Active Directory Security: The Journey

Sean Metcalf (@Pyrotek3)
sean [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

ABOUT

- Founder Trimarc, a security company.
- Microsoft Certified Master (MCM) Directory Services
- Microsoft MVP
- Speaker: BSides, Shakacon, Black Hat, DEF CON, DerbyCon
- Security Consultant / Security Researcher
- Own & Operate ADSecurity.org
  (Microsoft platform security info)

ABOUT

- Founder Trimarc, a security company.
- Microsoft Certified Master (MCM) Directory Services
- ~~Microsoft MVP~~
- Speaker: BSides, Shakacon, Black Hat, DEF CON, DerbyCon
- Security Consultant / Security Researcher
- Own & Operate ADSecurity.org
  (Microsoft platform security info)

ABOUT

- Founder Trimarc, a security company.
- Microsoft Certified Master (MCM) Directory Services
- Speaker: BSides, Shakacon, Black Hat, DEF CON, DerbyCon
- Security Consultant / Security Researcher
- Own & Operate ADSecurity.org
  (Microsoft platform security info)

AGENDA

- Current state of Active Directory Security
- AD Security Evolution
- Expanding AD Permissions
- Attacker Capability
- Microsoft’s AD Security Guidance
- What Really Matters
- Recommendations

Todays agenda:
1) Be stylin' and profilin' ✅
2) Lunch
3) Go home

Slides: Presentations.ADSecurity.org

The Current State of Active Directory: The Good, the Bad, & the UGLY

The Good

- Better awareness of the importance of AD security.
- AD security more thoroughly tested.
- Less Domain Admins (overall).
- Less credentials in Group Policy Preferences.
- More local Admin passwords are automatically rotated (LAPS).
- PowerShell security improvements (v5).

The BAD

- Too many Domain Admins still administer AD from their regular workstation.
- Privilege escalation from regular user is still too easy.
- Lots of legacy cruft reduces security.
- Not enough (PowerShell) logging deployed.
- Too many blind spots (poor visibility).

The Evolution of Active Directory Security

AD Security: The early days

- The year is 2000, the OS is too!
- Active Directory key design decisions
- Replication is feared
- Kerberos is embraced and extended
- Enter SIDHistory
- Compromises to support Windows NT legacy
- NT lives on! ☹

AD Security: AD v2 & v3

- Windows 2003 Server
- Lots of improvements
- AD matures significantly
- LastLogonTimestamp tracks last logon (& replicates!)
- Constrained Delegation
- Selective Authentication for Trusts. Everyone ignores…
- Many organizations deploy Active Directory

AD: Let’s Do Security!

- Windows Server 2008/2008 R2
- Enter the AD Recycle Bin
- Last interactive logon information
- Fine-grained password policies
- Authentication mechanism assurance which identifies logon method type (smart card or user name/password)
- Managed Service Accounts (let AD handle the password)
- Automatic SPN management for services running under context of a Managed Service Account.
- Goodbye Kerberos DES, hello AES

AD: Security Enhancements

- Windows Server 2012/2012 R2
- Focus on protecting credentials
- Shift in security focus
- DC-side protections for Protected Users
  - No NTLM authentication
  - No Kerberos DES or RC4 ciphers
  - No Delegation – unconstrained or constrained delegation
  - No user tickets (TGTs) renewed beyond the initial 4 hr lifetime
- Authentication Policies & Authentication Policy Silos

Rearchitecting Security

- Windows Server 2016/Windows 10
- Major changes in OS security architecture
- From Normal World to Secure World (VSM)
- Credential Guard & Remote Credential Guard
- Lots of minor changes, big impact
- New shadow security principals (groups)
- An expiring links feature (Group TTL)
- KDC enhancements to restrict Kerberos ticket lifetime to the lowest group TTL

AD Permissions:
What you don’t know can hurt

It's important to understand that it ***doesn't matter what Active Directory permissions a user has*** *when using the Exchange management tools.* ***If the user is authorized, via RBAC***, *to perform an action in the Exchange management tools,* ***the user can perform the action regardless of his or her Active Directory permissions.***

https://technet.microsoft.com/en-us/library/dd638106.aspx

Highly Privileged Exchange Groups

- Exchange Trusted Subsystem (like SYSTEM, only better)
    - *"The Exchange Trusted Subsystem is a highly privileged …Group that has read/write access to every Exchange-related object in the Exchange organization."*
    - Members: Exchange Servers
    - MemberOf: Exchange Windows Permissions
- Exchange Windows Permissions
    - Provides rights to AD objects (users, groups, etc)
    - Members: Exchange Trusted Subsystem
- Organization Management (the DA of the Exchange world)
    - *"Members … have administrative access to the entire Exchange 2013 organization and can perform almost any task against any Exchange 2013 object, with some exceptions.*
      …is a very powerful role and as such, only users or … groups that perform organizational-level administrative tasks that can potentially impact the entire Exchange organization should be members of this role group."
    - Members: 2 to 3 Exchange organization admin accounts (or less)

Exchange RBAC

- Early Exchange versions required AD object delegation for Exchange rights
- Exchange 2010: Exchange Trusted Subsystem
- Exchange has it’s own parallel security (RBAC) model
- The Exchange local System account has the power
- Add an account/group to the Exchange Trusted Subsystem group
- Get Local SYSTEM on an Exchange Server…

Exchange Rights

- Exchange has extensive rights throughout Active Directory.
- Modify rights on most objects, including users and groups (even admins).
    - Except AdminSDHolder protected groups/users.
- Access provided through Exchange groups (like Trusted Subsystem)
- In environments where Exchange 2000/2003 was originally installed, those rights persist, potentially providing even more access.
- Migrated to O365?
  Great, all these permissions are still in AD.

Old Exchange Permissions Persist Upgrade after Upgrade…

Exchange 2000 → 2003 → 2007 → 2010 → 2013 → 2016

Microsoft,
we need a way to fix this

Microsoft System Center Configuration Manager (SCCM)

- Originally SMS (not text messaging)
- Granular delegation was a challenge, much better in SCCM 2012.
- Role-Based Access breakout
  - All Desktops - Workstation Assets
  - All Servers - Server Assets
- Typically manages (& patches) all Windows systems
  - Workstations
  - Servers
  - ***Domain Controllers***

3rd Party Product Permission Requirements

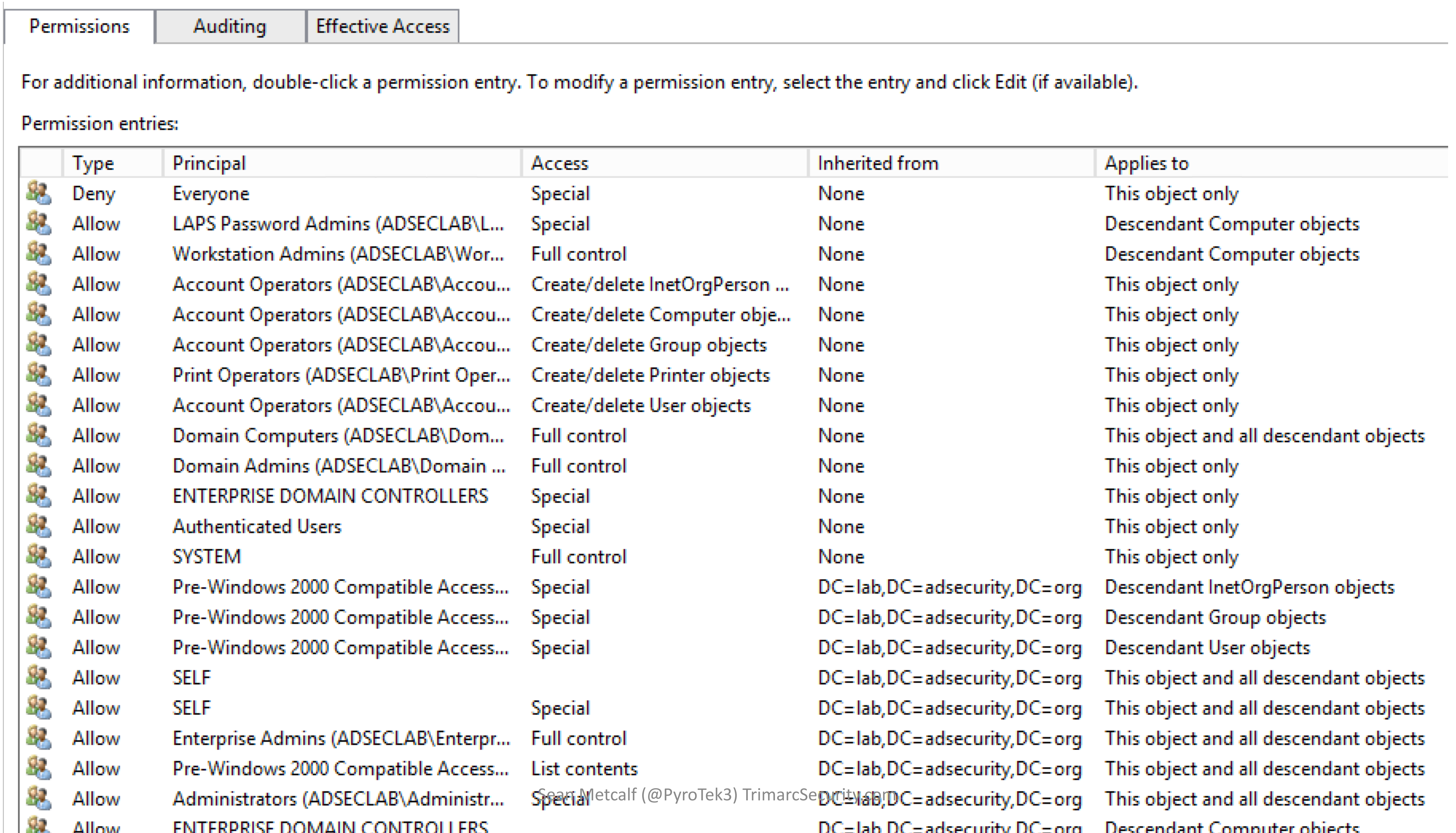
- Domain user access
- Operations systems access
- Mistaken identity – trust the installer
- AD object rights
- Install permissions on systems
- Needs System rights
- Active Directory privileged rights
- Domain permissions during install
- More access required than often needed.
- Initial start/run permissions
- Needs full AD rights

3rd Party Product Permission Requirements

- **D**omain user access
- **O**perations systems access
- **M**istaken identity – trust the installer
- **A**D object rights
- **I**nstall permissions on systems
- **N**eeds System rights
- **A**ctive Directory privileged rights
- **D**omain permissions during install
- **M**ore access required than often needed.
- **I**nitial start/run permissions
- **N**eeds full AD rights

Over-permissioned Delegation

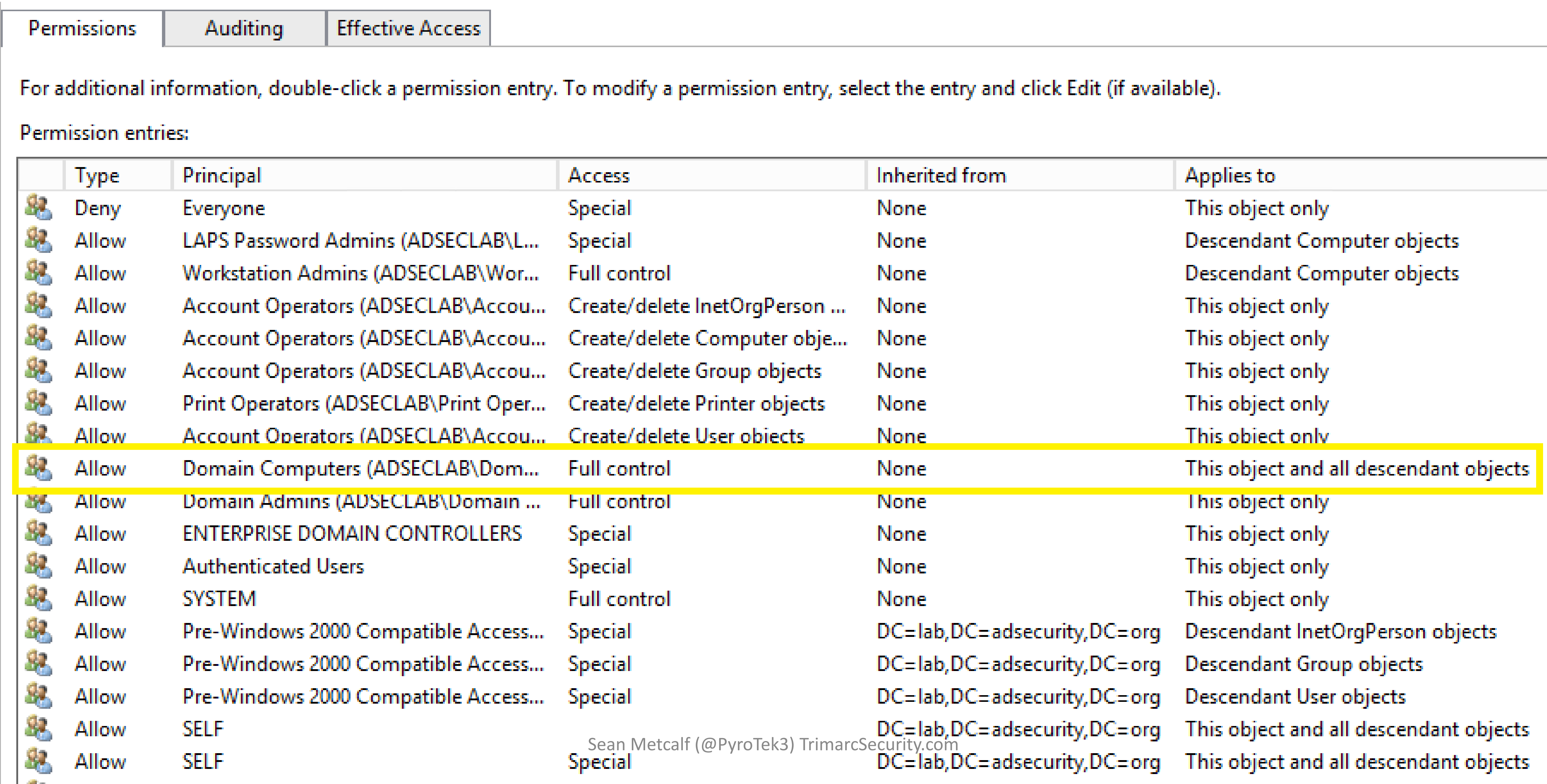
- Use of built-in groups for delegation
- Clicking the "easy button": Full Control at the domain root.
- Let's just "make it work"
- Delegation tools in AD are challenging to get right
- We need better managing/reporting tools



For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Special	None	This object only
Allow	LAPS Password Admins (ADSECLAB\L...	Special	None	Descendant Computer objects
Allow	Workstation Admins (ADSECLAB\Wor...	Full control	None	Descendant Computer objects
Allow	Account Operators (ADSECLAB\Accou...	Create/delete InetOrgPerson ...	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete Computer obje...	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete Group objects	None	This object only
Allow	Print Operators (ADSECLAB\Print Oper...	Create/delete Printer objects	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete User objects	None	This object only
Allow	Domain Computers (ADSECLAB\Dom...	Full control	None	This object and all descendant objects
Allow	Domain Admins (ADSECLAB\Domain ...	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONTROLLERS	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant InetOrgPerson objects
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant Group objects
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant User objects
Allow	SELF		DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	SELF	Special	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	Enterprise Admins (ADSECLAB\Enterpr...	Full control	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	Pre-Windows 2000 Compatible Access...	List contents	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	Administrators (ADSECLAB\Administr...	Special	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	ENTERPRISE DOMAIN CONTROLLERS		DC=lab,DC=adsecurity,DC=org	Descendant Computer objects



