ICT POWER.IT

Microsoft

#POWERCON2022

Implementare Active Directory Tier Model e LAPS (Local Administrator Password Solution)

Stefano Nieri

Senior Consultant – Project Informatica

Stefano.Nieri@project.it

/snieri

/stefanonieri

Active Directory Poll

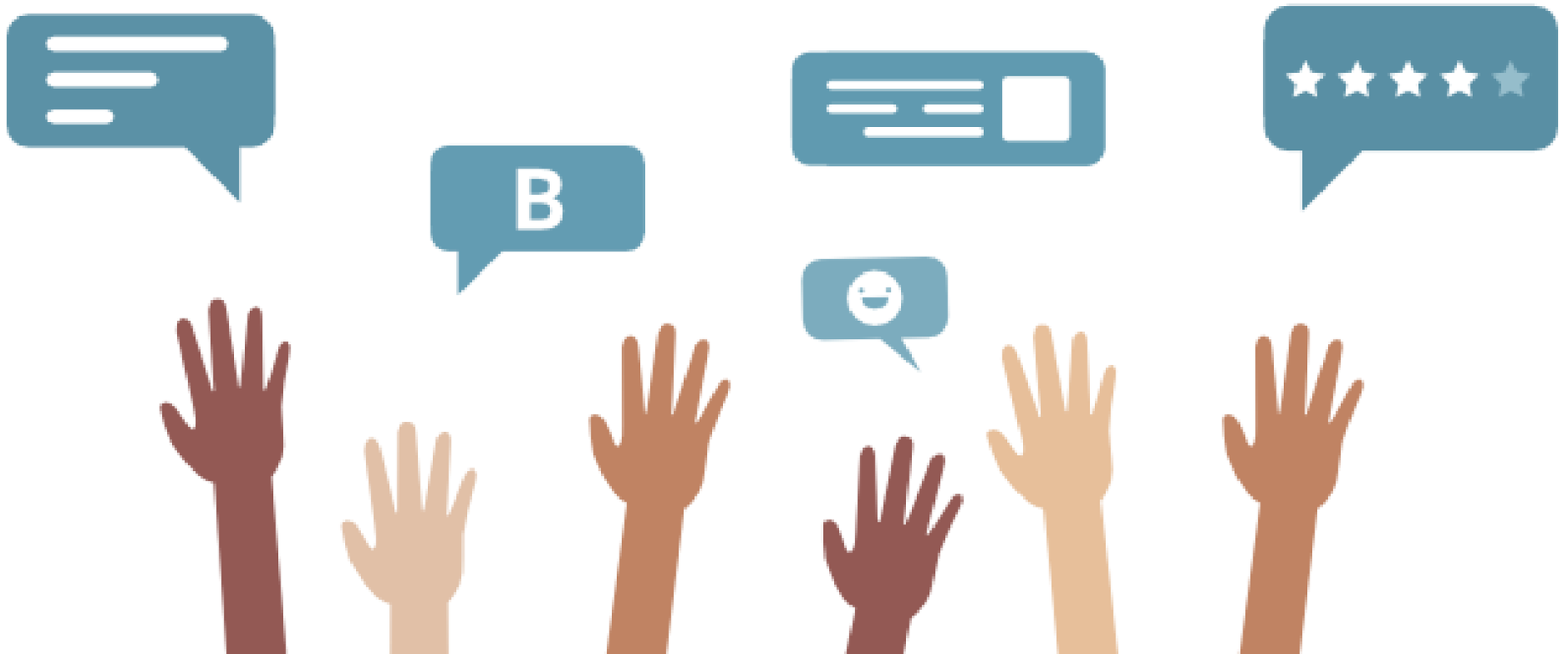
Do you know how many and who are the Domain Admins & AAD GA?

Are you syncing your Domain Admin to Azure AD?

Are you using a single user to authenticate anywhere?

