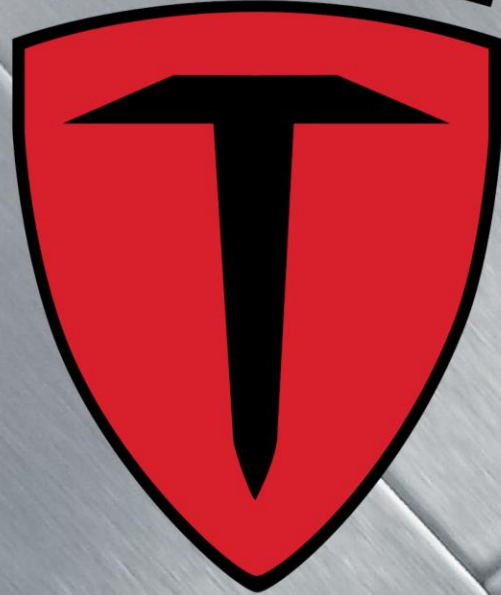


TRIMARC



WEBCAST

**WILL BEGIN SHORTLY**

# TRIMARC SECURITY





**Trimarc is your Trusted Advisor  
For Securing your Enterprise**



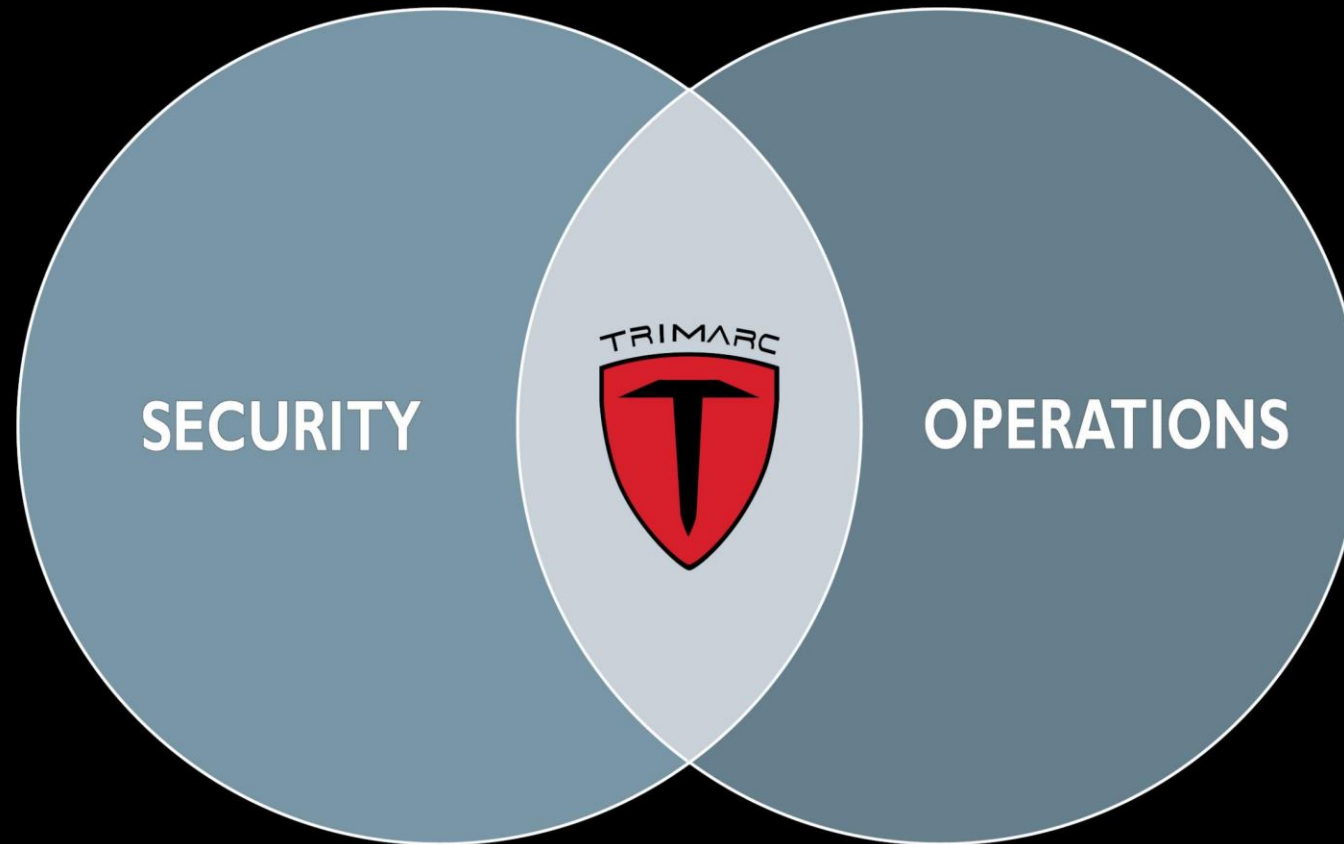
# **CONCERNED ABOUT YOUR ACTIVE DIRECTORY SECURITY POSTURE?**



**Trimarc's Active Directory Security Assessment provides  
actionable information enabling you to quickly resolve critical issues.**



# Trimarc Expertise



**Trimarc Combines Operational Knowledge & Experience with Security Vision**

# Trimarc Security Assessments

- Comprehensive security review & analysis
- Detailed, actionable recommendations
- Provides a roadmap to improve security posture
- Trimarc Security Assessments:
  - Active Directory
    - Active Directory Security Assessment (ADSA)
  - Azure AD & Microsoft Office 365
    - Microsoft Cloud Security Assessments (MCSA)
  - VMware vSphere
    - Virtual Infrastructure Security Assessment (VISA)



# Trimarc Active Directory Security Assessment (ADSA)

- 
- Comprehensive AD security posture assessment.
  - Effectively advanced reconnaissance paired with detailed, customized, & actionable recommendations.
  - AD Administration review & analysis.
  - Includes in-depth review of AD & GPO permissions.
  - Identification of custom privileged AD groups with rights defined outside of group membership.
  - Domain Controller security configuration analysis.
  - Only requires AD user rights.
  - Typical engagement is 4 to 6 weeks (depending on scoping).



# Trimarc Microsoft Cloud Security Assessment (MCSA)

- Trimarc MCSA provides an in-depth security analysis of the Azure AD & Microsoft Office 365 tenant.
- Focuses on the most important security configuration controls, including administration, access controls, and key security features.
- Identifies issues in the environment that attackers could leverage to access data, escalate permissions, and persist.
- Trimarc reviews the Microsoft cloud configuration using a proprietary Trimarc toolset and the Microsoft cloud web portal.
- Only read-only/view-only access is required.
- Typical engagement is 4 to 6 weeks (depending on scoping).





# Trimarc Virtual Infrastructure Security Assessment (VISA)

- 
- Thorough security analysis of vSphere environment: ESXi hosts, vCenter servers, & virtual machines.
  - Trimarc provides a PowerShell script to capture information via PowerCLI.
  - Trimarc provides recommendations on existing license levels for additional beneficial security controls.
  - Review of how the vSphere environment is managed as well as recommendations for secure administration.
  - Virtual machine security review including recommendations for VM template baselines.
  - Typical engagement is 4 to 6 weeks (depending on scoping).





# Top 10 Ways to Improve Active Directory Security Quickly

Sean Metcalf (@PyroTek3),  
Tyler Robinson  
(@tyler\_Robinson)  
Darryl Baker (@DFIRdeferred)

[ @TrimarcSecurity | TrimarcSecurity.com ]

# About Us

## Sean Metcalf (@PyroTek3)

- Founder & CTO of Trimarc ([Trimarc.io](https://Trimarc.io))
- Microsoft Certified Master (MCM) Directory Services
- Microsoft MVP
- Speaker: Black Hat, BSides, DEF CON, DerbyCon, etc.

## Tyler Robinson

- Offensive Security for Decades (Red/Purple/Blue Teamer)
- Speaker: BSides, Military, Blackhat Trainer
- Podcast Personality on Security Weekly
- Tested many of the largest companies in the world (Fortune 100, ICS, Gov)

## Darryl Baker (@DFIRdeferred)

- Blue Teamer, Purple Teamer, Threat Emulator
- Creator of AD Hacking Village
- Speaking @ The Experts Conference 2022
- Amateur Radio Extra





# Agenda

---

- Modern AD Attacks
- Ways to Improve AD Security Quickly
  - Limiting Password Attacks
  - Review AD Admins & Highly Privileged Service Accounts
  - ADCS Security Checks
  - Kerberos Delegation Security
  - Auditing Insecure Protocols & Dangerous Defaults
  - Limiting Local Admin Accounts
  - Domain Controller Security
  - The Path to Tier 0
- The Trimarc Top Ten List\*
- Conclusion
- Q & A





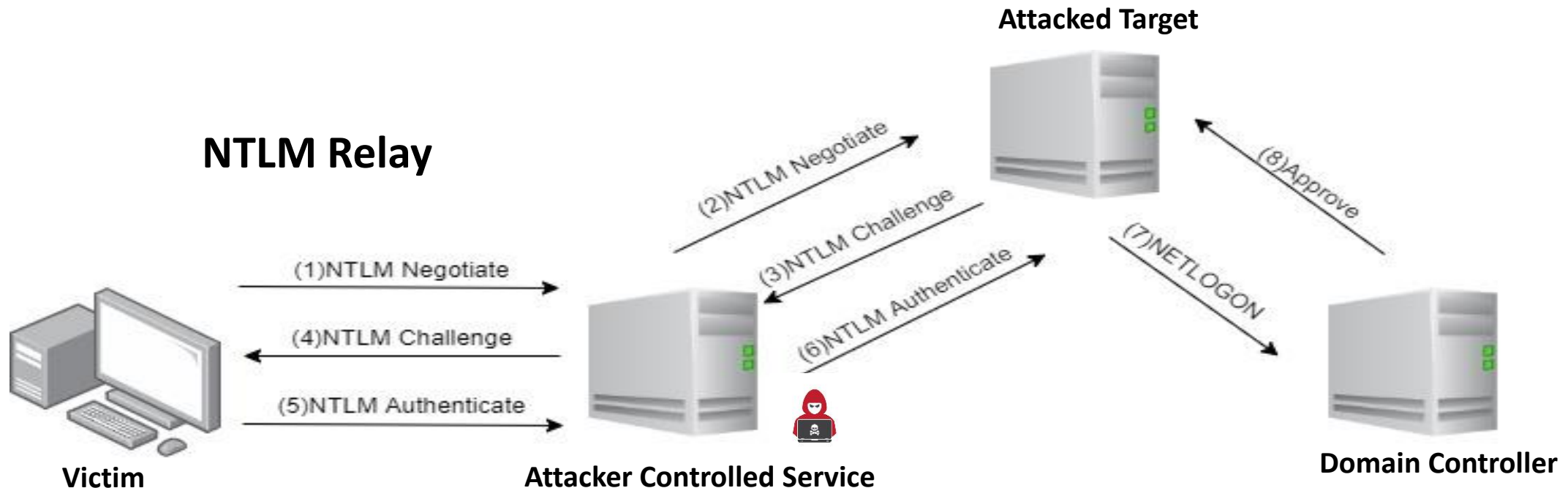
# Modern AD Attacks





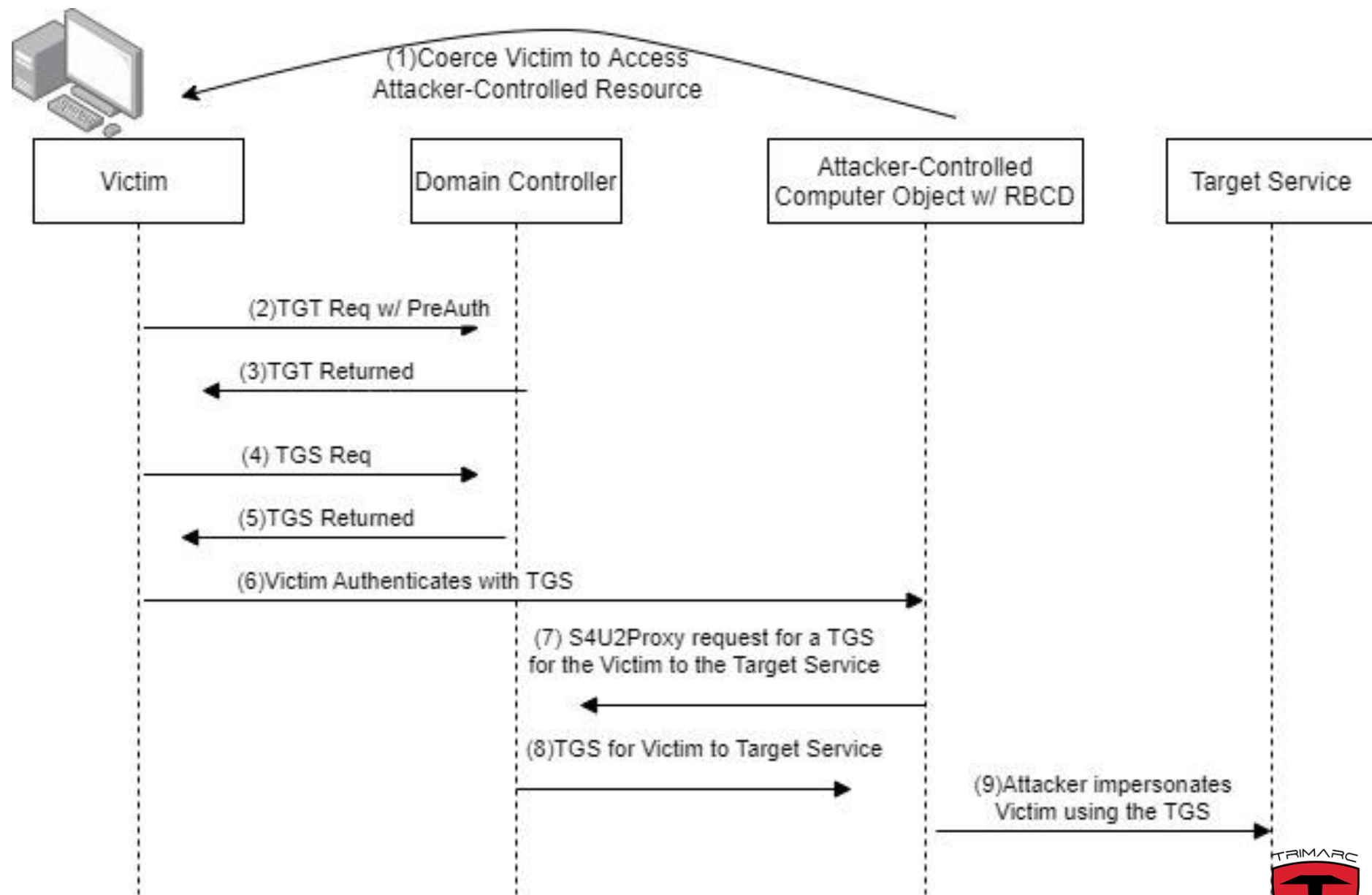
# Authentication Protocol Relay Attacks

A relay attack is when authentication credential details are captured from a victim resource, then relayed to another target resource; impersonating the identity of the victim. NTLM and Kerberos are commonly relayed authentication protocols.





