# NIC Cloud Connect

Oslo Spektrum
November 7 - 9

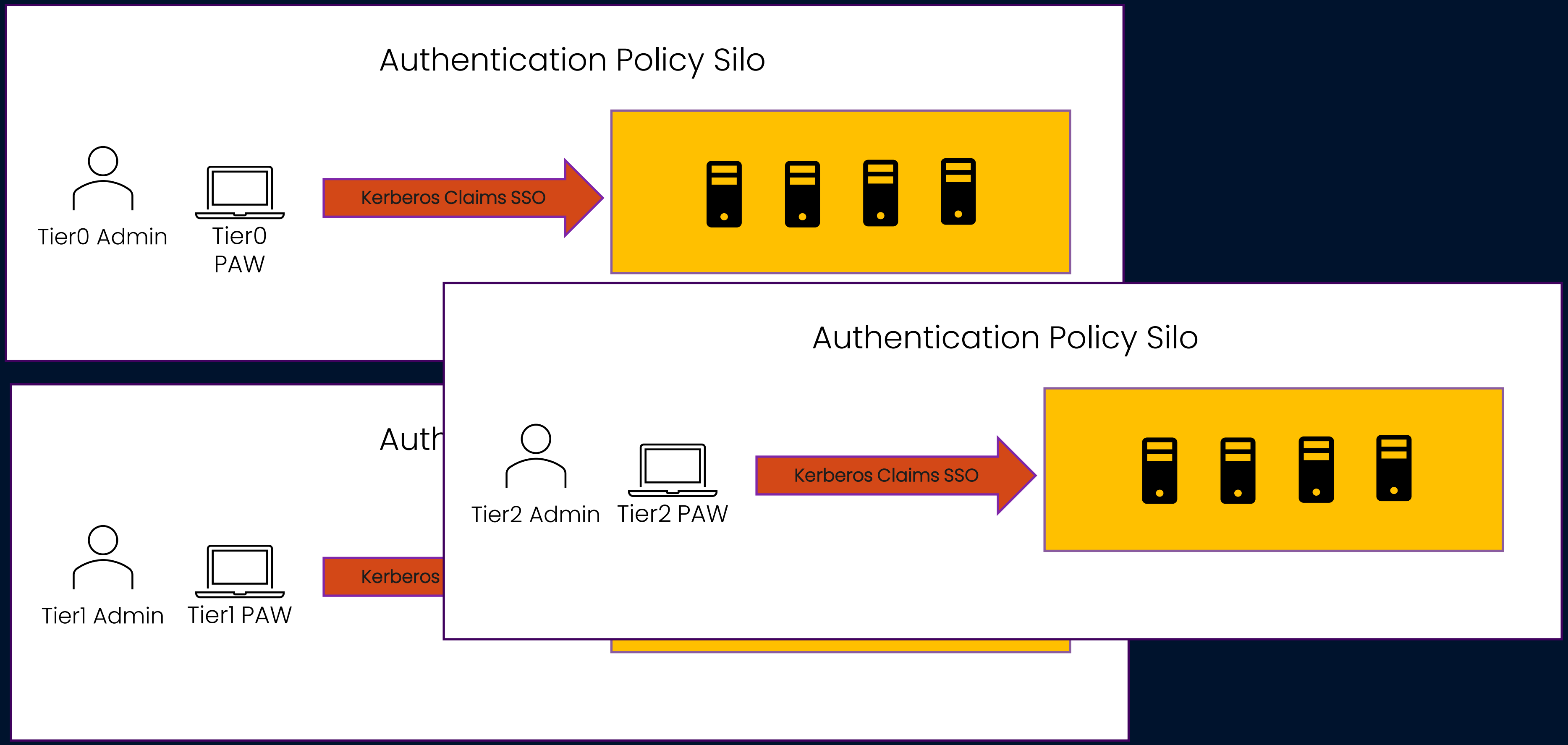
# Implementing Administrative Tiering

# Methods used by attackers

- Phishing
- Dump credentials from tools, browsers
- Dump credentials from services
- Dump AD
- Pass the Hash/Pass the Ticket/Pass the Token
- New tools everyday

# A tiered Active Directory

Demo



Authentication Policy Silo

Tier0 Admin

Tier0 PAW

Kerberos Claims SSO

Auth

Tier1 Admin

Tier1 PAW

Kerberos

Authentication Policy Silo

Tier2 Admin

Tier2 PAW

Kerberos Claims SSO

# Things be aware of

- Agents from lower-level tier or SaaS – domain admin by proxy
- Group policies – delegated permissions
- Creator/owner permissions
- Service accounts
- Emergency break-the-glass accounts

