semaphore
CONSULTING PARTNERS

IdentityDay 2024

People like us are the reason you need IAM

tailored
SECURITY ASSESSMENT

Agenda

- **Speaker intro**
- **What is penetration testing?**
- **What could possibly go wrong in IAM?**
- **Key points**

semaphore
CONSULTING PARTNERS

Speaker intro

thomas.goytil@semaphore.no

Thomas Gøytil

Semaphore Security expert and penetration tester

- Former software developer turned security professional
- Head of security for SaaS company for 5+ years
- Active bug bounty hunter
- Martial arts enthusiast and passionate lock picker

What is penetration testing?

Our approach to Penetration testing

- **TSA – Tailored Security Assessment**
- **What makes us different**

semaphore
CONSULTING PARTNERS

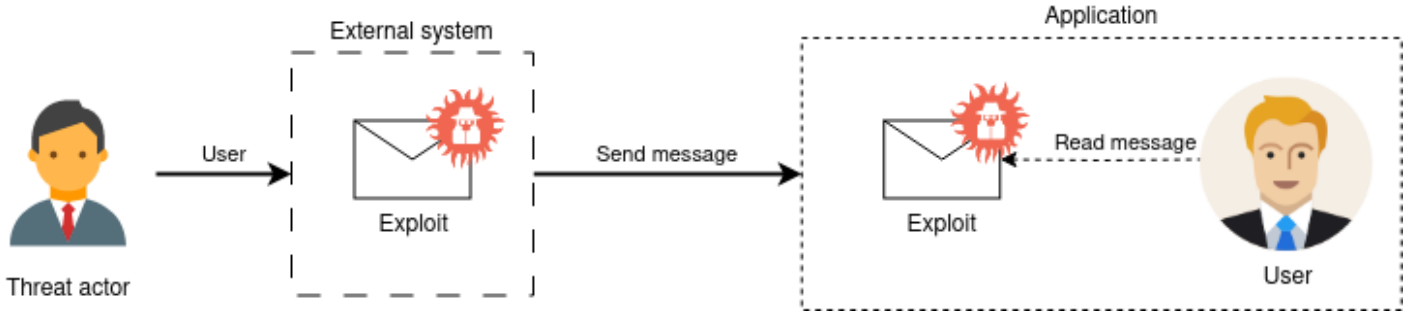
What could possibly go wrong in IAM?

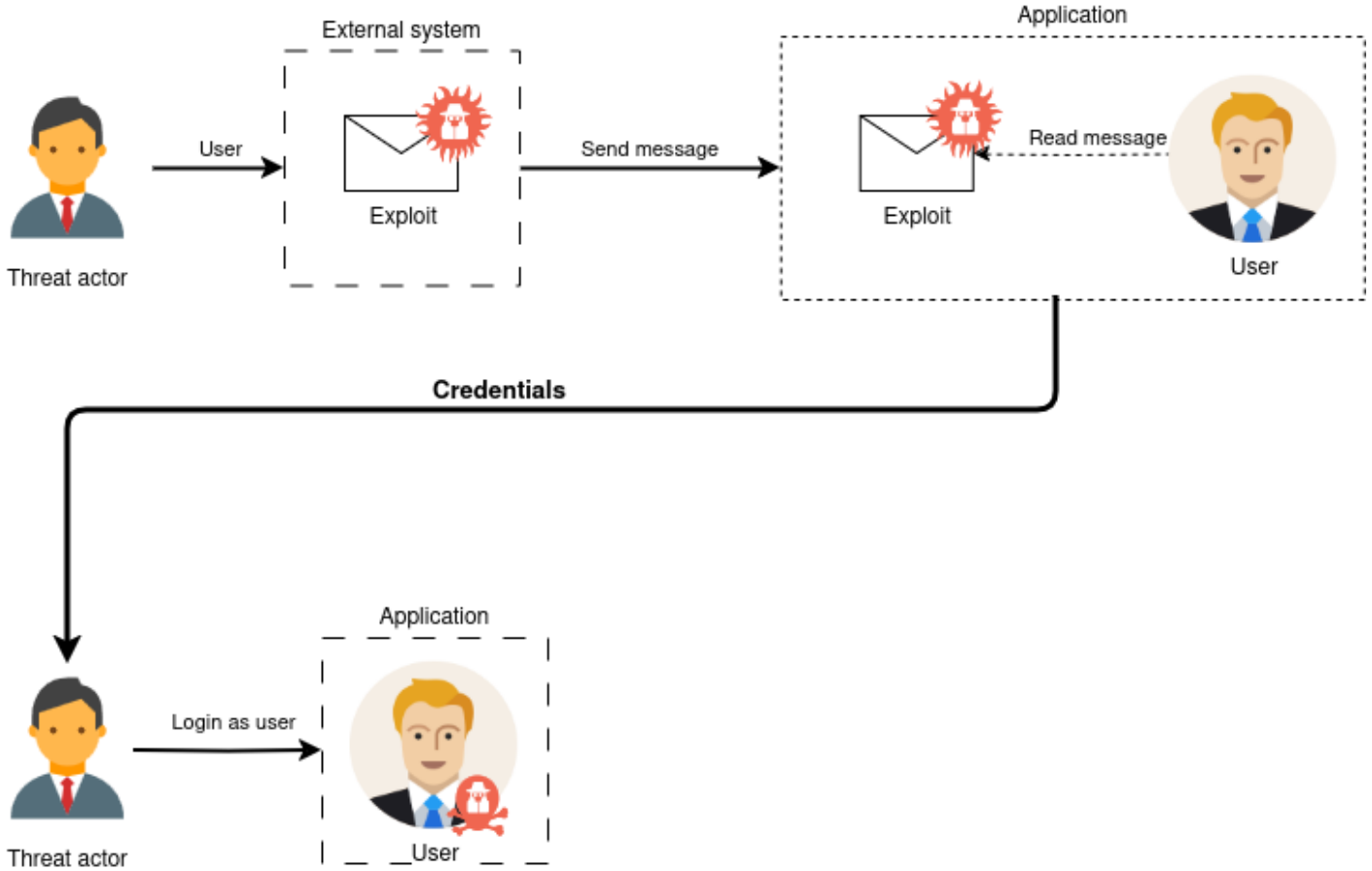
Clients are anonymized
The findings are **real world** examples