# Kerberos Relay



# So How Does an Attacker Become the PiTM?

---

Usually through poisoning or spoofing of a service and coercing a victim account to connect to an attacker-controlled machine (though it is possible to directly intercept an NTLM Authentication). There are many techniques to accomplish this, but here are a few of the most commonly poisoned/coerced protocols:

- LLMNR
- SMB
- HTTP
- Print Spooler
- AD Certificate Services (via PetitPotam)
- Netbios (NBT-NS)
- Multicast DNS (MDNS)
- SMTP



# Credential Dumping

---

Dumping LSASS- Tools like Mimikatz and Rubeus make this a straight forward process.

---

DCSync- invokes a domain controller to replicate directory data to a target (with proper permissions).

---

Copying NTDS.dit- (usually via Volume Shadow Copy or "Install from Media" method allowing for offline cracking or Domain Controller promotion).





# Commonly abused Protocols for Kerberos Relay attacks

Protocol	Attack
SMB	Printer Bug
HTTP--> LDAP	PrivExchange
SMB--> LDAPS	Drop the Mic
AD Certificate Services	PetitPotam





Trash



File System



Home



# Detection and Mitigation

Easy

Extended Protection for Authentication (EPA)

Disabling mDNS/LLMNR

Limit Machine Account Quota (MAQ) attribute and/or restrict the SeMachineAccountPrivilege to a specific group rather than Authenticated Users\*

Medium

LDAP queries to identify potential SPNs available & Protocol Signing

Intra-Kerberos Relay Detections:

- DCOM Server connection with TCP connection to localhost (Using SIEM and Window Security Event ID 5156)

Post-Kerberos Relay Detections:

- RBCD Exploitation (Using SIEM and Window Security Event ID 5136/4768/4769)

Hard

Disabling NTLM

Channel Binding

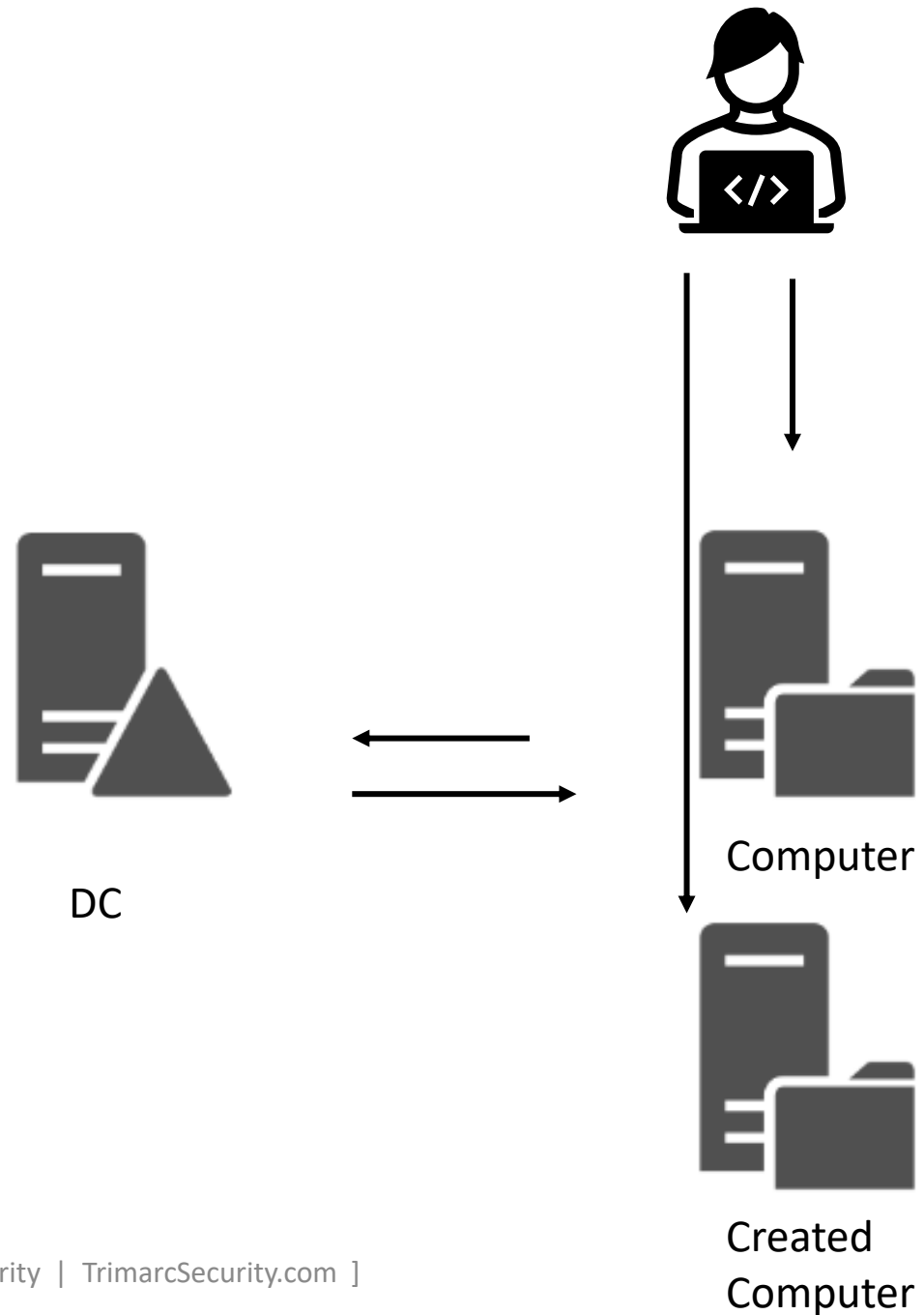
Require authenticated IPsec/IKEv2





# KrbRelayUp

High-level overview



# KrbRelayUp Putting It All Together



## Stage 1

Attacker gains access to the target computer

Attacker creates a new computer object in AD (or ADCS, etc) for S4U2Self

Attacker sets AD attribute on computer account for RBCD (msDS-AllowedToActOnBehalfOfOtherIdentity)

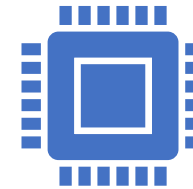


## Stage 2

Getting Kerberos tickets (TGT & TGS) for impersonation

Leverages computer account SPN allowing Kerberos S4U2Self to impersonate the user (AD account with admin rights on target)

Leverage Kerberos S4UProxy to access the target computer account



## Stage 3

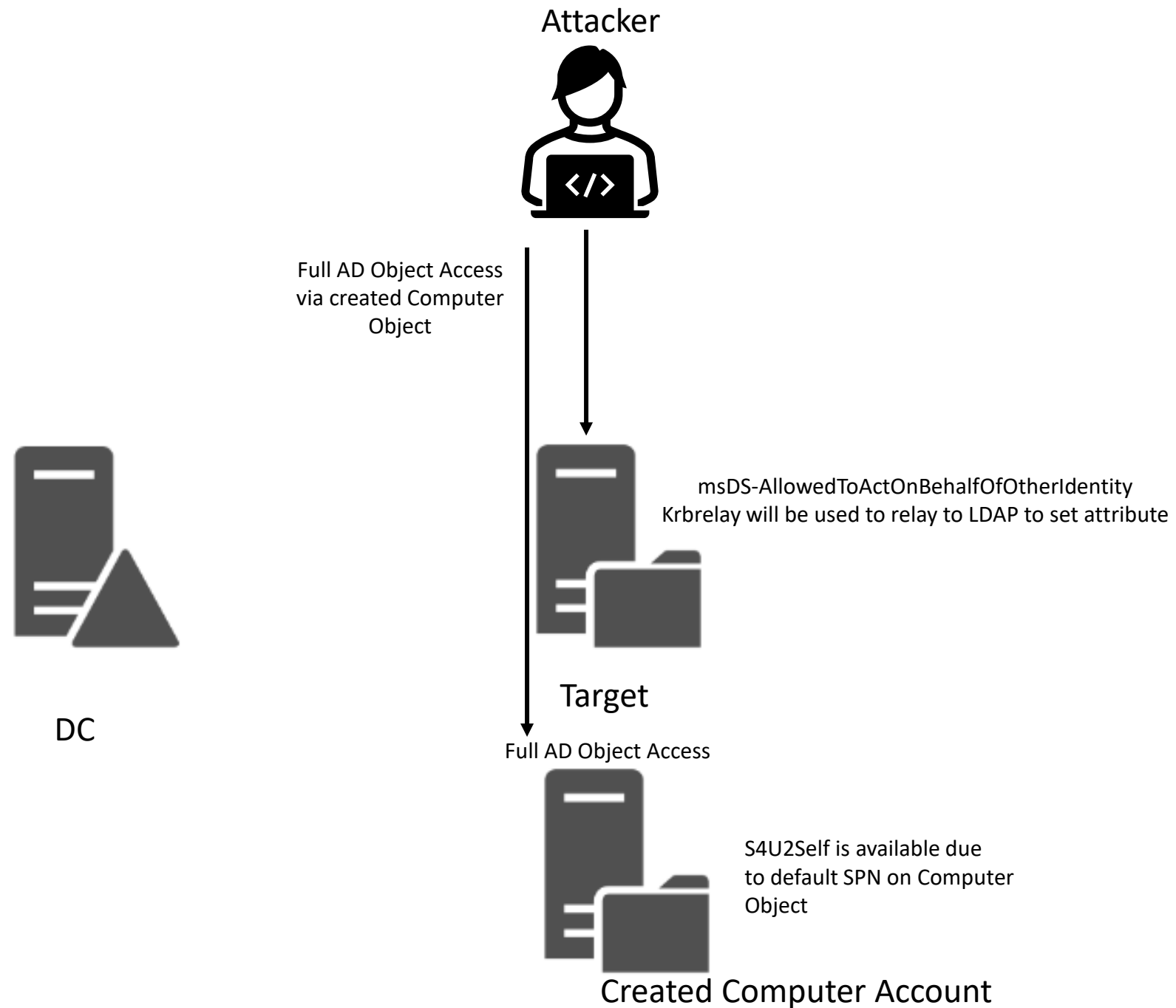
Leveraging Host SPN to get Silver Ticket to authenticate as the computer to itself

SYSTEM level access obtained when Attacker creates a service as System

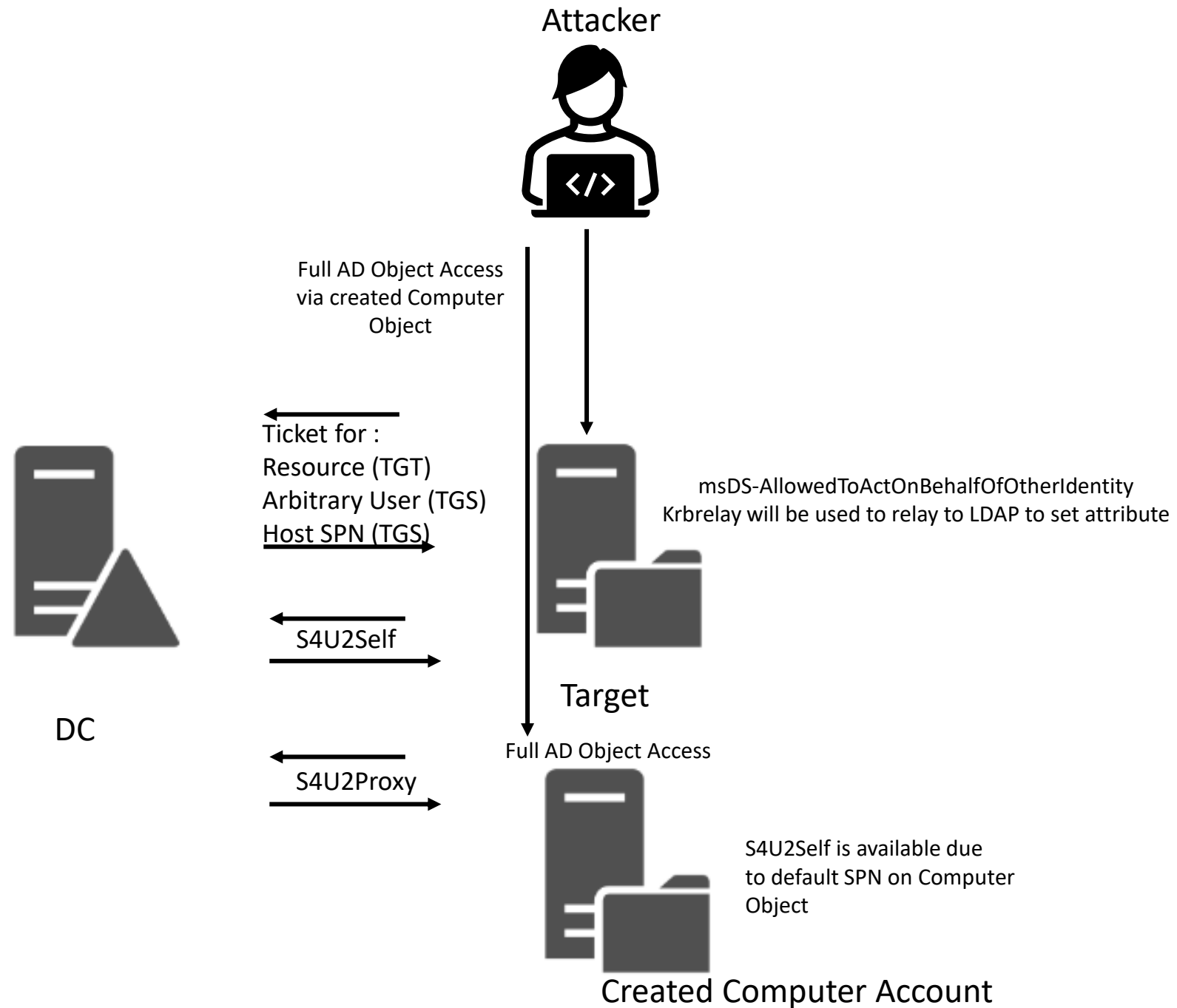
Attacker now has full admin rights on the target computer as SYSTEM