For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

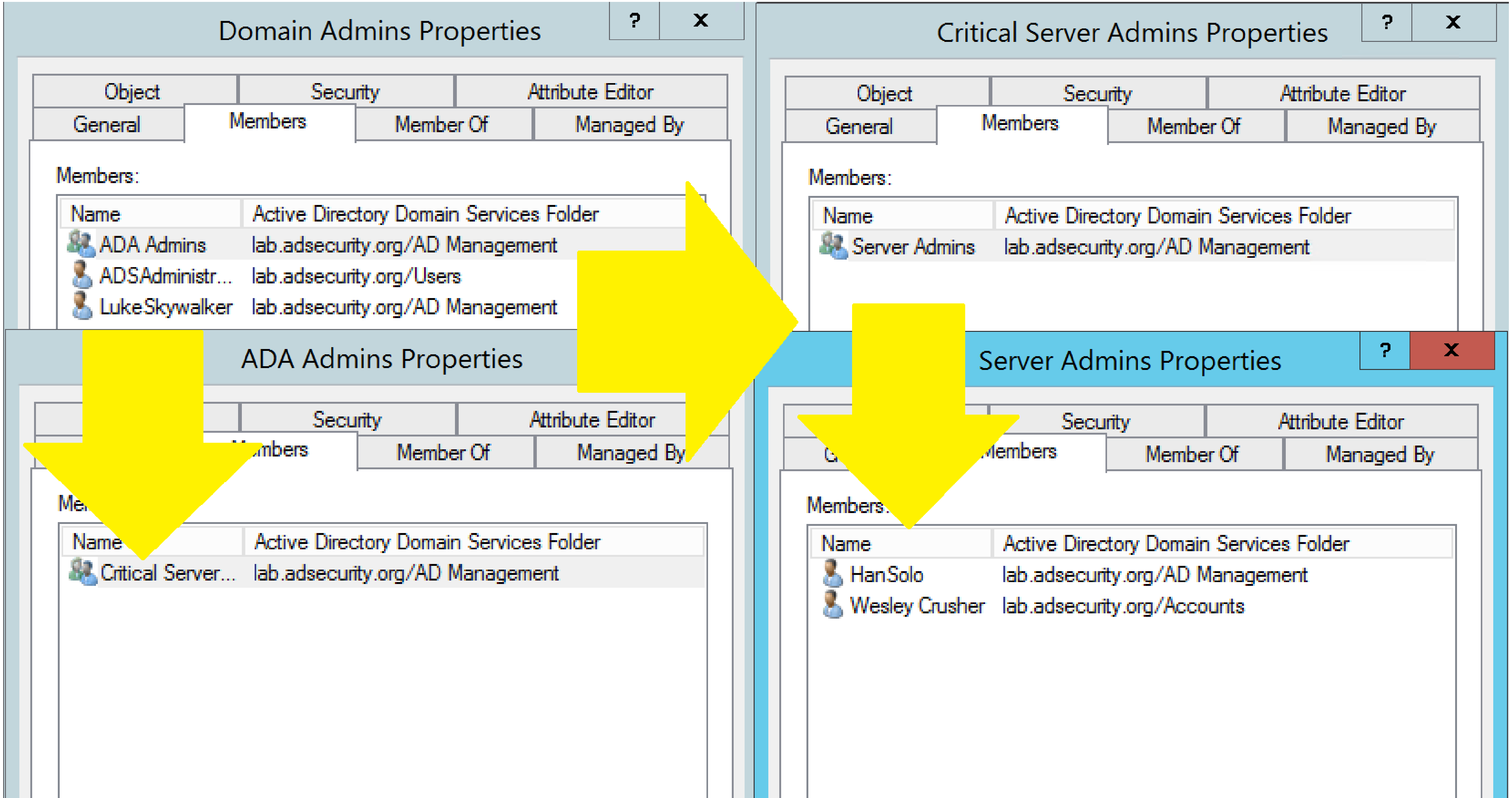
Permission entries:

Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Special	None	This object only
Allow	LAPS Password Admins (ADSECLAB\L...	Special	None	Descendant Computer objects
Allow	Workstation Admins (ADSECLAB\Wor...	Full control	None	Descendant Computer objects
Allow	Account Operators (ADSECLAB\Accou...	Create/delete InetOrgPerson ...	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete Computer obje...	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete Group objects	None	This object only
Allow	Print Operators (ADSECLAB\Print Oper...	Create/delete Printer objects	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete User objects	None	This object only
Allow	Domain Computers (ADSECLAB\Dom...	Full control	None	This object and all descendant objects
Allow	Domain Admins (ADSECLAB\Domain ...	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONTROLLERS	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant InetOrgPerson objects
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant Group objects
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant User objects
Allow	SELF		DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	SELF	Special	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Common Issues Persist…

- Old GPO settings
- Group membership expands (and expands…)
- Group nesting makes rights auditing challenging
- Default Domain Controller security
- Over-permissioned GPO security
- Spider web of AD ACLs, layer upon layer



Domain Admins Properties

Members:

Name	Active Directory Domain Services Folder
ADA Admins	lab.adsecurity.org/AD Management
ADSAdministr...	lab.adsecurity.org/Users
LukeSkywalker	lab.adsecurity.org/AD Management

Critical Server Admins Properties

Members:

Name	Active Directory Domain Services Folder
Server Admins	lab.adsecurity.org/AD Management

ADA Admins Properties

Me

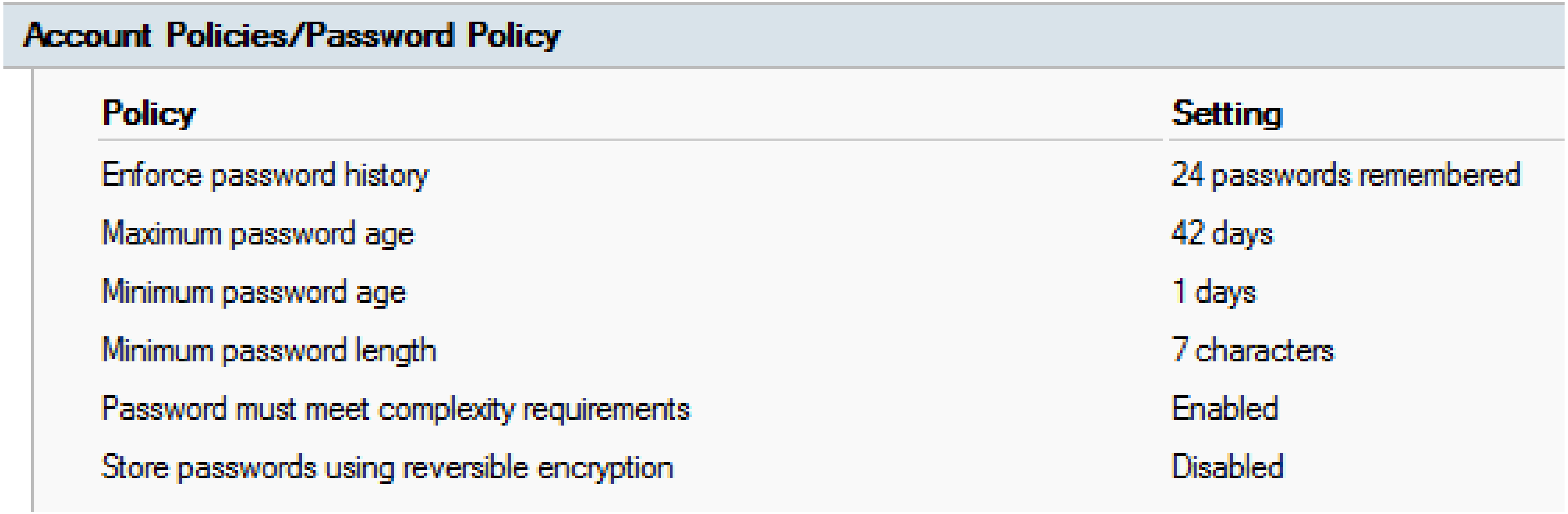
Name	Active Directory Domain Services Folder
Critical Server...	lab.adsecurity.org/AD Management

Server Admins Properties

Members:

Name	Active Directory Domain Services Folder
HanSolo	lab.adsecurity.org/AD Management
Wesley Crusher	lab.adsecurity.org/Accounts

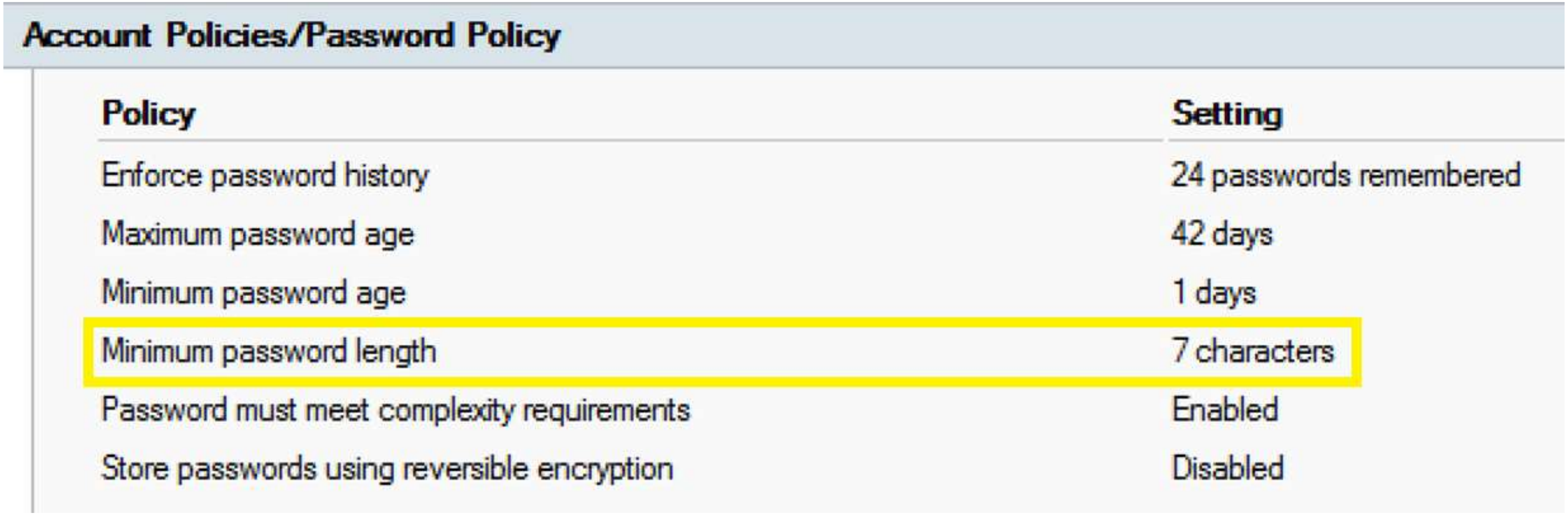
Default Domain Policy



Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

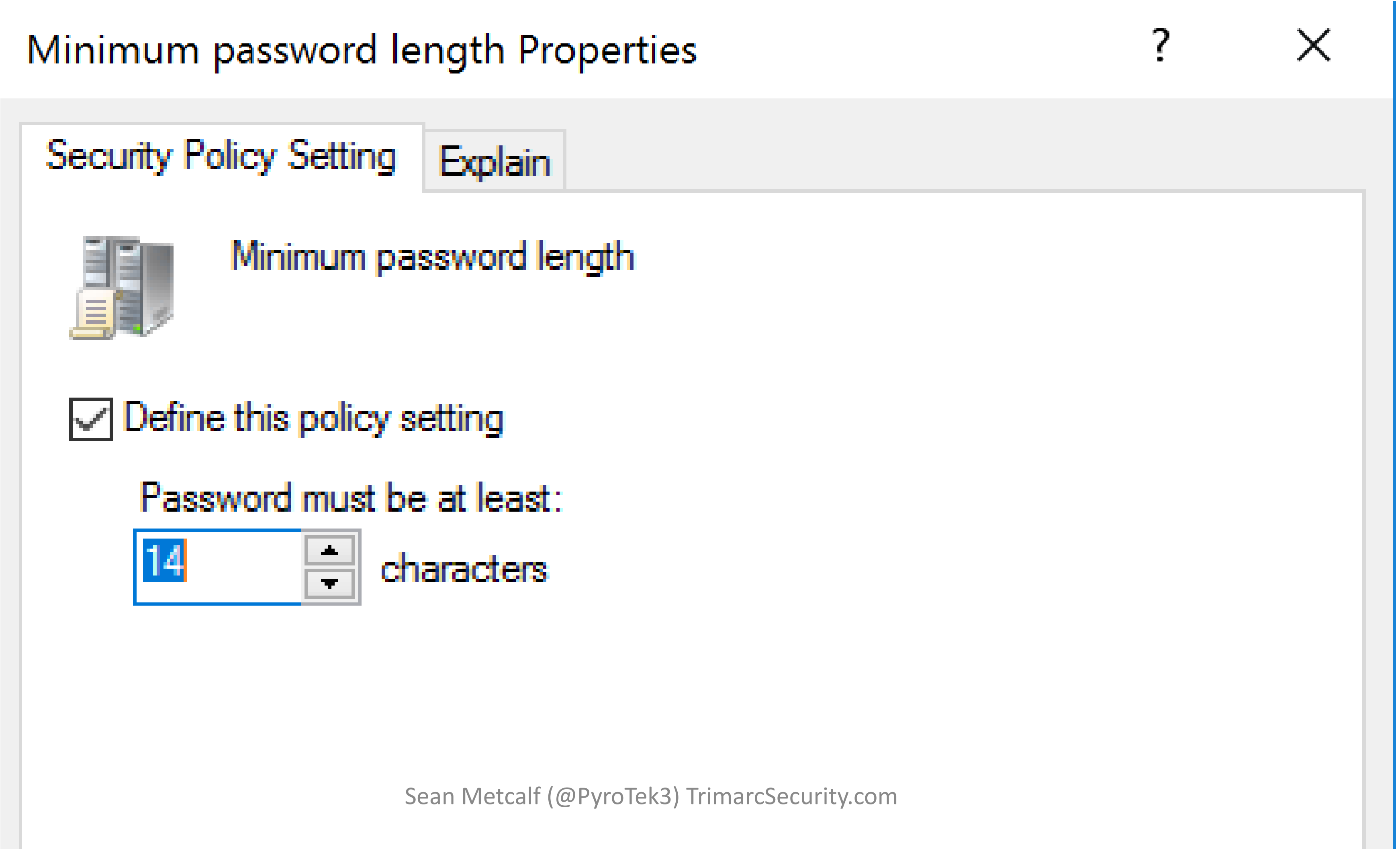
Default Domain Policy



Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

In a new Windows Server 2016 AD Forest,
Still unable to set password minimum to >14 characters (group policy template limitation)