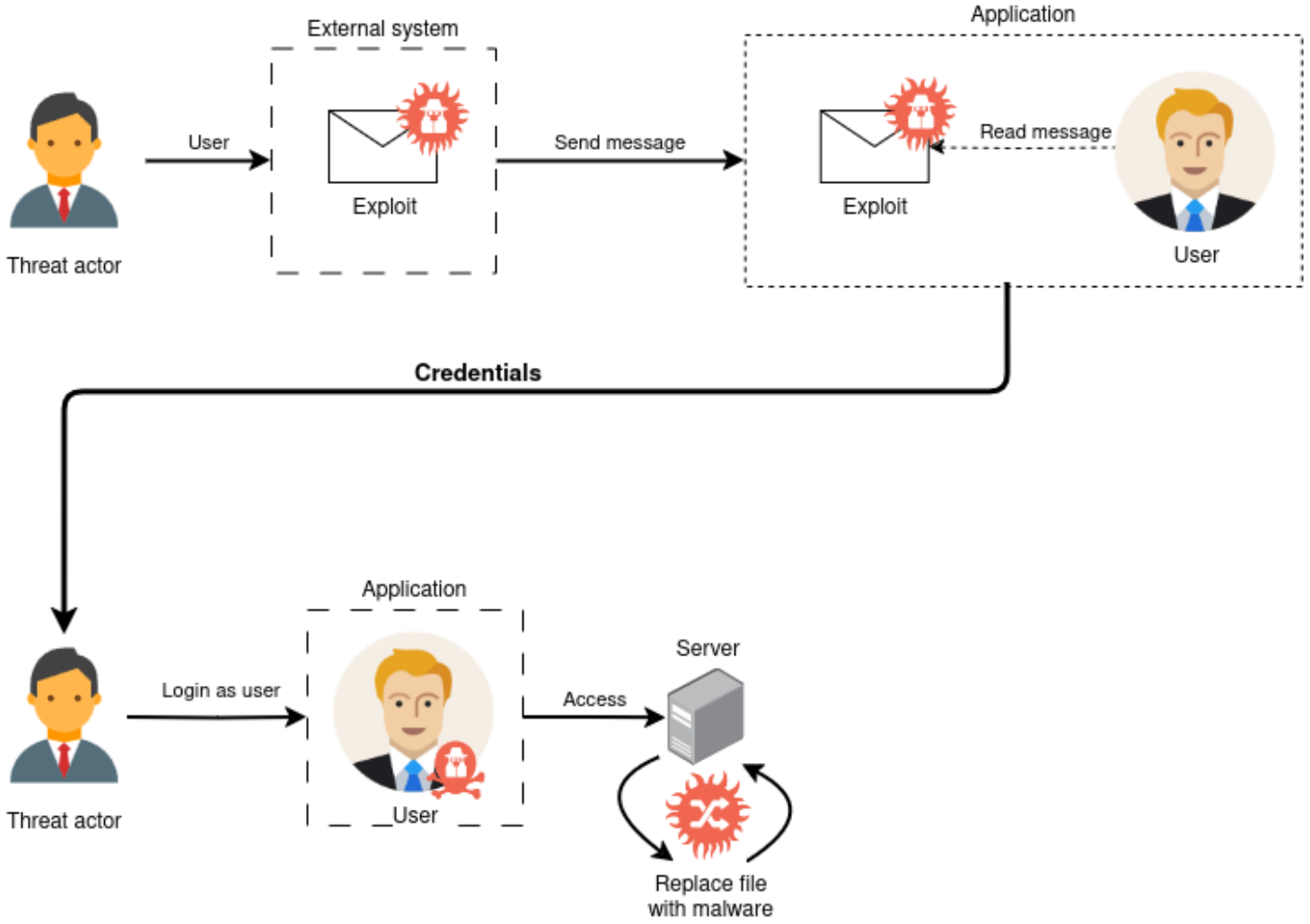
"Crafty tower" - 2024

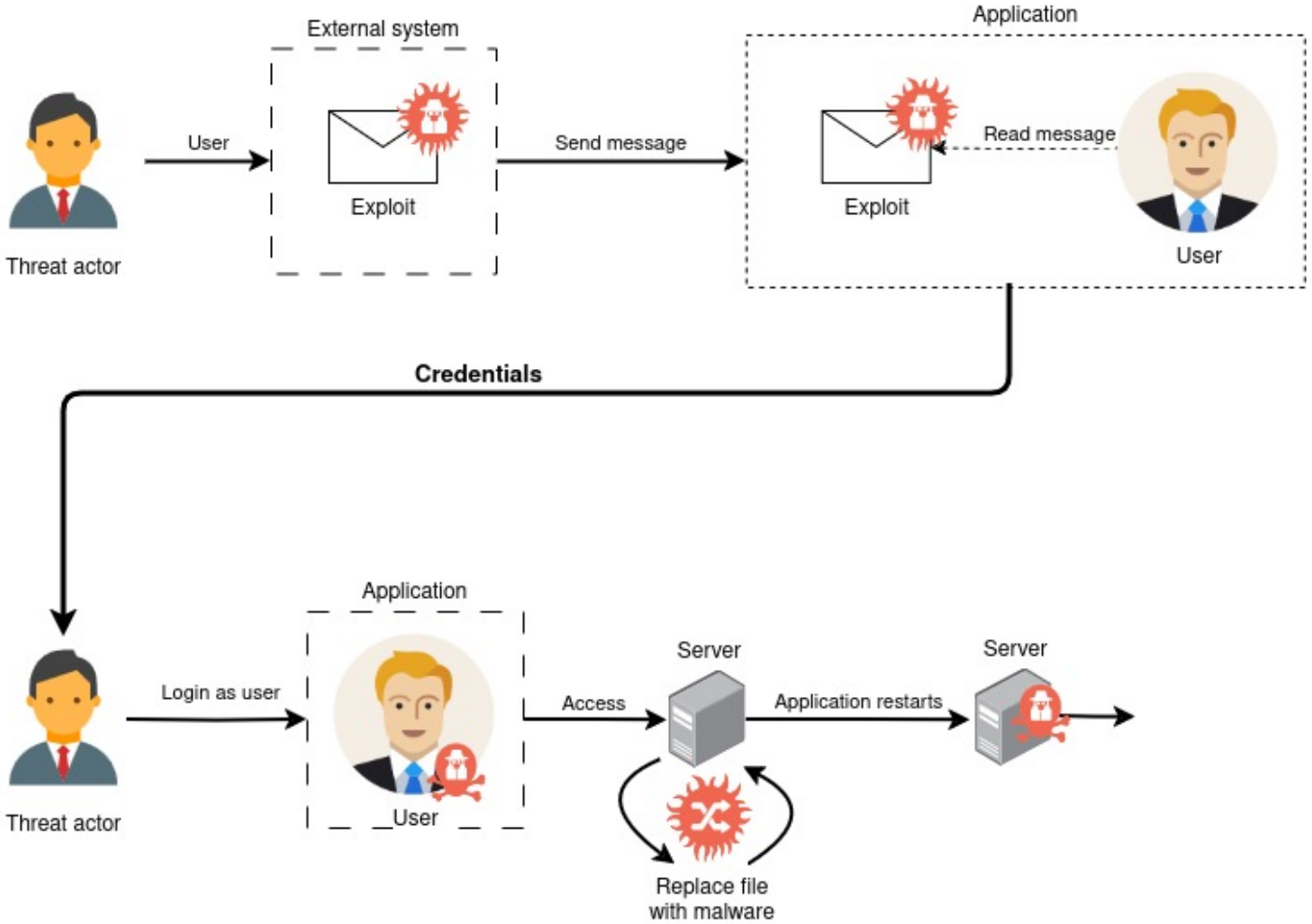
Background

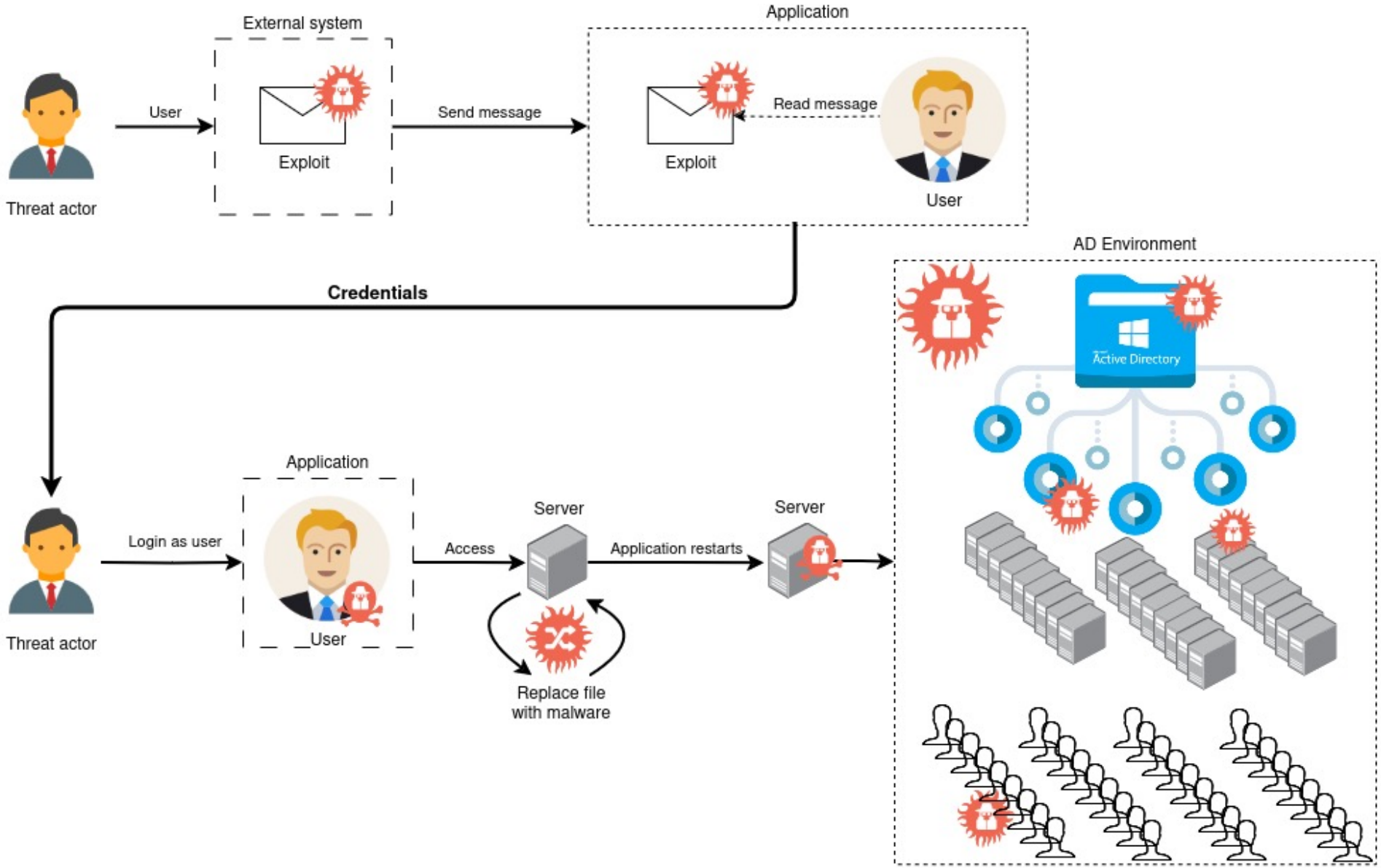
- **First ever** pentest for the client
- A SaaS solution with *some* technical debt
- Infrastructure was close to **best practice**
  - Micro segmentation
  - Fully patched modern operating systems
  - Principle of least privilege (for their database)
- The SaaS solution was *a bit* too permissive …
- IAM fault: Too high permissions


External system
Application
User
Send message
Read message
Exploit
Exploit
Threat actor
User


External system
Application
User
Exploit
Send message
Exploit
Read message
Threat actor
User
Credentials
Application
Login as user
Threat actor
User


External system
Application
User
Send message
Read message
Threat actor
Exploit
Exploit
User
Credentials
Application
Server
Login as user
Access
Threat actor
User
Replace file
with malware


External system
Application
User
Send message
Read message
Exploit
Exploit
Threat actor
User
Credentials
Application
Server
Server
Login as user
Access
Application restarts
Threat actor
User
Replace file
with malware


External system
Application
Threat actor
User
Exploit
Send message
Exploit
Read message
User
AD Environment
Credentials
Active Directory
Application
Server
Server
Threat actor
Login as user
User
Access
Application restarts
Replace file
with malware

"Cool Supernova" - 2023

- Norwegian SMB
- First ever pentest
- “Our MSP guarantees we are protected”
- IAM fault: Lacking segregation of duties/admin

Cool Supernova

1 step away from disaster

Number of IT people: 0

Username: admin

C-suite username: john

Number of domain admins: 17

It’s easier that way!

Password: admin

NO MFA

C-suite password: 1234

semaphore CONSULTING PARTNERS

Hackers don't break into your account..... they **login**

Cool Supernova

1 step away from disaster

Number of IT people: 0

Username: admin

C-suite username: john

Operating system still in use

Number of domain admins: 17

It's easier that way!