# Stage 1

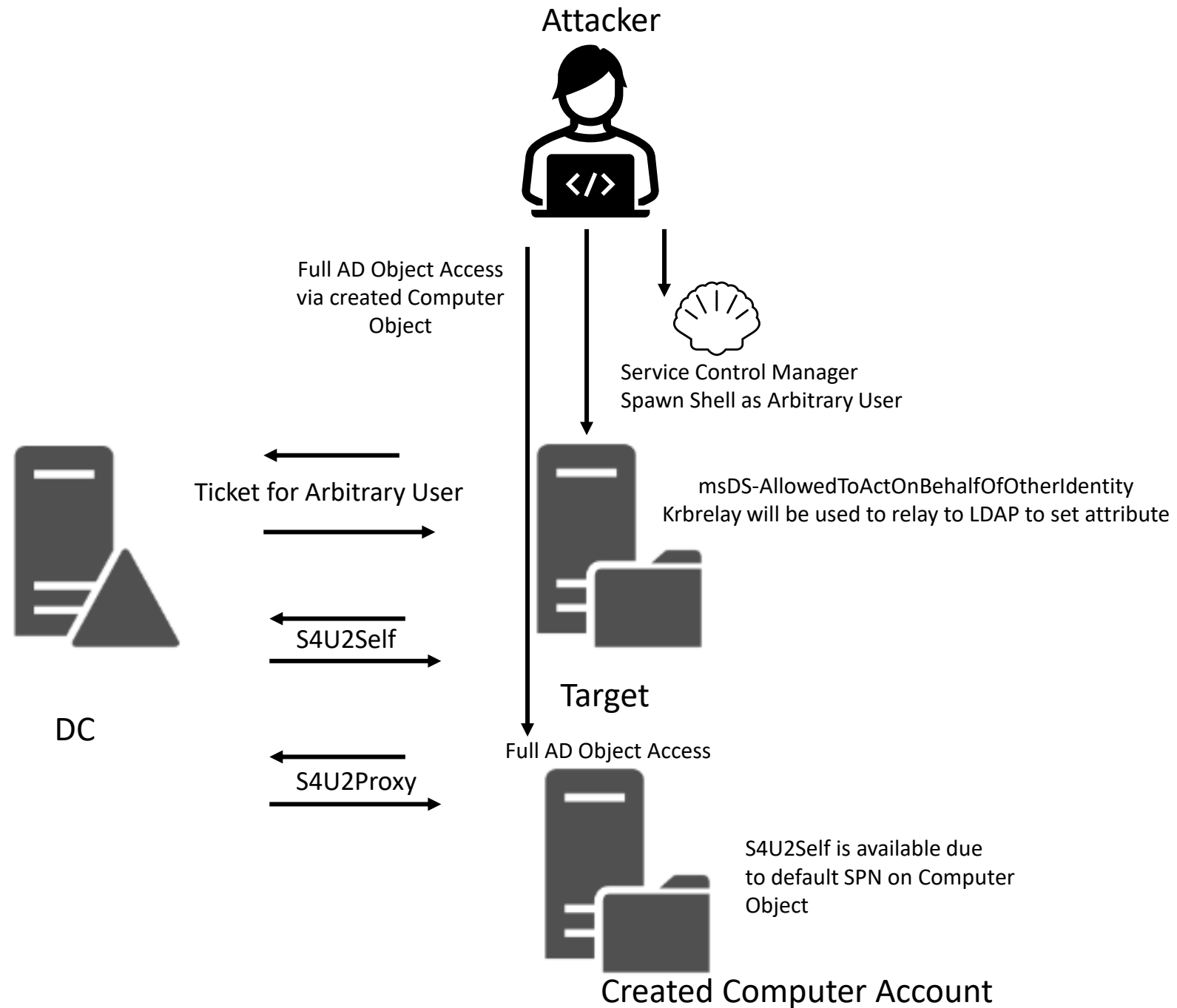


## Stage 2

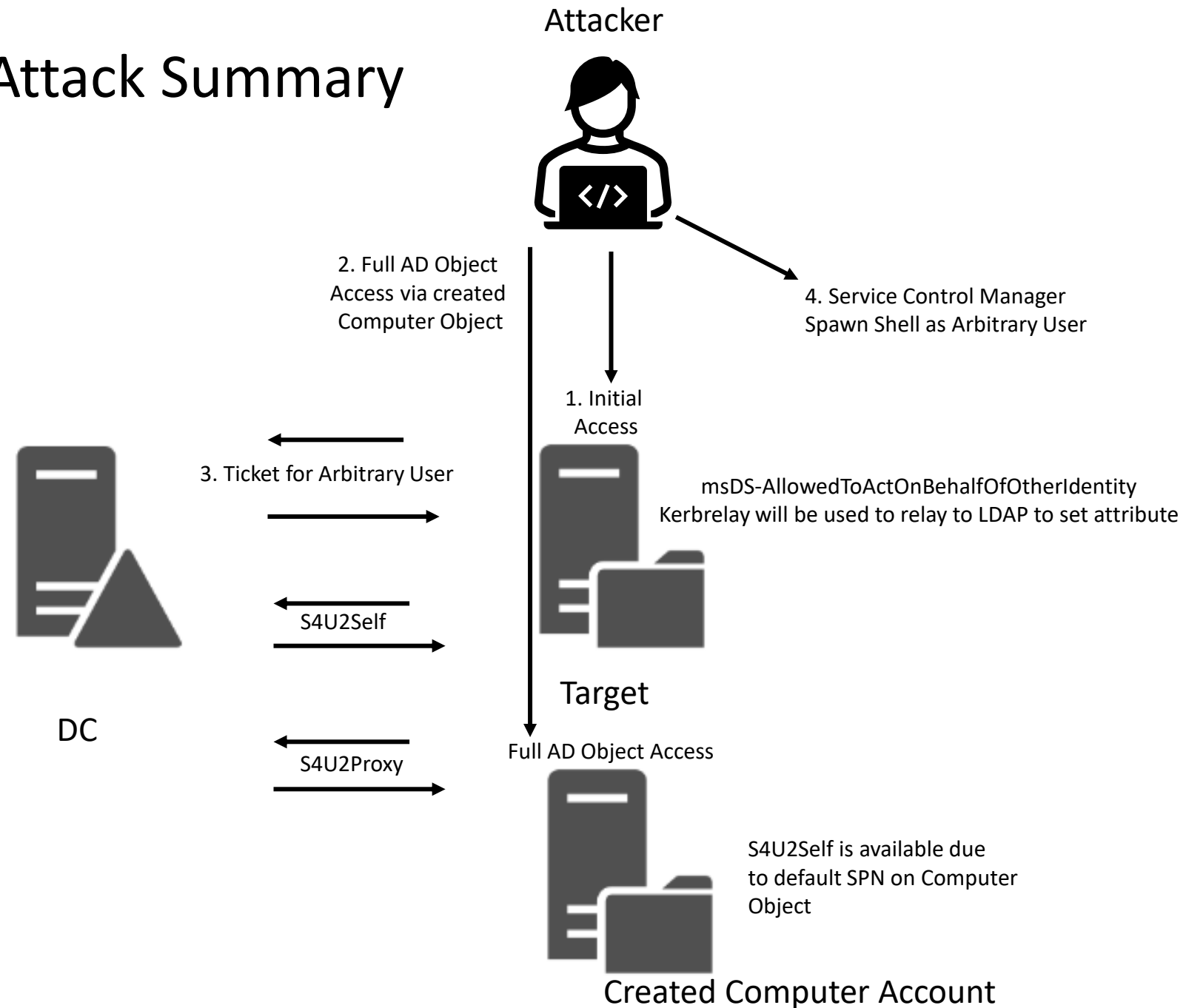




## Stage 3



# KrbRelayUp Attack Summary



# Detection and Mitigation

## Detection

- Security Event ID 4624 with an elevation token=\*1842 for Auth package Kerberos and UserName= "\*\$"
- Event ID 5145 Anonymous LOGON for shares
- Network level 445 DCE\_RPC connections
- Service Creation EventCode=7045  
Service\_Name ("KrbSCM")

## Mitigation

- **Block users from creating computer accounts**
- Add “account is sensitive and cannot be delegated” on all admin accounts then add to the Protected Users group
- Restrict access to sensitive systems (local logon, etc.)
- **Configure LDAP Signing to “required” on Domain Controllers**
- **Implement LDAP Signing (part 1)**
- **Implement Channel Binding (part 2)**
- Restrict lateral movement with host-based firewall (block SMB)





# Agenda

---

- Modern AD Attacks
- Ways to Improve AD Security Quickly
  - **Limiting Password Attacks**
  - Review AD Admins & Highly Privileged Service Accounts
  - ADCS Security Checks
  - Kerberos Delegation Security
  - Auditing Insecure Protocols & Dangerous Defaults
  - Limiting Local Admin Accounts
  - Domain Controller Security
  - The Path to Tier 0
- The Trimarc Top Ten List\*
- Conclusion
- Q & A