Minimum password length Properties

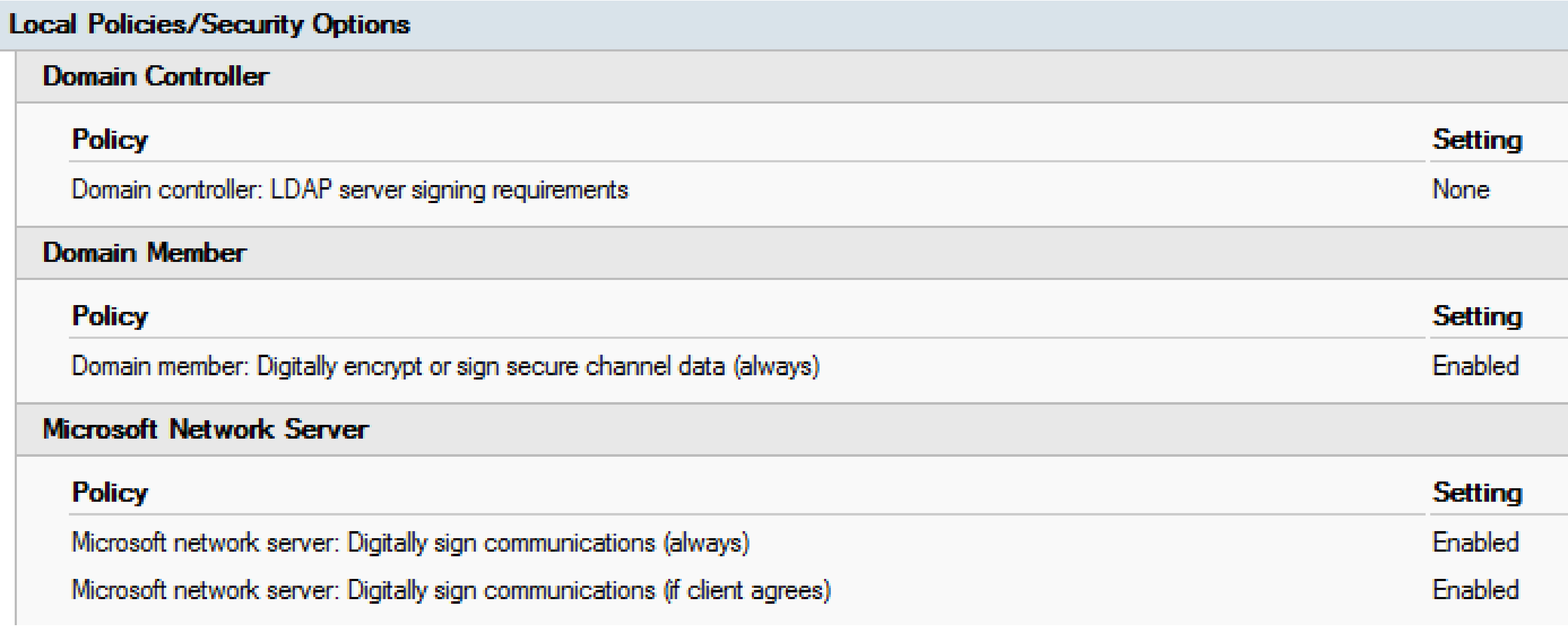
Minimum password length

☑ Define this policy setting

Password must be at least:

14 characters

Default Domain Controllers Policy



Local Policies/Security Options

Domain Controller

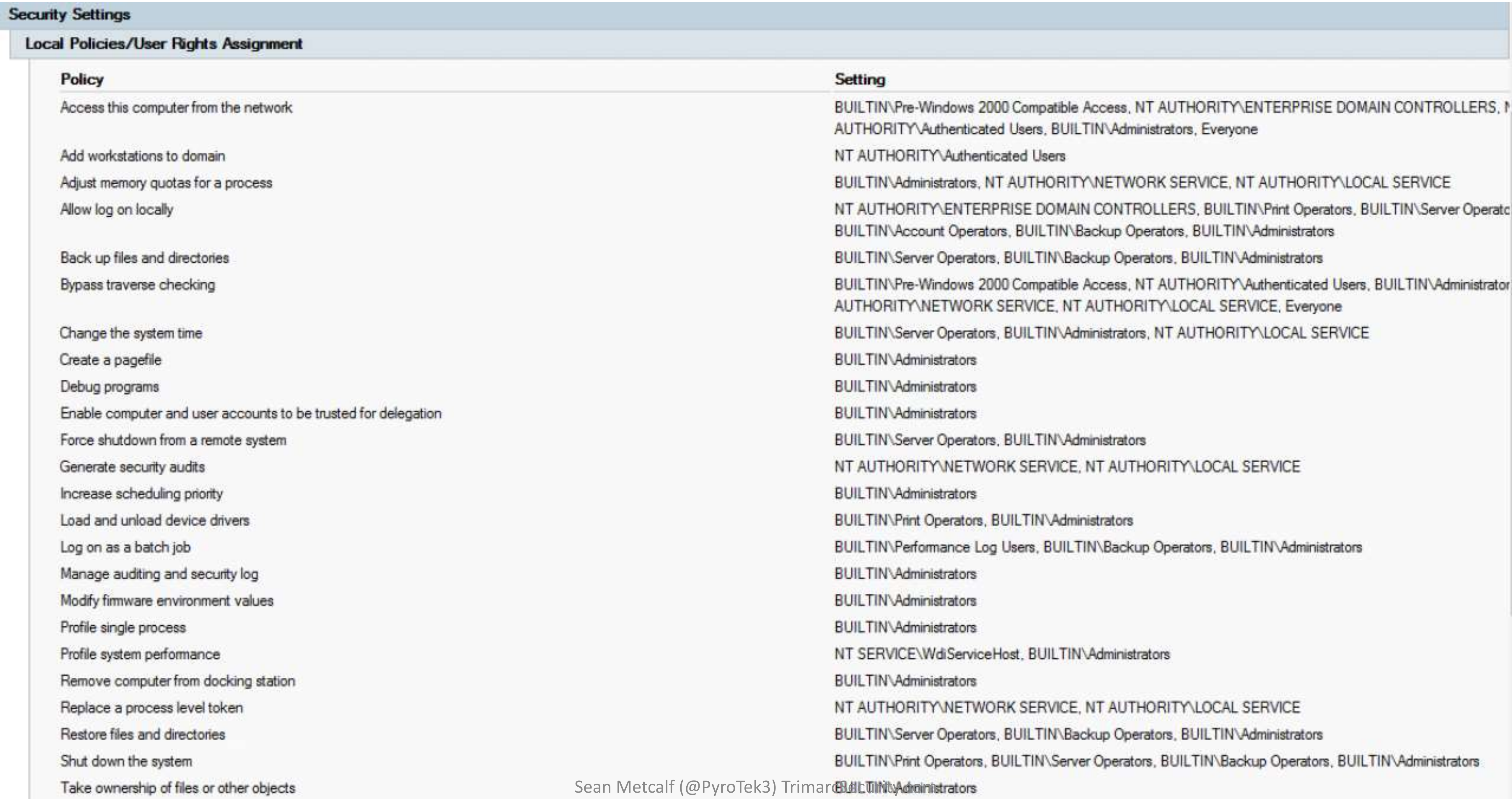
Policy	Setting
Domain controller: LDAP server signing requirements	None

Domain Member

Policy	Setting
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled

Microsoft Network Server

Policy	Setting
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled



Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Access this computer from the network	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, N AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone
Add workstations to domain	NT AUTHORITY\Authenticated Users
Adjust memory quotas for a process	BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Allow log on locally	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Print Operators, BUILTIN\Server Operatc BUILTIN\Account Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Back up files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Bypass traverse checking	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrator AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, Everyone
Change the system time	BUILTIN\Server Operators, BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Create a pagefile	BUILTIN\Administrators
Debug programs	BUILTIN\Administrators
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators
Force shutdown from a remote system	BUILTIN\Server Operators, BUILTIN\Administrators
Generate security audits	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Increase scheduling priority	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Print Operators, BUILTIN\Administrators
Log on as a batch job	BUILTIN\Performance Log Users, BUILTIN\Backup Operators, BUILTIN\Administrators
Manage auditing and security log	BUILTIN\Administrators
Modify firmware environment values	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators
Profile system performance	NT SERVICE\WdiServiceHost, BUILTIN\Administrators
Remove computer from docking station	BUILTIN\Administrators
Replace a process level token	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Restore files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Shut down the system	BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Take ownership of files or other objects	BUILTIN\Administrators

Attacker Capability & Mitigations

Attackers Require…

- Account (credentials)
- Rights (privileges)
- Access (connectivity to resources)

Disrupt the Attacker’s Playbook

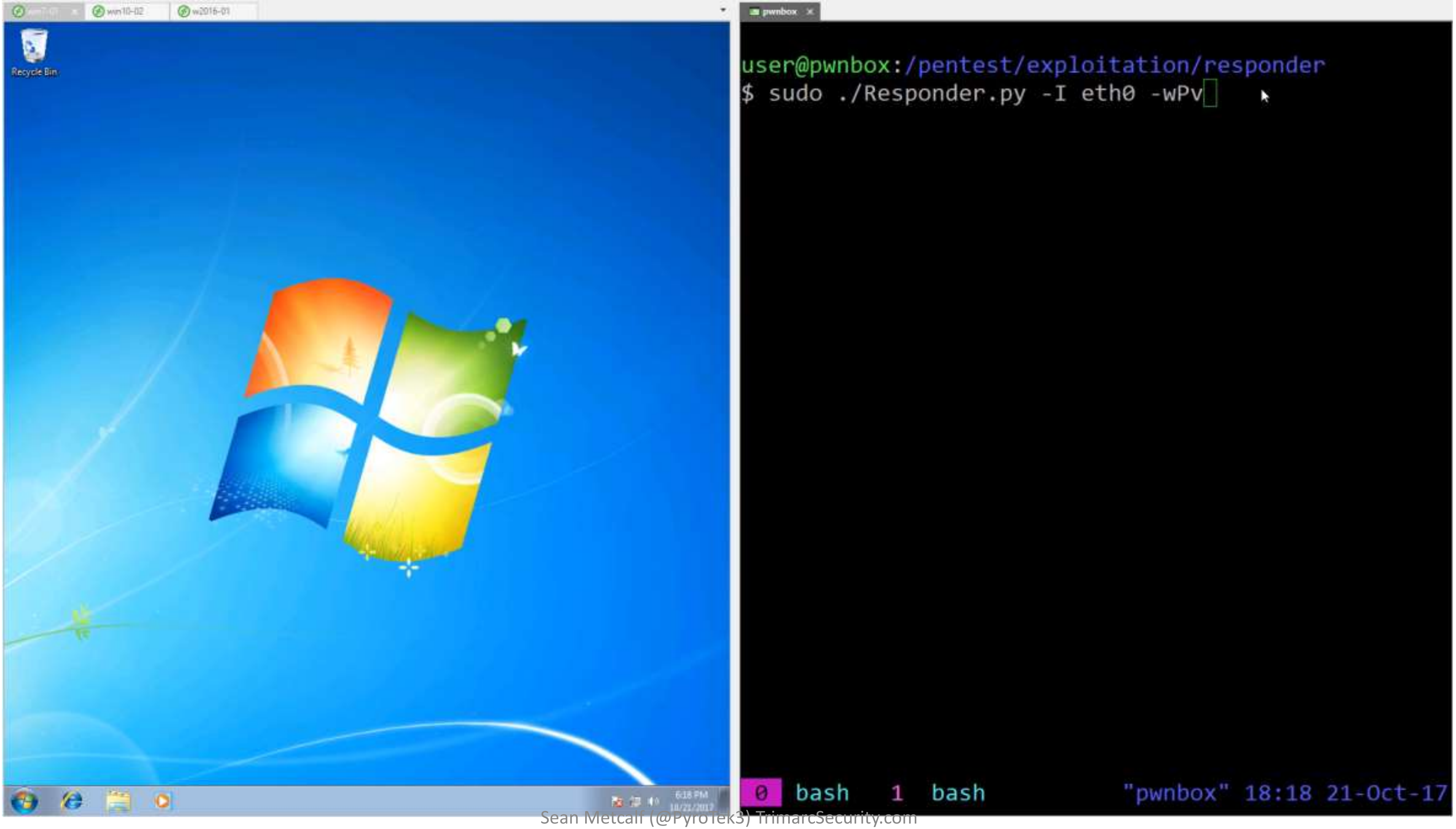
- Prevent access to privileged accounts.
- Limit rights on accounts attackers could gain access to.
- Restrict network communication to admin systems.
- Implement “tripwires” to identify anomalous activity.
- Align detection with potential escalation paths.

Traditional AD Administration

- All admins are Domain Admins.
- Administration from anywhere – servers, workstations, Starbucks.
- Need a service account with AD rights – Domain Admin!
- Need to manage user accounts – Account Operators!
- Need to run backups (anywhere) – Backup Operators!
- Management system deploys software & patches all workstations, servers, & Domain Controllers.
- Agents, everywhere!
- Full Compromise… Likely

Getting Credentials Is Easy

Have you heard of Responder (or Inveigh)?



```
user@pwnbox:/pentest/exploitation/responder
$ sudo ./Responder.py -I eth0 -wPv
```

```
 0  bash   1  bash        "pwnbox" 18:18 21-Oct-17
```

Stopping the Credential "Easy Button"

- Disable NetBIOS
  - DHCP or script
- Disable WPAD
  - Partial mitigation of WPAD issues is possible by installing the Microsoft patch KB3165191 (MS16-077). Hardens the WPAD process and when the system responds to NetBIOS requests.
  - Disable via GPO regkey:
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad, New DWORD (32-Bit Value) called "WpadOverride" and set to "1"
    - Disable the service "WinHTTP Web Proxy Auto-Discovery Service" via GPO
- Disable LLMNR
  - GPO: Computer Configuration/Administrative Templates/Network/DNS Client
  - Set "Turn Off Multicast Name Resolution" to "Enabled"
- Enable SMB Signing

Net Session Enumeration

- NT method for determining where users have authenticated.
- Authenticated users have this right by default.
- Some identity products use this method to map user to IP on the network.
- Bloodhound uses this to identify admin logons.
- Typically target Domain Controllers or file servers.