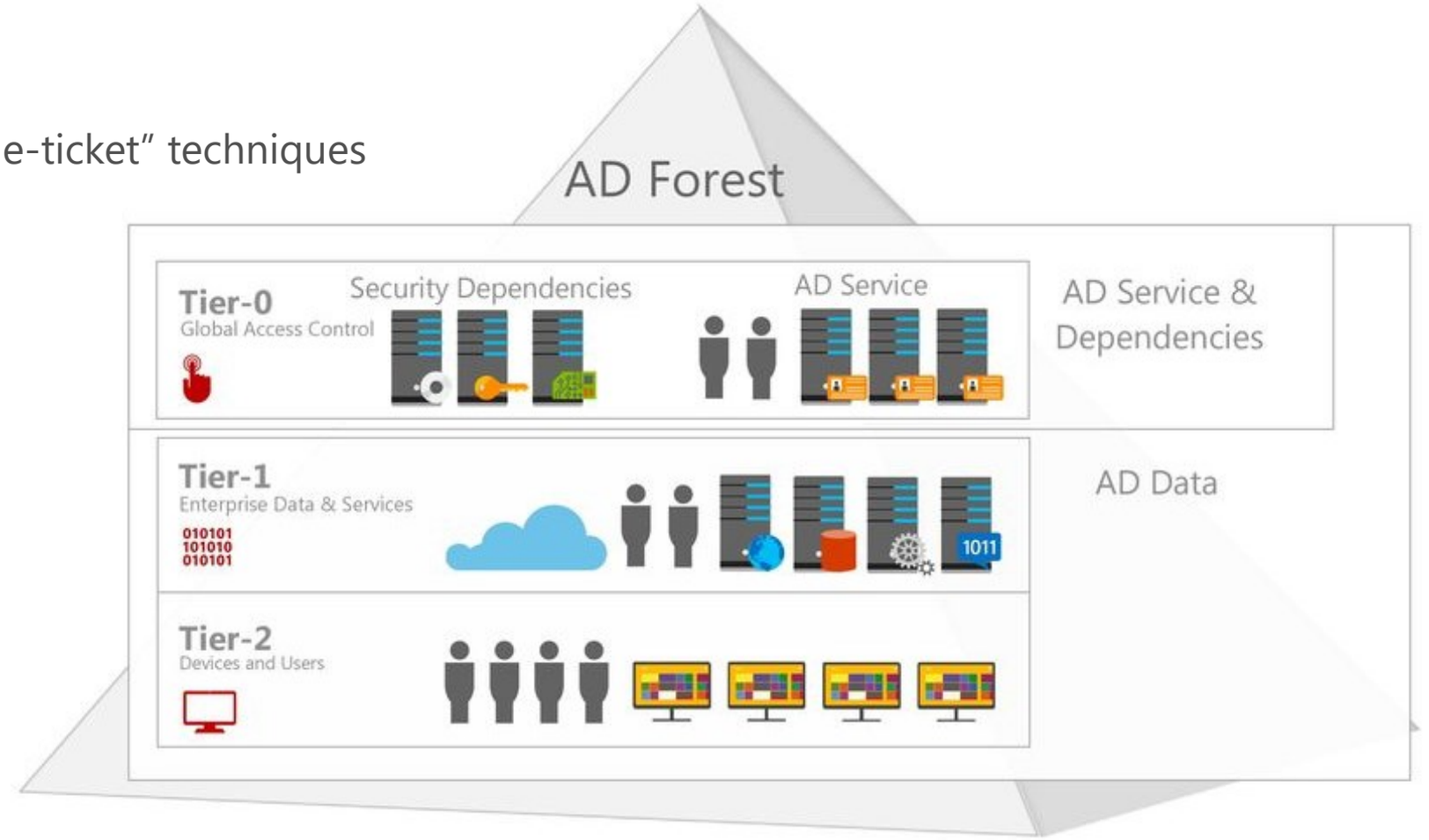
Are you cloning computers and servers with the same local admin pw?

Are you using a Domain Admin account for Scheduled Task and Service?