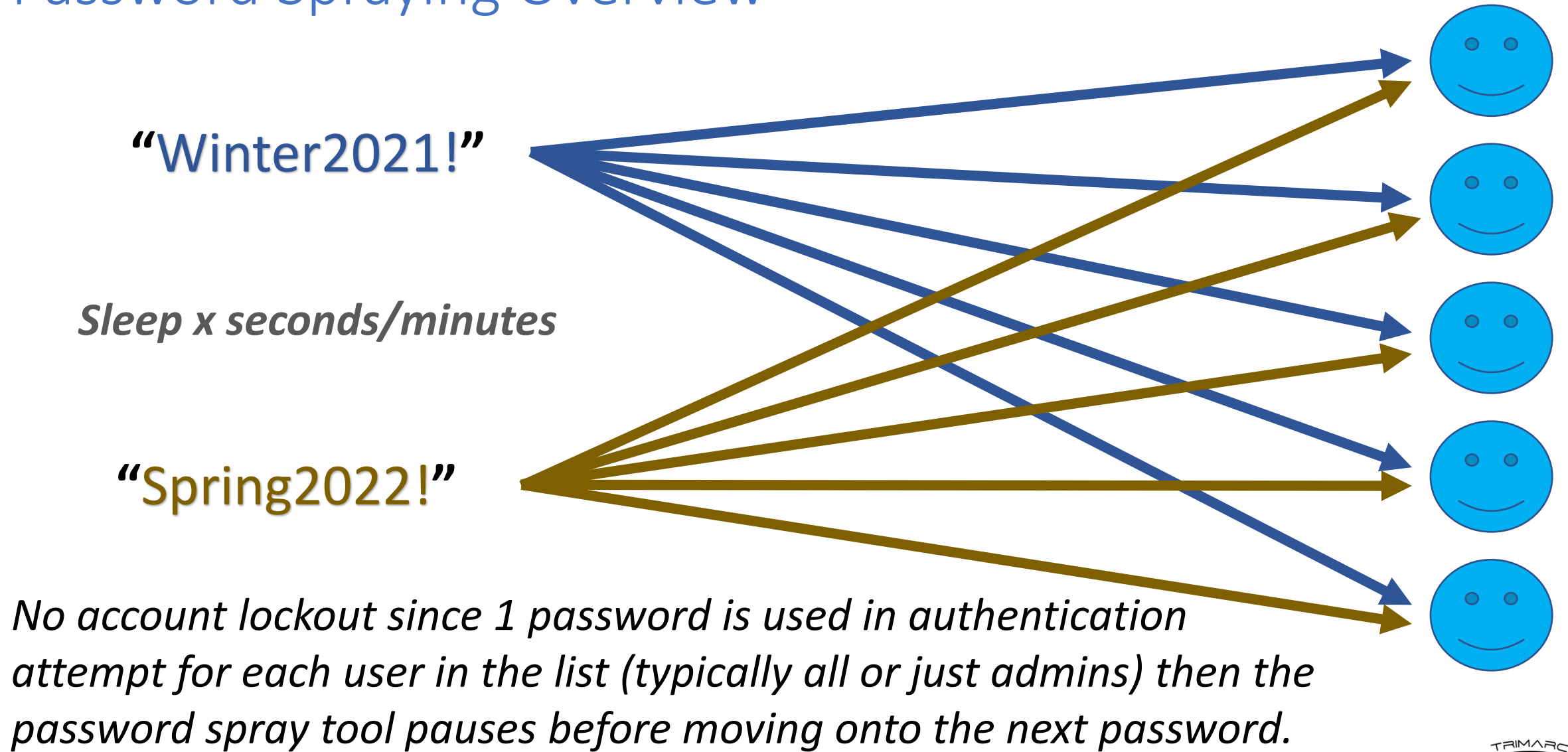


# Limiting Password Attacks

---

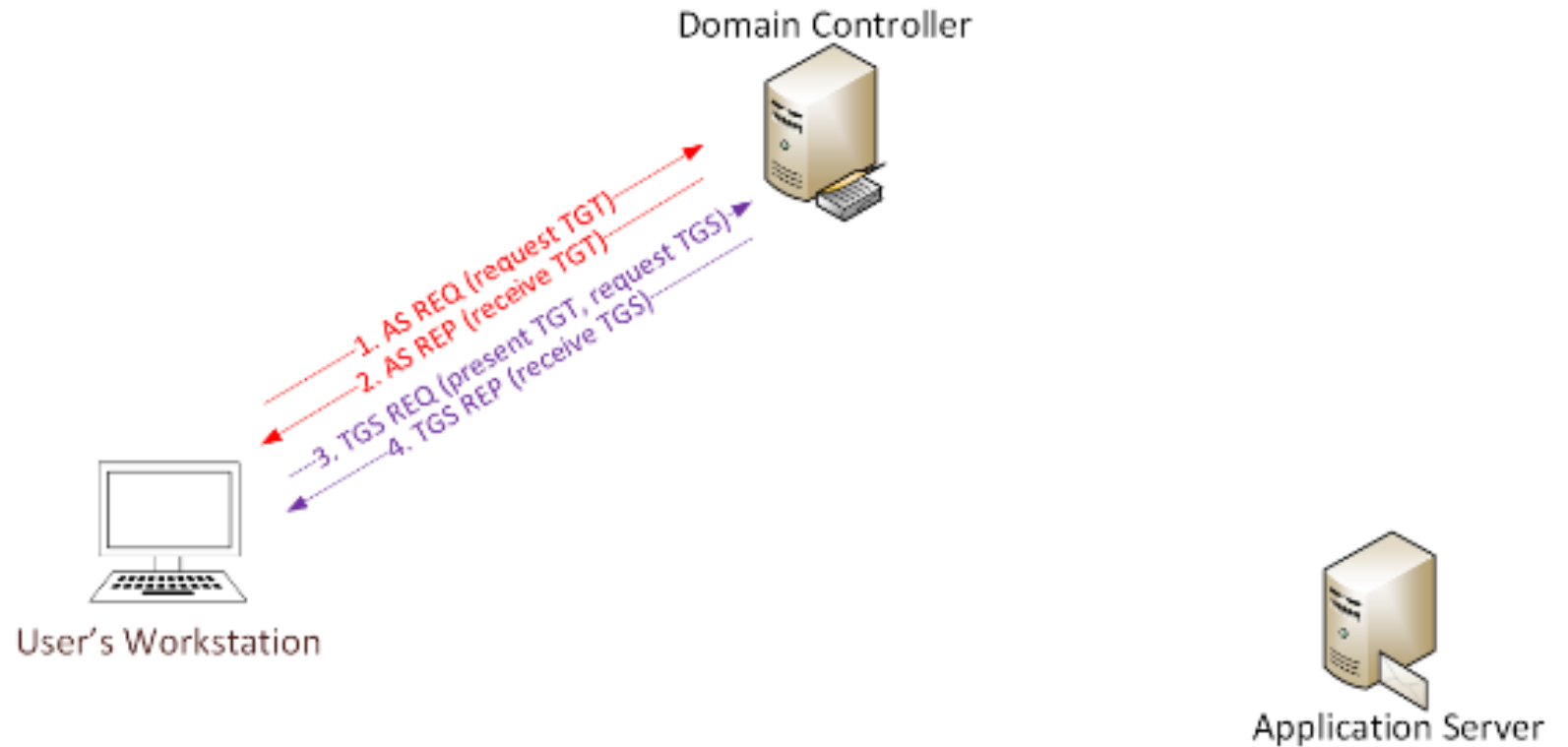


# Password Spraying Overview



# Cracking Service Account Passwords (Kerberoast)

Request/Save TGS service tickets & crack offline.



- User requests service tickets for targeted service account.
- No elevated rights required.
- No traffic sent to target.



# Kerberoast: Request TGS Service Ticket

```
PS C:\Users\JoeUser> Add-Type -AssemblyName System.IdentityModel
PS C:\Users\JoeUser> New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken
                        -ArgumentList 'MSSQLSvc/adsdb01.lab.adsecurity.org:1433'
```

```
Id                : uuid-ce260b5a-6992-4906-a8cf-2d48439c4fc8-1
SecurityKeys      : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom         : 1/23/2017 3:58:03 PM
ValidTo           : 1/24/2017 1:43:35 AM
ServicePrincipalName : MSSQLSvc/adsdb01.lab.adsecurity.org:1433
SecurityKey       : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

```
#2> Client: JoeUser @ LAB.ADSECURITY.ORG
Server: MSSQLSvc/adsdb01.lab.adsecurity.org:1433 @ LAB.ADSECURITY.ORG
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 1/23/2017 7:58:03 (local)
End Time: 1/23/2017 17:43:35 (local)
Renew Time: 1/30/2017 7:43:35 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0
Kdc Called: ADSLABDC16.lab.adsecurity.org
```



# Action: Limit Password Attack Capability



## Password Spraying

Implement a Password filter to reduce “bad passwords” in the environment.

Domain Password Policy should be set to 12 characters or more (preferably 15).

Fine-Grained Password Policies (FGPP) provide flexibility.



## Kerberoast

Ensure service accounts have passwords >25 characters.

Leverage Group Managed Service Accounts (GMSAs) where possible.

Create honeypot account & monitor for Kerberos Authentication.

<https://www.hub.trimarcsecurity.com/post/trimarc-research-detecting-kerberoasting-activity>



# Agenda

---

- Modern AD Attacks
- Ways to Improve AD Security Quickly
  - Limiting Password Attacks
  - Review AD Admins & Highly Privileged Service Accounts
  - ADCS Security Checks
  - Kerberos Delegation Security
  - Auditing Insecure Protocols & Dangerous Defaults
  - Limiting Local Admin Accounts
  - Domain Controller Security
  - The Path to Tier 0
- The Trimarc Top Ten List\*
- Conclusion
- Q & A





# Review AD Admins & Highly Privileged Service Accounts

---





# Groups with Highly Privileged Rights to AD (Default)

Domain Admins

Administrators

Enterprise Admins

Schema Admins

Account Operators

Backup Operators

Print Operators

Server Operators

DNSAdmins



name	DistinguishedName	PasswordLastSet
admMBailey	CN=admMBailey,OU=Admin Accounts,OU=AD Management,DC=Lab,DC=trimarcresearch,DC=com	11/10/2019 11:26:46 PM
admEGray	CN=admEGray,OU=Admin Accounts,OU=AD Management,DC=Lab,DC=trimarcresearch,DC=com	11/10/2019 11:27:06 PM
VMWareAdmin	CN=VMWareAdmin,OU=Service Accounts,DC=trimarcresearch,DC=com	11/10/2019 11:57:14 PM
SharepointSVC	CN=SharepointSVC,OU=Service Accounts,DC=Lab,DC=trimarcresearch,DC=com	11/13/2019 9:18:33 AM
Administrator	CN=Administrator,CN=Users,DC=trimarcresearch,DC=com	2/11/2020 2:08:55 PM
Administrator	CN=Administrator,CN=Users,DC=Lab,DC=trimarcresearch,DC=com	5/19/2020 4:32:44 PM
SVC-LAB-GMSA1	CN=SVC-LAB-GMSA1,CN=Managed Service Accounts,DC=Lab,DC=trimarcresearch,DC=com	6/10/2020 8:15:07 AM

# AD Admins with Old Passwords

- Ensure privileged account passwords change annually.
- Older passwords are typically poor and easier to guess.
- Password Spraying & Kerberoasting are popular attack methods for compromising accounts lacking strong passwords.



# Service Accounts that Don't Require AD Admin Rights

AV/McAfee/Trend  
Micro/etc

AGPM

Azure

Cisco

Entrust/PKI

Exchange

Fax

SCCM

SQL

VMWare

VPN

*If these are in Domain Admins, work to get them removed*

[ @TrimarcSecurity | TrimarcSecurity.com ]



# Check Default Domain Administrator Account for Issues

- Account Enabled?
  - Password changed recently?
  - Account has a SPN?
  - Recent logon?
- Account should be reserved as an emergency account (aka “break glass”)

lab.trimarcresearch.com Default Domain Administrator Account:

Name	Enabled	Created	PasswordLastSet	LastLogonDate	ServicePrincipalName
Administrator	True	11/10/2019 3:36:51 PM	5/19/2020 4:32:44 PM	5/11/2020 1:16:56 PM	{MSSQLSvc/GammaDB23:1434, MSSQLSvc/GammaDB14:1434, MSSQLSvc/GammaDB14:1434}



# AD Admin Account Checks



```
Get-ADGroupMember Administrators -Recursive
```

- Passwords change regularly (every year)
- Disable inactive accounts
- Remove disabled accounts
- No SPNs on accounts associated with people
- Member of Protected Users group
- No computer accounts
- Scrutinize Service Accounts
  - What do they do?
  - Where do they run?
  - What computers do they authenticate to?
  - What rights are actually required?





# Action: Improving AD Admin Account Security



Limit accounts in privileged AD admin groups.



Ensure AD admin accounts have passwords change annually (at a minimum).



Assume no service accounts need to be in AD admin groups.



Ensure all AD admin accounts have “sensitive” bit set and are members of the Protected Users group.



Ensure no AD admin accounts associated with people have Kerberos Service Principal Names (SPNs).



Disable accounts that are no longer in use (and eventually remove from privileged groups).



# Action: Reducing Service Account Rights

- Determine rights actually required.
- Delegate only these rights.
- Remove from Domain Admins (Enterprise Admins, domain Administrators, etc).
- Leverage Group Managed Service Account (GMSA) to manage account password automatically.
- Limit service account access & location (especially if highly privileged).
- Prevent Interactive logon capability



# Agenda

---

- Modern AD Attacks
- Ways to Improve AD Security Quickly
  - Limiting Password Attacks
  - Review AD Admins & Highly Privileged Service Accounts
  - **ADCS Security Checks**
  - Kerberos Delegation Security
  - Auditing Insecure Protocols & Dangerous Defaults
  - Limiting Local Admin Accounts
  - Domain Controller Security
  - The Path to Tier 0
- The Trimarc Top Ten List\*
- Conclusion
- Q & A





# ADCS Security Checks

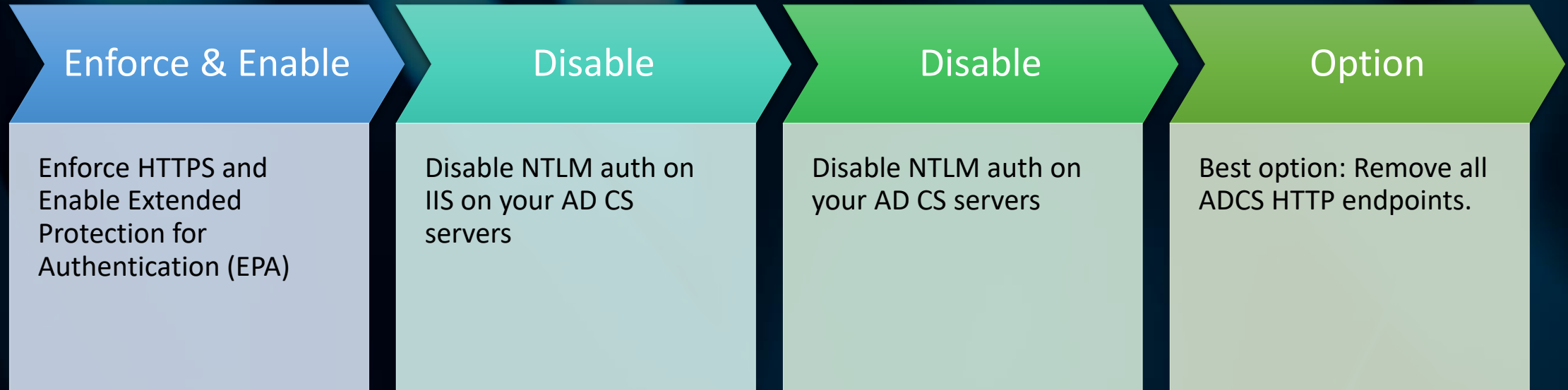
---

Active Directory Certificate Services





# Secure your HTTP endpoints





# Discover Overly-permissive AD Object ACLs

Safe configurations allow AD admins and PKI admins to modify objects in the PKS container but no one else.

```
$Safe_Users = "Domain Admins|Enterprise Admins|BUILTIN\Administrators|NT  
AUTHORITY\SYSTEM|$env:userdomain\Cert Publishers|$env:userdomain\Administrator"  
  
$DangerousRights = "GenericAll|WriteDacl|WriteOwner"  
  
foreach ( $object in $ADCS_Objects ) {  
    $BadACE = $object.nTSecurityDescriptor.Access | Where-Object {  
        ( $_.IdentityReference -notmatch $Safe_Users ) -and  
        ( $_.ActiveDirectoryRights -match $DangerousRights )  
    }  
    if ( $BadACE ) {  
        Write-Host "Object: $object" -ForegroundColor Red  
        $BadACE  
    }  
}
```

<https://github.com/TrimarcJake/adcs-snippets>



# Discover Overly-permissive AD Object ACLs

```
Administrator: Windows PowerShell

PS C:\Users\Administrator> foreach ( $object in $ADCS_Objects ) {
>> $BadACE = $object.nTSecurityDescriptor.Access | Where-Object { ( $_.IdentityReference -notmatch $Safe_Users ) -and ( $_.ActiveDirectoryRights -match $DangerousRights ) }
>> If ( $BadACE ) {
>> Write-Host "Object: $object" -ForegroundColor Red
>> $BadACE
>> }
>> }

Object: CN=horse-CA1-CA-1,CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration,DC=horse,DC=local

ActiveDirectoryRights : CreateChild, DeleteChild, Self, WriteProperty, DeleteTree, Delete, GenericRead, WriteDacl, WriteOwner
InheritanceType       : All
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IdentityReference     : HORSE\CA1$
IsInherited           : False
InheritanceFlags      : ContainerInherit, ObjectInherit
PropagationFlags      : None

Object: CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=horse,DC=local
ActiveDirectoryRights : GenericAll
InheritanceType       : None
ObjectType            : 00000000-0000-0000-0000-000000000000
InheritedObjectType   : 00000000-0000-0000-0000-000000000000
ObjectFlags           : None
AccessControlType     : Allow
IdentityReference     : Everyone
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None
```

<https://github.com/TrimarcJake/adcs-snippets>



# Discover Dangerous Flag on Certificate Authority (CAs)

```
C:\>certutil -getreg policy\EditFlags
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\horse-CA1-CA-1\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:

EditFlags REG_DWORD = 15014e (1376590)
  EDITF_REQUESTEXTENSIONLIST -- 2
  EDITF_DISABLEEXTENSIONLIST -- 4
  EDITF_ADDOLDKEYUSAGE -- 8
  EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
  EDITF_ENABLEAKIKEYID -- 100 (256)
  EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
  EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
  EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)
CertUtil: -getreg command completed successfully.
```

# Fix Dangerous Flag on CA

- Unset the flag (output slightly edited for readability)

