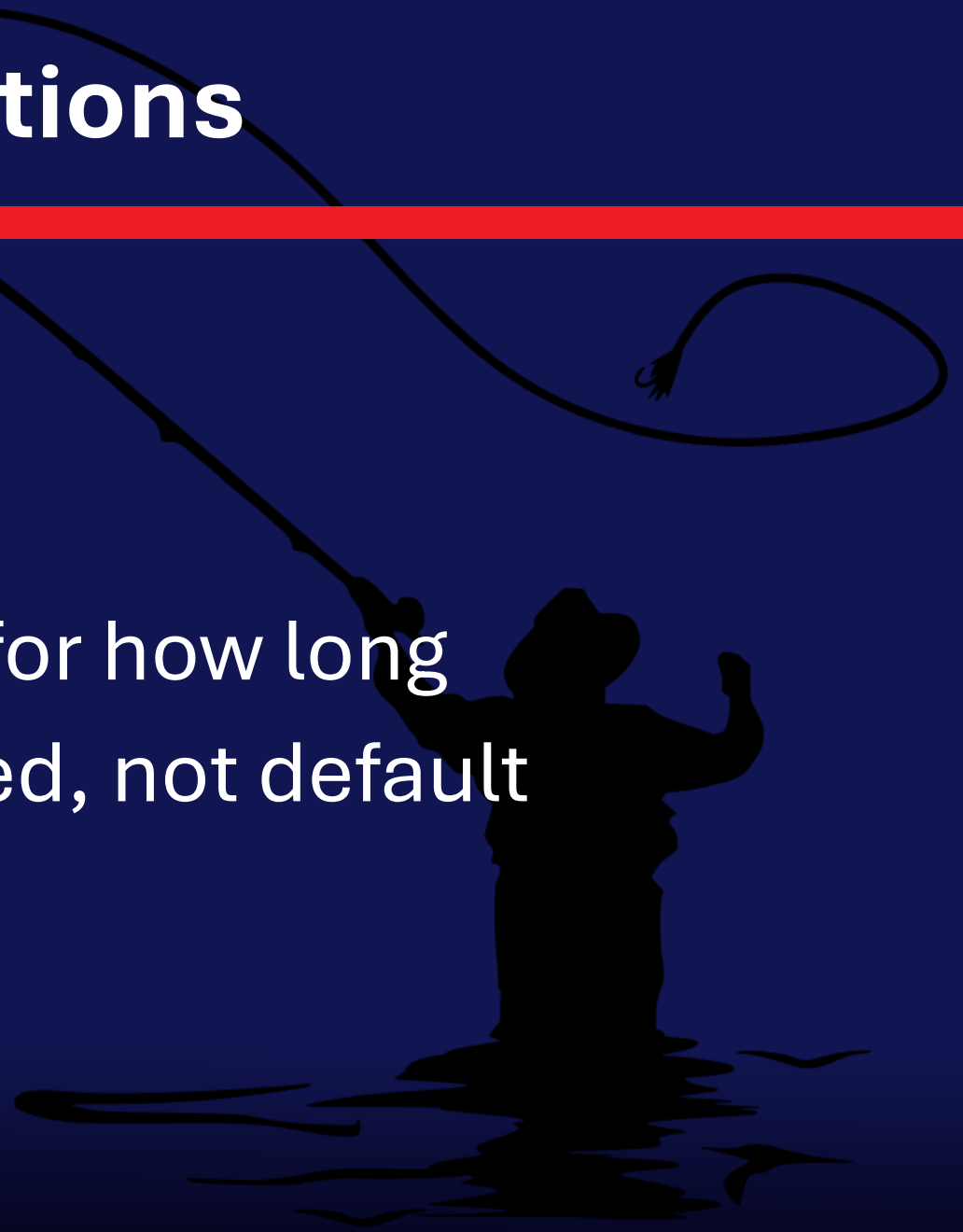
Let’s reset some assumptions

- Most breaches don’t start as admins
  - Over-privileged users
  - Long-lived role assignments
  - Forgotten emergency or project access



Let’s reset some assumptions

- PIM is not “MFA on admins”
- It’s a governance control
- Controls who, when, why, and for how long
- Makes privilege exception-based, not default