Password: admin

NO MFA

C-suite password: 1234

Last changed 2007

Windows XP SP2

semaphore
CONSULTING PARTNERS

Summary

It took **4 hours** to gain domain admin

It took **3 weeks** to work with their MSP to make changes

Most critical change was a **new and robust IAM process**

They are now **at least** 2 steps away from disaster!

semaphore
CONSULTING PARTNERS

IAM in cloud is easy.....

"Beginner's guide to AWS IAM policies"

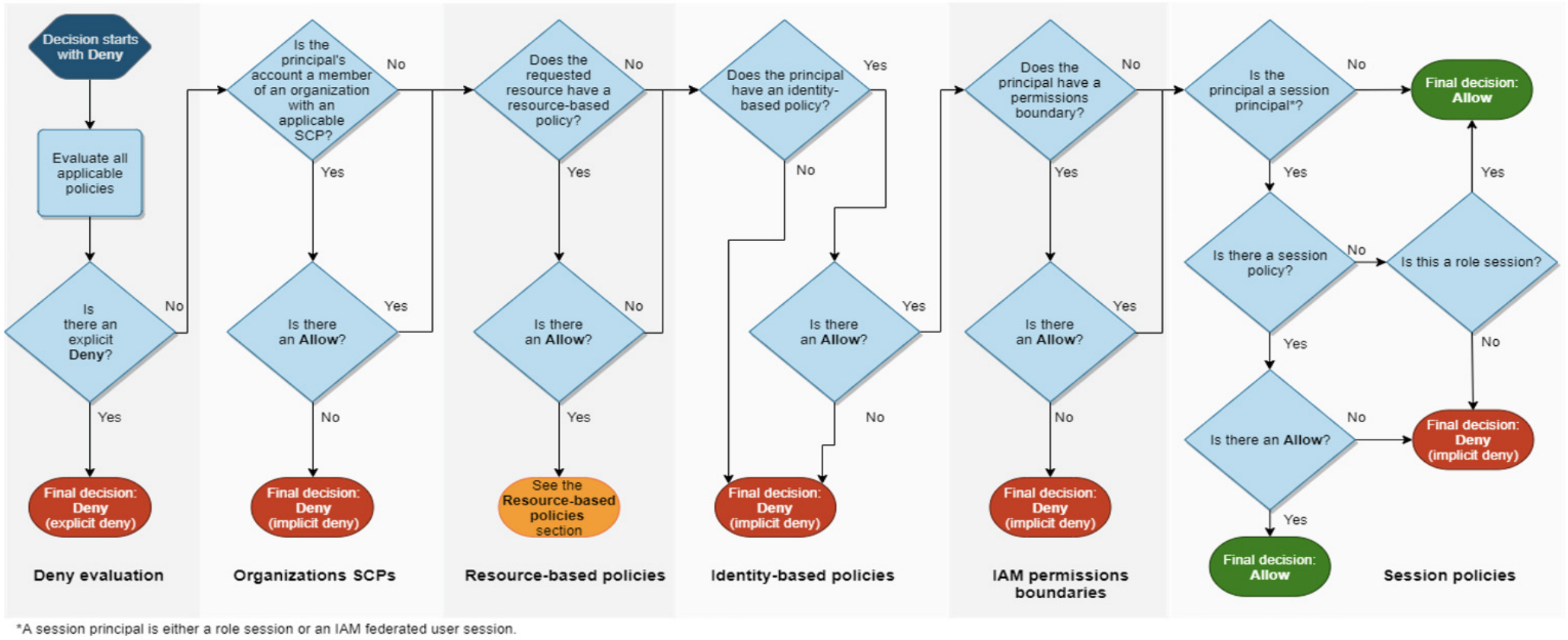


Figure 1: Authorization flow

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

Azure SP to cloud takeover

IAM fault: Overprivileged Identities

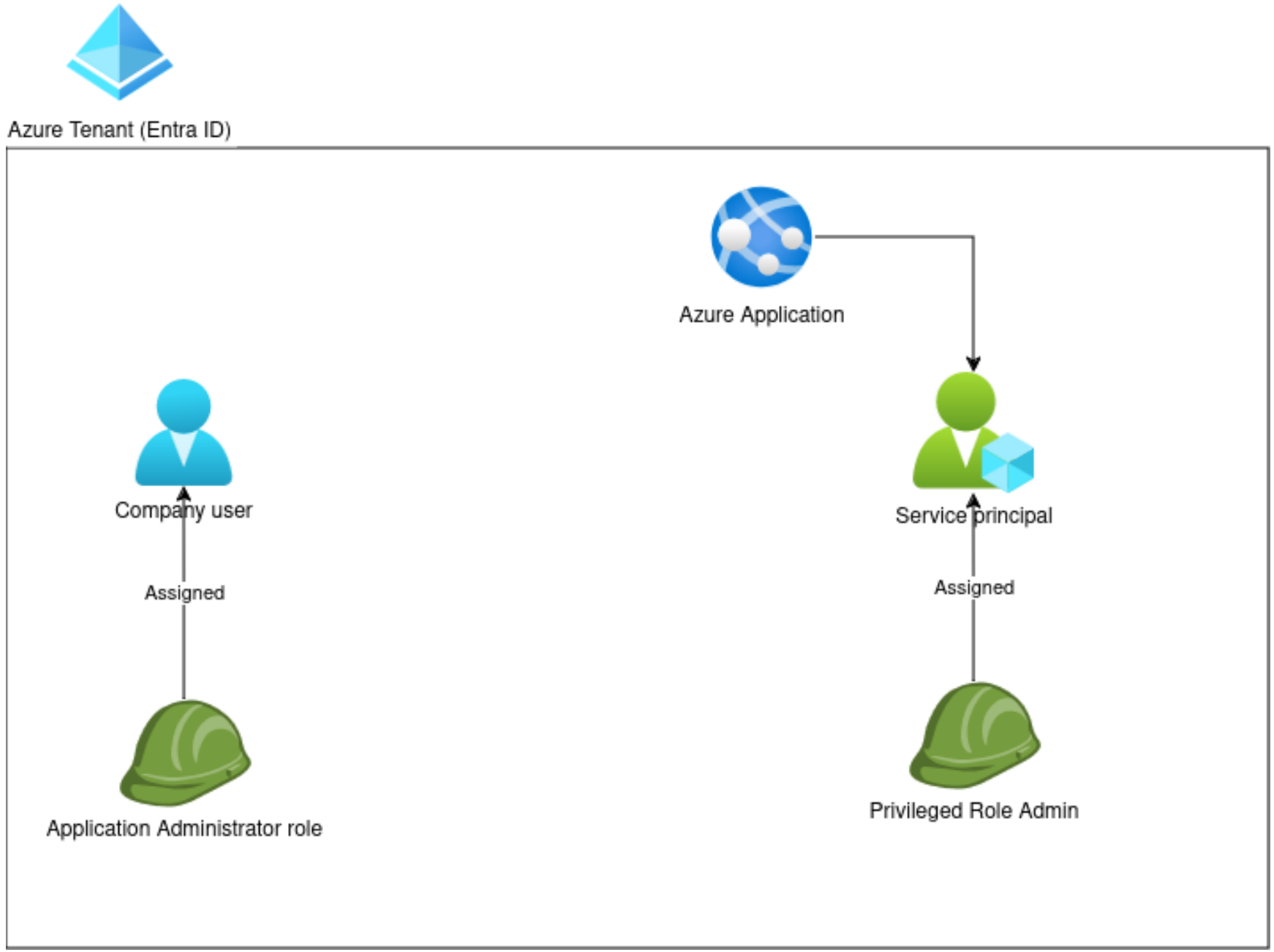
Azure intro

Azure terminology

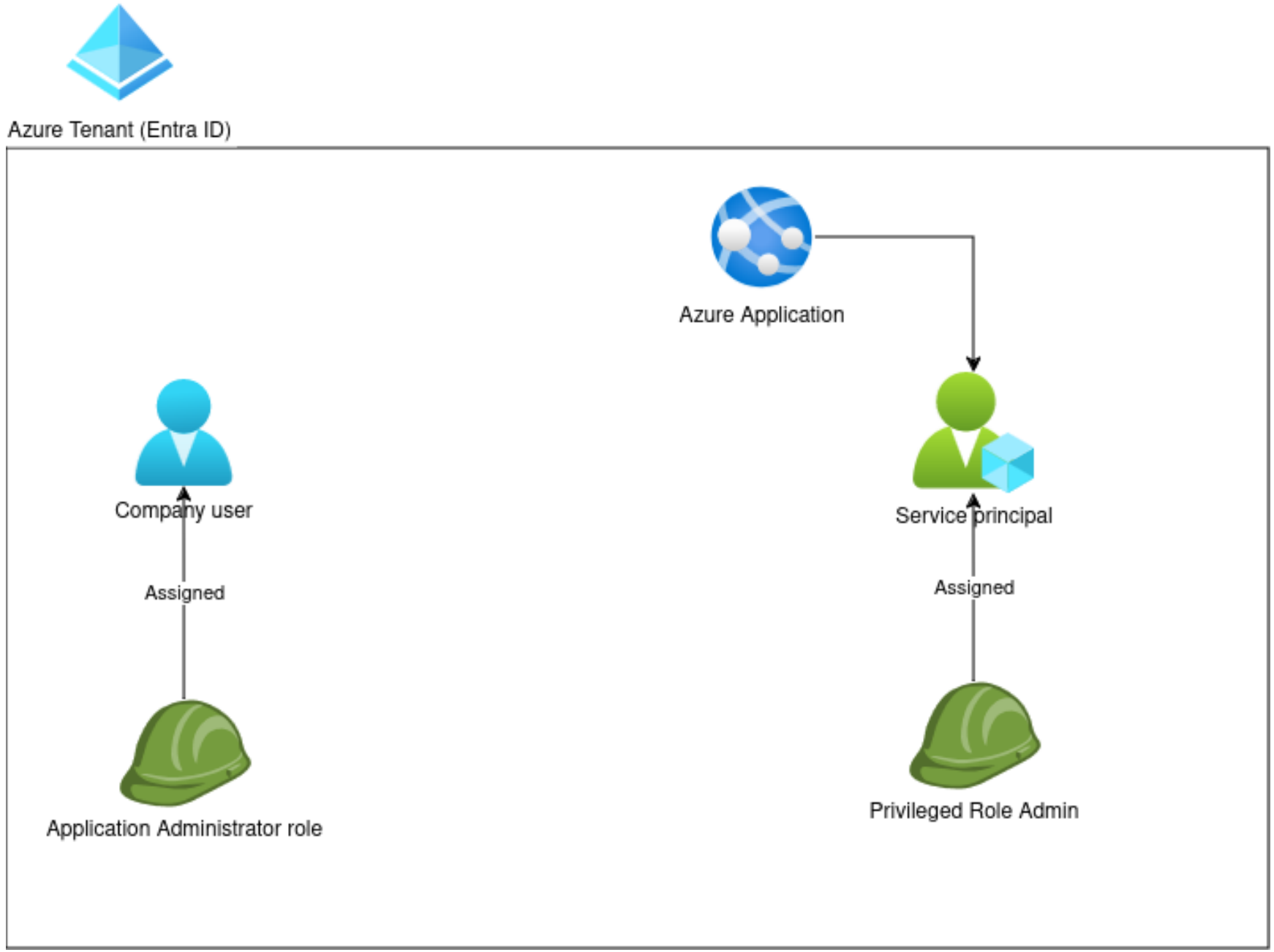
- Azure Tenant
- Azure User
- Azure application
  - Application Object
  - Service principal