```
C:\>certutil -setreg policy\EditFlags -EDITF_ATTRIBUTESUBJECTALTNAME2
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\horse-CA1-
CA-1\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:
```

Old Value:

```
EditFlags REG_DWORD = 15014e (1376590)
EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
```

New Value:

```
EditFlags REG_DWORD = 11014e (1114446)
```

```
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
```



# Templates with Dangerous Configs



- Templates options include:
  - Who can enroll/auto-enroll
  - Certificate purpose(s)/approved use(s)
  - Who is this certificate for?
  - Is approval required?
- If a normal user can specify the subject of the certificate, that *user can request a certificate on behalf of any other entity in the domain **including a Domain Admin or Domain Controller.***
- ***Trimarc has found at least one certificate that matches this description in ~95% of the environments we've assessed.***



# Templates with Dangerous Configs

Easy to find, slightly complex to fix

```
$ClientAuthEKUs = "1\.3\.6\.1\.5\.5\.7\.3\.2|  
1\.3\.6\.1\.5\.2\.3\.4|  
1\.3\.6\.1\.4\.1\.311\.20\.2\.2|  
2\.5\.29\.37\.0"  
  
$ADCS_Objects | Where-Object {  
    ($_.ObjectClass -eq "pKICertificateTemplate") -and  
    ($_.pkiExtendedKeyUsage -match $ClientAuthEKUs) -and  
    ($_. "msPKI-Certificate-Name-Flag" -eq 1) -and  
    ($_. "msPKI-Enrollment-Flag" -ne 2) -and  
    ( ($_. "msPKI-RA-Signature" -eq 0) -or ($null -eq $_. "msPKI-RA-Signature") )  
} | Format-Table Name,DistinguishedName
```



# Templates with Dangerous Configs

Results:

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> $ClientAuthEKUs = "1\3\6\1\5\5\7\3\2|1\3\6\1\5\2\3\4|1\3\6\1\4\1\311\20\2\2|2\5\29\37\0"
>> $ADCS_Objects | Where-Object {
>> ($_.ObjectClass -eq "pKICertificateTemplate") -and
>> ($_.pkiExtendedKeyUsage -match $ClientAuthEKUs) -and
>> ($_.msPKI-Certificate-Name-Flag -eq 1) -and
>> ($_.msPKI-Enrollment-Flag -ne 2) -and
>> ( ($_.msPKI-RA-Signature -eq 0) -or ($null -eq $_.msPKI-RA-Signature) )
>> } | Format-Table Name,DistinguishedName

Name                                DistinguishedName
----                                -
OfflineRouter                      CN=OfflineRouter,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Con...
horse-User                         CN=horse-User,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Config...
horse-Workstation Authentication  CN=horse-Workstation Authentication,CN=Certificate Templates,CN=Public Key Services...
```



# Fix Templates with Dangerous Configs

## Solution 1 – Prevent enrollee from self-assigning Subject Name

```
$ADCS_Objects_BadConfig = $ADCS_Objects | Where-Object {  
    ($_.ObjectClass -eq "pKICertificateTemplate") -and  
    ($_.pkiExtendedKeyUsage -match $ClientAuthEKUs) -and  
    ($_. "msPKI-Certificate-Name-Flag" -eq 1) -and  
    ($_. "msPKI-Enrollment-Flag" -ne 2) -and  
    ( ($_. "msPKI-RA-Signature" -eq 0) -or ($null -eq $_. "msPKI-RA-Signature") )  
}  
  
$ADCS_Objects_BadConfig | ForEach-Object {  
    $_. "msPKI-Certificate-Name-Flag" = 0  
}
```



# Fix Templates with Dangerous Configs

- Solution 2 – Require Manager Approval (lower chance of impact)

```
$ADCS_Objects_BadConfig = $ADCS_Objects | Where-Object {  
    ($_.ObjectClass -eq "pKICertificateTemplate") -and  
    ($_.pkiExtendedKeyUsage -match $ClientAuthEKUs) -and  
    ($_. "msPKI-Certificate-Name-Flag" -eq 1) -and  
    ($_. "msPKI-Enrollment-Flag" -ne 2) -and  
    ( ($_. "msPKI-RA-Signature" -eq 0) -or ($null -eq $_. "msPKI-RA-Signature") )  
}  
  
$ADCS_Objects_BadConfig | ForEach-Object {  
    $_. "msPKI-Enrollment-Flag" = 2  
}
```



# ACTION: ADCS Security Checks

- Lots of areas in default configs for attackers to take advantage of.
- Trimarc finds Critical issues in 99% of environments with AD CS.
- Trimarc now reviews ADCS security as part of the Trimarc Active Directory Security Assessment (ADSA).
- Perform the following to improve ADCS security:
  - Secure ADCS HTTP endpoints
  - Review AD PKI object permissions
  - Check for EDITF\_ATTRIBUTESUBJECTALTNAME2
  - Review template configuration

<https://github.com/TrimarcJake/adcs-snippets>





# Agenda

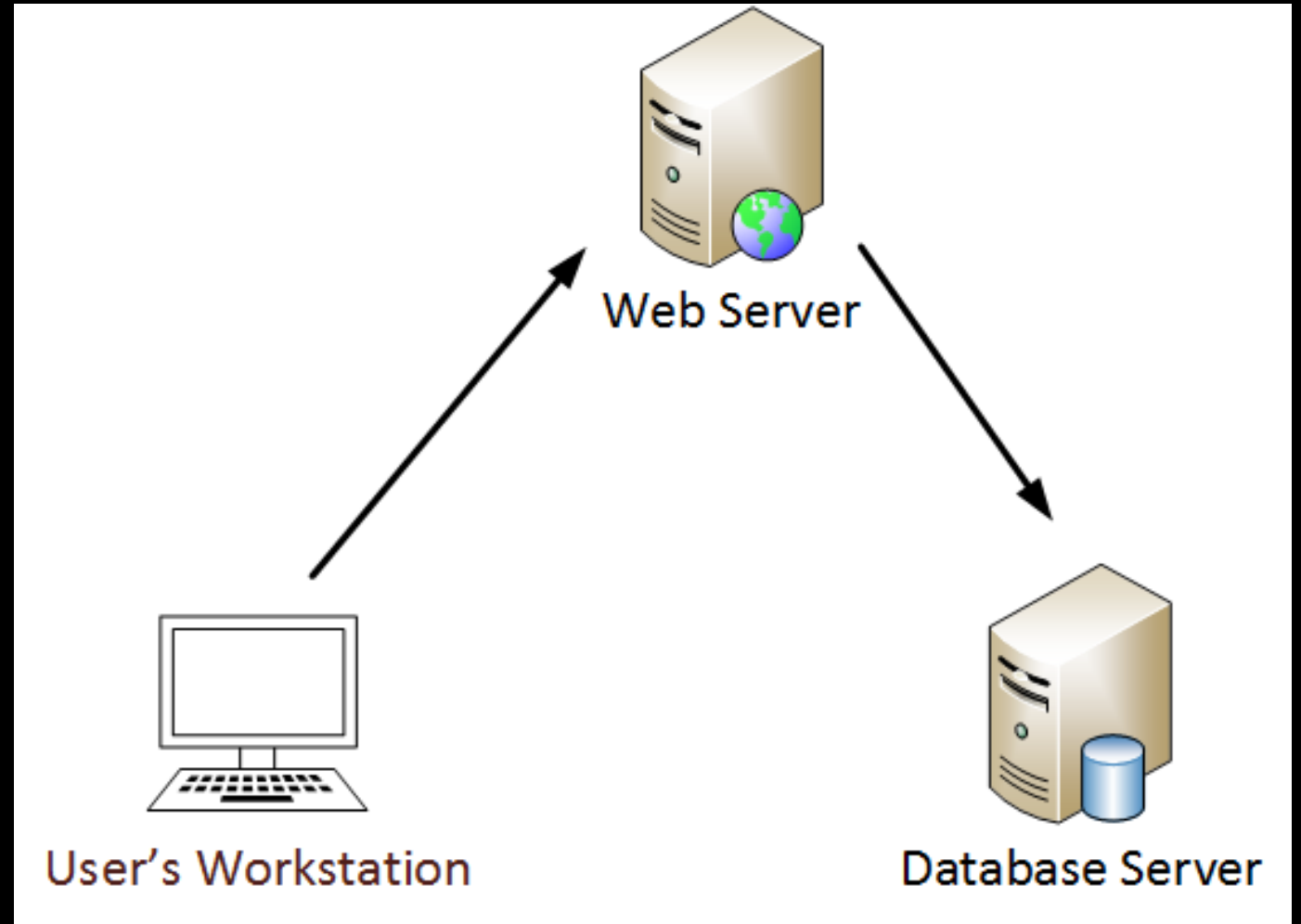
---

- Modern AD Attacks
- Ways to Improve AD Security Quickly
  - Limiting Password Attacks
  - Review AD Admins & Highly Privileged Service Accounts
  - ADCS Security Checks
  - **Kerberos Delegation Security**
  - Auditing Insecure Protocols & Dangerous Defaults
  - Limiting Local Admin Accounts
  - Domain Controller Security
  - The Path to Tier 0
- The Trimarc Top Ten List\*
- Conclusion
- Q & A



# Kerberos Delegation

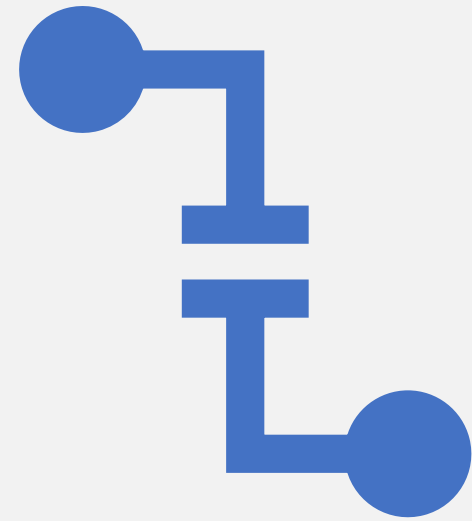
---



# Kerberos Delegation

Delegation = Impersonation

- **Unconstrained:**  
Impersonate users connecting to service to ANY Kerberos service.
- **Constrained:**  
Impersonate authenticated users connecting to service to SPECIFIC Kerberos services on servers.
- **Constrained with Protocol Transition:**  
Impersonate any user to SPECIFIC Kerberos services on servers. (aka “Kerberos Magic”)
- **Resource-based Constrained Delegation:**  
Enables delegation configured on the resource instead of the account.



# Discovering Kerberos Delegation

<https://Trimarc.co/ADCheckScript>

```
## Identify Accounts with Kerberos Delegation
$KerberosDelegationArray = @()
[array]$KerberosDelegationObjects = Get-ADObject -filter { ((UserAccountControl -BAND 0x0080000) -OR (UserAccountControl -BAND 0x1000000) `
-OR (msDS-AllowedToDelegateTo -like '*') -OR (msDS-AllowedToActOnBehalfOfOtherIdentity -like '*')) -AND (PrimaryGroupID -ne '516') `
-AND (PrimaryGroupID -ne '521') } -Server $DomainDC -prop Name,ObjectClass,PrimaryGroupID,UserAccountControl,ServicePrincipalName,`
msDS-AllowedToDelegateTo,msDS-AllowedToActOnBehalfOfOtherIdentity -SearchBase $DomainDN

ForEach ($KerberosDelegationObjectItem in $KerberosDelegationObjects)
{
    IF ($KerberosDelegationObjectItem.UserAccountControl -BAND 0x0080000)
    { $KerberosDelegationServices = 'All Services' ; $KerberosType = 'Unconstrained' }
    ELSE
    { $KerberosDelegationServices = 'Specific Services' ; $KerberosType = 'Constrained' }

    IF ($KerberosDelegationObjectItem.UserAccountControl -BAND 0x1000000)
    { $KerberosDelegationAllowedProtocols = 'Any (Protocol Transition)' ; $KerberosType = 'Constrained with Protocol Transition' }
    ELSE
    { $KerberosDelegationAllowedProtocols = 'Kerberos' }

    IF ($KerberosDelegationObjectItem.'msDS-AllowedToActOnBehalfOfOtherIdentity')
    { $KerberosType = 'Resource-Based Constrained Delegation' }

    $KerberosDelegationObjectItem | Add-Member -MemberType NoteProperty -Name Domain -Value $Domain -Force
    $KerberosDelegationObjectItem | Add-Member -MemberType NoteProperty -Name KerberosDelegationServices -Value $KerberosDelegationServices -Force
    $KerberosDelegationObjectItem | Add-Member -MemberType NoteProperty -Name DelegationType -Value $KerberosType -Force
    $KerberosDelegationObjectItem | Add-Member -MemberType NoteProperty -Name KerberosDelegationAllowedProtocols -Value $KerberosDelegationAllowedProtocols -Force

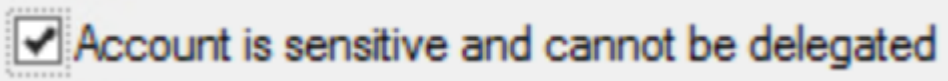
    [array]$KerberosDelegationArray += $KerberosDelegationObjectItem
}

Write-Host ""
Write-Host "$Domain Domain Accounts with Kerberos Delegation:" -Fore Cyan
$KerberosDelegationArray | Sort DelegationType | Select DistinguishedName,DelegationType,Name,ServicePrincipalName | Format-Table -AutoSize
```



# Action List: Kerberos Delegation

## GOOD:

- Set all AD Admin accounts to:  
“Account is sensitive and cannot be delegated” 
- Remove all delegation accounts that don't have Kerberos SPNs

## BEST:

- Add all AD Admin accounts to the “Protected Users” group.
- Convert Unconstrained delegation to Constrained delegation.
- Work to remove Kerberos delegation from accounts where no longer required.
- Ensure service accounts with Kerberos delegation have long, complex passwords (preferably group Managed Service Accounts).
- Don't use Domain Controller SPNs when delegating.
- Restrict & monitor who has the ability to configure Kerberos delegation.