How Attacks Actually Happen

Step 1

- User is phished using a targeted or opportunistic trap
- Auth token is stolen

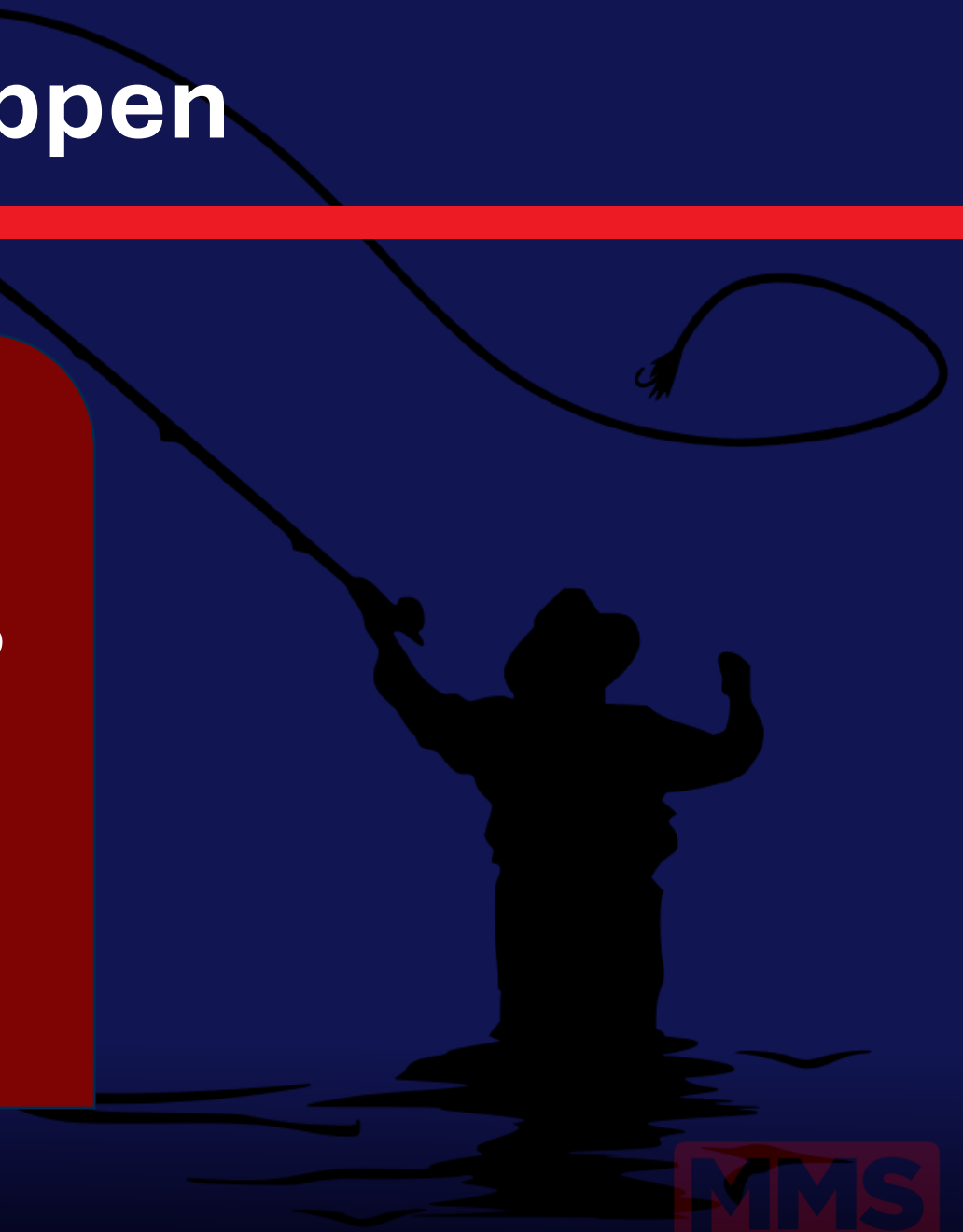
How Attacks Actually Happen

Step 1

- User is phished using a targeted or opportunistic trap
- Auth token is stolen

Step 2

- Attacker replays the auth token to successfully sign into a resource



How Attacks Actually Happen

Step 1

- User is phished using a targeted or opportunistic trap
- Auth token is stolen

Step 2

- Attacker replays the auth token to successfully sign into a resource

Step 3

- Existing permissions are abused

Assignments vs Activations vs Role Settings

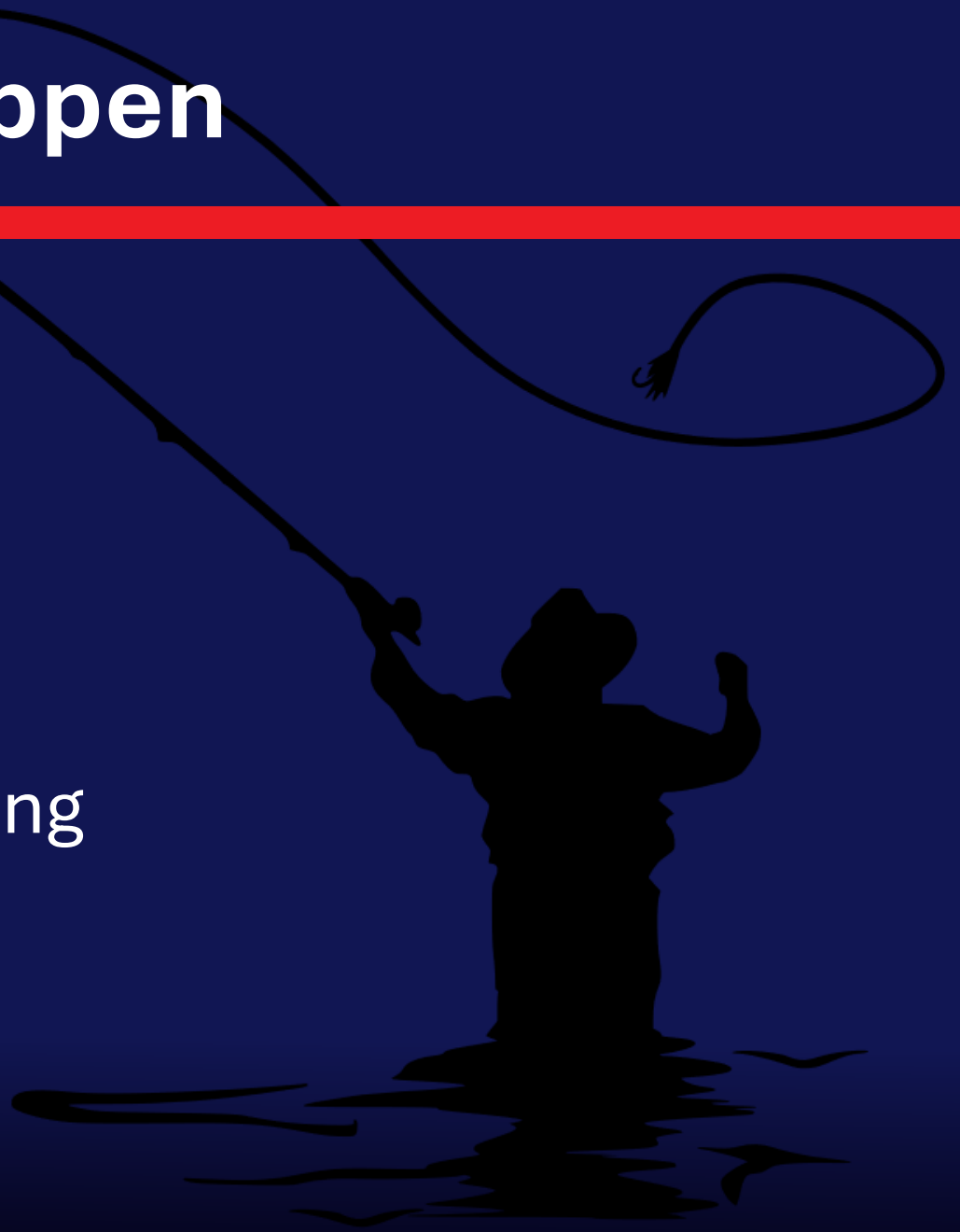
Step 4

- Roles are used to persist, escalate, or exfiltrate

➞ No exploit
➞ No zero-day
➞ Just too much access for too long

How Attacks Actually Happen

- Where PIM fits
  - Removes standing privilege
  - Limits blast radius
  - Forces intent and accountability
  - Adds time-boxed access + auditing



PIM in the Entra Security Stack

Control layer, not a bolt-on

- PIM complements — it doesn't replace
  - Conditional Access
  - MFA & phishing-resistant auth
  - Identity Protection
  - Access Reviews

Think of PIM as:

The "seatbelt" for privileged access— you don't notice it until it saves you

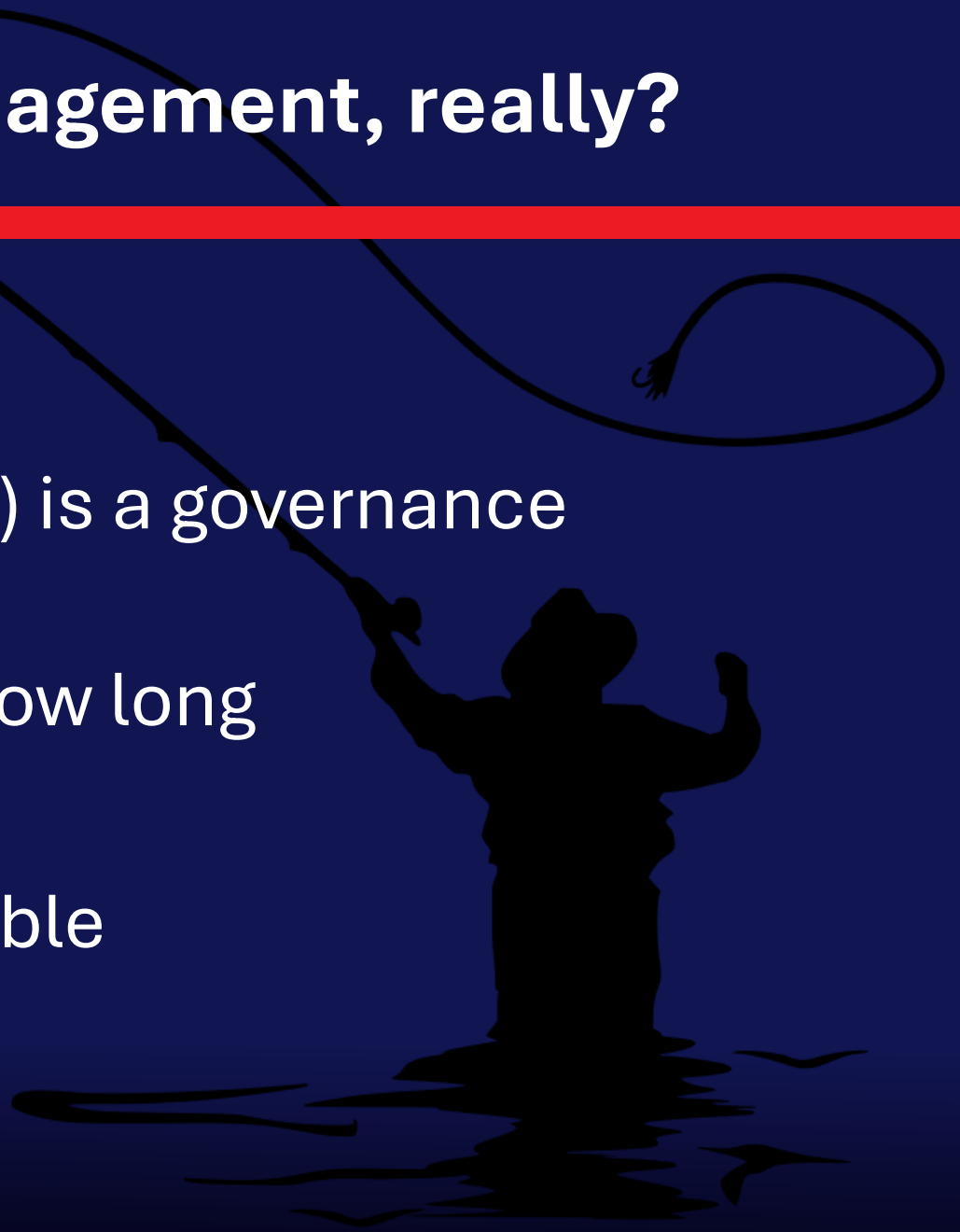
PIM Fundamentals (The Mental Model)

“How PIM actually works (and where people go wrong)”

What is Privileged Identity Management, really?