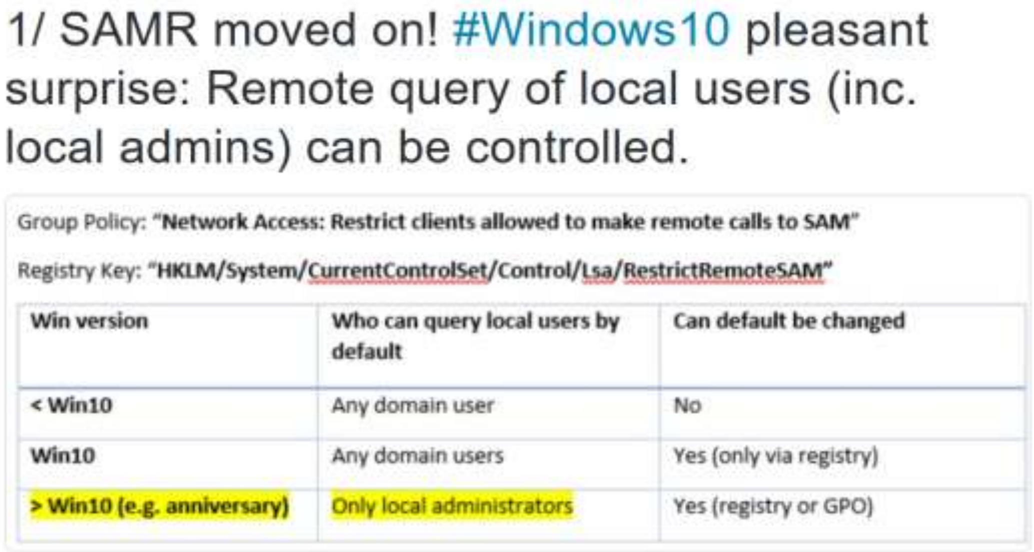
Blocking Net Session Enumeration with NetCease

- The following regkey controls who can perform NetSession Enum:
    - HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/LanmanServer/DefaultSecurity/SrvsvcSessionInfo
- RegKey value *SrvsvcSessionInfo* includes Permissions for:
    - Member of Administrators group (Security Identifier (Sid) S-1-5-32-544)
    - Member of Server Operators group (Sid S-1-5-32-549)
    - Member of Power Users group (Sid S-1-5-32-547)
    - Last but not least Authenticated Users group (Sid S-1-5-11)

https://gallery.technet.microsoft.com/Net-Cease-Blocking-Net-1e8dcb5b

Local Group Enumeration via SAMR

- SAMR provides a method to enumerate local group membership on a Windows system as a user. This includes the local Administrators group!
- Windows 10 provides the ability to limit this capability.
- Windows 10 Anniversary Update (v1607) limits this right to only local Administrators.



1/ SAMR moved on! #Windows10 pleasant surprise: Remote query of local users (inc. local admins) can be controlled.

Group Policy: "**Network Access: Restrict clients allowed to make remote calls to SAM**"

Registry Key: "**HKLM/System/CurrentControlSet/Control/Lsa/RestrictRemoteSAM**"

Win version	**Who can query local users by default**	**Can default be changed**
< Win10	Any domain user	No
Win10	Any domain users	Yes (only via registry)
> Win10 (e.g. anniversary)	Only local administrators	Yes (registry or GPO)

Need Better Controls for These (GPO)

- Fully disable WPAD.
- Disable NETBIOS.
- Change NetSession behavior to limit to specific AD group.
- Ability to enumerate local groups as a user (SAMR) and backport functionality to Windows 7/2008R2

As an Attacker, Do I Need Domain Admin?

No.

Avenues to Compromise

- GPO permissions
- AD Permissions
- Improper group nesting
- Over-permissioned accounts
- Service account access
- Kerberos Delegation
- Password Vaults
- Backup Process

In the Real World, Rights are Everywhere

- Workstation Admins have full control on workstation computer objects and local admin rights.
- Server Admins have full control on server computer objects and local admin rights.
- Often, Server Admins are Exchange Admins.
- Sometimes Server Admins have rights to Domain Controllers.
- Help Desk Admins have local admin rights and remote control on user workstations.
- Local admin accounts & passwords often the same among workstations, and sometimes the same among servers.
- “Temporary” admin group assignments often become permanent.

Red Team Perspective

Securing AD Counterpoint

- AD is only as secure as the AD admin accounts.
- Domain Admin accounts are everywhere!
  - DAs logon to Exchange, SCCM, servers, and workstations.
  - Service Accounts in DA are often used on domain computers.
  - Authenticated security scans can leave privileged creds behind
- Account right is combination of:
  - Group Membership (AD & local computer)
  - Delegated OU & GPO permissions
- Compromise the right account or computer to 0wn AD

Jump (Admin) Servers

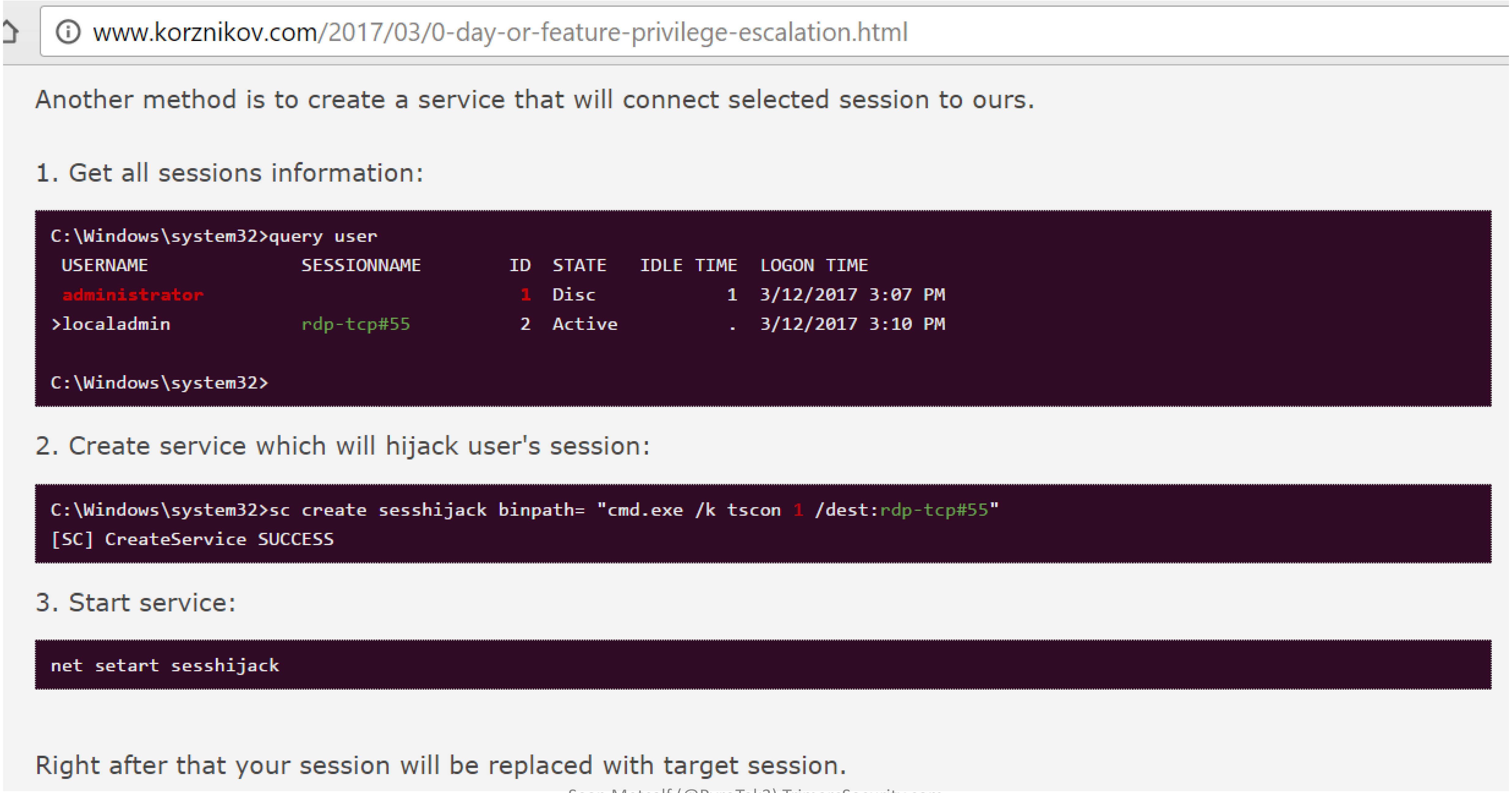
- If Admins are **not** using Admin workstations, keylog for creds on admin’s workstation.
- Discover all potential remoting services.
  - RDP (2FA?)
  - WMI
  - WinRM/PowerShell Remoting
  - PSExec
  - NamedPipe
- Compromise a Jump Server, 0wn the domain!

Hijacking the Admin/Jump Server

- Get Admin on the server
- Get SYSTEM
- Run tscon.exe as SYSTEM

*”if you run tscon.exe as the SYSTEM user, **you can connect to any session without a password”***

https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6



www.korznikov.com/2017/03/0-day-or-feature-privilege-escalation.html

Another method is to create a service that will connect selected session to ours.

1. Get all sessions information:

```
C:\Windows\system32>query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
 administrator                             1  Disc            1  3/12/2017 3:07 PM
>localadmin            rdp-tcp#55          2  Active          .  3/12/2017 3:10 PM

C:\Windows\system32>
```

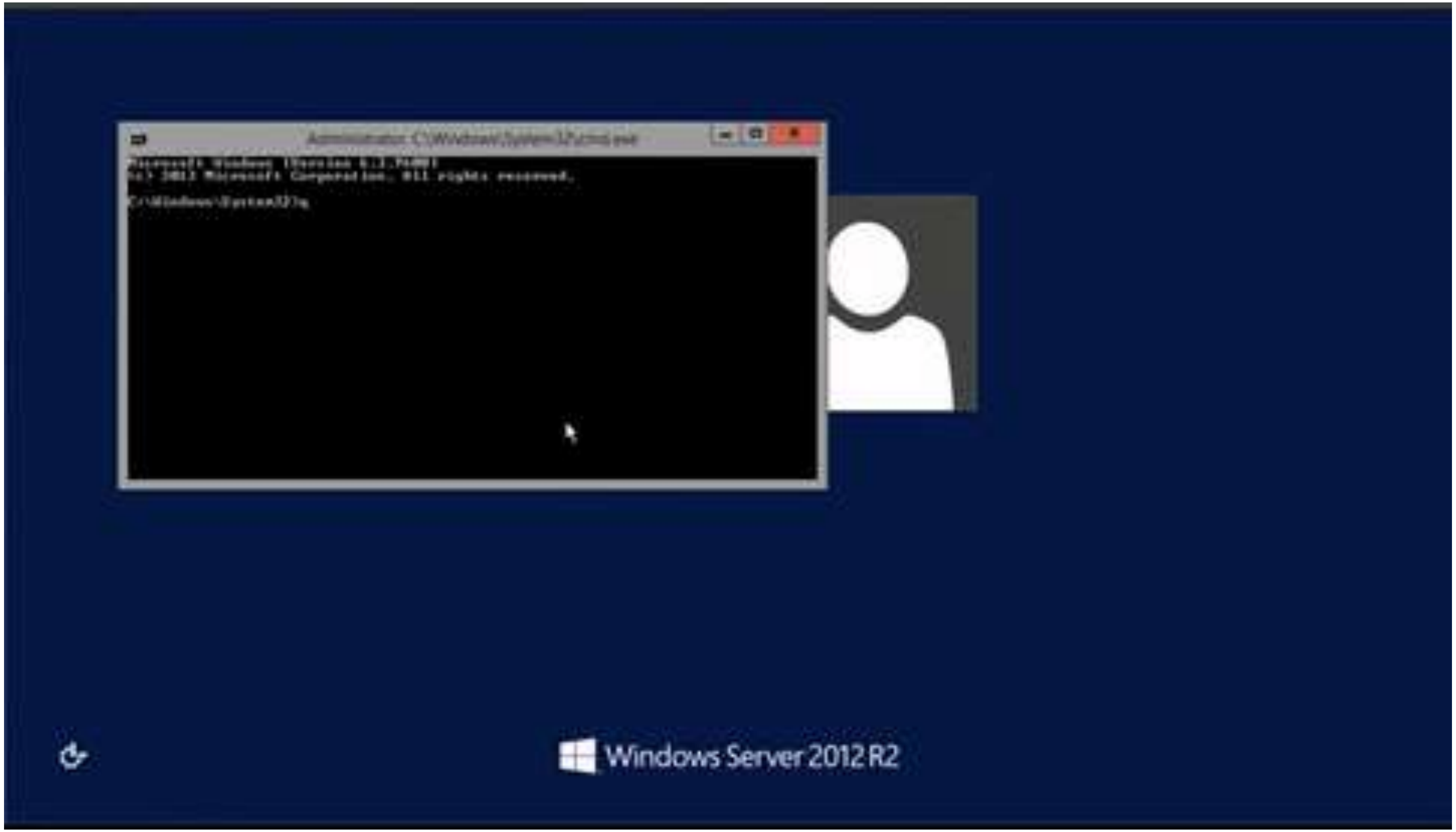
2. Create service which will hijack user's session:

```
C:\Windows\system32>sc create sesshijack binpath= "cmd.exe /k tscon 1 /dest:rdp-tcp#55"
[SC] CreateService SUCCESS
```

3. Start service:

```
net setart sesshijack
```

Right after that your session will be replaced with target session.