## Limitation:

Service Accounts may not operate fully when added to Protected Users and may also experience issues with “Account is sensitive and cannot be delegated”





# Agenda

---

- Modern AD Attacks
- Ways to Improve AD Security Quickly
  - Limiting Password Attacks
  - Review AD Admins & Highly Privileged Service Accounts
  - ADCS Security Checks
  - Kerberos Delegation Security
  - **Auditing Insecure Protocols & Dangerous Defaults**
  - Limiting Local Admin Accounts
  - Domain Controller Security
  - The Path to Tier 0
- The Trimarc Top Ten List\*
- Conclusion
- Q & A



# Auditing Insecure Protocols & Dangerous Defaults



# Auditing NTLM & SMB

## Audit NTLM on DCs

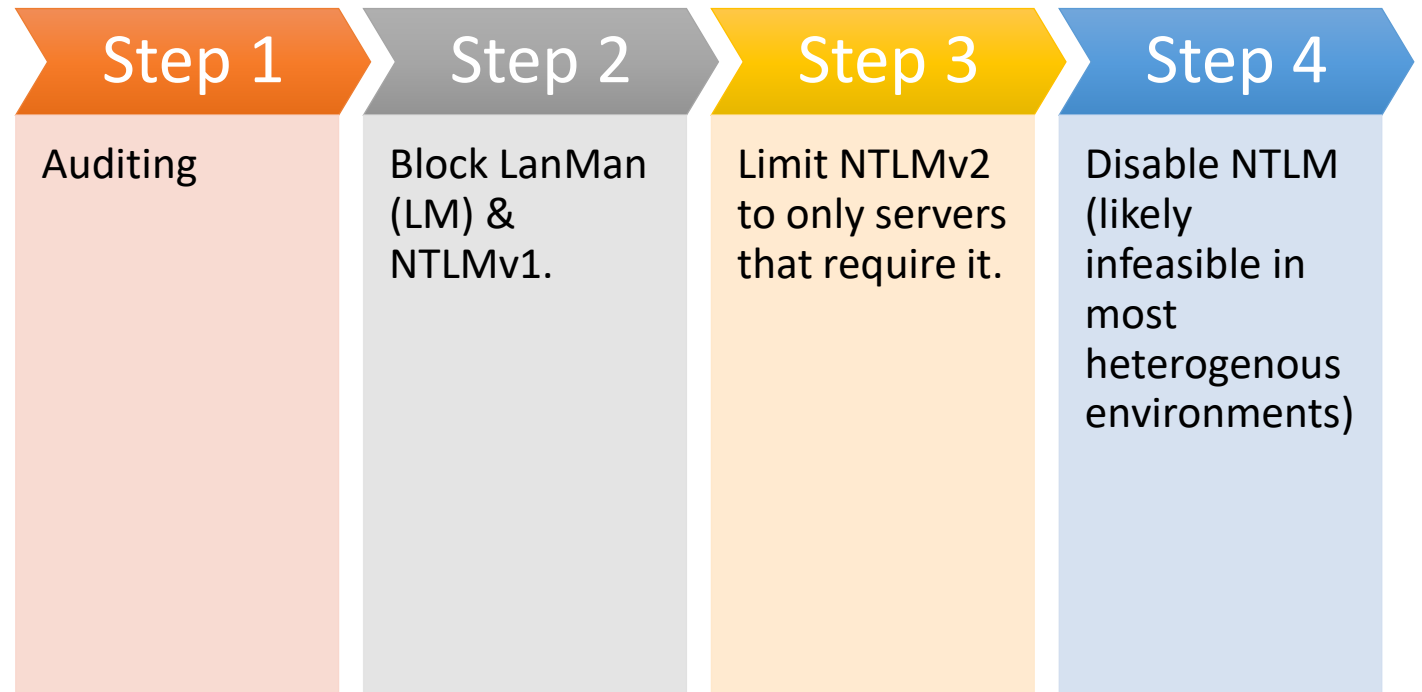
- Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options
  - Network security:  
Restrict NTLM: Outgoing NTLM traffic to remote servers = Audit All
  - Network security:  
Restrict NTLM: Audit NTLM authentication in this domain = Enable all
  - Network security:  
Restrict NTLM: Audit Incoming NTLM Traffic = Enable auditing for all accounts

## Audit SMB on DCs & Servers

- Set-SmbServerConfiguration -AuditSmb1Access \$true



# Improving NTLM Authentication Security



# Dangerous Defaults

- **Domain Password Policy**
  - 7 characters
  - The Issue: Enables password spraying
- **Add Workstations to the Domain**
  - Authenticated Users
  - The Issue: Enables several attacks, including RBCD
- **Admin rights on all domain-joined computers**
  - Domain Admins
  - The Issue: Enables/encourages AD admins to logon to workstations
- **Decentralized Name Resolution**
  - LLMNR
  - Netbios over TCP/IP (NBT port 445)
  - WPAD
  - MDNS
  - The Issue: Provides the attacker an easy way to get credentials on the network

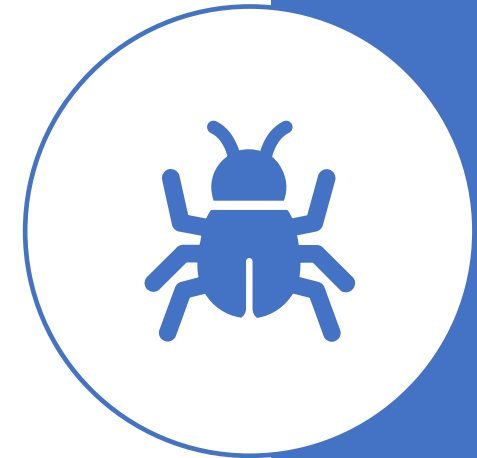




# Anonymous LDAP

**“Pre-Windows 2000 Compatible Access”** group (for Windows NT)

- Everyone / Anonymous / Authenticated Users
- Configured in many environments Trimarc assesses
- Enables all members the ability to read information about users & groups
- MITIGATION: Remove Everyone & Anonymous  
Mitigation+: Test removing Authenticated Users



# Action: Auditing Insecure Protocols & Dangerous Defaults

- Audit NTLM on DCs
- Audit SMB on DCs & Servers
- Work to restrict NTLMv1 & SMBv1
- Review DC-linked GPOs to ensure Authenticated Users/Domain Users do not have the right “Add Workstations to the Domain” (User Rights Assignment).
- Restrict LLMNR
- Restrict Netbios
- Work to remove Everyone & Anonymous from the “Pre-Windows 2000 Compatible Access” group



# Agenda

---

- Modern AD Attacks
- Ways to Improve AD Security Quickly
  - Limiting Password Attacks
  - Review AD Admins & Highly Privileged Service Accounts
  - ADCS Security Checks
  - Kerberos Delegation Security
  - Auditing Insecure Protocols & Dangerous Defaults
  - **Limiting Local Admin Accounts**
  - Domain Controller Security
  - The Path to Tier 0
- The Trimarc Top Ten List\*
- Conclusion
- Q & A





# Limiting Local Admin Accounts

---

& AD Admins using regular  
workstations to administer Active  
Directory

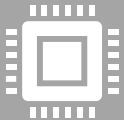


# Local Admin Accounts Overview

---



Local “Administrator” account (RID 500) exists on every Windows workstation and server.



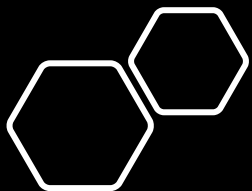
In many environments, all workstations have the same local Admin account password to simplify support.



Despite being “local”, if the account name & password are the same on two computers, the local Administrator account can authenticate to the other over the network.

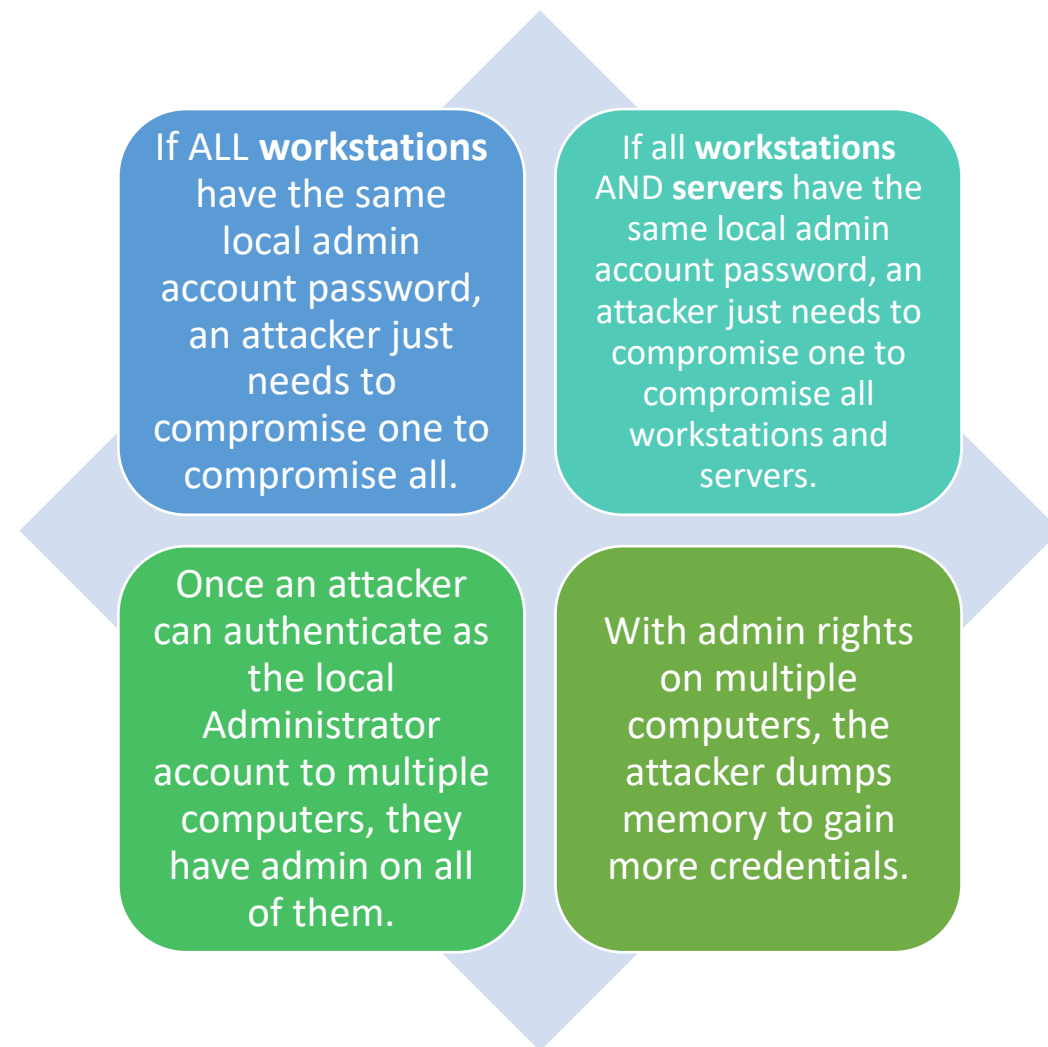


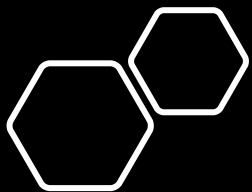




# Attacking Local Admin Accounts

[ @TrimarcSecurity | TrimarcSecurity.com ]



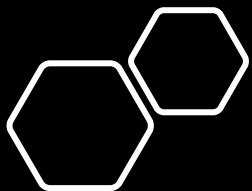


# Compromise 1 Computer to Compromise AD (DA account logged on to computer)

## **Scenario 1:**

AD Admin logs onto their regular workstation with AD Admin account to perform admin tasks. This credential ends up in LSASS (memory) on that computer. Attacker gets admin/system rights on the computer and dumps memory, including all logged on credentials (including service accounts).





# Compromise 1 Computer to Compromise AD (DA account logged on to computer)

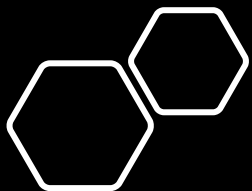
## Scenario 1:

AD Admin logs onto their regular workstation with AD Admin account to perform admin tasks. This credential ends up in LSASS (memory) on that computer. Attacker gets admin/system rights on the computer and dumps memory, including all logged on credentials (including service accounts).

## Scenario 2:

AD Admin logs onto their regular workstation using regular user account and then uses RunAs to perform admin tasks. This credential ends up in LSASS (memory) on that computer. Attacker gets admin/system rights on the computer and dumps memory, including all logged on credentials (including service accounts).





# Compromise 1 Computer to Compromise AD (DA account logged on to computer)

## Scenario 1:

AD Admin logs onto their regular workstation with AD Admin account to perform admin tasks. This credential ends up in LSASS (memory) on that computer. Attacker gets admin/system rights on the computer and dumps memory, including all logged on credentials (including service accounts).

## Scenario 2:

AD Admin logs onto their regular workstation using regular user account and then uses RunAs to perform admin tasks. This credential ends up in LSASS (memory) on that computer. Attacker gets admin/system rights on the computer and dumps memory, including all logged on credentials (including service accounts).

## Scenario 3:

AD Admin RDPs to an Admin server to perform admin tasks. No credentials are in LSASS (memory) on that computer. A smart attacker could monitor keystrokes to identify the password for the AD Admin account.