Privileged Identity Management (PIM) is a governance system

- Controls who, when, why, and for how long
- **Removes standing privilege**
- Makes elevation explicit and auditable



Eligible vs Active: the single most important concept

Eligible = you may activate

Active = you are elevated right now

Activation is:

- Time-bound
- Logged
- Optionally approved
- Optionally re-authenticated

“Eligible != admin — until activation happens”

Assignments vs Activations vs Role Settings

Assignments

- Who can activate
- User or group based
- Permanent or time-bound

Activiations

- Just-in-time
- User initiated
- Duration, justification, approval, reauth

Role Settings

(Pim Policies)

- MFA or step-up auth
- Activation duration
- Approval required?
- Notifications
- Applies to all assignments for that role

What PIM can protect (scope matters)

PIM Does

Microsoft Entra ID Roles
Azure RBAC Roles
PIM for Groups Membership
Ownership

PIM Does Not

Replace Conditional Access
Secure Non-Privileged Access
Fix Bad Role Design

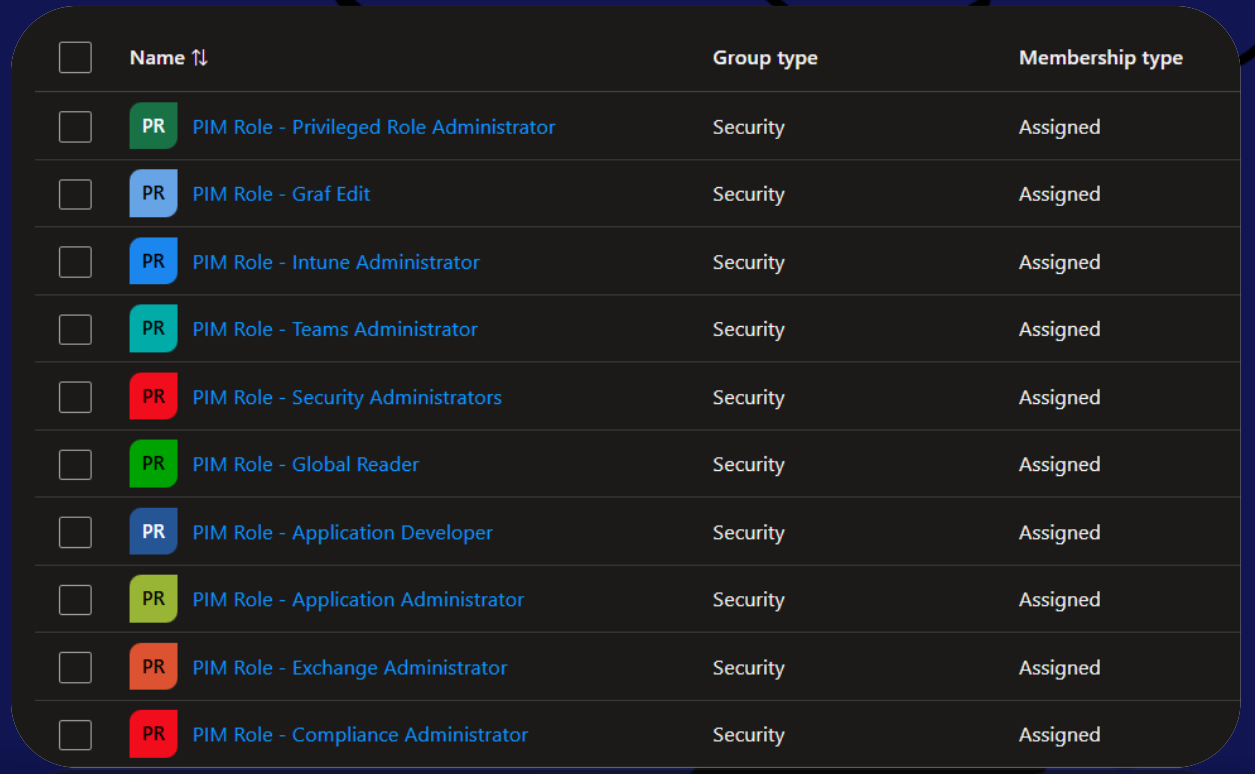
Why PIM for Groups exists (and why you should care)

Group-based assignment = Scale

One policy → Many Users

- Enables:
  - Intune granular admin access
  - Azure access
  - App roles
  - Custom RBAC

- Anti-pattern (avoid):
- Direct user → role assignments

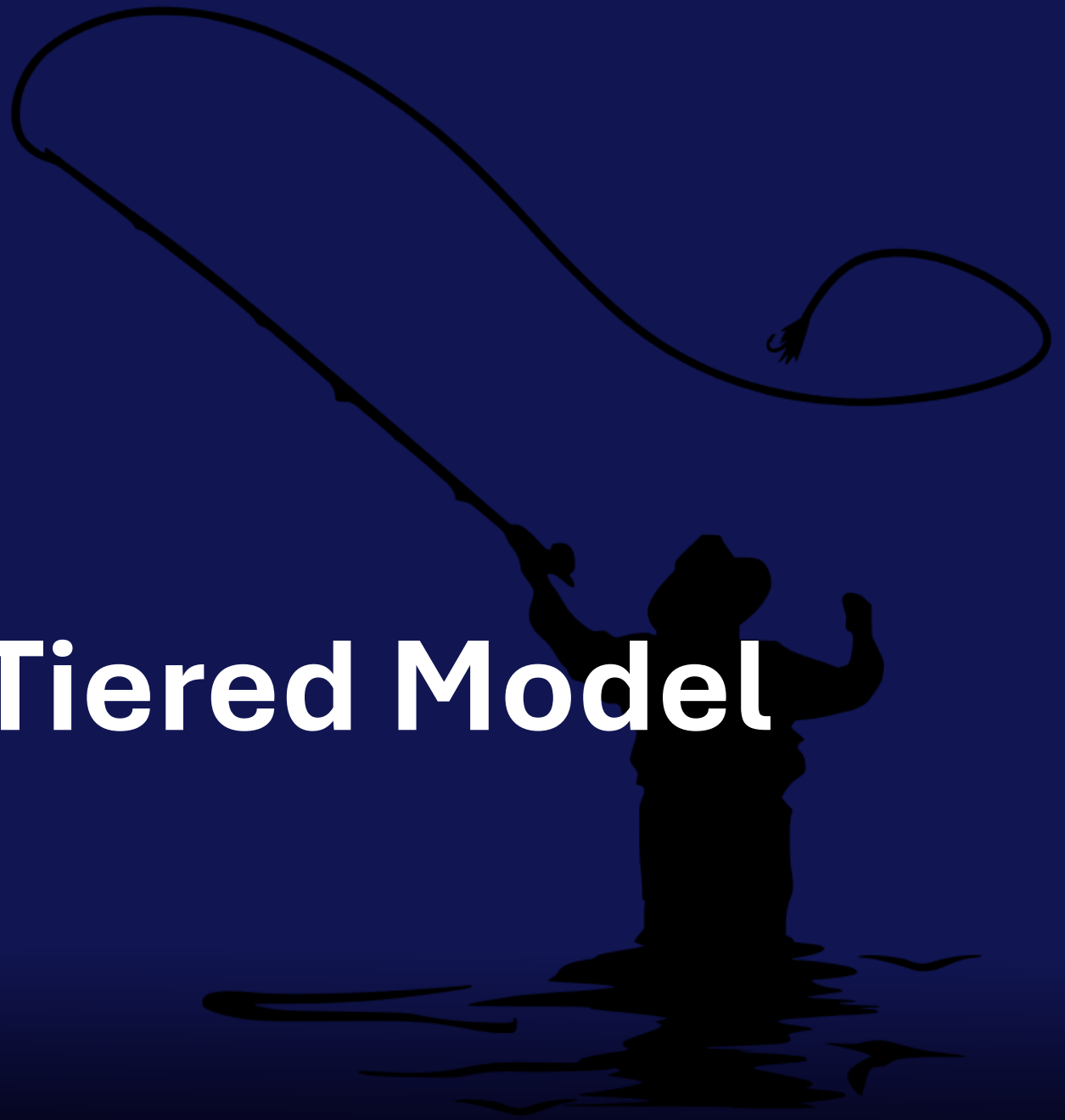


Name ⇅	Group type	Membership type
PIM Role - Privileged Role Administrator	Security	Assigned
PIM Role - Graf Edit	Security	Assigned
PIM Role - Intune Administrator	Security	Assigned
PIM Role - Teams Administrator	Security	Assigned
PIM Role - Security Administrators	Security	Assigned
PIM Role - Global Reader	Security	Assigned
PIM Role - Application Developer	Security	Assigned
PIM Role - Application Administrator	Security	Assigned
PIM Role - Exchange Administrator	Security	Assigned
PIM Role - Compliance Administrator	Security	Assigned