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\System32>q
```

Alexander Korznikov demonstrates using Sticky Keys and tscon to access an administrator RDP session — without even logging into the server.

https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6

Universal Bypass for Most Defenses

Service Accounts

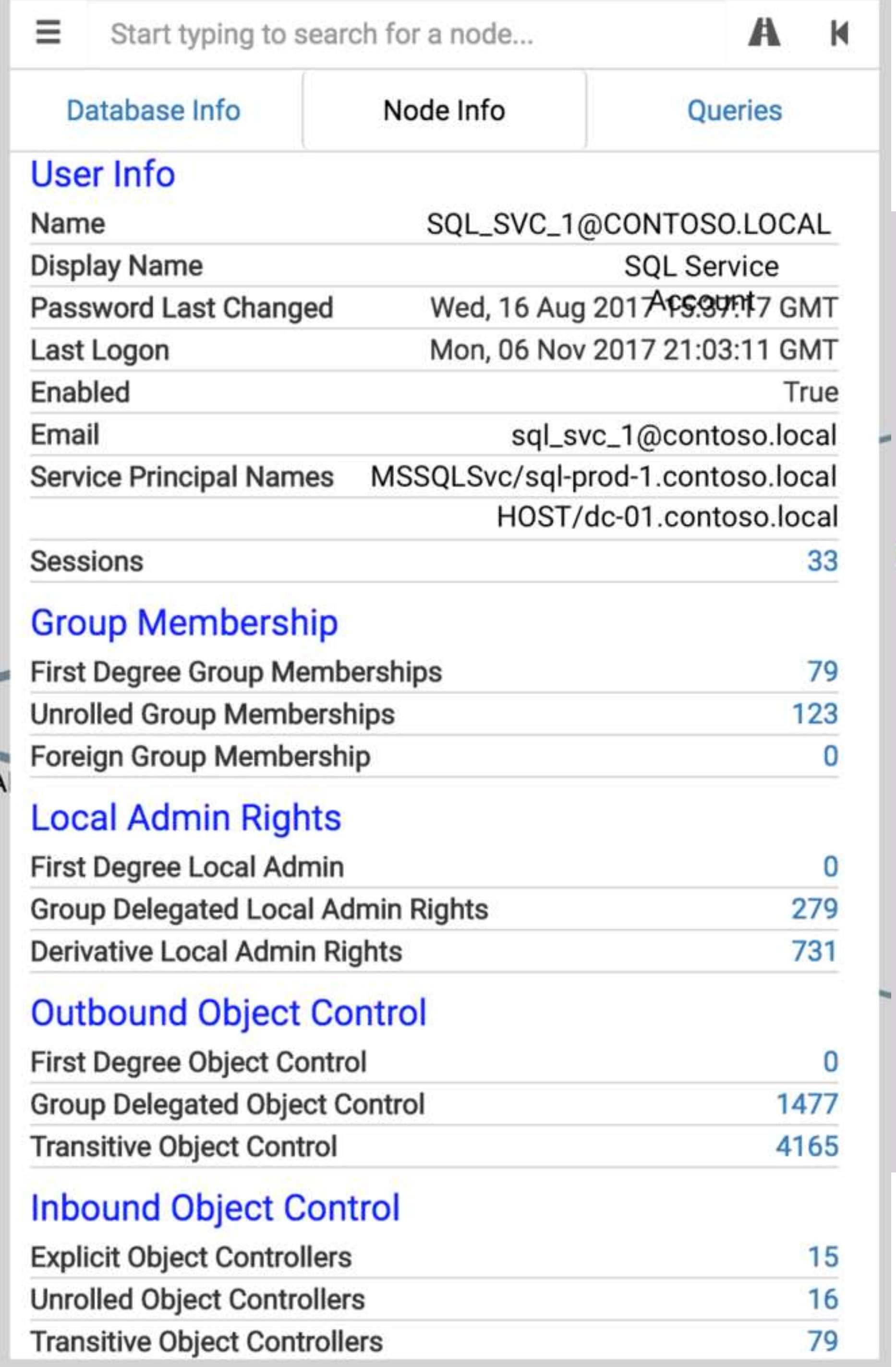
- Over-permissioned
- Not protected like Admins
- Weak passwords
- No 2FA/MFA
- Limited visibility/understanding
- Too much FUD RE: changing

Next-Level Recon: Bloodhound

“BloodHound is a single page Javascript web application, built on top of Linkurious, compiled with Electron, with a Neo4j database fed by a PowerShell ingestor.” (now C#)

- Enumerates users, computers, & groups + NetSession info on logons + AD ACLs.
- Provides a visual representation of attack paths from a computer to Domain Admin.
- Developed by Andy Robbins, Rohan Vazarkar, & Will Schroeder.

https://github.com/BloodHoundAD/BloodHound/wiki



User Info

Name	SQL_SVC_1@CONTOSO.LOCAL
Display Name	SQL Service Account
Password Last Changed	Wed, 16 Aug 2017 15:37:17 GMT
Last Logon	Mon, 06 Nov 2017 21:03:11 GMT
Enabled	True
Email	sql_svc_1@contoso.local
Service Principal Names	MSSQLSvc/sql-prod-1.contoso.local HOST/dc-01.contoso.local
Sessions	33

Group Membership

First Degree Group Memberships	79
Unrolled Group Memberships	123
Foreign Group Membership	0

Local Admin Rights

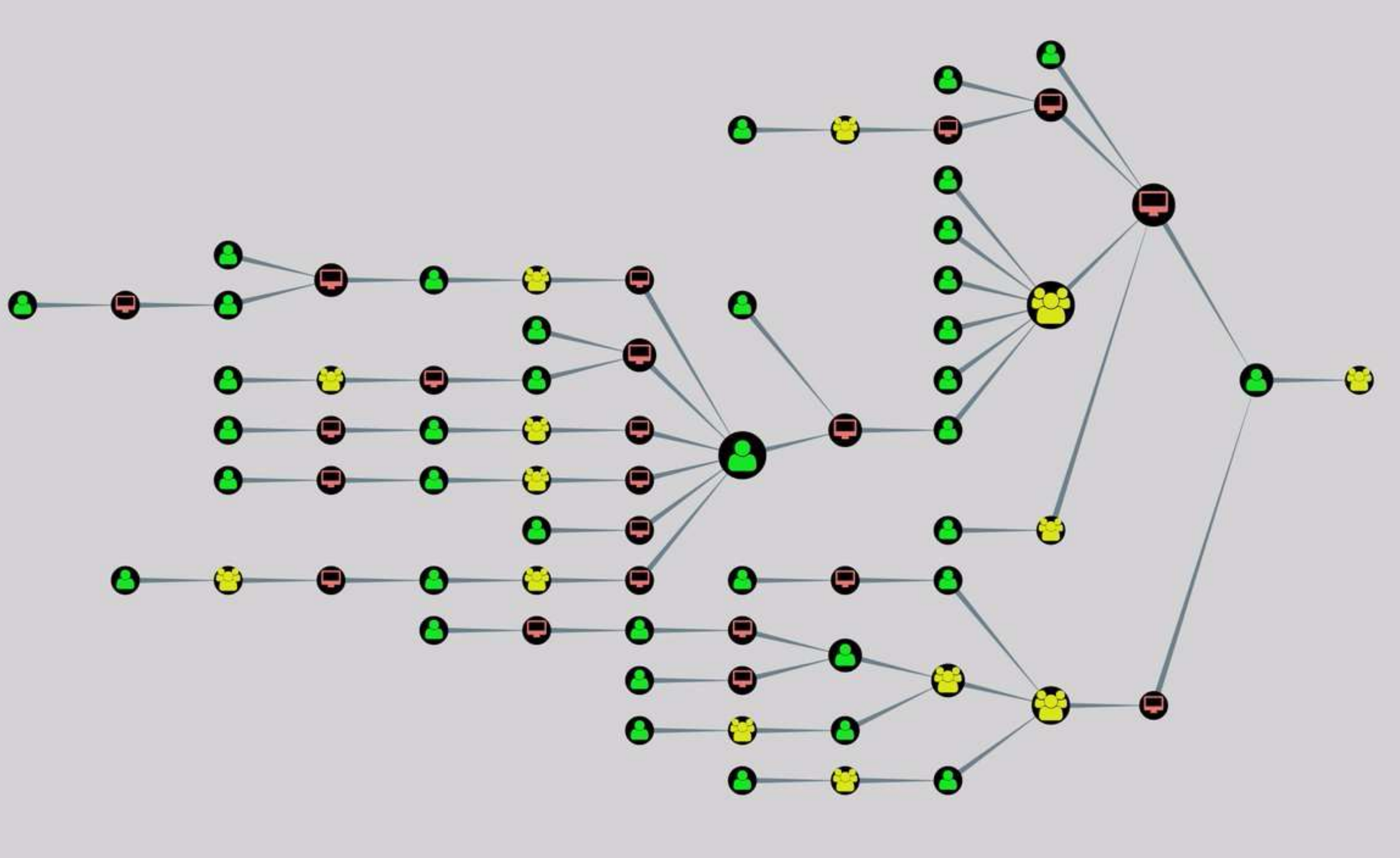
First Degree Local Admin	0
Group Delegated Local Admin Rights	279
Derivative Local Admin Rights	731

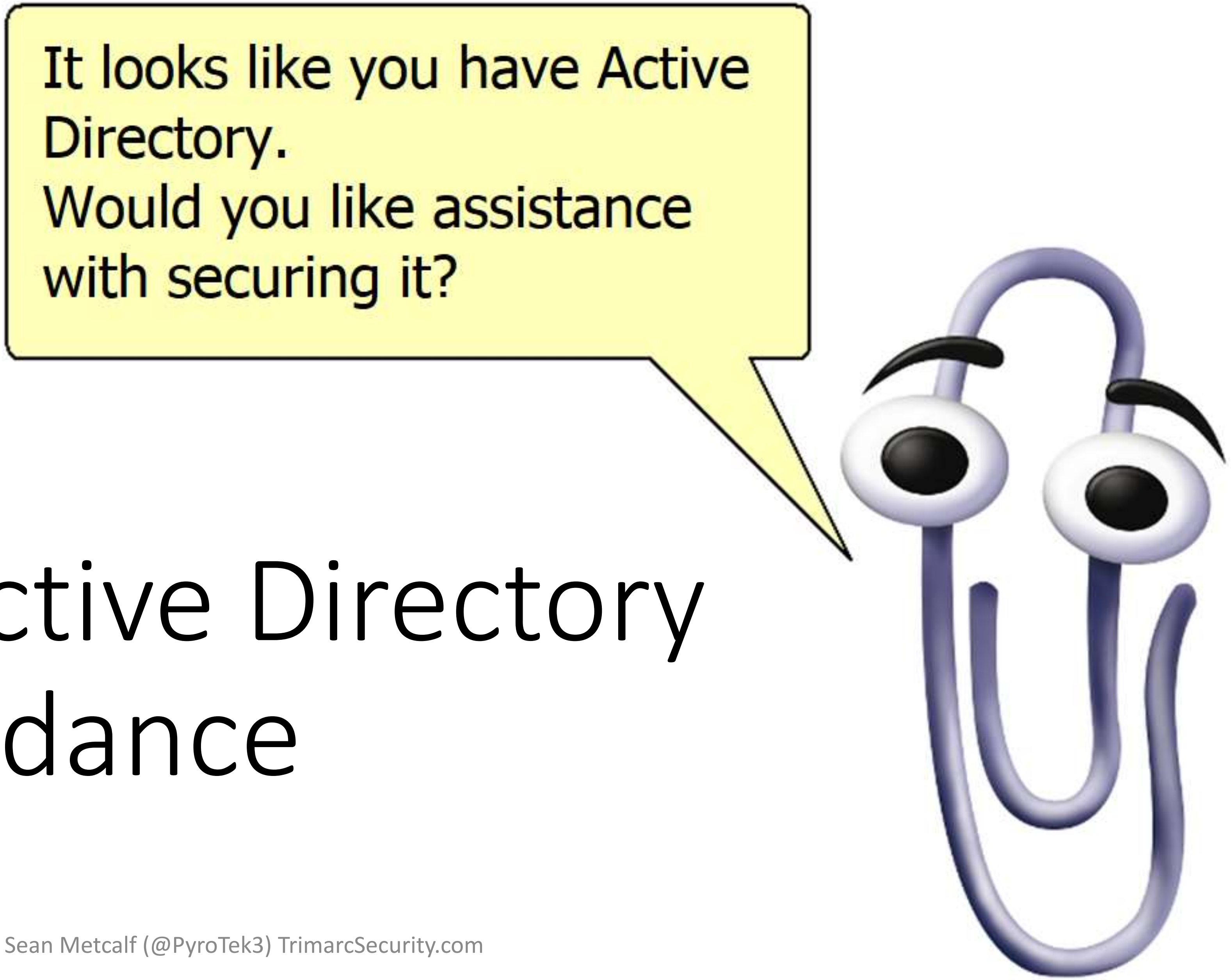
Outbound Object Control

First Degree Object Control	0
Group Delegated Object Control	1477
Transitive Object Control	4165

Inbound Object Control

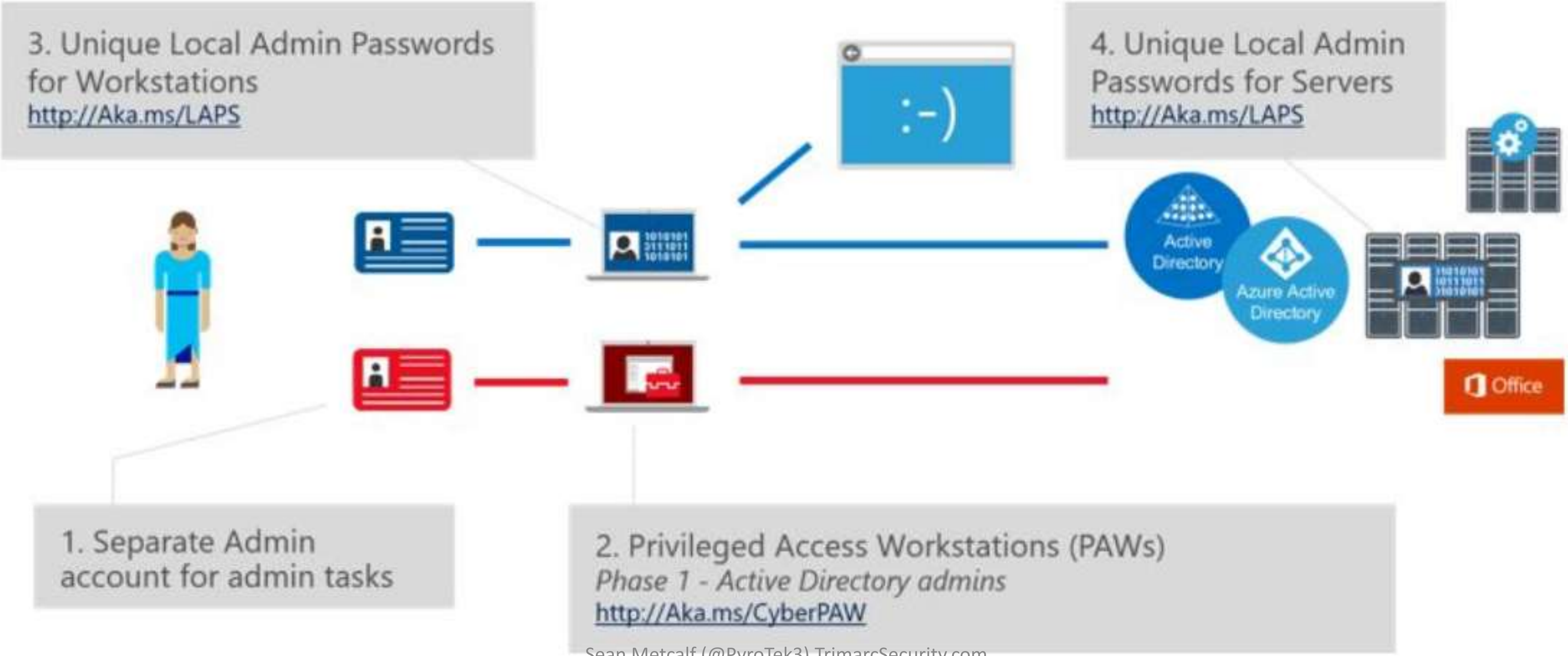
Explicit Object Controllers	15
Unrolled Object Controllers	16
Transitive Object Controllers	79




It looks like you have Active Directory.
Would you like assistance with securing it?

Microsoft Active Directory Security Guidance

Security Privileged Access Roadmap: Stage 1



3. Unique Local Admin Passwords for Workstations
http://Aka.ms/LAPS

4. Unique Local Admin Passwords for Servers
http://Aka.ms/LAPS

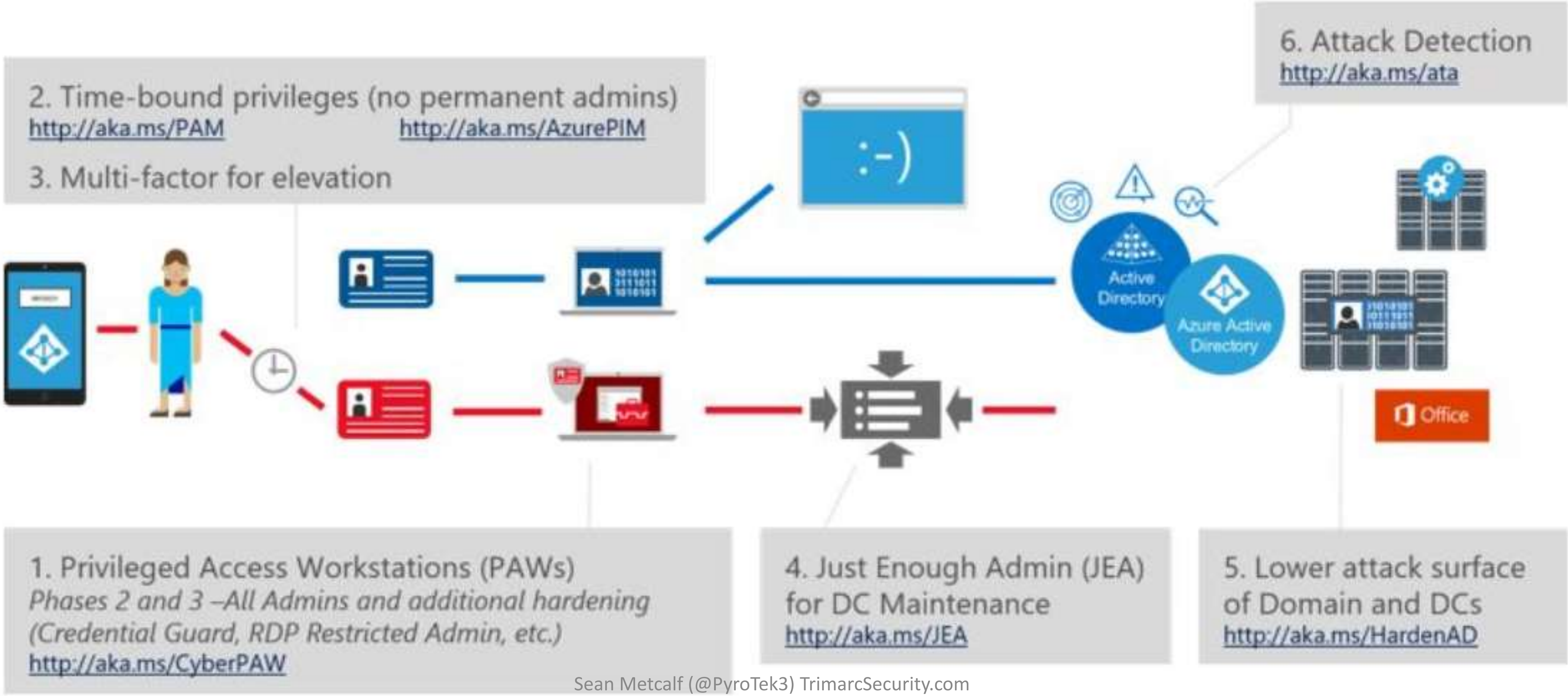
1. Separate Admin account for admin tasks

2. Privileged Access Workstations (PAWs)
Phase 1 - Active Directory admins
http://Aka.ms/CyberPAW

Security Privileged Access Roadmap: Stage 1

- Separate Accounts for User & Admin tasks
  - Agreed, and this should be an easy task to complete.
- Privileged Access Workstations (PAWs) for AD Admin
  - Yes, this should be done. This is really tough in practice.
- Unique Local Admin Accounts (LAPS) for Workstations
  - Not too difficult to deploy, delegation is another story…
  - More difficult to get rid of additional local admin accounts.
- Unique Local Admin Accounts (LAPS) for Servers
  - Many orgs are concerned about this and unsure of path forward.

Security Privileged Access Roadmap: Stage 2



2. Time-bound privileges (no permanent admins)
http://aka.ms/PAM http://aka.ms/AzurePIM

3. Multi-factor for elevation

6. Attack Detection
http://aka.ms/ata

1. Privileged Access Workstations (PAWs)
Phases 2 and 3 –All Admins and additional hardening (Credential Guard, RDP Restricted Admin, etc.)
http://aka.ms/CyberPAW

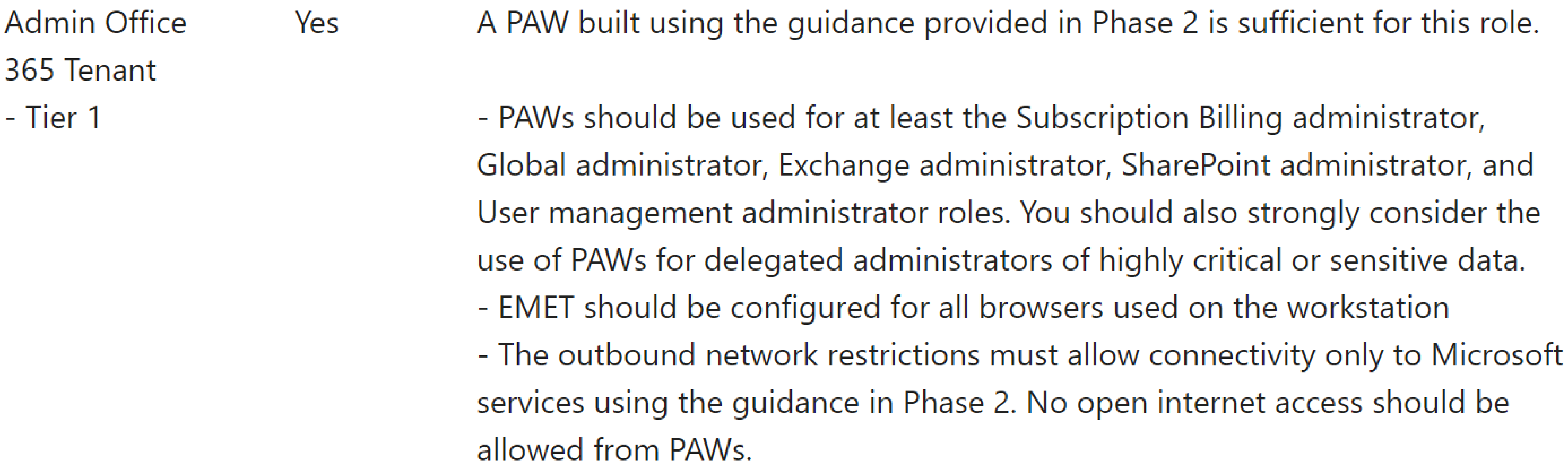
4. Just Enough Admin (JEA) for DC Maintenance
http://aka.ms/JEA

5. Lower attack surface of Domain and DCs
http://aka.ms/HardenAD

Security Privileged Access Roadmap: Stage 2

- Privileged Access Workstation (PAW) for all system administration
  - Ideal, but difficult
- Time-bound privileges (PAM)
  - Aka.ms/PAM → https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services
  - Sounds good, but how?
- Multi Factor for Elevation
  - This can be accomplished with MIM PAM and Azure AD PIM using Azure Multi-factor authentication (MFA).
  - MIM is expensive and requires extensive resources
- Just Enough Administration (JEA) for DC maintenance*
- Lower attack surface of Domain & DCs*
- Attack Detection (ATA)*

PAW Update:
O365 Global Admin Role = Tier 0



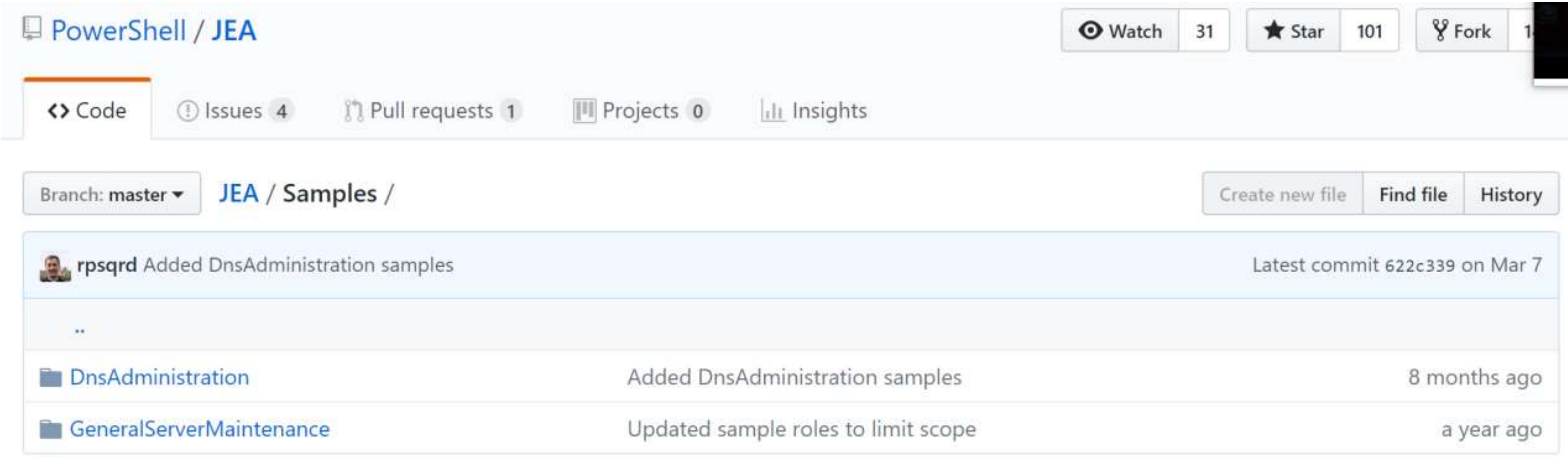
Admin Office 365 Tenant - Tier 1	Yes	A PAW built using the guidance provided in Phase 2 is sufficient for this role. - PAWs should be used for at least the Subscription Billing administrator, Global administrator, Exchange administrator, SharePoint administrator, and User management administrator roles. You should also strongly consider the use of PAWs for delegated administrators of highly critical or sensitive data. - EMET should be configured for all browsers used on the workstation - The outbound network restrictions must allow connectivity only to Microsoft services using the guidance in Phase 2. No open internet access should be allowed from PAWs.