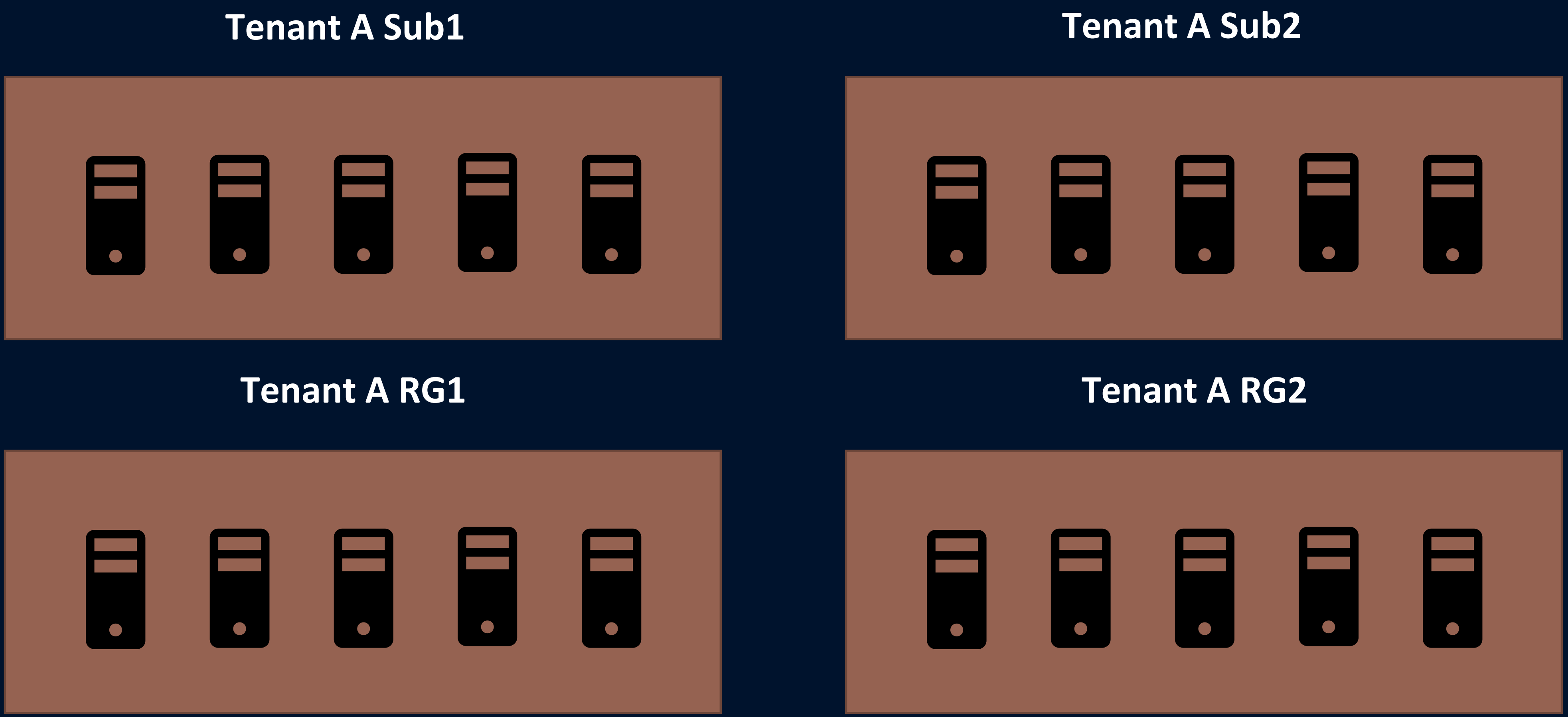
# Use PAW/SAW

- To limit the location where the administrators' credentials are being used, you should use a Privileged Access Workstation
- Solution:
  - Deploy Physical PAWs
  - Deploy Virtual PAWs for each environment/tier
  - Jumpstations as an interim solution

# Working with Siloed Jumpstation and remote tools

Demo

# What about the cloud?



Tenant A Sub1

Tenant A Sub2

Tenant A RG1

Tenant A RG2

# Deploy Cloud Tiering

Demo

# Summary

- Protect high privileged account credentials, tokens and tickets by limiting which device they can authenticate from.
- Never sync on-premises admin accounts to the cloud. Use cloud-only accounts.
- Never add on-premises users to cloud roles. Use cloud-only accounts.
- **Think big, start small!** Protect Global Admin/Security Admin and Domain Admin first.

- Tiering covers day 1-99, not day 0 nor day 100.