DEMO

Clean PIM Setup the Right Way

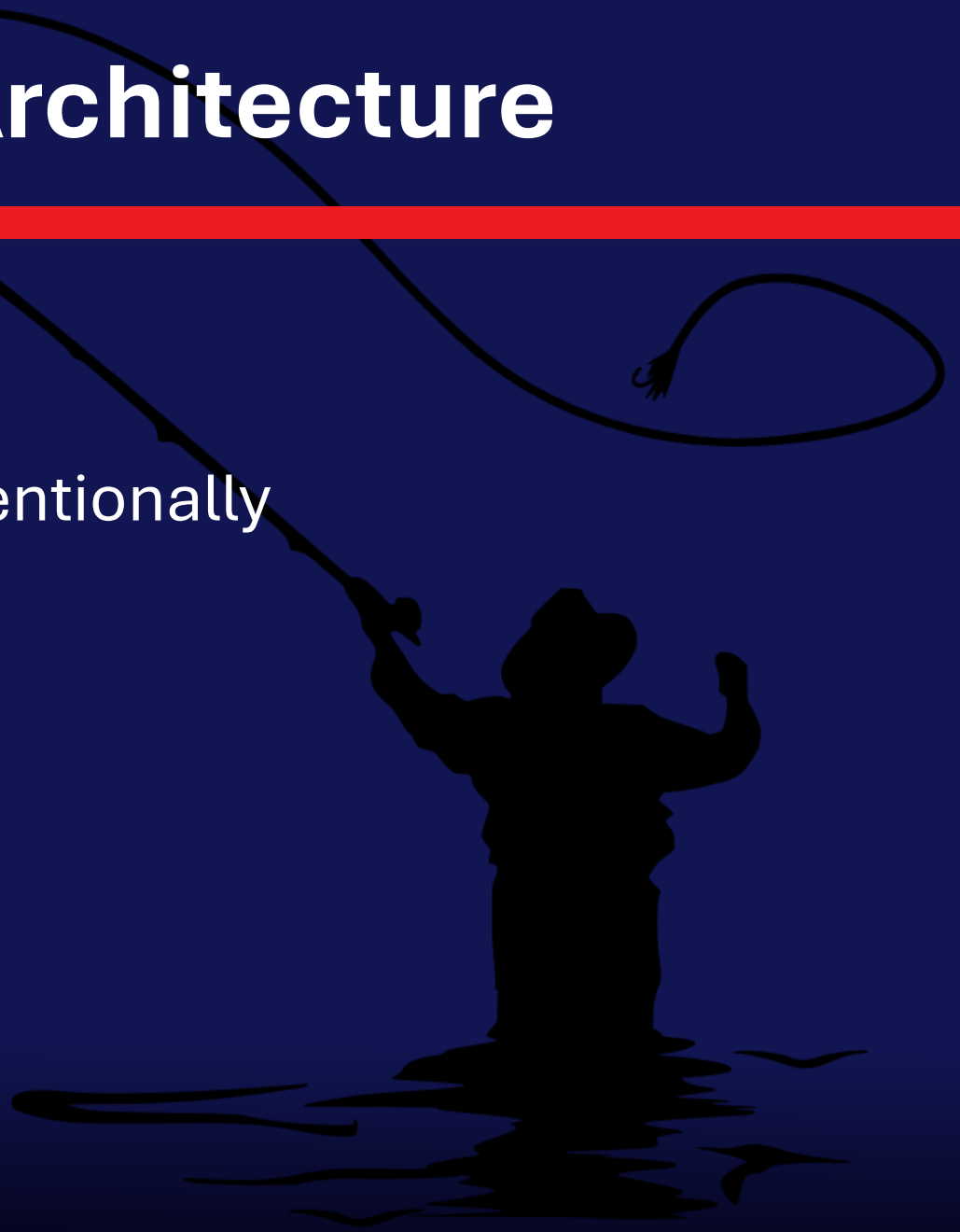
Architecture & Tiered Model



Designing a Secure PIM Architecture

PIM is powerful — but only if designed intentionally

- Not all roles are equal
- Not all admins need the same controls
- Architecture beats tuning every time



Tiered Privileged Access Model

Not all privileged roles carry the same risk

Tier 0 – Tenant control

- Global Admin
- Privileged Role Admin

Tier 1 – Service & security control

- Intune, Exchange, Security Admin

Tier 2 – Scoped or operational roles

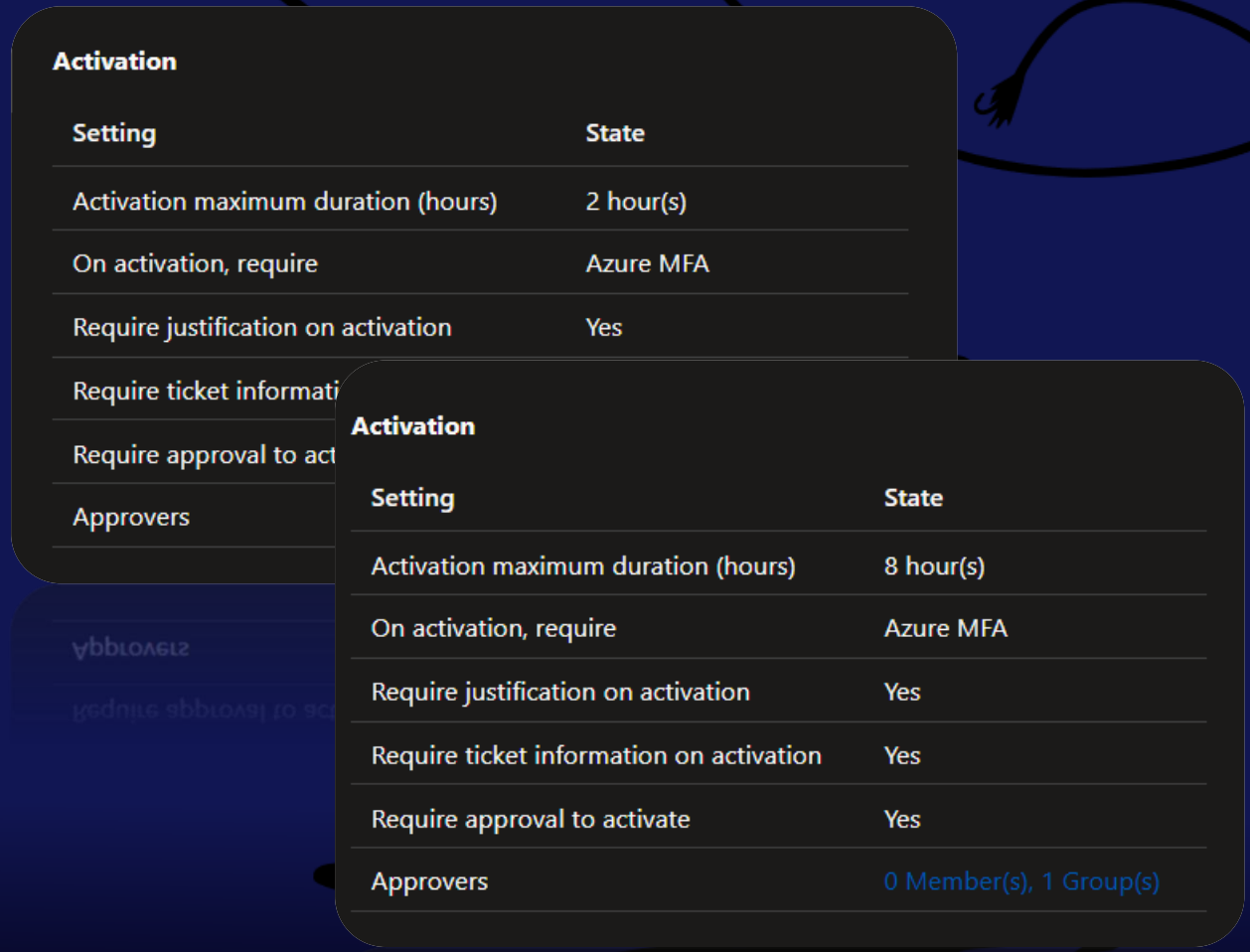
- User, App, Groups Admin

PIM Policy by Tier (Best Practice)