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations

JEA Guidance

4. Just Enough Admin (JEA) for DC Maintenance
http://aka.ms/JEA

- aka.ms/JEA → https://github.com/PowerShell/JEA
- JEA doc only provides info on how to configure DNS service administration on DCs.
- This isn't enough & doesn't warrant pointing to JEA as a "solution" in Stage 2 (better in Stage 3).



JEA / Samples /

rpsqrd Added DnsAdministration samples — Latest commit 622c339 on Mar 7

..

DnsAdministration	Added DnsAdministration samples	8 months ago
GeneralServerMaintenance	Updated sample roles to limit scope	a year ago

Lower attack surface of Domain & DCs

- Physical Security
  - Physical DCs
  - Virtual DCs
- Branch Locations
- Domain Controller Operating Systems
- Secure Configuration of Domain Controllers
- Security Configuration Wizard
- Microsoft Security Compliance Manager
- AppLocker
- RDP Restrictions
- Patch and Configuration Management for Domain Controllers
- Blocking Internet Access for Domain Controllers
- Perimeter Firewall Restrictions
- DC Firewall Configurations
- Preventing Web Browsing from Domain Controllers

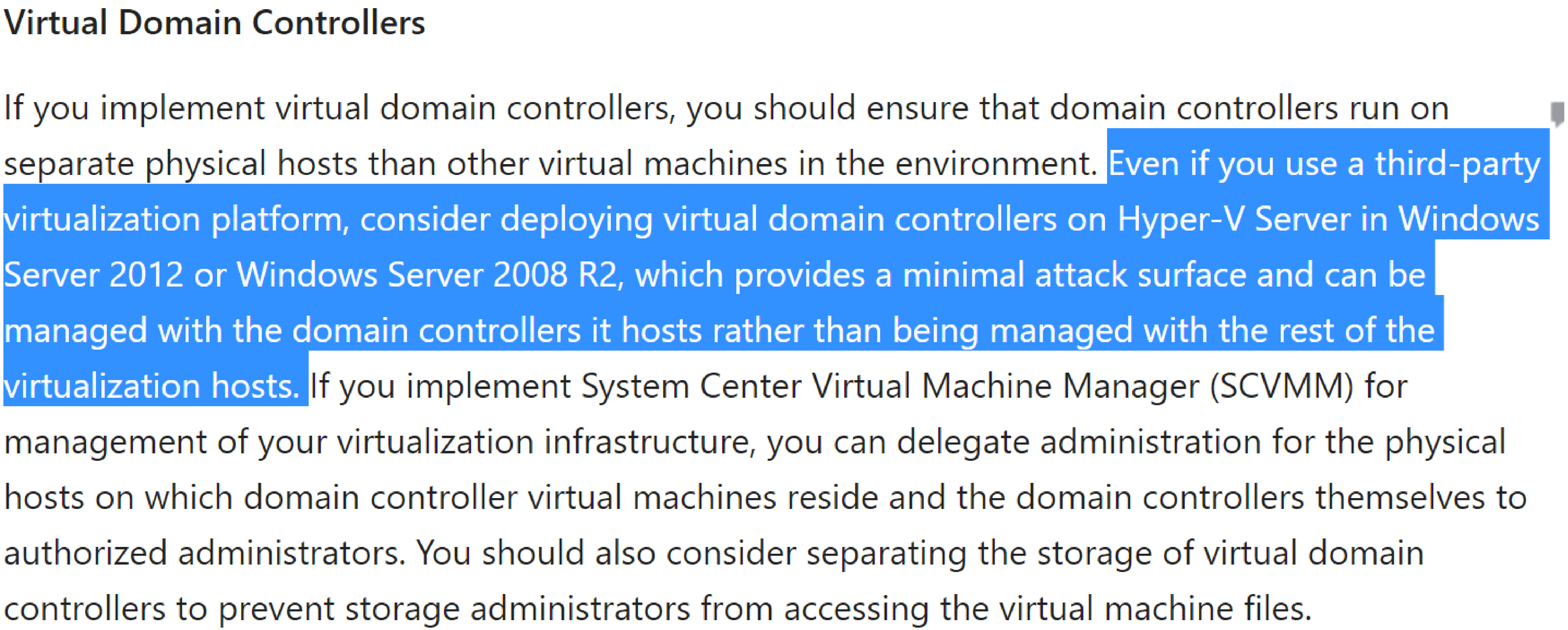
5. Lower attack surface of Domain and DCs
http://aka.ms/HardenAD

Lower attack surface of Domain & DCs: What's Missing?

- Clear guidance on recommended GPO security settings beyond default.
- Protocol/feature reduction/lockdown
- Implementation guidance for implementing Admin systems (PAWs, Admin/Jump servers, etc) to limit management protocols.
- Beyond RDP: Limit WMI, WinRM, etc
- AppLocker on DCs…
- The last 4 - 5 items are focused on preventing DC internet access. Use a host firewall/IPSec rule and reinforce on perimeter firewalls and call it a day.

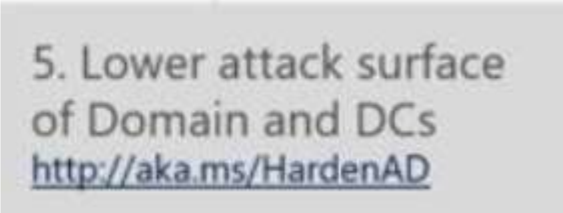
5. Lower attack surface of Domain and DCs
http://aka.ms/HardenAD

Lower attack surface of Domain & DCs



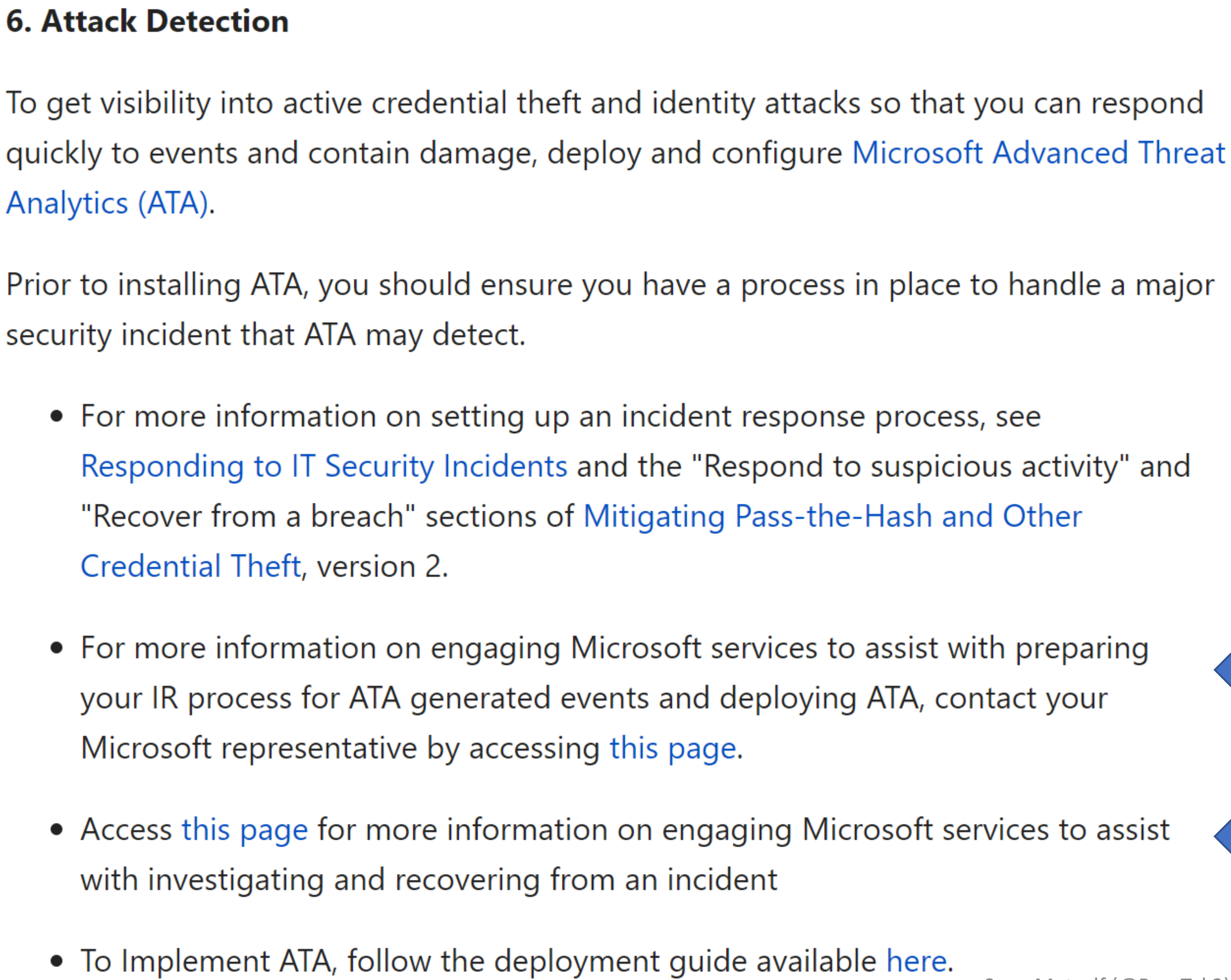
Virtual Domain Controllers

If you implement virtual domain controllers, you should ensure that domain controllers run on separate physical hosts than other virtual machines in the environment. Even if you use a third-party virtualization platform, consider deploying virtual domain controllers on Hyper-V Server in Windows Server 2012 or Windows Server 2008 R2, which provides a minimal attack surface and can be managed with the domain controllers it hosts rather than being managed with the rest of the virtualization hosts. If you implement System Center Virtual Machine Manager (SCVMM) for management of your virtualization infrastructure, you can delegate administration for the physical hosts on which domain controller virtual machines reside and the domain controllers themselves to authorized administrators. You should also consider separating the storage of virtual domain controllers to prevent storage administrators from accessing the virtual machine files.



5. Lower attack surface of Domain and DCs
http://aka.ms/HardenAD

6. Attack Detection
http://aka.ms/ata



6. Attack Detection

To get visibility into active credential theft and identity attacks so that you can respond quickly to events and contain damage, deploy and configure Microsoft Advanced Threat Analytics (ATA).

Prior to installing ATA, you should ensure you have a process in place to handle a major security incident that ATA may detect.

- For more information on setting up an incident response process, see Responding to IT Security Incidents and the "Respond to suspicious activity" and "Recover from a breach" sections of Mitigating Pass-the-Hash and Other Credential Theft, version 2.
- For more information on engaging Microsoft services to assist with preparing your IR process for ATA generated events and deploying ATA, contact your Microsoft representative by accessing this page.
- Access this page for more information on engaging Microsoft services to assist with investigating and recovering from an incident
- To Implement ATA, follow the deployment guide available here.

$$

$$

6. Attack Detection
http://aka.ms/ata

Attack Detection: What We Need

A Note About Logon Types (4624)

Logon Type #	Name	Description	Creds on Disk	Creds in Memory
0	**System**	Typically rare, but could alert to malicious activity	Yes	Yes
2	Interactive	Console logon (local keyboard) which includes server KVM or virtual client logon. Also standard RunAs.	No	Yes
3	Network	Accessing file shares, printers, IIS (integrated auth, etc), PowerShell remoting	No	No