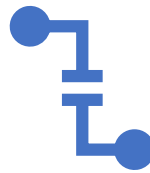


# Action:

## Risks with Workstation Admins



**Use Microsoft Local Administrator Password Solution (LAPS) or similar for automatic local admin password change to ensure every computer has a unique password.**



**Disallow local account logon across network via GPO.**

Deny access to this computer from the network:

- Local account and member of Administrators group

Deny log on through Remote Desktop Services:

- Local account and member of Administrators group



**Use GPO(s) to prevent AD Admins from logging on to workstations & servers. Test before deploying (especially with service accounts in DA).**

Deny access to this computer from the network:

- Domain Admins, Administrators, Enterprise Admins

Deny log on locally

- Domain Admins, Administrators, Enterprise Admins

Deny log on through Remote Desktop Services

- Domain Admins, Administrators, Enterprise Admins

*Domain Admins != server admin or application admin or workstation admin*





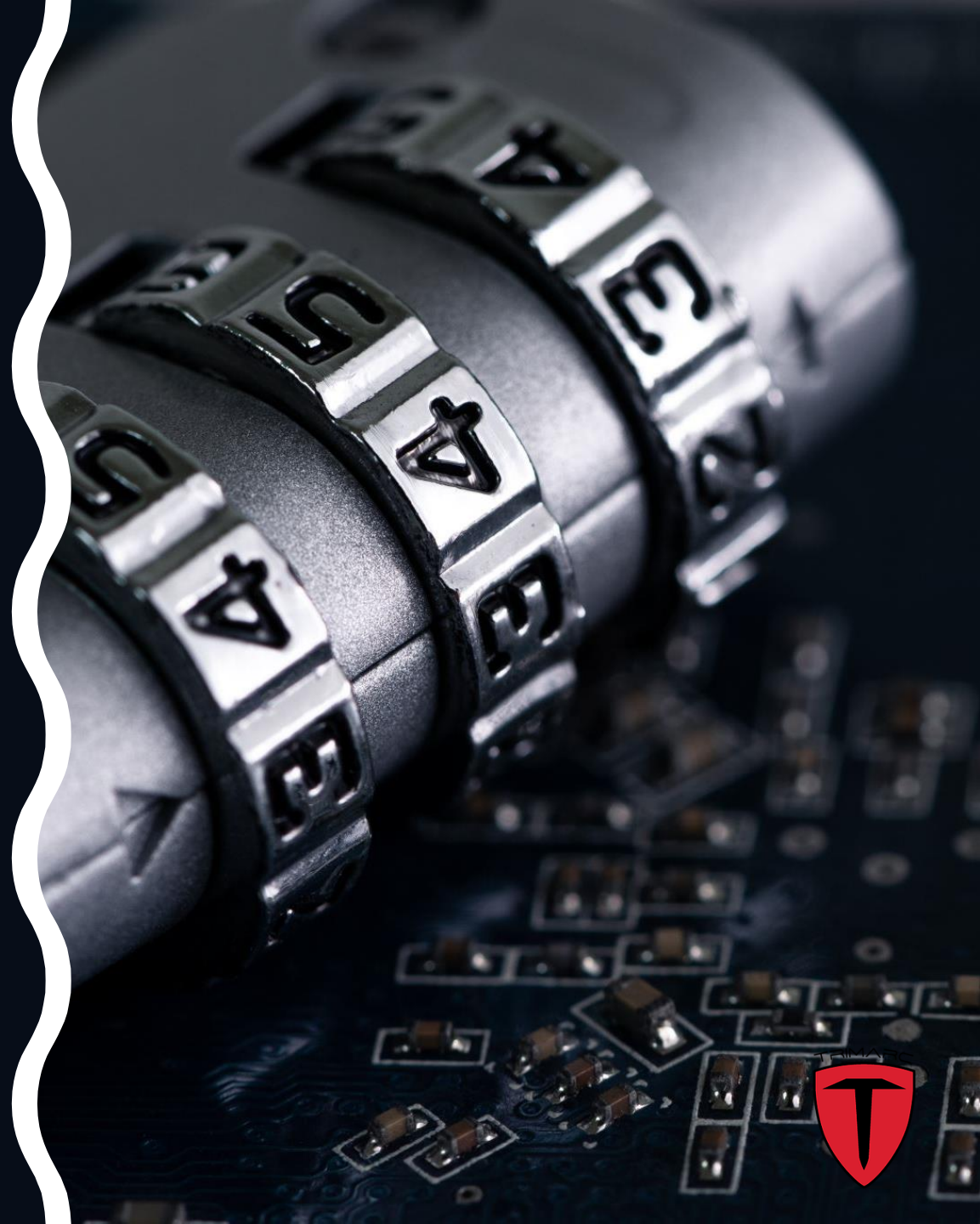
# Agenda

---

- Modern AD Attacks
- Ways to Improve AD Security Quickly
  - Limiting Password Attacks
  - Review AD Admins & Highly Privileged Service Accounts
  - ADCS Security Checks
  - Kerberos Delegation Security
  - Auditing Insecure Protocols & Dangerous Defaults
  - Limiting Local Admin Accounts
  - **Domain Controller Security**
  - The Path to Tier 0
- The Trimarc Top Ten List\*
- Conclusion
- Q & A



# Domain Controller Security



# Print Spooler Service on DCs: The Issue

The Print Spooler provides capability for any user to request print notifications.

This request can be tested by sending a notification to any computer on the network.

This notification can use Kerberos.



# Print Spooler Service Issues

---

PrinterBug/SpoolSample is a no-fix vuln in print spooler notification that can be used to coerce authentication that can be captured or relayed.

---

There's also attack surface left over from the PrintNightmare series of vulnerabilities if everything isn't configured absolutely perfectly.

---

Security researchers are still actively looking into the Print Spooler service due to its legacy and anticipated volume of remaining issues

---

Trimarc Recommends disabling the Print Spooler service on all DCs and servers that don't actually use it.



# Print Spooler Service: Mitigation

## Configure GPO to Stop the Print Spooler Service

- ▼ Domain Controllers
  - Default Domain Controllers Policy
    - Disable Print Spooler - DC

Disable Print Spooler - DC [TM-WIN19 ^	Service Name ^	Startup	Permission
▼ Computer Configuration	Network Store Interface Se...	Not Defined	Not Defined
▼ Policies	Offline Files	Not Defined	Not Defined
> Software Settings	OpenSSH Authentication ...	Not Defined	Not Defined
▼ Windows Settings	Optimize drives	Not Defined	Not Defined
> Name Resolution Policy	Payments and NFC/SE Ma...	Not Defined	Not Defined
> Scripts (Startup/Shutdo	Performance Counter DLL ...	Not Defined	Not Defined
> Deployed Printers	Performance Logs & Alerts	Not Defined	Not Defined
▼ Security Settings	Phone Service	Not Defined	Not Defined
> Account Policies	Plug and Play	Not Defined	Not Defined
> Local Policies	Portable Device Enumerat...	Not Defined	Not Defined
> Event Log	Power	Not Defined	Not Defined
> Restricted Groups	Print Spooler	Disabled	Not Defined
> System Services	Printer Extensions and Not...	Not Defined	Not Defined
> Registry			

OR

Disable Print Spooler - DC [TM-WI	Name	Order	Action	Startup
▼ Computer Configuration	Spooler	1	Stop Service	Disabled
> Policies				
▼ Preferences				
> Windows Settings				
▼ Control Panel Settings				
> Data Sources				
> Devices				
> Folder Options				
> Local Users and Grc				
> Network Options				
> Power Options				
> Printers				
> Scheduled Tasks				
> Services				





# Domain Controller Advanced Audit Policy

LAB DC Audit Policy		
Scope Details Settings Delegation		
Name	Allowed Permissions	Inherited
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No
TRDLab\Domain Admins	Edit settings, delete, modify security	No
TrimarcRD\Enterprise Admins	Edit settings, delete, modify security	No
Computer Configuration (Enabled)		hide
Policies		hide
Windows Settings		hide
Security Settings		hide
Local Policies/Audit Policy		hide
Policy	Setting	
Audit account logon events	Success	
Audit account management	Success	
Audit logon events	Success	
Audit privilege use	Success, Failure	
Advanced Audit Configuration		hide
Account Logon		hide
Policy	Setting	
Audit Credential Validation	Success, Failure	
Account Management		hide
Policy	Setting	
Audit Application Group Management	Failure	
Audit User Account Management	Failure	

## Policy

Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings

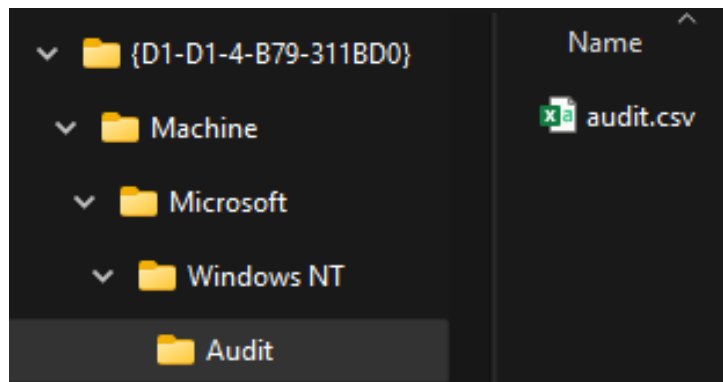
## Setting

Enabled



# Quickly Find Advanced Audit GPO Settings

Want to find GPOs that set Advanced Auditing?  
Search SYSVOL for “audit.csv” files



Policy Target	Subcategory	Subcategory GUID	Inclusion Setting	Exclusion Setting	Setting Value
System	Audit Computer Account Management	{0cce9236-69ae-11e1-b43d-000000000000}	Success		1
System	Audit Distribution Group Management	{0cce9238-69ae-11e1-b43d-000000000000}	Success		1
System	Audit User Account Management	{0cce9235-69ae-11e1-b43d-000000000000}	Success and Failure		3
System	Audit Security Group Management	{0cce9237-69ae-11e1-b43d-000000000000}	Success		1
System	Audit Process Creation	{0cce922b-69ae-11e1-b43d-000000000000}	Success		1
System	Audit Process Termination	{0cce922c-69ae-11e1-b43d-000000000000}	Success		1
System	Audit Audit Logon	{0cce9215-69ae-11e1-b43d-000000000000}	Success and Failure		3
System	Audit Audit Logoff	{0cce9216-69ae-11e1-b43d-000000000000}	Success		1
System	Audit Network Policy Server	{0cce9243-69ae-11e1-b43d-000000000000}	Success and Failure		3
System	Audit Other Logon/Logoff Events	{0cce921c-69ae-11e1-b43d-000000000000}	Success		1
System	Audit Other Object Access Events	{0cce9227-69ae-11e1-b43d-000000000000}	Success		1
System	Audit Authorization Policy Change	{0cce9231-69ae-11e1-b43d-000000000000}	Success		1
System	Audit Authentication Policy Change	{0cce9230-69ae-11e1-b43d-000000000000}	Success		1
System	Audit Audit Policy Change	{0cce922f-69ae-11e1-b43d-000000000000}	Success and Failure		3
System	Audit Security State Change	{0cce9210-69ae-11e1-b43d-000000000000}	Success		1
System	Audit File System	{0cce921d-69ae-11e1-b43d-000000000000}	Success and Failure		3
System	Audit Handle Manipulation	{0cce9223-69ae-11e1-b43d-000000000000}	Success and Failure		3
System	Audit File Share	{0cce9224-69ae-11e1-b43d-000000000000}	Success		1
System	Audit Security System Extension	{0cce9211-69ae-11e1-b43d-000000000000}	Success		1
System	Audit Application Generated	{0cce9222-69ae-11e1-b43d-000000000000}	Success and Failure		3
System	Audit PNP Activity	{0cce9248-69ae-11e1-b43d-000000000000}	Success and Failure		3



# Most Important DC Auditing Settings

- Account Logon
  - Audit Credential Validation: S&F
  - Audit Kerberos Authentication Service: S&F
  - **Audit Kerberos Service Ticket Operations: Success**
  - Account Logon: Audit Other Account Logon Events: S&F
- Account Management
  - Audit Computer Account Management: S&F
  - Audit Other Account Management Events: S&F
  - Audit Security Group Management: S&F
  - Audit User Account Management: S&F
- Detailed Tracking
  - Audit DPAPI Activity: S&F
  - Audit Process Creation: S&F
- DS Access
  - *Audit Directory Service Access: S&F*
  - Audit Directory Service Changes: S&F
- Privilege Use
  - Audit Sensitive Privilege Use: S&F
- Logon and Logoff
  - Audit Account Lockout: Success
  - Audit Logoff: Success
  - Audit Logon: S&F
  - **Audit Special Logon: Success & Failure**
  - Audit Other Logon/Logoff Events
- Object Access
  - Audit File System: Failure
  - Audit Registry: Failure
- Policy Change
  - Audit Audit Policy Change : S&F
  - Audit Authentication Policy Change : S&F
  - Audit MPSSVC Rule-Level Policy Change: Success
- System
  - Audit IPsec Driver: S&F
  - Audit Other System Events: S&F
  - Audit Security State Change : S&F
  - Audit Security System Extension : S&F
  - Audit System Integrity : S&F



# Domain Controller Security: User Rights Assignment

Default Domain Controllers Policy	
Scope	Details Settings Delegation
Local Policies/User Rights Assignment	
Policy	Setting
Access this computer from the network	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone
Act as part of the operating system	TrimarcRD\TRD Domain Controller Administrators
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	BUILTIN\Account Operators, BUILTIN\Administrators, BUILTIN\Backup Operators, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Print Operators, BUILTIN\Server Operators, TrimarcRD\Enterprise Admins, TrimarcRD\TRD Domain Controller Administrators
Allow log on through Terminal Services	BUILTIN\Administrators, TrimarcRD\TRD Domain Controller 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	TrimarcRD\TRD Domain Controller Administrators, TRDDEV\ServerAdmins, BUILTIN\Administrators
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators
Force shutdown from a remote system	BUILTIN\Administrators, BUILTIN\Server Operators, TRDLab\LAB Domain Controller Admins
Generate security audits	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Increase scheduling priority	Window Manager\Window Manager Group, 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	TRDLab\LAB Domain Controller Admins, TRDDEV\ServerAdmins, 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	TRDDEV\LAPSAdmins, BUILTIN\Server Operators, BUILTIN\Print Operators, enterprise admins, BUILTIN\Backup Operators, BUILTIN\Administrators
Take ownership of files or other objects	BUILTIN\Administrators



# Domain Controller Security: User Rights Assignment

- Add workstations to domain
  - Only AD Admins & specific groups/accounts should have this right
- Allow log on locally & Allow log through Terminal Services (RDP)
  - Only “Domain Admins” or “Administrators” should have this right
- Debug programs
  - Not required
- Enable computer and user accounts to be trusted for delegation (Kerberos)
  - Only “Domain Admins” or “Administrators” should have this right
- Load and unload device drivers (can compromise DC)
  - Not required
- Manage auditing and security log (can clear security logs)
  - AD Admins & Exchange groups only
- Take ownership of files or other objects (become owner of AD objects)
  - Only “Domain Admins” or “Administrators” should have this right



# Domain Controller Security: Trimarc's Don't Install These Applications List

SQL

ADFS

Azure AD Connect

Management Console (not the agent)

Firefox

Chrome

(old) Remote console software





# Domain Controller Security: DC Agents Trimarc Typically Discovers

## VMware Tools

- You are running the current version, right?
- Versions older than 10.1.0 are vulnerable to a significant security issue (VIX API)

## EDR

- Has live response capability (console) with system/admin rights on the DC

## Management (SCCM)

- Can install/run code on the DC

## Splunk Universal Forwarder

- Default install has the ability to run code



# Domain Controller Security: OS Version & Patching

Ensure DCs are  
running current,  
supported  
Windows versions

Should be 2016  
since 2012/2012R2  
leaves extended  
support in 2023.