Tier 0
- Short duration
- Approval required
- Step-up / phishing-resistant auth

Tier 1
- Moderate duration
- Strong MFA
- Optional approval

Tier 2
- Longer duration
- MFA enforced
- Low friction



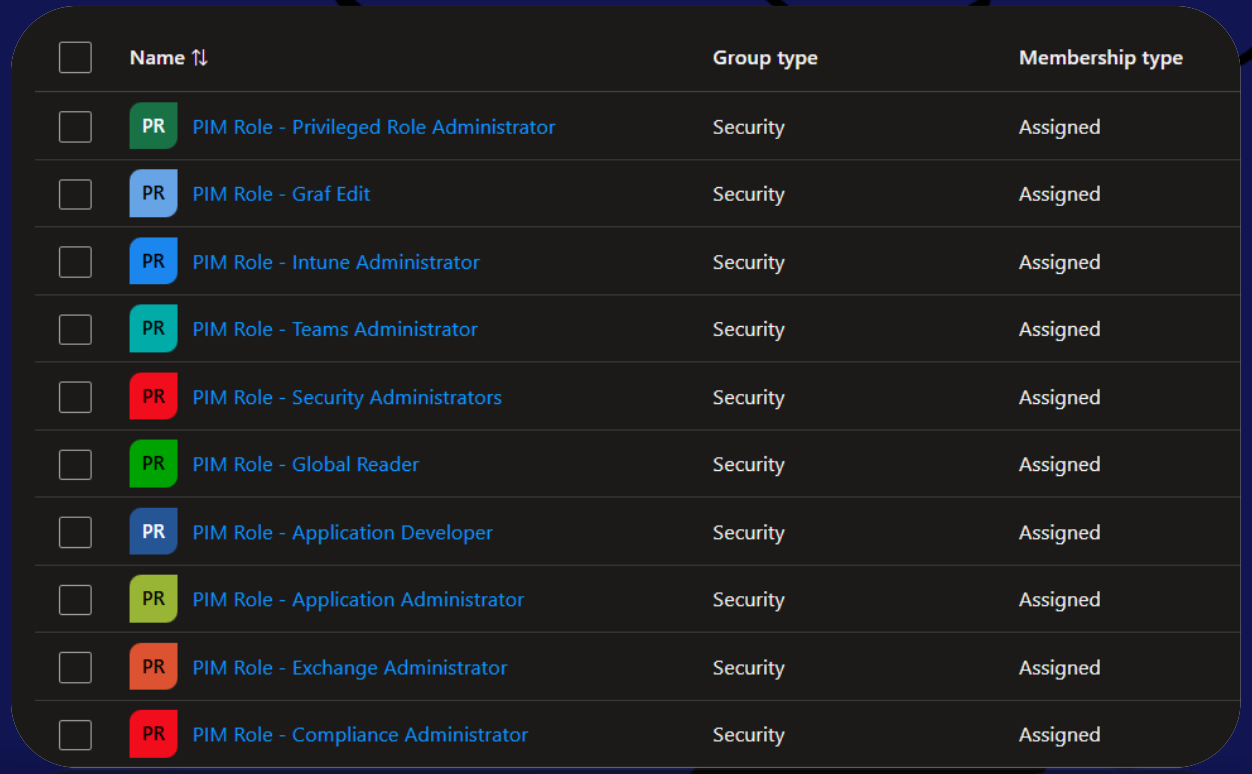
Group-Based PIM Architecture

Groups are the scaling mechanism

- Role-assignable groups
- Cloud-only
- One group → one role → one policy

Avoid:

- Direct user → role assignment
- Synced Administrators



Name ⇅	Group type	Membership type
PIM Role - Privileged Role Administrator	Security	Assigned
PIM Role - Graf Edit	Security	Assigned
PIM Role - Intune Administrator	Security	Assigned
PIM Role - Teams Administrator	Security	Assigned
PIM Role - Security Administrators	Security	Assigned
PIM Role - Global Reader	Security	Assigned
PIM Role - Application Developer	Security	Assigned
PIM Role - Application Administrator	Security	Assigned
PIM Role - Exchange Administrator	Security	Assigned
PIM Role - Compliance Administrator	Security	Assigned

OVER-PRIVILEGED ASSIGNMENT OF ENTRA ID ROLES FOR A SINGLE USER

One user. Too many roles. Massive blast radius.

POTENTIAL IMPACT

- Full tenant compromise
- Data exfiltration
- Privilege escalation
- Persistence & backdoors
- Lateral movement

Too much privilege in one account = Full tenant at risk

RIGHT-SIZED ACCESS

One user. Only the roles they need.

BENEFITS

- Limited blast radius
- Reduced risk of compromise
- Easier to audit & monitor
- Stronger security posture

Right access. Right role. Right protection.

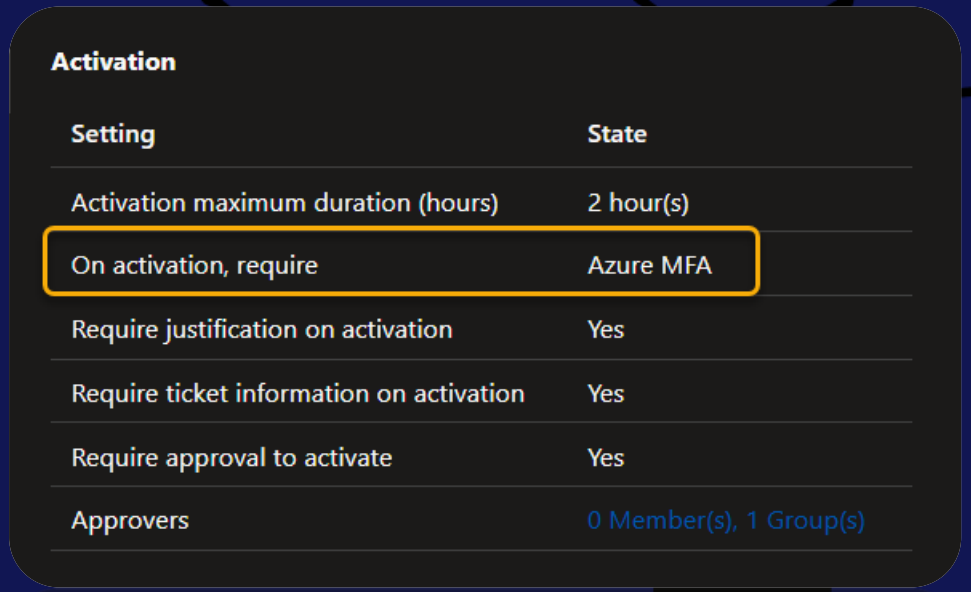
Review and right-size Entra ID role assignments regularly. Follow least privilege. Use PIM for just-in-time access.

Step-Up Authentication & Reauthentication

MFA ≠ Fresh Authentication

Modern PIM supports:

- Authentication Contexts
- Conditional Access re-evaluation
- **Per-role auth strength**



Goal:

Fresh authentication for sensitive elevation

How Step-Up Works (Conceptually)

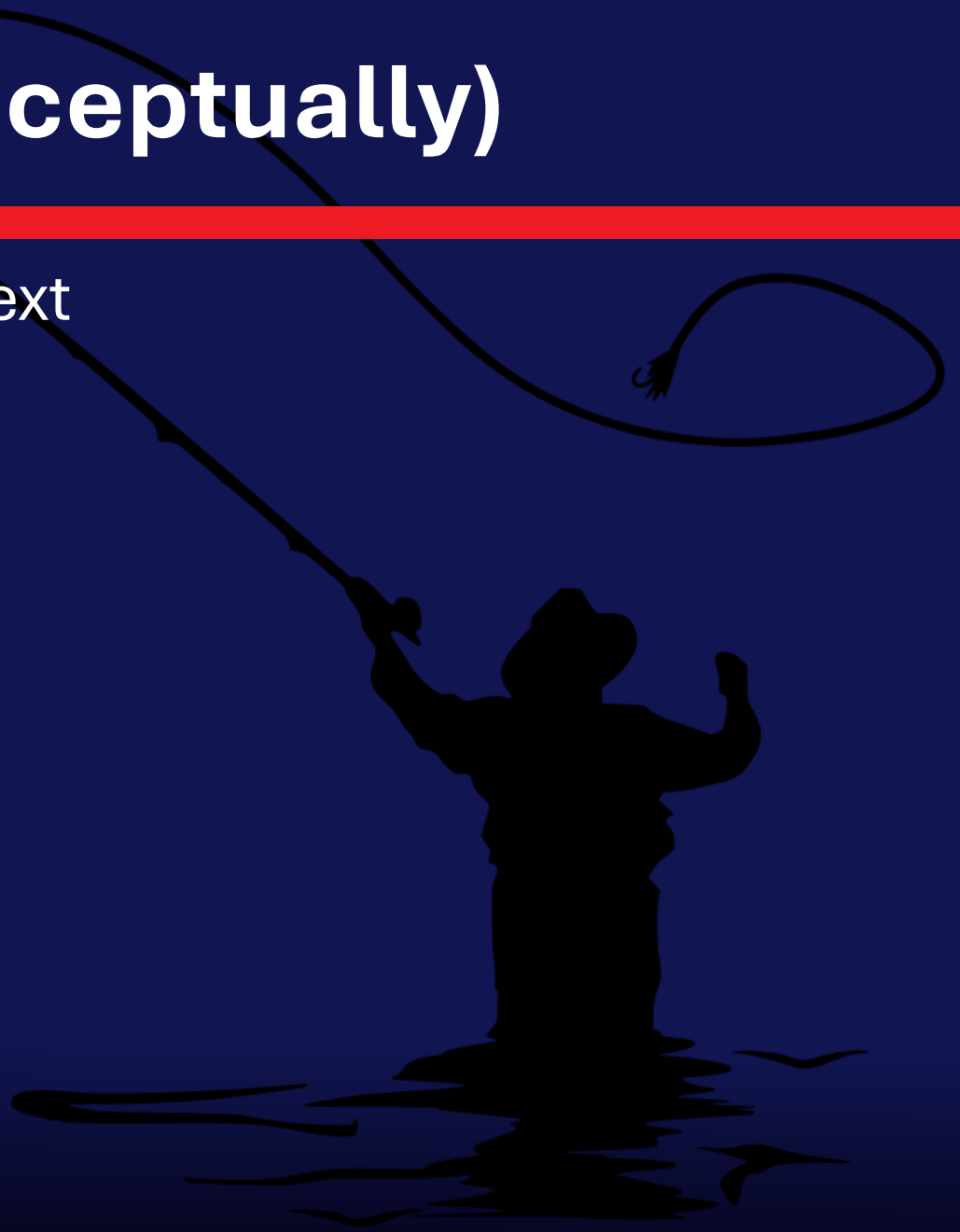
Activation triggers an authentication context