4	**Batch**	Scheduled tasks	Yes	Yes
5	**Service**	Services	Yes	Yes
7	Unlock	Unlock the system	No	Yes
8	Network Clear Text	Network logon with password in clear text (IIS basic auth). If over SSL/TLS, this is probably fine.	Maybe	Yes
9	**New Credentials**	RunAs /NetOnly which starts a program with different credentials than logged on user	No	Yes
10	**Remote Interactive**	RDP: Terminal Services, Remote Assistance, R.Desktop	Maybe	Yes*
11	Cached Interactive	Logon with cached credentials (no DC online)	Yes	Yes

Attack Detection: What We Need

6. Attack Detection
http://aka.ms/ata

Event IDs that Matter: All Windows systems

EventID	Description	Impact
1102/517	Event log cleared	Attackers may clear Windows event logs.
4610/4611/ 4614/4622	Local Security Authority modification	Attackers may modify LSA for escalation/persistence.
4648	Explicit credential logon	Typically when a logged on user provides different credentials to access a resource. Requires filtering of “normal”.
4661	A handle to an object was requested	SAM/DSA Access. Requires filtering of “normal”.
4672	Special privileges assigned to new logon	Monitor when someone with admin rights logs on. Is this an account that should have admin rights or a normal user?
4723	Account password change attempted	If it’s not an approved/known pw change, you should know.
4964	Custom Special Group logon tracking	Track admin & “users of interest” logons.
7045/4697	New service was installed	Attackers often install a new service for persistence.
4698 & 4702	Scheduled task creation/modification	Attackers often create/modify scheduled tasks for persistence. Pull all events in Microsoft-Windows-TaskScheduler/Operational
4719/612	System audit policy was changed	Attackers may modify the system’s audit policy.
4732	A member was added to a (security-enabled) local group	Attackers may create a new local account & add it to the local Administrators group.
4720	A (local) user account was created	Attackers may create a new local account for persistence.

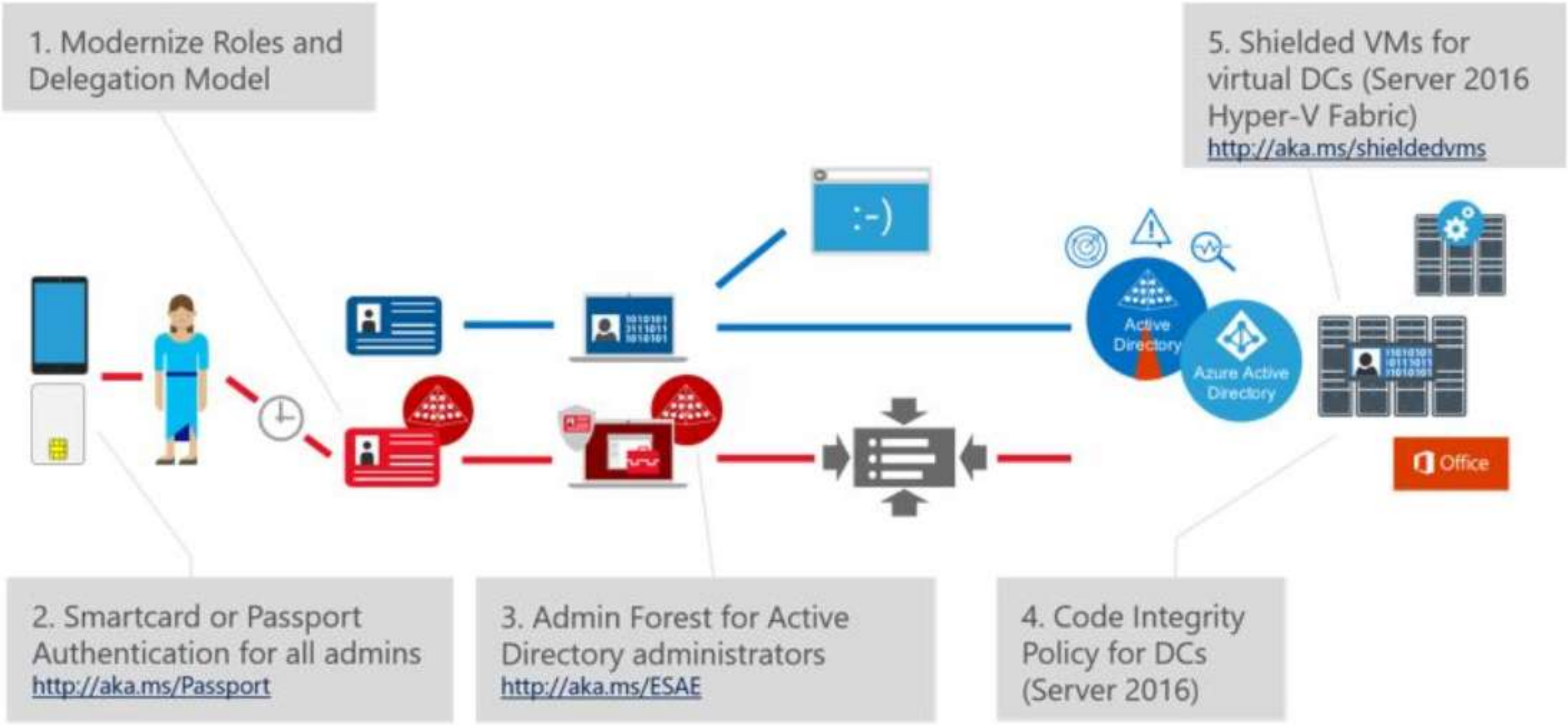
Attack Detection: What We Need

6. Attack Detection
http://aka.ms/ata

Event IDs that Matter: Domain Controllers

EventID	Description	Impact
4768	Kerberos auth ticket (TGT) was requested	Track user Kerb auth, with client/workstation name.
4769	User requests a Kerberos service ticket	Track user resource access requests & Kerberoasting
4964	Custom Special Group logon tracking	Track admin & "users of interest" logons
4625/4771	Logon failure	Interesting logon failures. 4771 with 0x18 = bad pw
4765/4766	SID History added to an account/attempt failed	If you aren't actively migrating accounts between domains, this could be malicious
4794	DSRM account password change attempt	If this isn't expected, could be malicious
4780	ACLs set on admin accounts	If this isn't expected, could be malicious
4739/643	Domain Policy was changed	If this isn't expected, could be malicious
4713/617	Kerberos policy was changed	If this isn't expected, could be malicious
4724/628	Attempt to reset an account's password	Monitor for admin & sensitive account pw reset
4735/639	Security-enabled local group changed	Monitor admin/sensitive group membership changes
4737/641	Security-enabled global group changed	Monitor admin/sensitive group membership changes
4755/659	Security-enabled universal group changed	Monitor admin & sensitive group membership changes
5136	A directory service object was modified	Monitor for GPO changes, admin account modification, specific user attribute modification, etc.

Security Privileged Access Roadmap: Stage 3



1. Modernize Roles and Delegation Model

2. Smartcard or Passport Authentication for all admins http://aka.ms/Passport

3. Admin Forest for Active Directory administrators http://aka.ms/ESAE

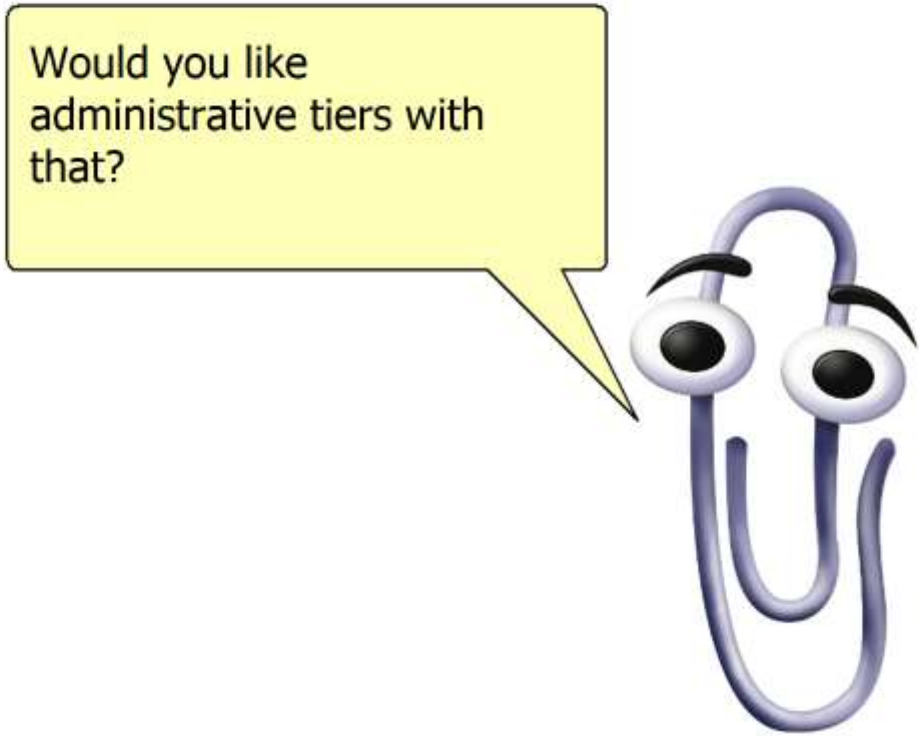
4. Code Integrity Policy for DCs (Server 2016)

5. Shielded VMs for virtual DCs (Server 2016 Hyper-V Fabric) http://aka.ms/shieldedvms

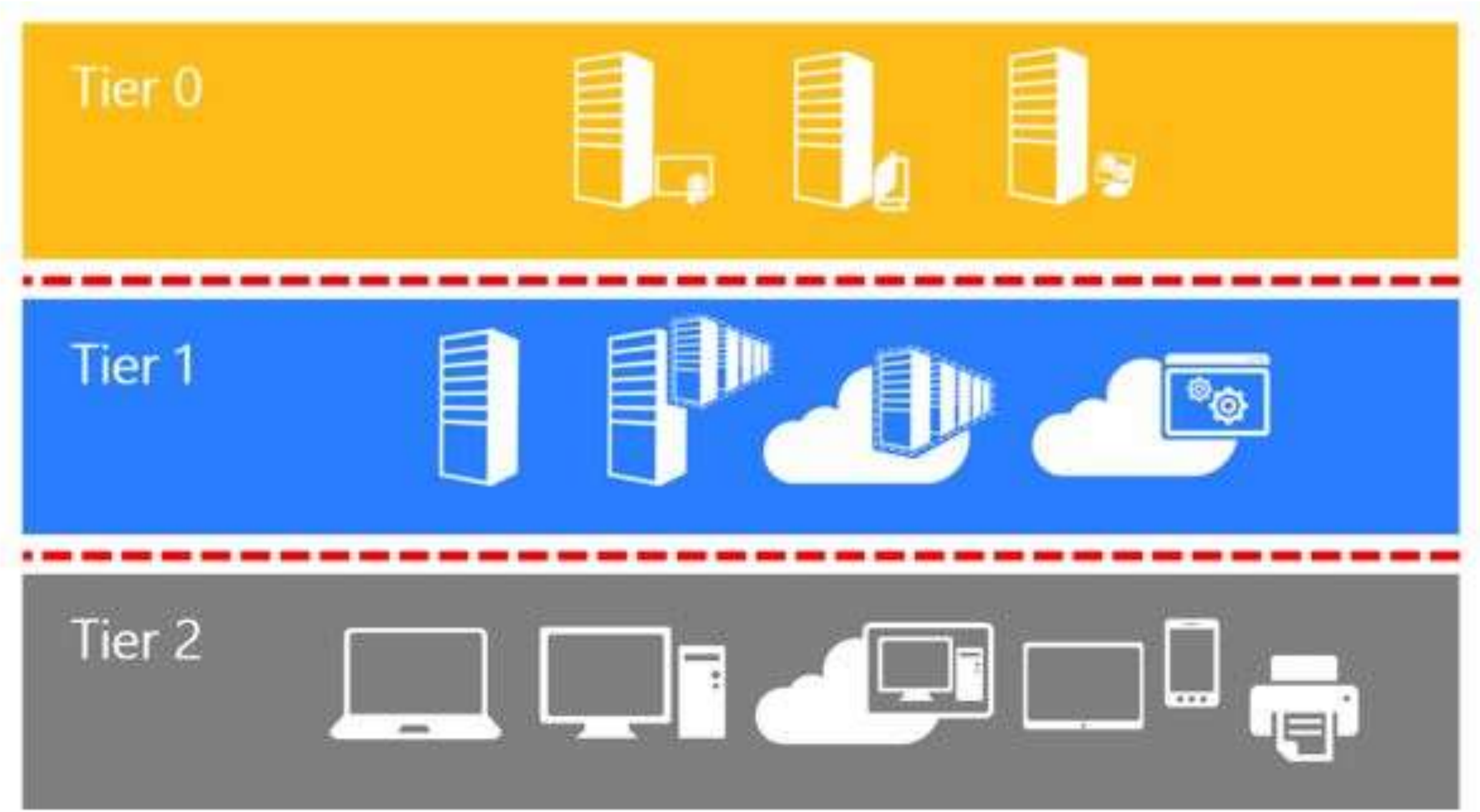
Security Privileged Access Roadmap: Stage 3

- Modernize Roles and Delegation Model
    - Requires discovery of true admin roles and determine what rights are required for each role.
- Smartcard or Passport Authentication for all admins
    - Passport is now Hello for Business & not well documented.
- Admin forest for Active Directory Administrators*
- Code integrity policy for DCs (2016)
    - Requires DCs run Windows Server 2016
- Shielded VMs for DCs (Server 2016 Hyper-V Fabric)
    - Requires Hyper-V servers run Windows Server 2016 and have TPM chips

Let’s Talk Tiers!

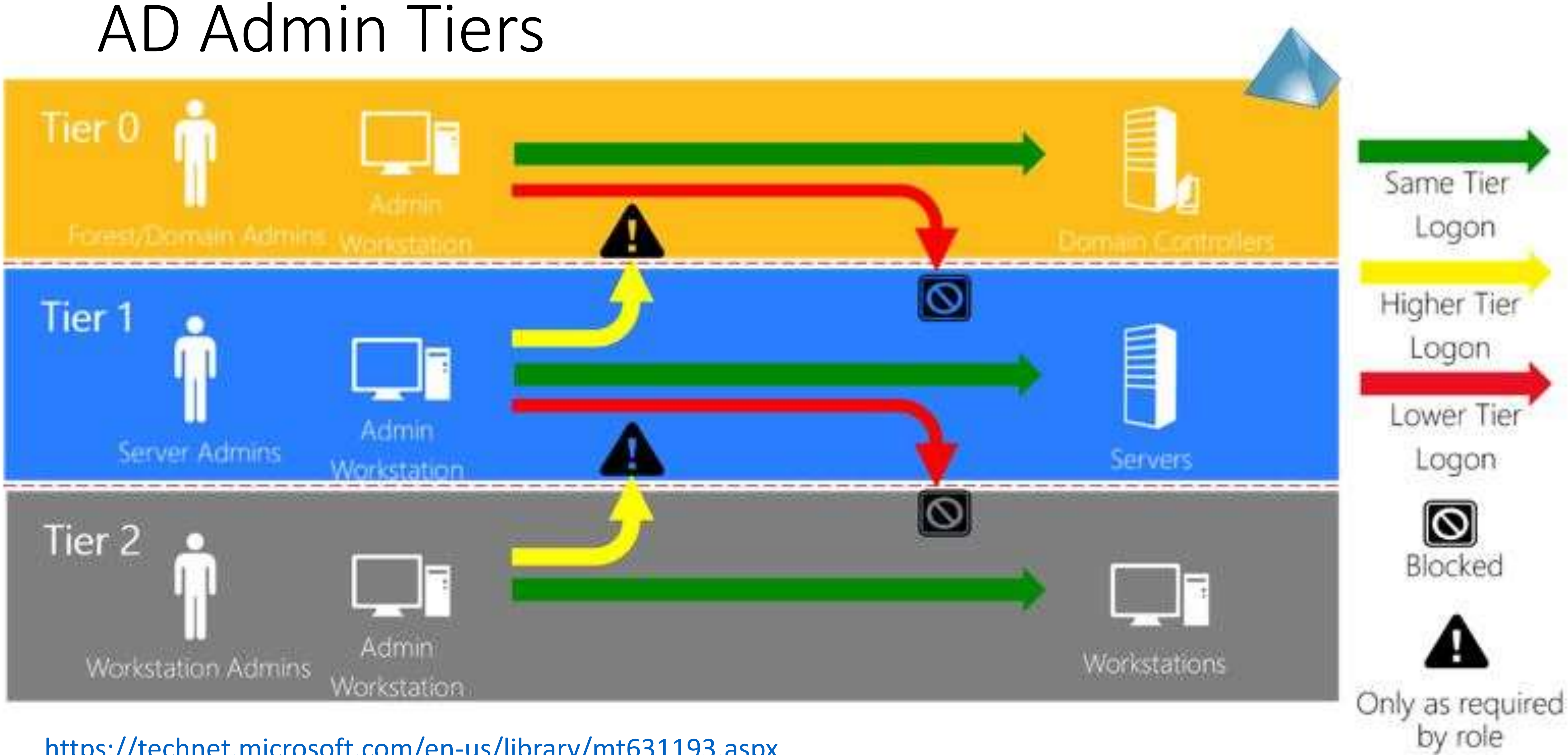


