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)

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
AGENDA

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

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.


Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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...

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
3rd Party Product Permission Requirements

• **Domain** user access
• **Oper**ations systems access
• **Mistaken** identity – trust the installer
• **AD** object rights
• **Install** permissions on systems

• **Active Directory** privileged rights
• **Domain** permissions during install
• **More access** required than often needed.
• **Initial** start/run permissions
• **Needs 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:

<table>
<thead>
<tr>
<th>Type</th>
<th>Principal</th>
<th>Access</th>
<th>Inherited from</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny</td>
<td>Everyone</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>LAPS Password Admins (ADSECLAB\LAPS...</td>
<td>Special</td>
<td>None</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Workstation Admins (ADSECLAB\Work...</td>
<td>Full control</td>
<td>None</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete InetOrgPerson...</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete Computer objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete Group objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete Printer objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete User objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Computers (ADSECLAB\Domain...</td>
<td>Full control</td>
<td>None</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Admins (ADSECLAB\Domain...</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>ENTERPRISE DOMAIN CONTROLLERS</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Authenticated Users</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>SYSTEM</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant InetOrgPerson objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant Group objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant User objects</td>
</tr>
<tr>
<td>Allow</td>
<td>SELF</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Enterprise Admins (ADSECLAB\Enterprise...</td>
<td>Full control</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>List contents</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Administrators (ADSECLAB\Administrators...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>ENTERPRISE DOMAIN CONTROLLERS</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Type</td>
<td>Principal</td>
<td>Access</td>
<td>Inherited from</td>
<td>Applies to</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Deny</td>
<td>Everyone</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>LAPS Password Admins (ADSECLAB\LAPSPASSW...</td>
<td>Special</td>
<td>None</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Workstation Admins (ADSECLAB\Workstatio...</td>
<td>Full control</td>
<td>None</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete InetOrgPerson ...</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete Computer objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete Group objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Print Operators (ADSECLAB\Print Ope...</td>
<td>Create/delete Printer objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Computers (ADSECLAB\Domain...</td>
<td>Full control</td>
<td>None</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Admins (ADSECLAB\Domain Admins...</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>ENTERPRISE DOMAIN CONTROLLERS</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Authenticated Users</td>
<td>Special</td>
<td>None</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>SYSTEM</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant InetOrgPerson objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant Group objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant User objects</td>
</tr>
<tr>
<td>Allow</td>
<td>SELF</td>
<td>Special</td>
<td>None</td>
<td>This object and all descendant objects</td>
</tr>
</tbody>
</table>
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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
## Default Domain Policy

<table>
<thead>
<tr>
<th>Policy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password history</td>
<td>24 passwords remembered</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>42 days</td>
</tr>
<tr>
<td>Minimum password age</td>
<td>1 days</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>7 characters</td>
</tr>
<tr>
<td>Password must meet complexity requirements</td>
<td>Enabled</td>
</tr>
<tr>
<td>Store passwords using reversible encryption</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
## Default Domain Policy

<table>
<thead>
<tr>
<th>Policy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password history</td>
<td>24 passwords remembered</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>42 days</td>
</tr>
<tr>
<td>Minimum password age</td>
<td>1 days</td>
</tr>
<tr>
<td><strong>Minimum password length</strong></td>
<td><strong>7 characters</strong></td>
</tr>
<tr>
<td>Password must meet complexity requirements</td>
<td>Enabled</td>
</tr>
<tr>
<td>Store passwords using reversible encryption</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
In a new Windows Server 2016 AD Forest, Still unable to set password minimum to >14 characters (group policy template limitation)
Default Domain Controllers Policy

<table>
<thead>
<tr>
<th>Local Policies/Security Options</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain Controller</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Policy</strong></td>
<td></td>
</tr>
<tr>
<td>Domain controller: LDAP server signing</td>
<td>None</td>
</tr>
<tr>
<td>requirements</td>
<td></td>
</tr>
<tr>
<td><strong>Domain Member</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Policy</strong></td>
<td></td>
</tr>
<tr>
<td>Domain member: Digitally encrypt or sign</td>
<td>Enabled</td>
</tr>
<tr>
<td>secure channel data (always)</td>
<td></td>
</tr>
<tr>
<td><strong>Microsoft Network Server</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Policy</strong></td>
<td></td>
</tr>
<tr>
<td>Microsoft network server: Digitally sign</td>
<td>Enabled</td>
</tr>
<tr>
<td>communications (always)</td>
<td></td>
</tr>
<tr>
<td>Microsoft network server: Digitally sign</td>
<td>Enabled</td>
</tr>
<tr>
<td>communications (if client agrees)</td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td>Setting</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Access this computer from the network</td>
<td>BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone</td>
</tr>
<tr>
<td>Add workstations to domain</td>
<td>NT AUTHORITY\Authenticated Users</td>
</tr>
<tr>
<td>Adjust memory quotas for a process</td>
<td>BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE</td>
</tr>
<tr>
<td>Allow log on locally</td>
<td>NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Account Operators, BUILTIN\Backup Operators, BUILTIN\Administrators</td>
</tr>
<tr>
<td>Back up files and directories</td>
<td>BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators</td>
</tr>
<tr>
<td>Bypass traverse checking</td>
<td>BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, Everyone</td>
</tr>
<tr>
<td>Change the system time</td>
<td>BUILTIN\Administrators</td>
</tr>
<tr>
<td>Create a pagefile</td>
<td>BUILTIN\Administrators</td>
</tr>
<tr>
<td>Debug programs</td>
<td>BUILTIN\Administrators</td>
</tr>
<tr>
<td>Enable computer and user accounts to be trusted for delegation</td>
<td>BUILTIN\Server Operators, BUILTIN\Administrators</td>
</tr>
<tr>
<td>Force shutdown from a remote system</td>
<td>NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE</td>
</tr>
<tr>
<td>Generate security audits</td>
<td>BUILTIN\Administrators</td>
</tr>
<tr>
<td>Increase scheduling priority</td>
<td>BUILTIN\Print Operators, BUILTIN\Administrators</td>
</tr>
<tr>
<td>Load and unload device drivers</td>
<td>BUILTIN\Administrators</td>
</tr>
<tr>
<td>Log on as a batch job</td>
<td>BUILTIN\Performance Log Users, BUILTIN\Backup Operators, BUILTIN\Administrators</td>
</tr>
<tr>
<td>Manage auditing and security log</td>
<td>BUILTIN\Administrators</td>
</tr>
<tr>
<td>Modify firmware environment values</td>
<td>BUILTIN\Administrators</td>
</tr>
<tr>
<td>Profile single process</td>
<td>BUILTIN\Administrators</td>
</tr>
<tr>
<td>Profile system performance</td>
<td>BUILTIN\Administrators</td>
</tr>
<tr>
<td>Remove computer from docking station</td>
<td>NT SERVICE\WdServiceHost, BUILTIN\Administrators</td>
</tr>
<tr>
<td>Replace a process level token</td>
<td>BUILTIN\Administrators</td>
</tr>
<tr>
<td>Restore files and directories</td>
<td>NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE</td>
</tr>
<tr>
<td>Shut down the system</td>
<td>BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators</td>
</tr>
<tr>
<td>Take ownership of files or other objects</td>
<td>BUILTIN\Administrators</td>
</tr>
</tbody>
</table>
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
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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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/Lan
    manServer/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
Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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.
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 own AD