Conditional Access enforces:

- Re-sign-in
- Stronger method
- Phishing-resistant auth if required

Result:

- Role activation = new trust boundary

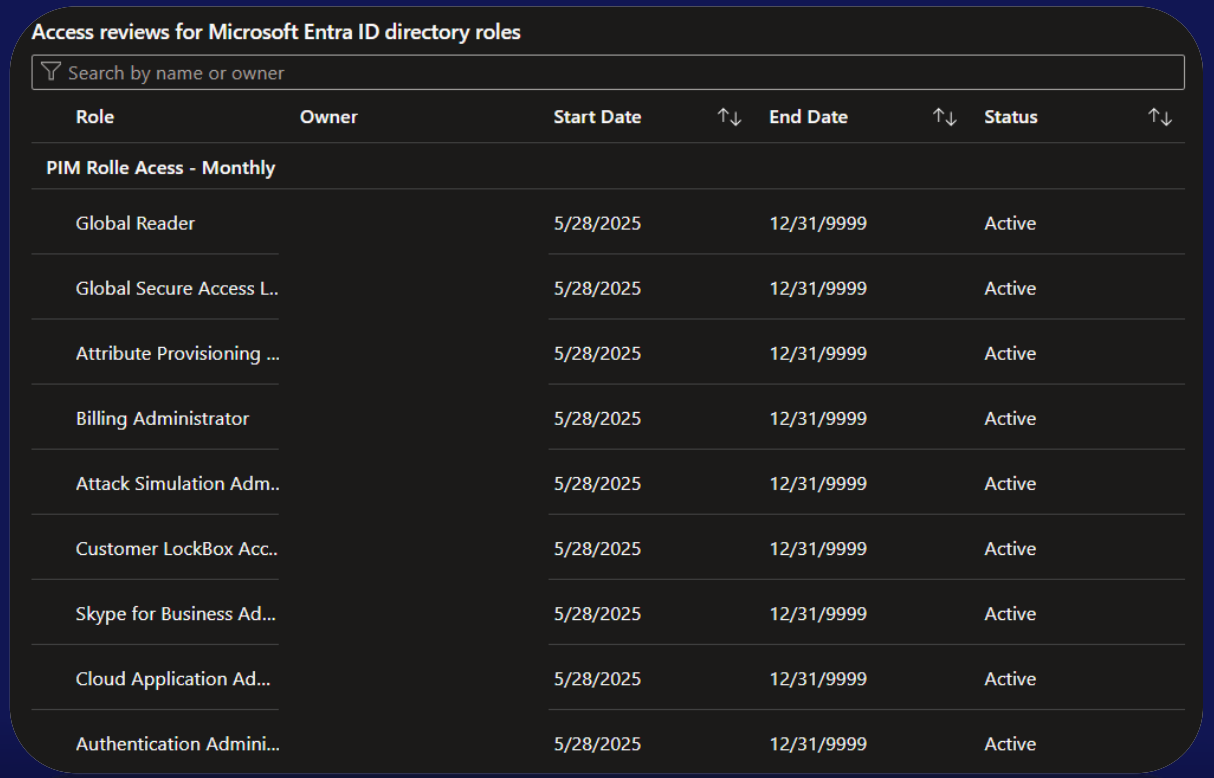


DEMO

“Sign-in Every Time” for Tier-0

MMS

Governance: Keeping PIM Healthy



PIM is not “set and forget”

Governance controls:

- Access Reviews
- Approval workflows
- Alerts & notifications
- Audit & logs

DEMO

Access Reviews

CloudWay

Azure Active Directory is now Microsoft Entra ID. Learn More.

Reminder: Please review access to the AZ-Role-Intune Administrator in the CloudWay

Jan Ketil Skanke, your organization requested that you approve or deny continued access to the **AZ-Role-Intune Administrator** group in the **Intune Administrator Access Quarterly Review** review. The review period will end on **May 2, 2026**.

Start review >

Learn how to perform an access review and more about Microsoft Entra access reviews.

Intune Administrator Access Quarterly Review

Please review assignment to 'AZ-Role-Intune Administrator' See details

Approve | Deny | Don't know | Reset decisions | Accept recommendations | filter

	Name ↑	Recommendation	Decision	Reviewed by	
○	[redacted]	Approve	Approved	Jan Ketil Skanke	Details
○		Approve	Approved	Jan Ketil Skanke	Details
○		Approve	Approved	Jan Ketil Skanke	Details

Sharepoint Administrator Access | Overview

Overview

Current

Results

Reviewers

Settings

Audit logs

Series

Reviewers

Settings

Scheduled review

Review history

Audit logs

Delete series

Group	: AZ-Role-SharePoint Administrator
Access review period	: 04/05/2022 - No end date
Object Id	: 86eed551-5cc6-49b8-af9e-cac419b22135
Scope	: Everyone
Review status	: Active
Selected reviewers	: Selected users
Description	: Sharepoint Admin Access
Recurrence type	: Semi-annually