AD Admin Tiers



https://technet.microsoft.com/en-us/library/mt631193.aspx

AD Admin Tiers



https://technet.microsoft.com/en-us/library/mt631193.aspx

Achieving Tier 0: AD Admin & DCs

- DCs have separate management and patching system than other tiers (ex. WSUS or SCCM).
- All admin systems for DCs and other systems in Tier 0 only exist in this tier.
- All AD admin accounts use PAWs.
- All privileged AD service accounts are only on Tier 0 systems.
- Requires all relevant systems to exist in this tier.
  - Domain Controllers
  - ADFS
  - Azure AD Connect Server
  - Virtualization Platform servers

Difficulty Level: High

Achieving Tier 1: Servers & Server Admin

- Servers have separate management and patching system than other tiers (ex. WSUS or SCCM).
- All admin systems for Servers only exist in this tier.
- All admin accounts use PAWs.
- All privileged AD service accounts are only on Tier 1 systems.
- Requires all relevant systems to exist in this tier.

Difficulty Level: High

Achieving Tier 2: Workstations & Administration

- Workstations have separate management and patching system than other tiers (ex. WSUS or SCCM).
- All admin systems for Workstations only exist in this tier.
- All admin accounts use PAWs.
- All privileged AD service accounts are only on Tier 2 systems.
- Requires all relevant systems to exist in this tier.

Difficulty Level:
Medium-High

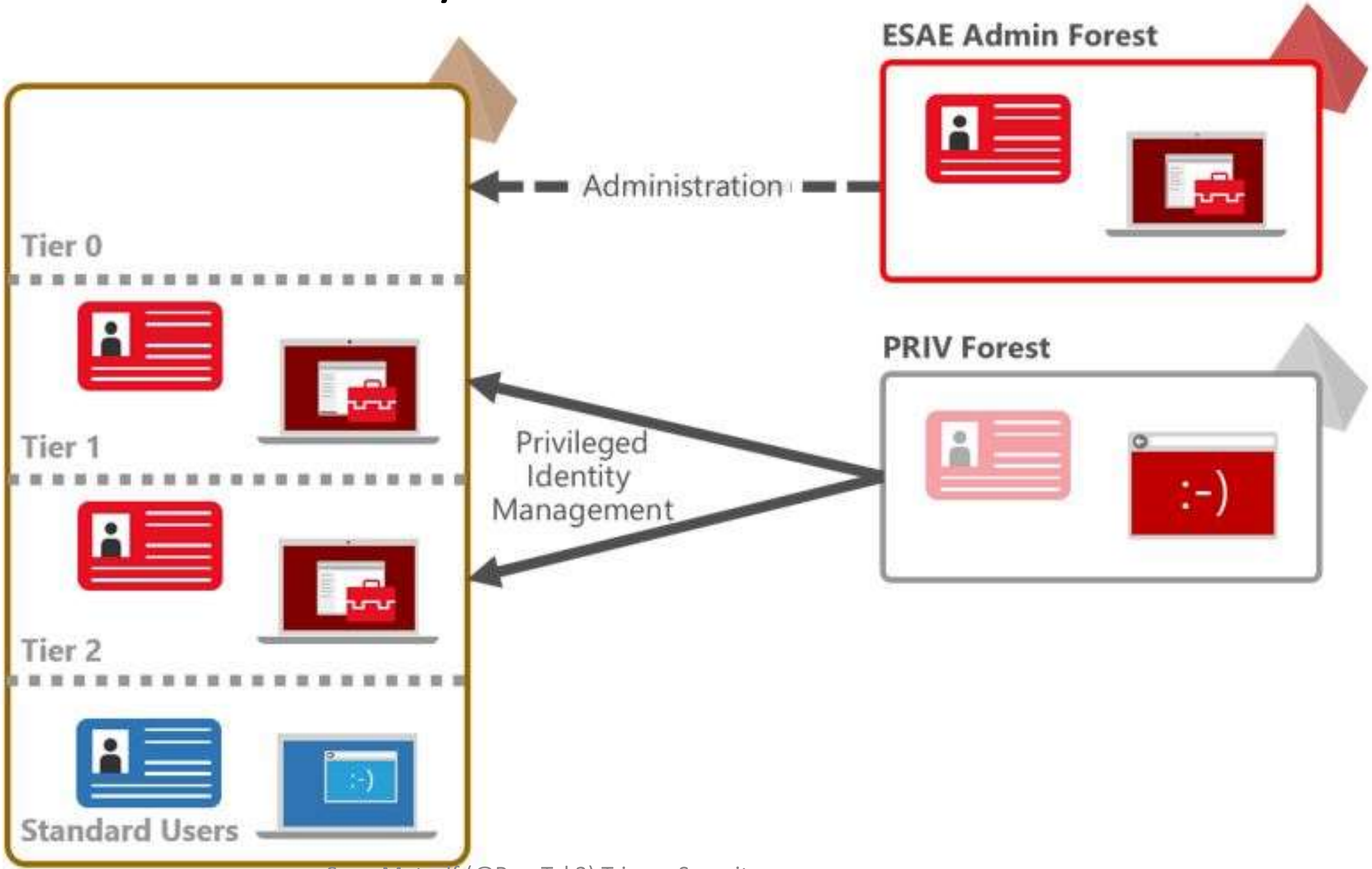
What’s Missing?

- Removing local admin rights from users.
- Limiting broad system access
  - Workstation Admin
  - Server Admin
- Limiting network access from any system to any system.
- Practical guidance on achieving each tier with case studies.
- Service Account risks

Red Forest aka ESAE

Separate forest for Active Directory Administration

Admin Forest
aka Enhanced Security Administrative Environment (ESAE)



ESAE Key Components

- New Windows Server 2016 AD Forest with high security configuration.
- ESAE forest is isolated from the production network with strong network controls and only allows encrypted communication to production DCs & select AD Admin systems.
- 1-way trust with Selective Authentication (production AD forest trusts ESAE).
- Production AD admin groups are empty, except group for ESAE admin groups.
- No production AD admin groups/accounts in ESAE have admin rights to ESAE.
- All systems run Windows 10/ Windows Server 2016.
- Auto-patching by ESAE management/patching system.
- Production AD admin accounts in ESAE should not retain full-time Production AD admin group membership and require MFA for authentication.
- ESAE should be carefully monitored for anomalous activity.

ESAE/Red Forest Implementation

- Assume Breach
- Before deploying, check the environment
- Start clean, stay clean
- If the production AD environment is compromised, what does ESAE buy you?
- What should be done first?

Red Forest Limitations

- Expensive to deploy
- Greatly increases management overhead & cost.
- Duplicate infrastructure.
- Requires physical hardware
- Requires PKI Infrastructure.
- Doesn’t fix production AD issues.
- Doesn’t resolve expansive rights over workstations & servers.

Best Case: Isolates AD Admin accounts

What about domain privileged Service Accounts?

Wrapping It Up

Things that Matter

- Ensure local admin passwords are unique and change regularly.
- Install/enable host firewall on all workstations to prevent lateral movement by attackers and ransomware.
- Host firewalls on servers and Domain Controllers.
- Reduce AD admin group membership.
- Limit service account privileges.
- Ensure AD admins only use AD admin systems (PAW).
- Breaking bad - disabling old & uncommon features and protocols to reduce the Windows attack surface
  - LM, NTLM, SMBv1, LLMNR, WPAD, NetBIOS, etc.
- Control Office macros.

Key Recommendations

- Identify who has AD admin rights (domain/forest) & isolate them to Admin systems. Reducing membership in Domain Admins is only the beginning. Reducing accounts with domain-level privileges is critical.
- Ensure AD & Cloud Admins use PAWs.
- Scan Active Directory Domains, OUs, AdminSDHolder, & GPOs for inappropriate custom permissions.
- Identify and reduce legacy permissions on Active Directory objects.
- Regularly rotate admin credentials (includes KRBTGT, DSRM, etc) quarterly/annually & when AD admins leave.
- Ensure service account password changes occur annually.
- Gain visibility by flowing the most useful security & PowerShell events into SIEM/Splunk.

Sean Metcalf (@Pyrotek3)
sean [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

Slides: Presentations.ADSecurity.org