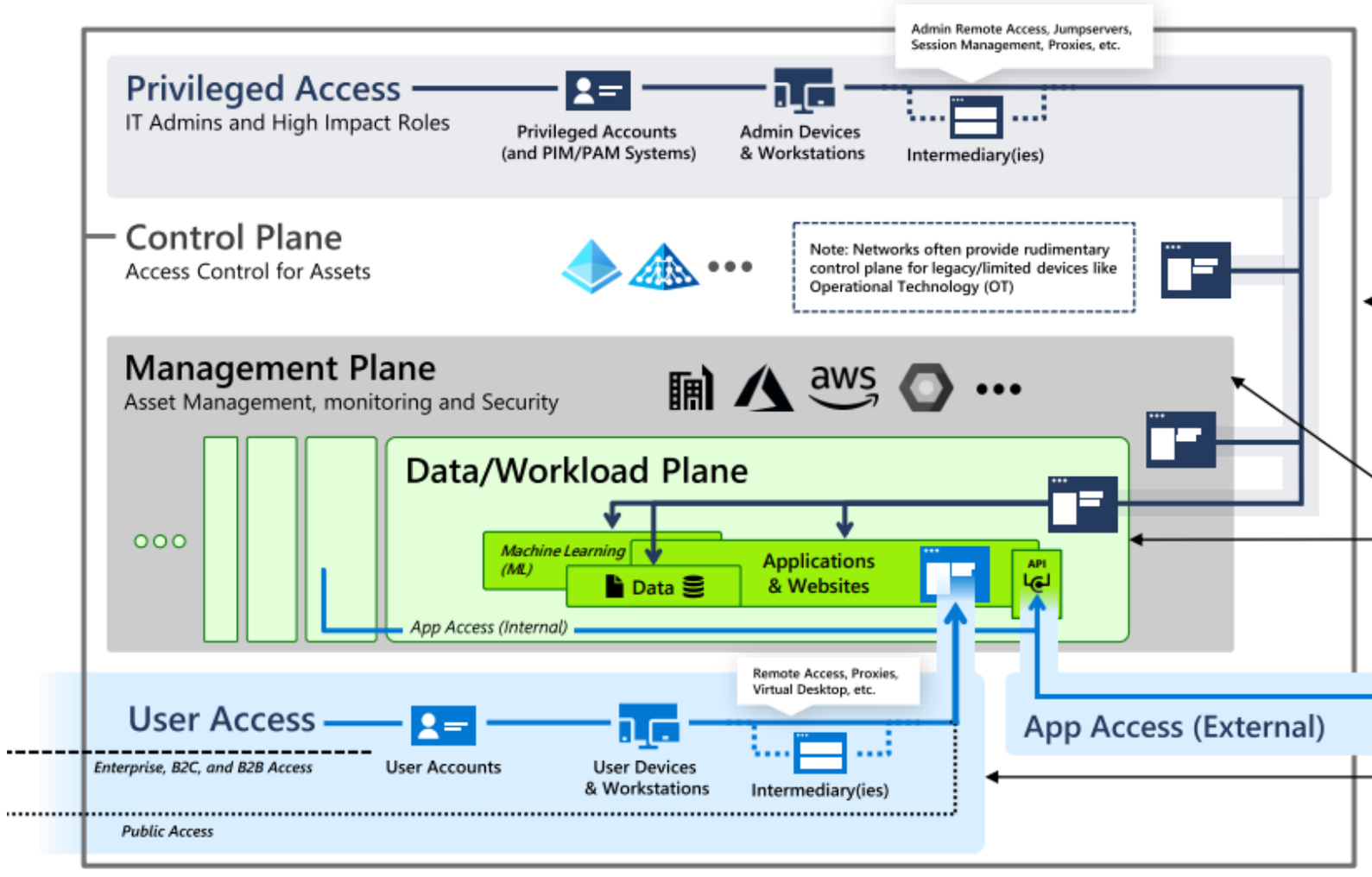
Active Directory Tier Model & LAPS goal

- Increase the cost for an attacker trying to compromise sensitive systems
- Avoid Domain Dominance
- Prevent Privileged Escalation
- Prevent Lateral Movement
- Mitigate Credential Stuff
- Mitigate “Pass-the-Hash” or “Pass-the-ticket” techniques



Comparison to legacy tier model

Upgrades legacy tier model to complete enterprise access model



Evolved purpose and scope

The original tier model was built to contain privilege escalation for on-premises active directory.