Current

Not reviewed
0

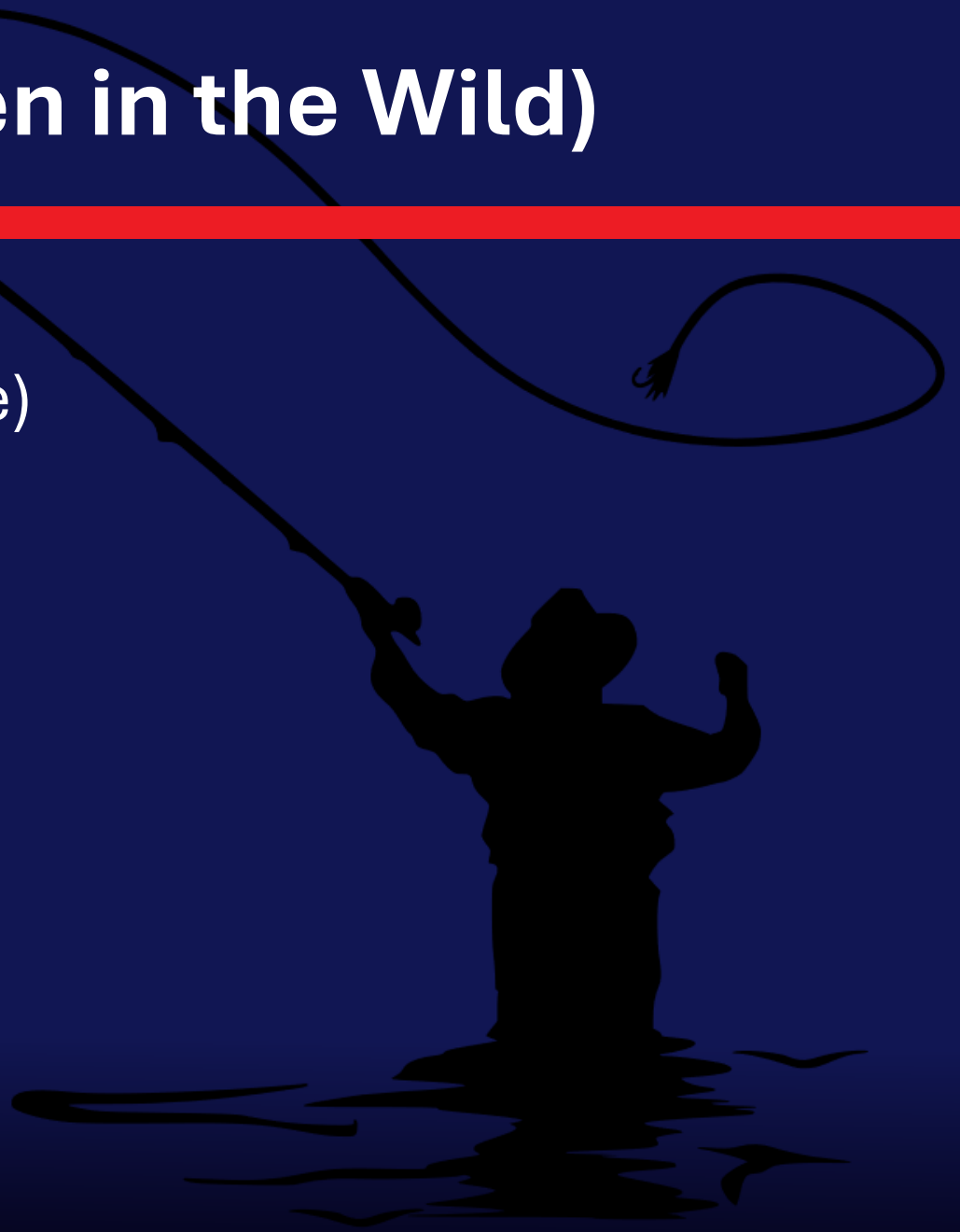
Approved
1

Denied
1

Don't know
0

Common Anti-Patterns (Seen in the Wild)

- Dozens of Global Admins (even if eligible)
- One-size-fits-all role settings
- No reviews of eligibility
- Break-glass used for convenience
- PIM without CA
- Nobody looking at the logs



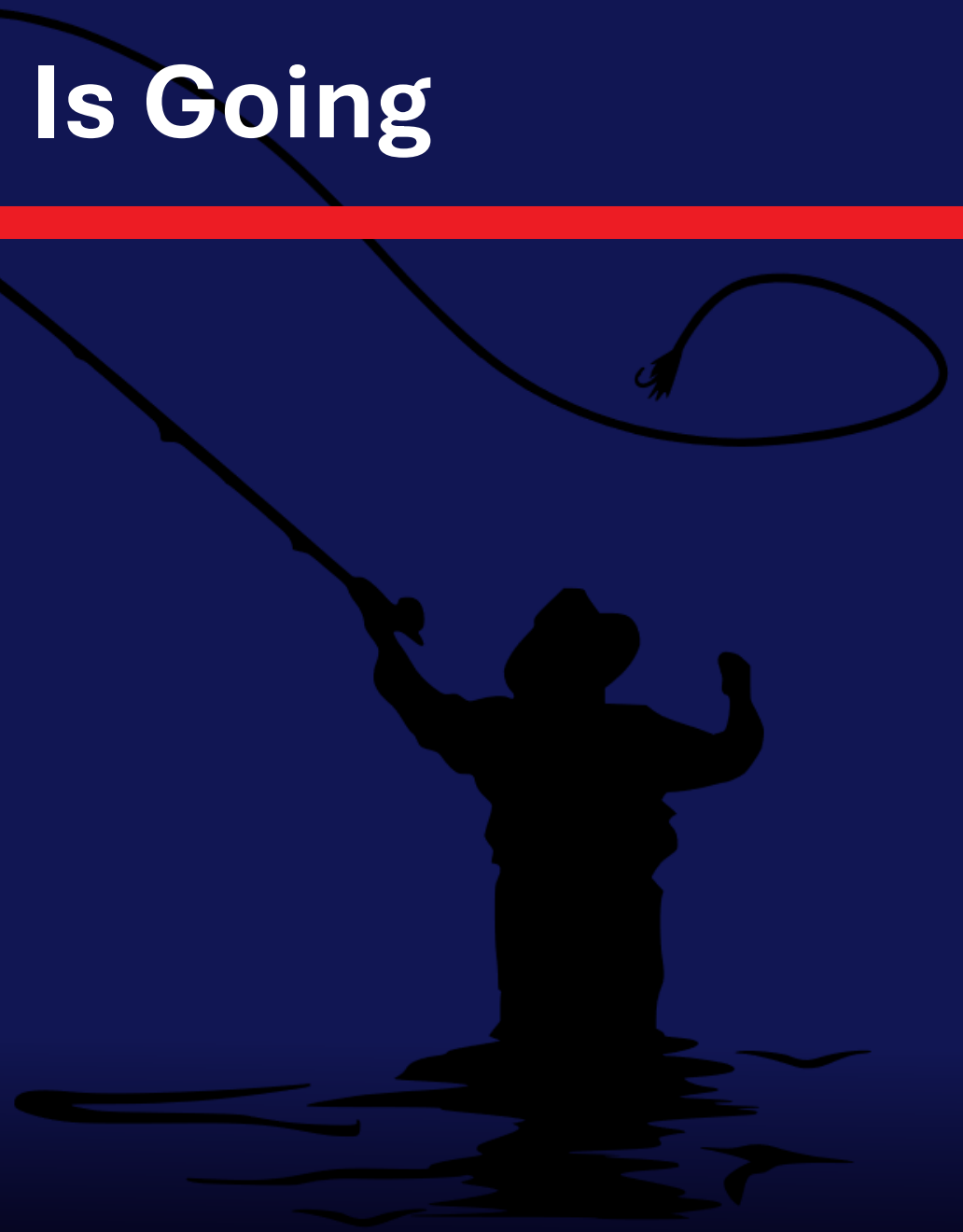
DEMO

PIM Audit Dashboard

What's New & Where PIM Is Going

- Direction from Microsoft:
  - Stronger auth integration
  - Authentication Strengths
  - External MFA support
  - Protected Actions
- Identity Security as control plane

- PIM is becoming foundational



Key Takeaways

- No standing privileged access
- Eligible ≠ Active
- Group-based PIM scales
- Tier-based controls matter
- Step-up authentication is critical