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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
  • PSEexec
  • NamedPipe

• Compromise a Jump Server, Own 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
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  rdp-tcp#55      1 Disc     1 3/12/2017 3:07 PM
>localadmin    rdp-tcp#55      2 Active    3 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 start sesshijack
```

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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
<table>
<thead>
<tr>
<th>User Info</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td><a href="mailto:SQL_SVC_1@CONTOSO.LOCAL">SQL_SVC_1@CONTOSO.LOCAL</a></td>
</tr>
<tr>
<td>Display Name</td>
<td>SQL Service</td>
</tr>
<tr>
<td>Password Last Changed</td>
<td>Wed, 16 Aug 2017 17:27 GMT</td>
</tr>
<tr>
<td>Last Logon</td>
<td>Mon, 06 Nov 2017 21:03:11 GMT</td>
</tr>
<tr>
<td>Enabled</td>
<td>True</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:sql_svc_1@contoso.local">sql_svc_1@contoso.local</a></td>
</tr>
<tr>
<td>Service Principal Names</td>
<td>MSSQLSvc/sql-prod-1.contoso.local</td>
</tr>
<tr>
<td></td>
<td>HOST/dc-01.contoso.local</td>
</tr>
<tr>
<td>Sessions</td>
<td>33</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group Membership</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>First Degree Group Memberships</td>
<td>79</td>
</tr>
<tr>
<td>Unrolled Group Memberships</td>
<td>123</td>
</tr>
<tr>
<td>Foreign Group Membership</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local Admin Rights</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>First Degree Local Admin</td>
<td>0</td>
</tr>
<tr>
<td>Group Delegated Local Admin Rights</td>
<td>279</td>
</tr>
<tr>
<td>Derivative Local Admin Rights</td>
<td>731</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outbound Object Control</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>First Degree Object Control</td>
<td>0</td>
</tr>
<tr>
<td>Group Delegated Object Control</td>
<td>1477</td>
</tr>
<tr>
<td>Transitive Object Control</td>
<td>4165</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inbound Object Control</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Explicit Object Controllers</td>
<td>15</td>
</tr>
<tr>
<td>Unrolled Object Controllers</td>
<td>16</td>
</tr>
<tr>
<td>Transitive Object Controllers</td>
<td>79</td>
</tr>
</tbody>
</table>
Microsoft Active Directory
Security Guidance

It looks like you have Active Directory. Would you like assistance with securing it?
Security Privileged Access Roadmap: Stage 1

1. Separate Admin account for admin tasks
2. Privileged Access Workstations (PAWs)
   Phase 1 - Active Directory admins
   http://Aka.ms/CyberPAW
3. Unique Local Admin Passwords for Workstations
   http://Aka.ms/LAPS
4. Unique Local Admin Passwords for Servers
   http://Aka.ms/LAPS

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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.

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Security Privileged Access Roadmap: Stage 2

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

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

3. Multi-factor for elevation

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

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

6. Attack Detection
   http://aka.ms/ata
Security Privileged Access Roadmap: Stage 2

• Privileged Access Workstation (PAW) for all system administration
  • Ideal, but difficult

• Time-bound privileges (PAM)
  • 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: Yes
365 Tenant - Tier 1

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
JEA Guidance

- 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).
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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

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.
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.
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.
## Attack Detection: What We Need

### A Note About Logon Types (4624)

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

## Event IDs that Matter: All Windows systems

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

### Event IDs that Matter: Domain Controllers

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

Sean Metcalfe (@PyroTek3 | sean@TrimarcSecurity.com)
Security Privileged Access Roadmap: Stage 3

1. Modernize Roles and Delegation Model

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

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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!

Would you like administrative tiers with that?
AD Admin Tiers

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Red Forest aka ESAE
Separate forest for Active Directory Administration
Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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.

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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.