The enterprise access model guides access security for full scope of a hybrid on-premises + multi-cloud enterprise following zero trust principles for employees, partners, customers, apps and more

Tier 0 → Control Plane

The control plane includes identity access controls as well as the use of network access control where it is the only/best option, such as legacy OT options

Tier 1 Split

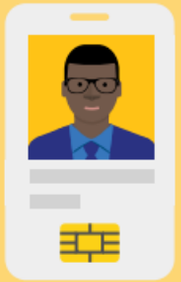
To increase clarity, actionability, and business focus:

- **Management Plane –** enterprise-wide IT management
- **Data/Workload Plane –** per-workload management focused on protecting business critical systems/data and accommodating DevOps

Tier 2 Split

- **User access –** now includes all B2B, B2C, and public access scenarios
- **App access –** to accommodate API attack surface

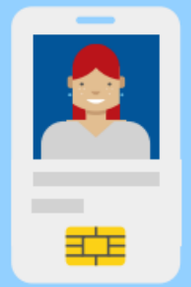
Active Directory Tier Model



Tier 0
Domain & Enterprise Admins

The highest level of privilege. Accounts which have administrative control over the entire environment through the ability to manage identity and permissions enterprise-wide.

- Domain Controllers
- Systems which operate or manage Domain Controllers
- Accounts which access or administrate any of the above



Tier 1
Server Admins

Accounts which have administrative control over enterprise resources that serve many users or manage business-critical data and applications. Cannot control Tier 0 resources.