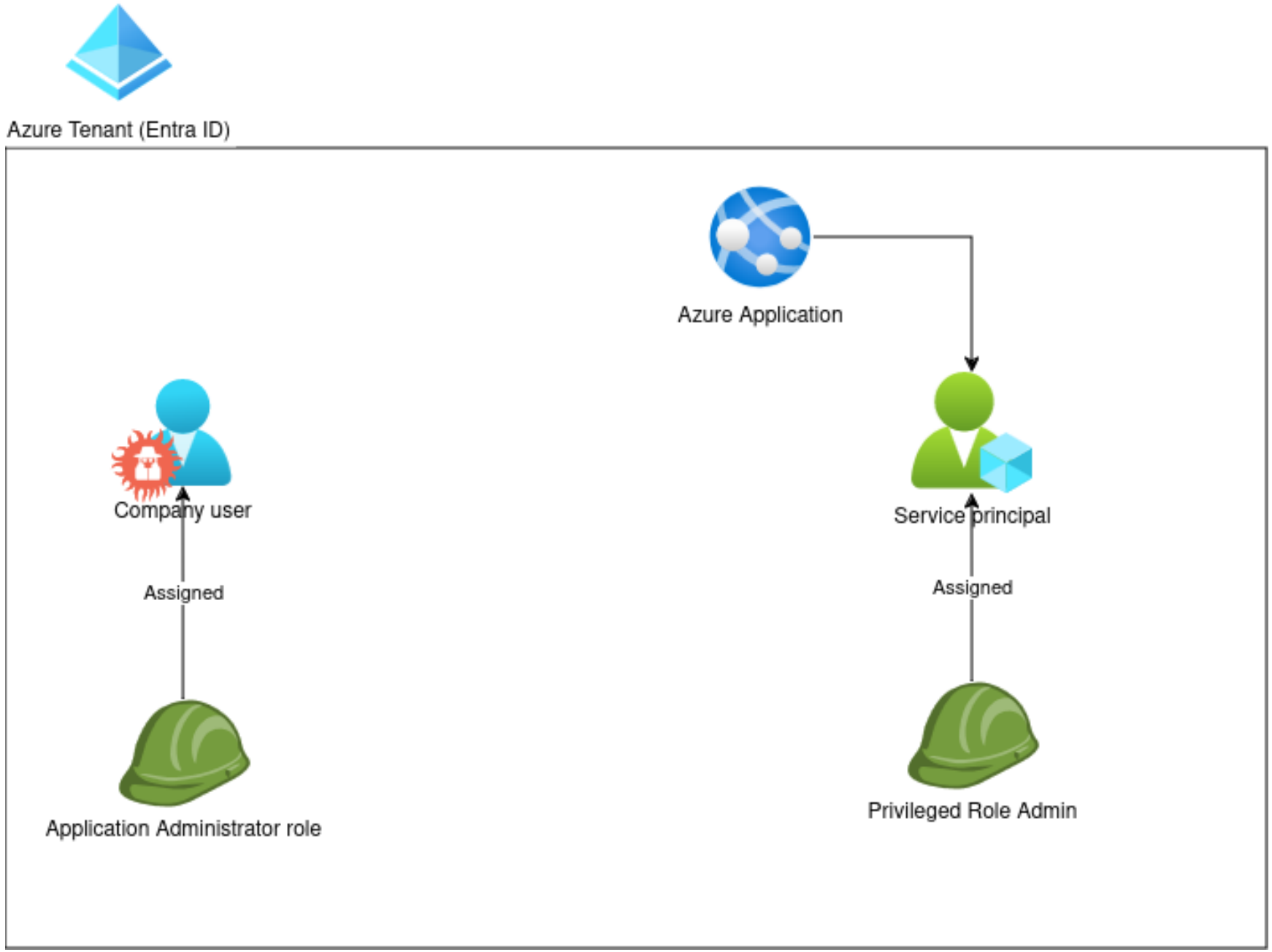
Azure Permission Model

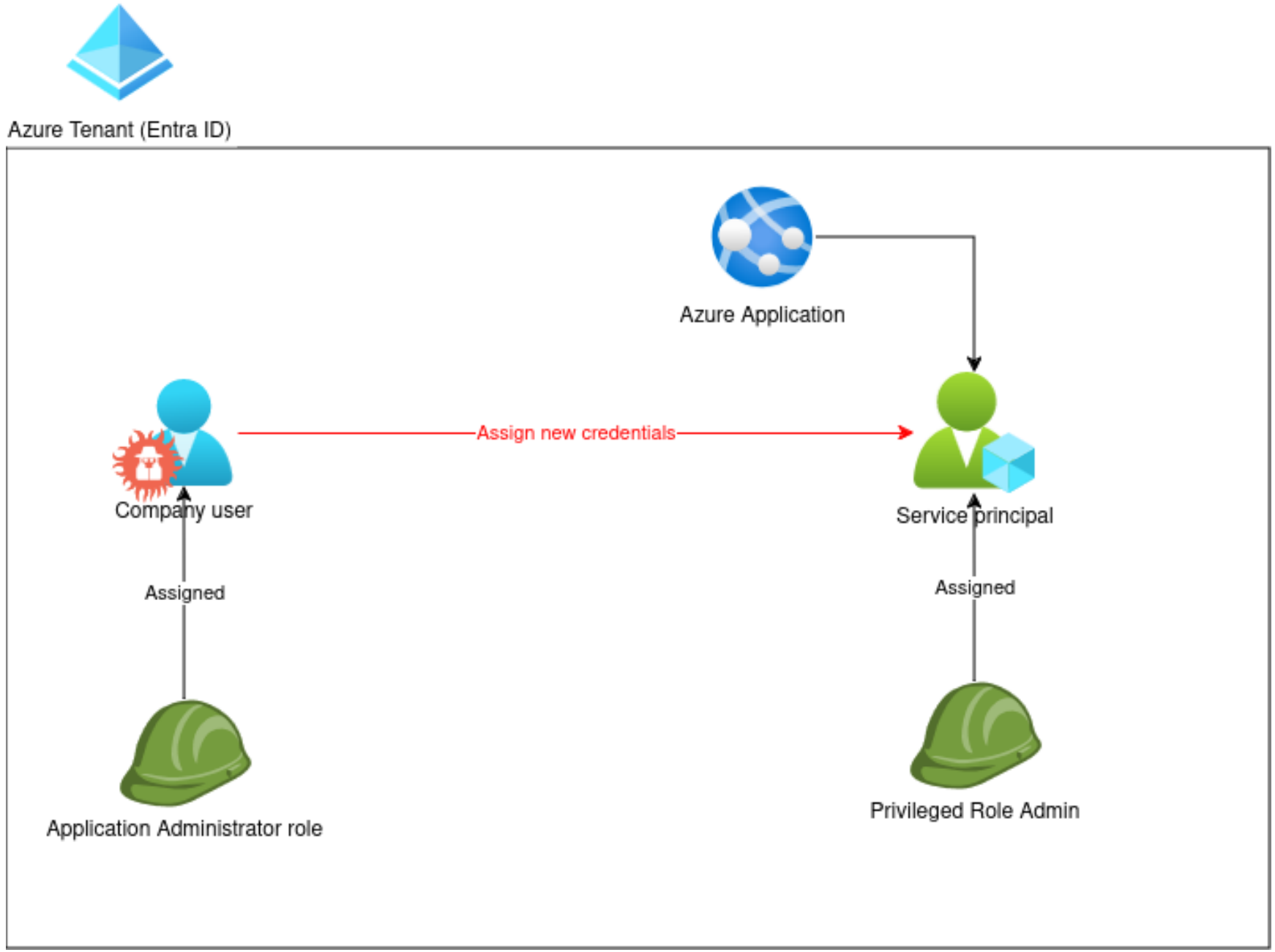
- Very flexible permission model
- Within a tenant, **global admin** have full administrative access to **all** resources and services.
  - Global admin assigns roles, controlling their access to a resources and services