DEMO

Pimportal

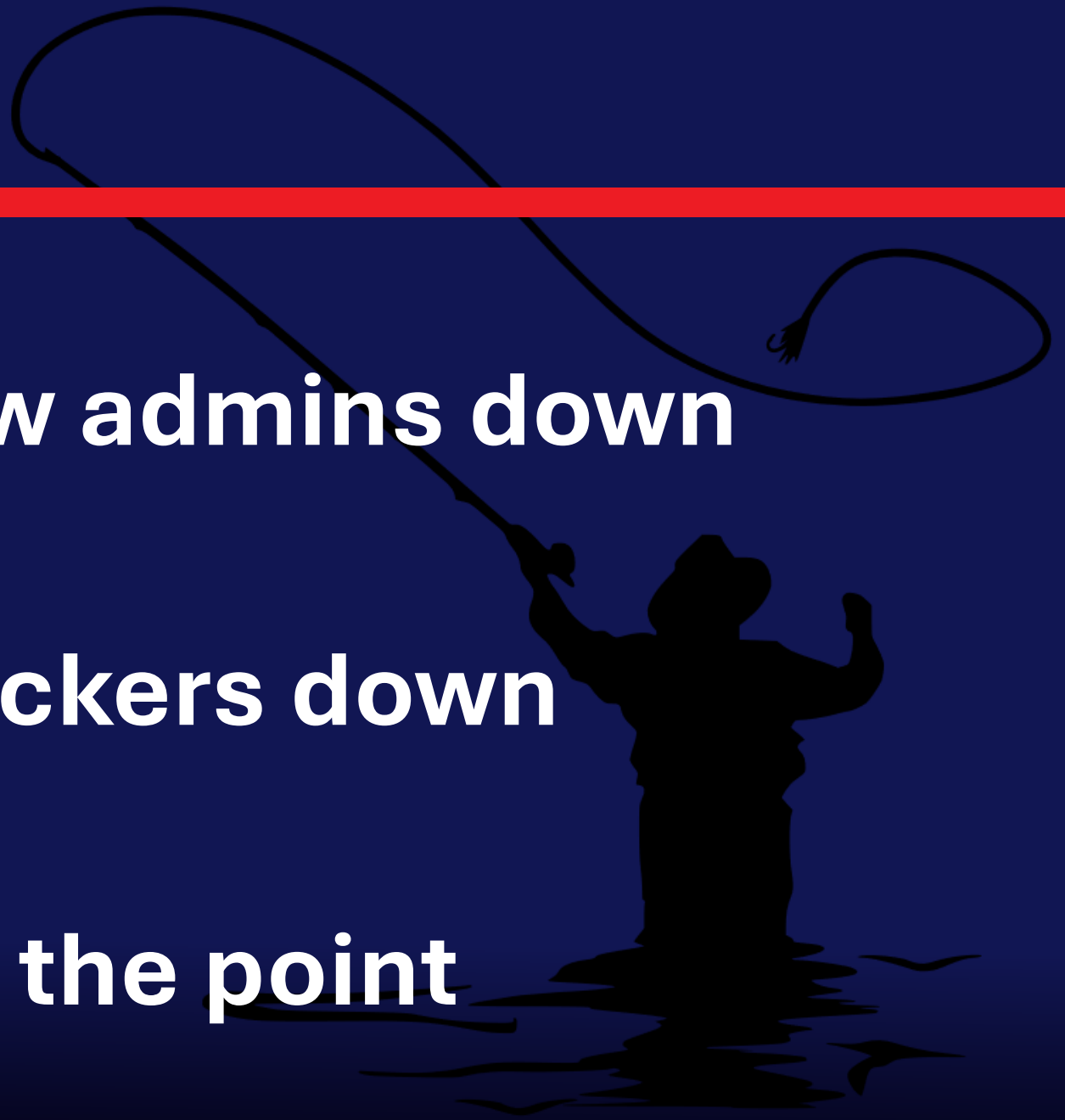
Community Tool

Final Thought

PIM doesn’t slow admins down

It slows attackers down

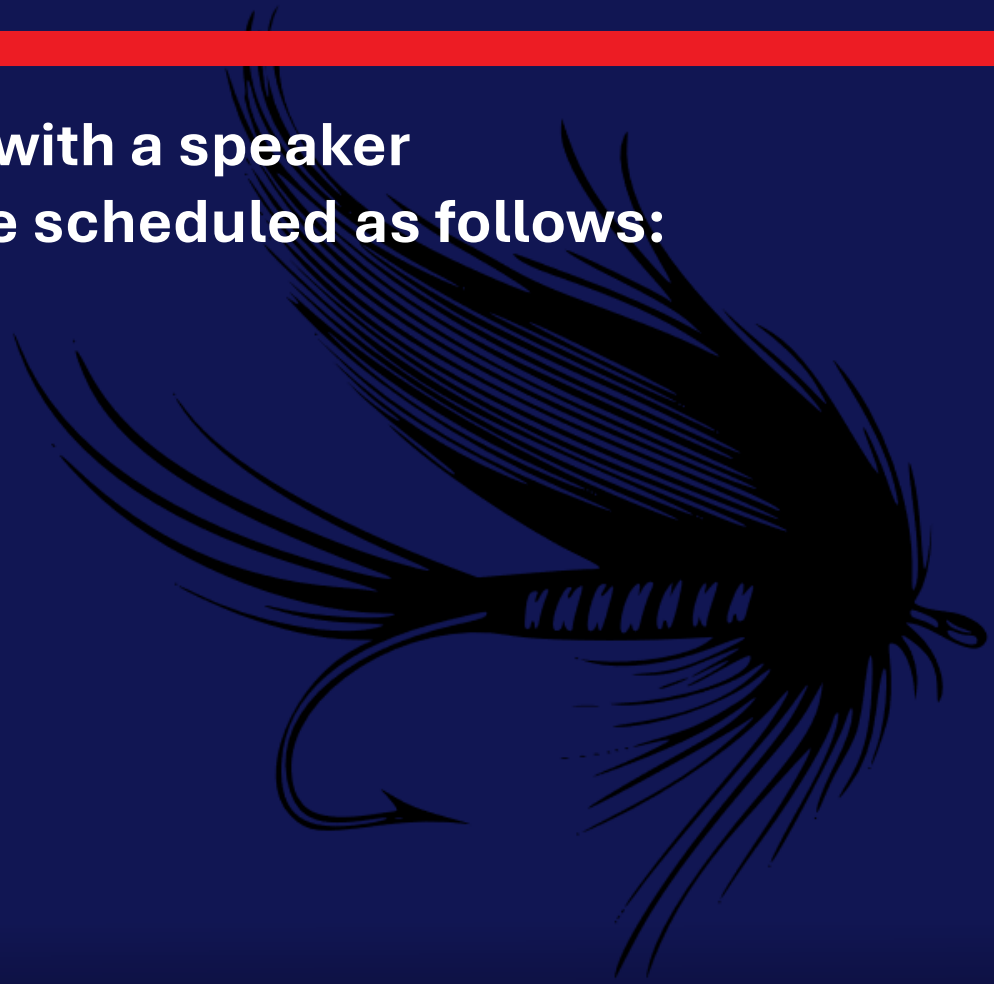
And that’s the point



Fishing Sessions

Be sure to find Wally and sign up for 1:1 time with a speaker
If you'd like to "catch" us for a session, we are scheduled as follows:

- Jan : Tuesday from 10:00 AM -12PM



Don't forget to leave feedback for your speakers!

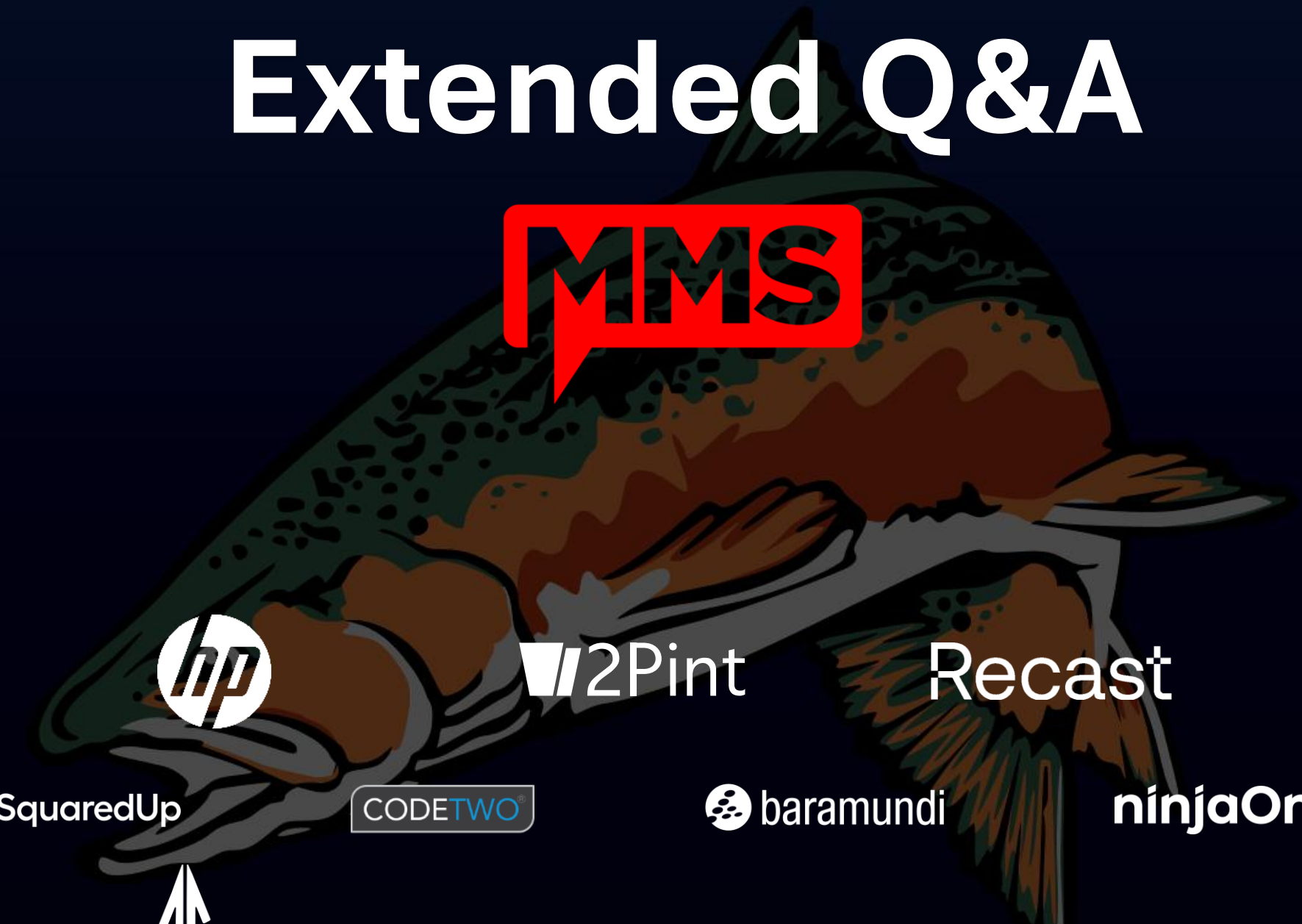
SAVE THE DATES

Oct 25-28, 2026

May 2-6, 2027

Oct 10-13, 2027

Extended Q&A



MMS

PATCH MY PC

hp

2Pint

Recast

robopack
empowered by SOFTWARE CENTRAL

SquaredUp

CODETWO

baramundi

ninjaOne

Rimo3

App Control

TeamViewer

numecent

aiden