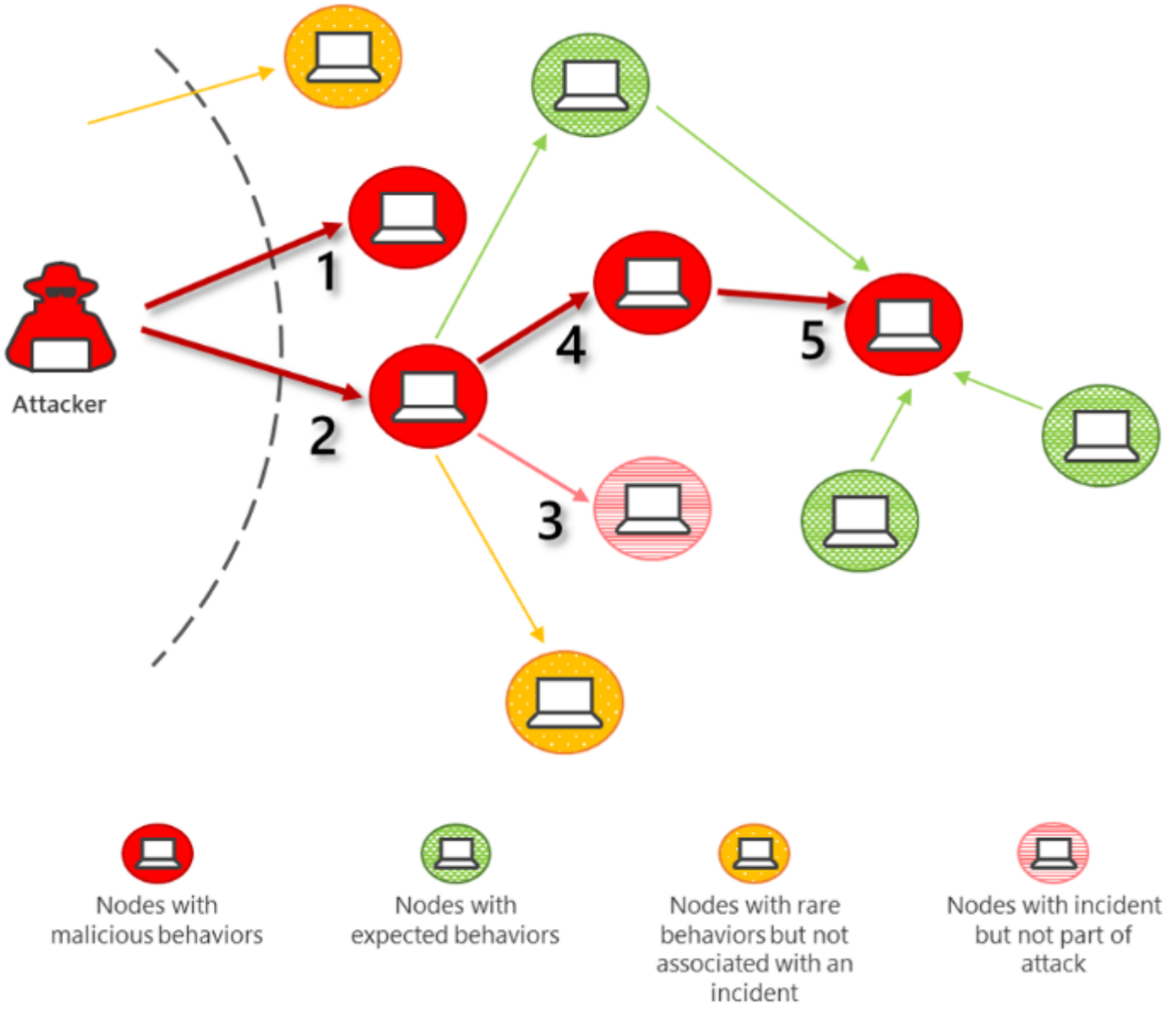
- Member servers and administrators
- Enterprise application administrators
- Cloud service administrators

Tier 2
Workstation & Device Admins

Accounts with administrative privileges over only standard user accounts and single-user devices. Cannot control Tier 1 or Tier 0 resources.