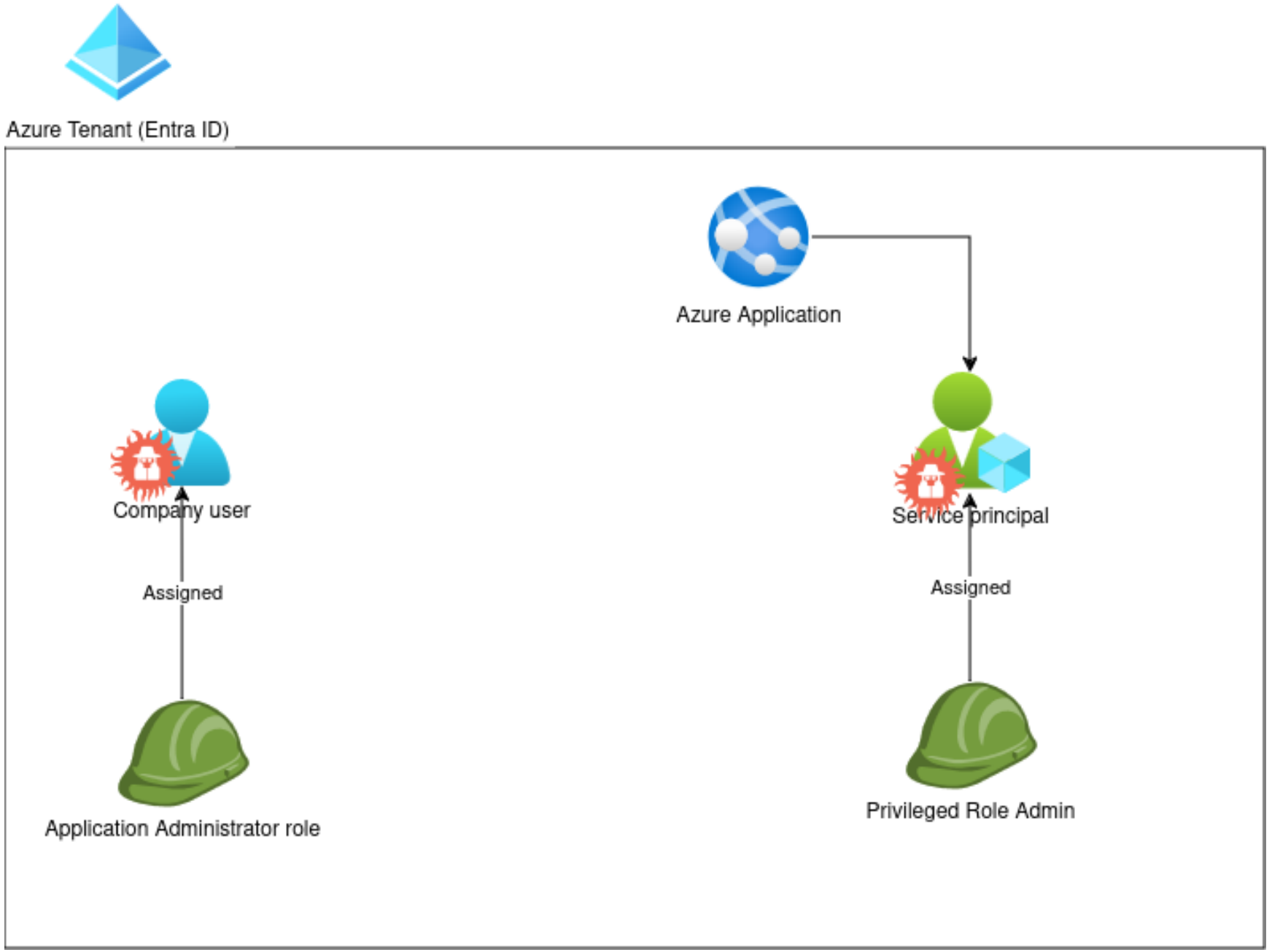

Azure Tenant (Entra ID)
Azure Application
Company user
Assigned
Application Administrator role
Service principal
Assigned
Privileged Role Admin

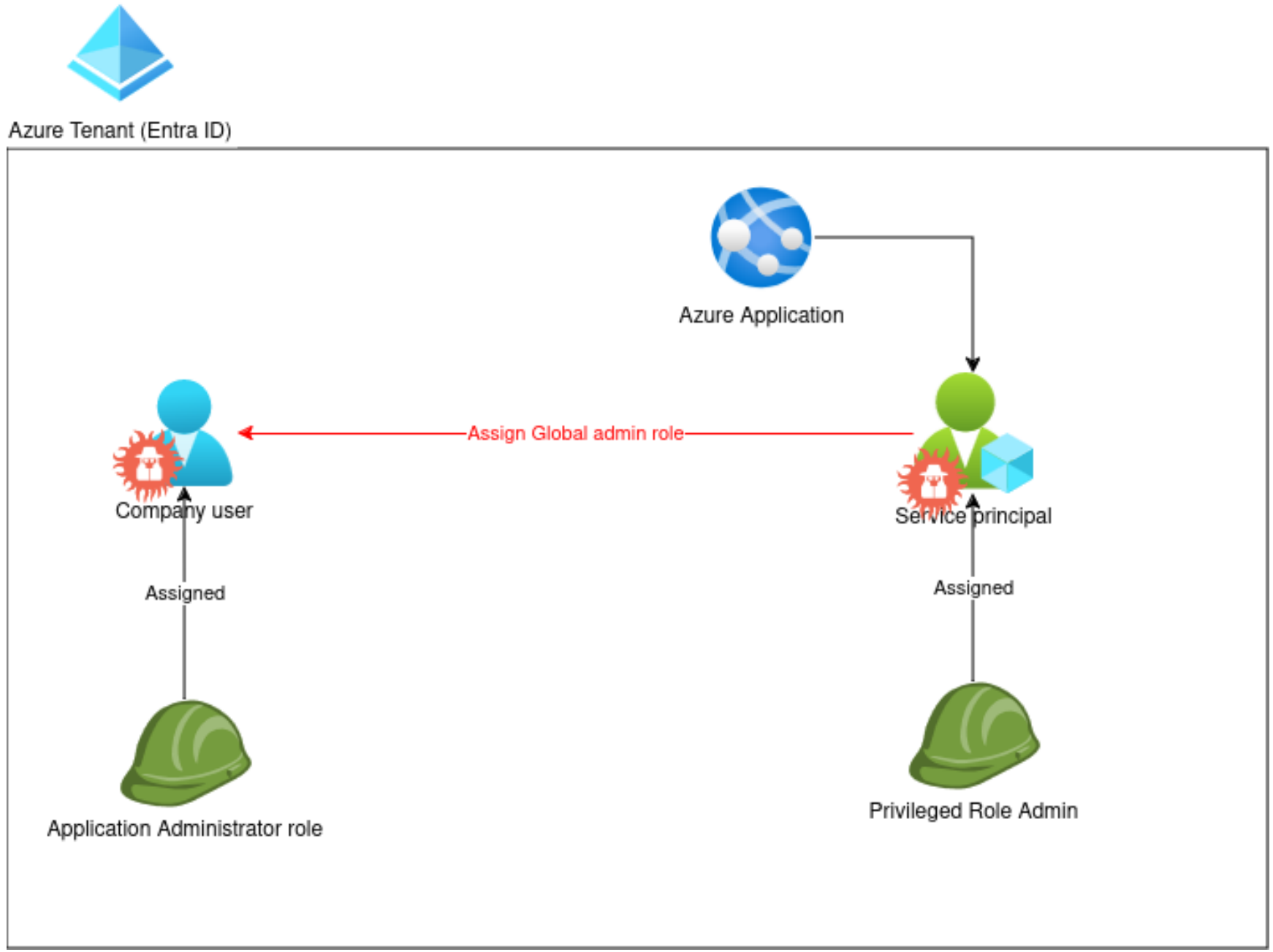
A Privileged Role Administrator can grant **any** other admin role to another principal at the tenant level.

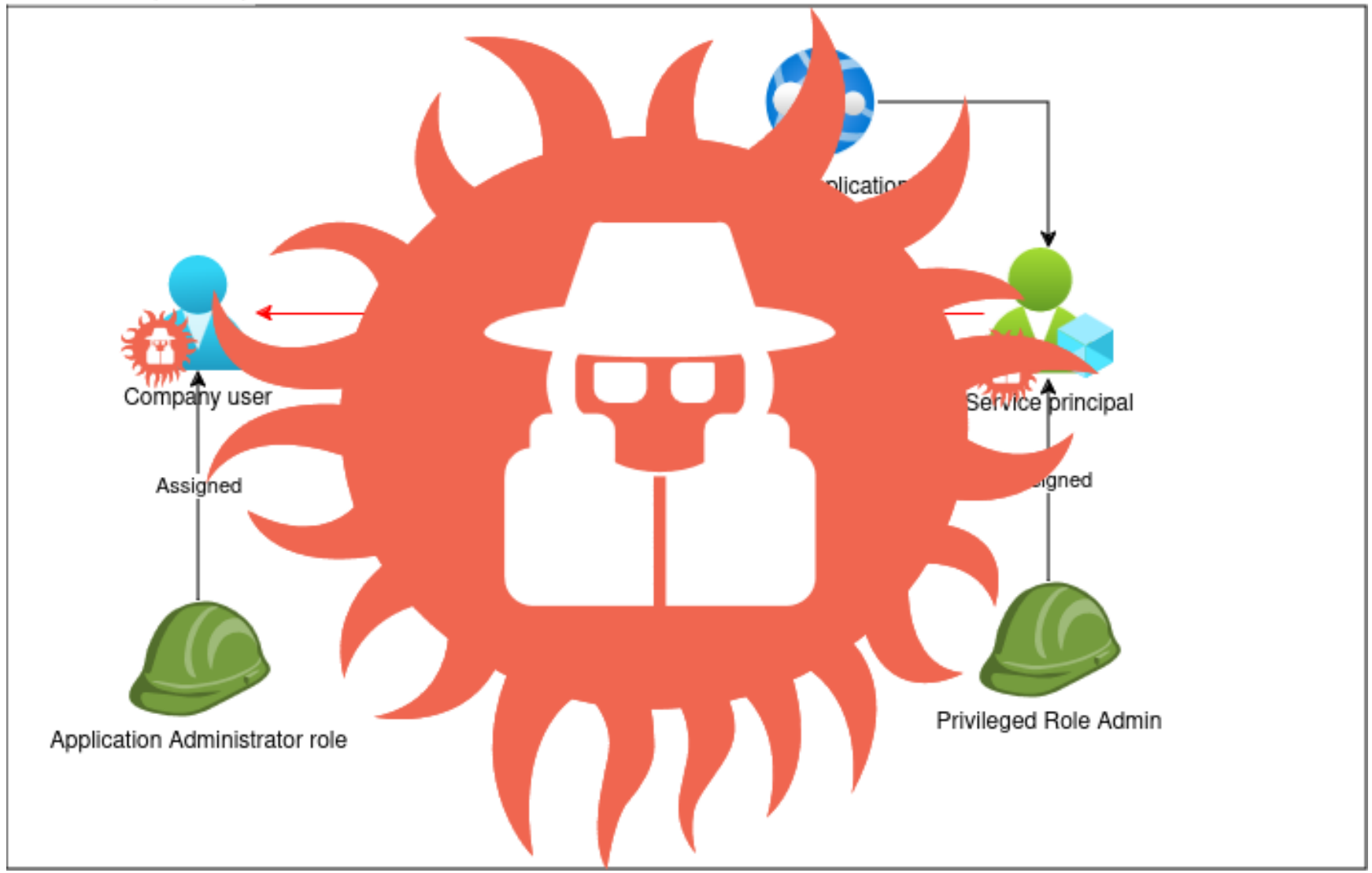

Azure Tenant (Entra ID)
Azure Application
Company user
Assigned
Application Administrator role
Service principal
Assigned
Privileged Role Admin


Azure Tenant (Entra ID)
Azure Application
Company user
Assigned
Application Administrator role
Service principal
Assigned
Privileged Role Admin


Azure Tenant (Entra ID)
Azure Application
Assign new credentials
Company user
Service principal
Assigned
Assigned
Application Administrator role
Privileged Role Admin


Azure Tenant (Entra ID)
Azure Application
Company user
Assigned
Application Administrator role
Service principal
Assigned
Privileged Role Admin


Azure Tenant (Entra ID)
Azure Application
Assign Global admin role
Company user
Service principal
Assigned
Assigned
Application Administrator role
Privileged Role Admin


Azure Tenant (Entra ID)
Company user
Assigned
Application Administrator role
Service principal
Privileged Role Admin

Key points

Key points

- Robust routines for IAM are important
- Principle of least privilege
- **IAM in cloud is complex**
  - Know your cloud
  - Do not rely on default tools
  - Connect events to an identity – detection
  - Secrets management
- **Test your assumptions**

Agenda

- **Speaker intro**
- **What is penetration testing?**
- **What could possibly go wrong in IAM?**
- **Key points**

semaphore
CONSULTING PARTNERS

Thank you for listening!

semaphore
CONSULTING PARTNERS