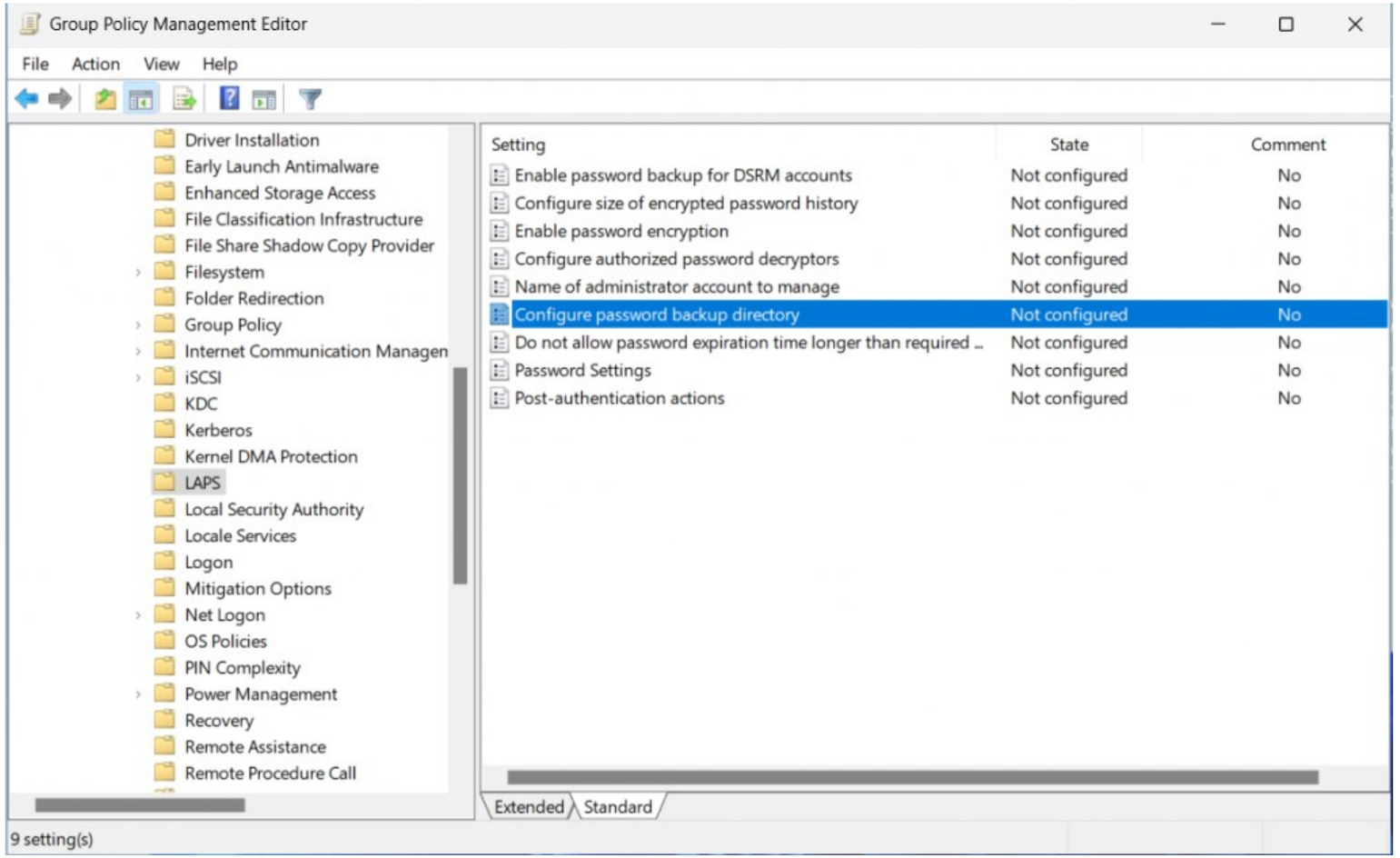
- Helpdesk support
- Device support
- User support

Prevent Lateral Movement



LAPS new features

LAPS is now **Windows native** AND Microsoft is working on support for Azure Active Directory
Roadmap Features: AAD Join Device Support, password save choise (AD or AAD), Dedicated LAPS Tab on AD

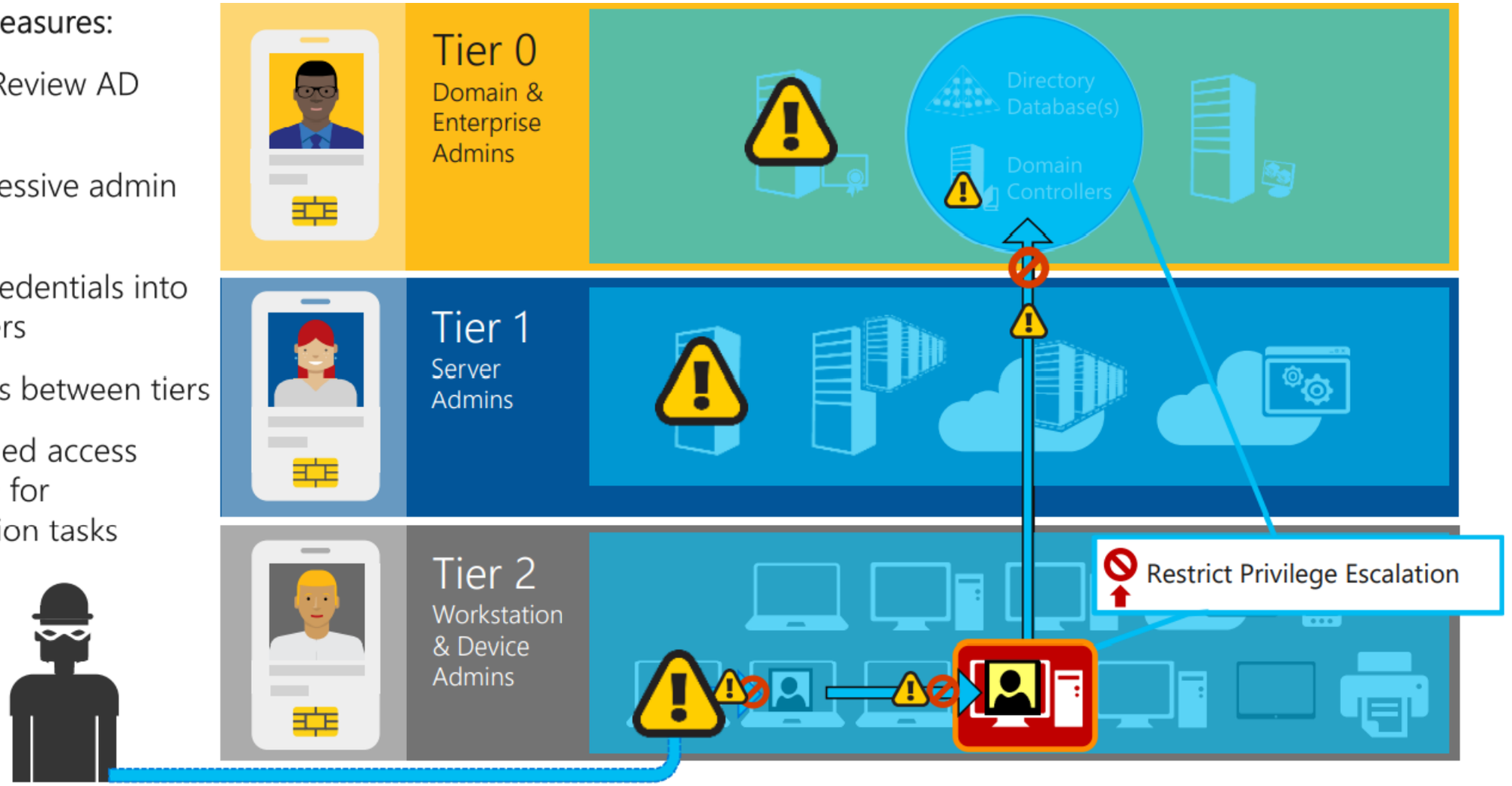


[Announcing Windows 11 Insider Preview Build 25145 | Windows Insider Blog]

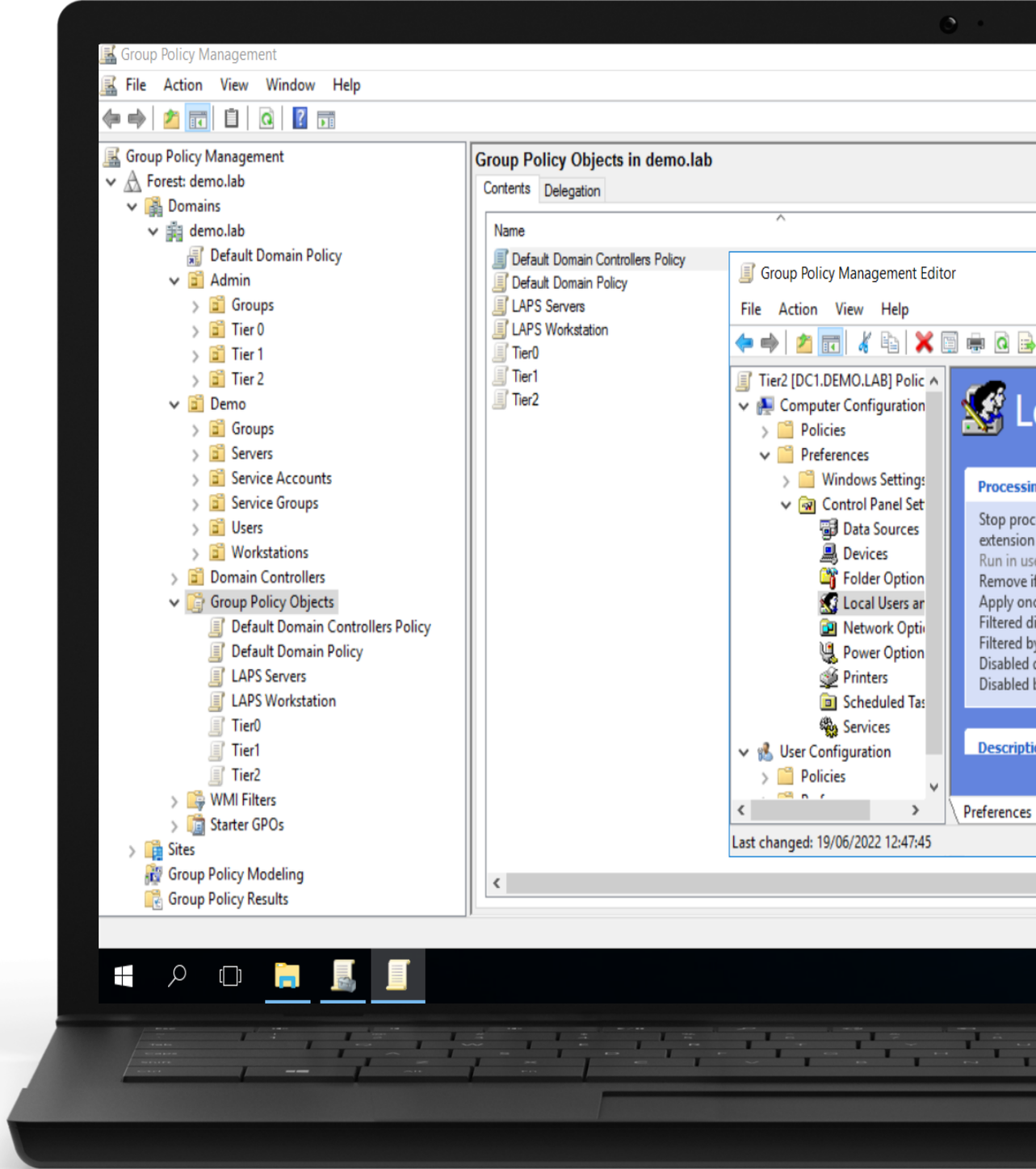
Prevent Privileged Escalation

Deployment Measures:

1. Analyze & Review AD Security
2. Reduce excessive admin privileges
3. Segment credentials into privilege tiers
4. Block access between tiers
5. Use privileged access workstation for administration tasks



DEMO


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: demo.lab
Domains
demo.lab
Default Domain Policy
Admin
Groups
Tier 0
Tier 1
Tier 2
Demo
Groups
Servers
Service Accounts
Service Groups
Users
Workstations
Domain Controllers
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
LAPS Servers
LAPS Workstation
Tier0
Tier1
Tier2
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Objects in demo.lab
Contents
Delegation
Name
Default Domain Controllers Policy
Default Domain Policy
LAPS Servers
LAPS Workstation
Tier0
Tier1
Tier2
Group Policy Management Editor
File Action View Help
Tier2 [DC1.DEMO.LAB] Polic
Computer Configuration
Policies
Preferences
Windows Settings
Control Panel Set
Data Sources
Devices
Folder Option
Local Users ar
Network Opti
Power Option
Printers
Scheduled Tas
Services
User Configuration
Policies
Preferences
Last changed: 19/06/2022 12:47:45

ICT POWER.IT

Microsoft

Grazie

Stefano Nieri

Senior Consultant – Project Informatica

Stefano.Nieri@project.it

/snieri

/stefanonieri