Ensure DCs are  
regularly patched



# Action: DC Security

---

- Ensure Advanced Auditing is enabled & configured appropriately in DC-linked GPO
- Ensure DC User Rights Assignments are configured appropriately in DC-linked GPOs
- Ensure DCs are only operating as Domain Controllers and don't have unnecessary applications
- Ensure you are running the current VMWare Tools version on virtual DCs
- Review all agents on DCs and identify those that can install/run code (note that any agent with the ability to install/run code could become DA)
- Ensure DCs are running current Windows versions & keep patched



# Agenda

---

- Modern AD Attacks
- Ways to Improve AD Security Quickly
  - Limiting Password Attacks
  - Review AD Admins & Highly Privileged Service Accounts
  - ADCS Security Checks
  - Kerberos Delegation Security
  - Auditing Insecure Protocols & Dangerous Defaults
  - Limiting Local Admin Accounts
  - Domain Controller Security
  - **The Path to Tier 0**
- The Trimarc Top Ten List\*
- Conclusion
- Q & A



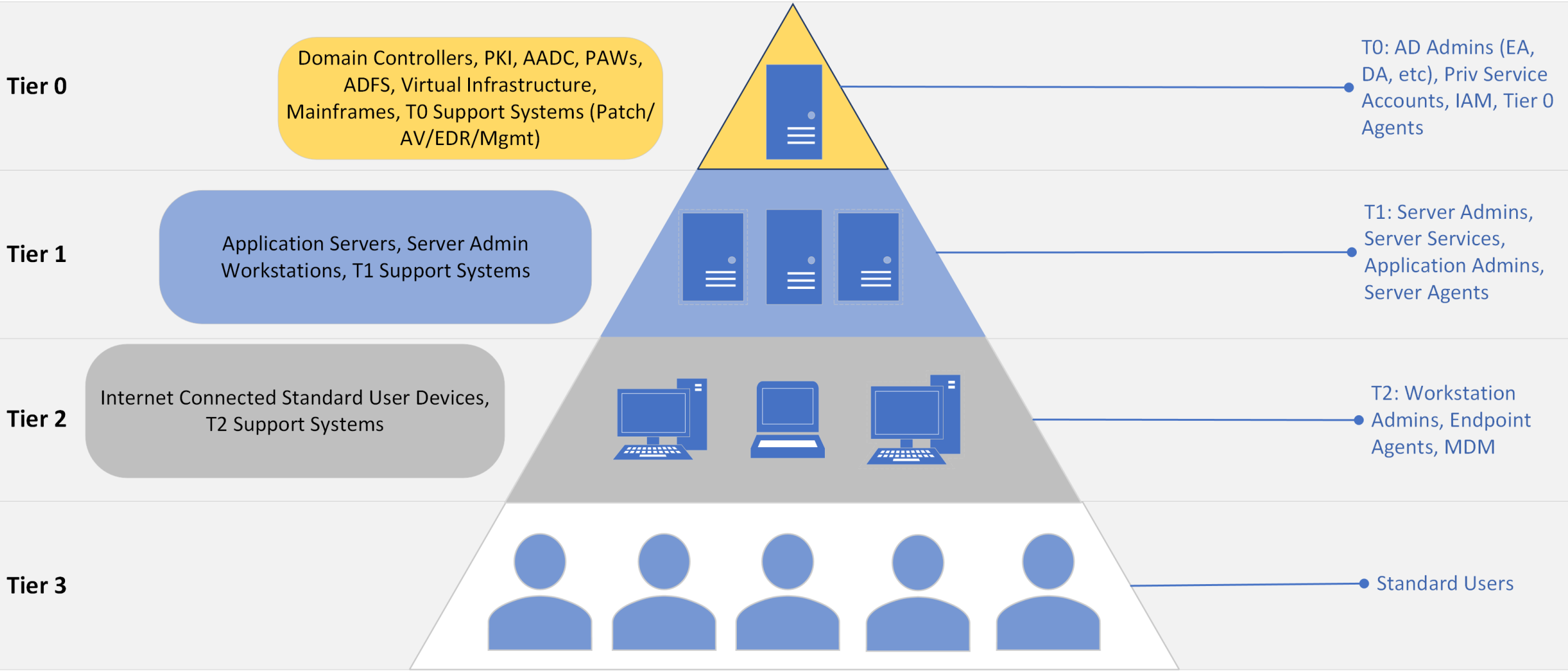


# Path to Tier 0

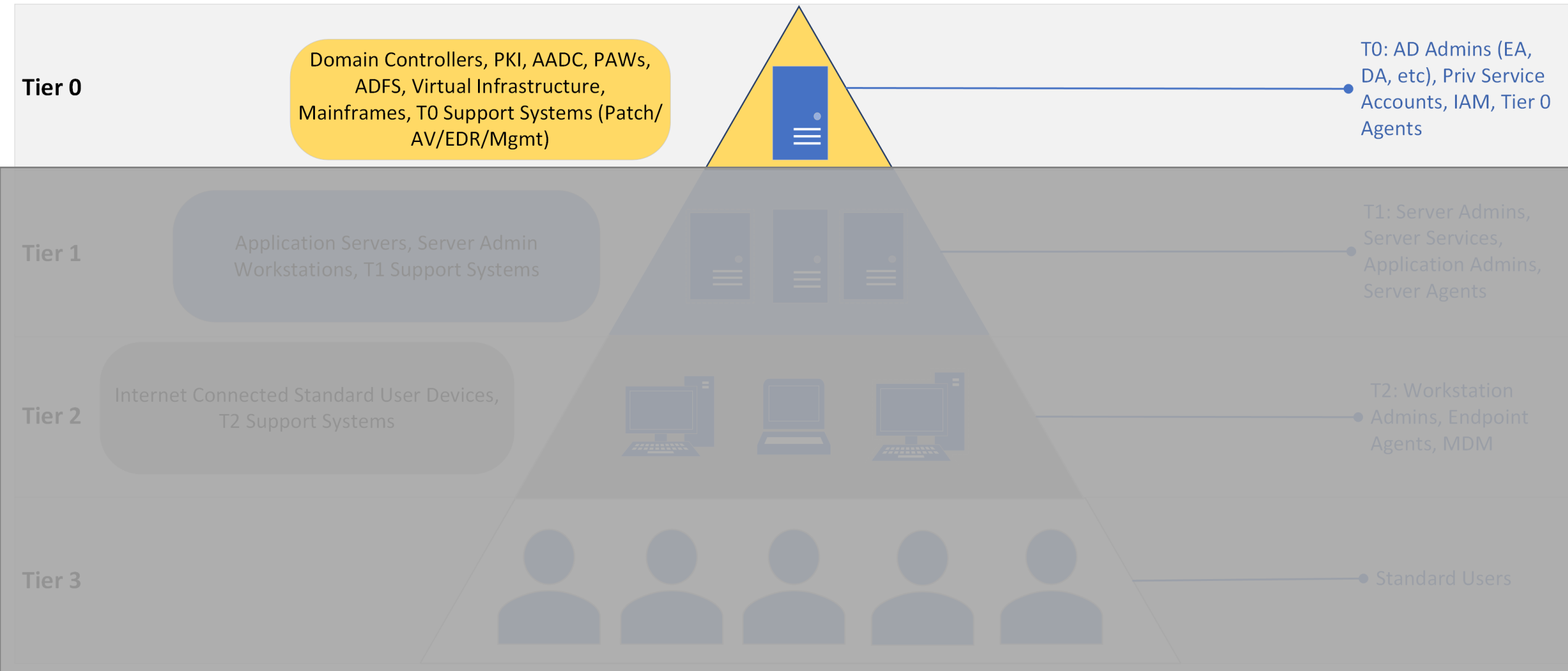
---

The path to Tier 0 is fraught with...









# Action: Getting to Tier 0

- Create top level OU called something like “Admin” which only AD Admins can access & control (via permissions & GPOs).
- Place all admin accounts in this Admin OU
- Leverage AD admin servers where AD admin accounts RDP to this server (which requires MFA) for admin tasks. Though this solves some security issues, but not all.
- Place all admin systems in the Admin OU.
- Use this until deploying admin workstations which actually mitigates attacks against AD admin credentials.





# Identify Common AD Security Issues

- Trimarc developed based on our Active Directory Security Assessment (ADSA) engagement focus.
- Gathers data for key AD security items in a domain:
  - User Account Issues
  - Domain Password Policy
  - Tombstone Lifetime & AD Backup Dates
  - Trusts
  - Duplicate SPNs
  - Group Policy Preference Passwords
  - AD Administration & Privileged Accounts
  - KRBTGT Account
  - Kerberos Delegation

Invoke-TrimarcADChecks (PowerShell)

<https://Trimarc.co/ADCheckScript>

[ @TrimarcSecurity | TrimarcSecurity.com ]



# Agenda

---

- Modern AD Attacks
- Ways to Improve AD Security Quickly
  - Limiting Password Attacks
  - Review AD Admins & Highly Privileged Service Accounts
  - ADCS Security Checks
  - Kerberos Delegation Security
  - Auditing Insecure Protocols & Dangerous Defaults
  - Limiting Local Admin Accounts
  - Domain Controller Security
  - The Path to Tier 0
- **The Trimarc Top Ten List\***
- Conclusion
- Q & A



# Agenda

---

- Modern AD Attacks
- Ways to Improve AD Security Quickly
  - Limiting Password Attacks
  - Review AD Admins & Highly Privileged Service Accounts
  - ADCS Security Checks
  - Kerberos Delegation Security
  - Auditing Insecure Protocols & Dangerous Defaults
  - Limiting Local Admin Accounts
  - Domain Controller Security
  - The Path to Tier 0
- **The Trimarc Top Ten (+20) List**
- Conclusion
- Q & A



# Trimarc's AD Security Checklist of Quick Wins (Now)

1. Review AD Admin group membership regularly, enforce annual password changes, and remove inactive AD Admin accounts.
2. Restrict accounts that are allowed to add workstations to the domain via Machine Account Quota and/or the SeMachineAccountPrivilege.
3. Review accounts that have Unconstrained Delegation and remove any with no associated Kerberos SPN.
4. Configure all AD admin accounts with "Account is Sensitive and cannot be delegated". Then add to the Protected Users group.
5. Disable Print Spooler service on DCs and all servers that do not perform Print services.
6. Work to move the domain password length up to 12-15 characters. Leverage Fine-Grained Password Policies for admin & service accounts in the near-term.
7. Ensure DCs are running current OSs and are regularly patched.
8. Restrict Anonymous LDAP access by limiting the "Pre-Windows 2000 Compatible Access" group and confirm the dsHeuristic value is NOT set to 0000002.
9. Review PKI objects in AD and remediate overly permissive rights.
10. Create Top Level OU for Admin accounts and systems. Lockdown the OU permissions and GPOs.

*This is the Top Ten list from this presentation to improve AD security quickly this week/next week*





# Trimarc's AD Security Checklist of Quick Wins (Next)

11. Secure HTTP endpoints by enforcing HTTPS, enabling Extended Protection for Authentication (EPA), and Disabling NTLM authentication.
12. Remove unnecessary roles, applications and agents on DCs.
13. Remove Kerberos Service Principal Names (SPNs) from any account associated with a person and the default domain Administrator account.
14. Ensure service accounts with SPNs have passwords greater than 25 characters to help protect against Kerberoasting.
15. Leverage Group Managed Service Accounts (GMSAs) where possible.
16. Assume that no service account needs to be in any of the privileged AD admin groups (Domain Admins, Administrators, Enterprise Admins) and challenge any that are.
17. Further reduce service account rights to only what is required. This includes GMSAs.
18. Implement a GPO blocking local Administrator accounts from logging in over the network & RDP. Implement a system like LAPS to ensure that all workstations (& servers) have unique local Administrator passwords.
19. Enable NTLM auditing on all DCs & SMB auditing on all DCs and servers. Review these logs to identify systems to upgrade/decommission.
20. Testing LDAP Channel Binding for deployment to Domain Controllers (significant attack mitigation when configured).

*This is the Top Ten list from this presentation to improve AD security quickly in the next few weeks*



# Trimarc's AD Security Checklist of Quick Wins (Soon)

21. Check EDITF\_ATTRIBUTESUBJECTALNAME2 value for all CAs and unset if required.
22. Review certificate templates for dangerous configurations.
23. Disable accounts no longer in use and remove from privileged groups.
24. Implement GPO blocking Domain Admins, Administrators, & Enterprise Admins from being able to logon on locally to workstations.
25. Restrict Decentralized Name Resolution such as LLMNR and Netbios over TCP.
26. Review Domain Controller GPOs to ensure Advanced Auditing is configured appropriately.
27. Review Domain Controller GPOs for potentially dangerous User Rights Assignments.
28. Implement password filter to reduce "bad password" use in the environment.
29. Implement AD Admin servers for Administrative tasks. Administrators should use MFA to RDP into these servers.
30. Create a honeypot account and monitor for Kerberos Authentication.

*This is the Top Ten list from this presentation to improve AD security quickly in near-term*



# This Active Directory Security Webcast is “Part 1”...

We will schedule another Active Directory Webcast in the coming months which will cover the most important AD security mitigation items (which tend to be more difficult)



## UPCOMING TRIMARC WEBCASTS

### Issues with Identity Security – a Trimarc Panel

*A discussion around Ransomware, Rights, & Remediation*



Thursday, July 28th

2pm to 3pm (Eastern)

Panel:

Sean Metcalf, Tyler Robinson, & Brandon Colley

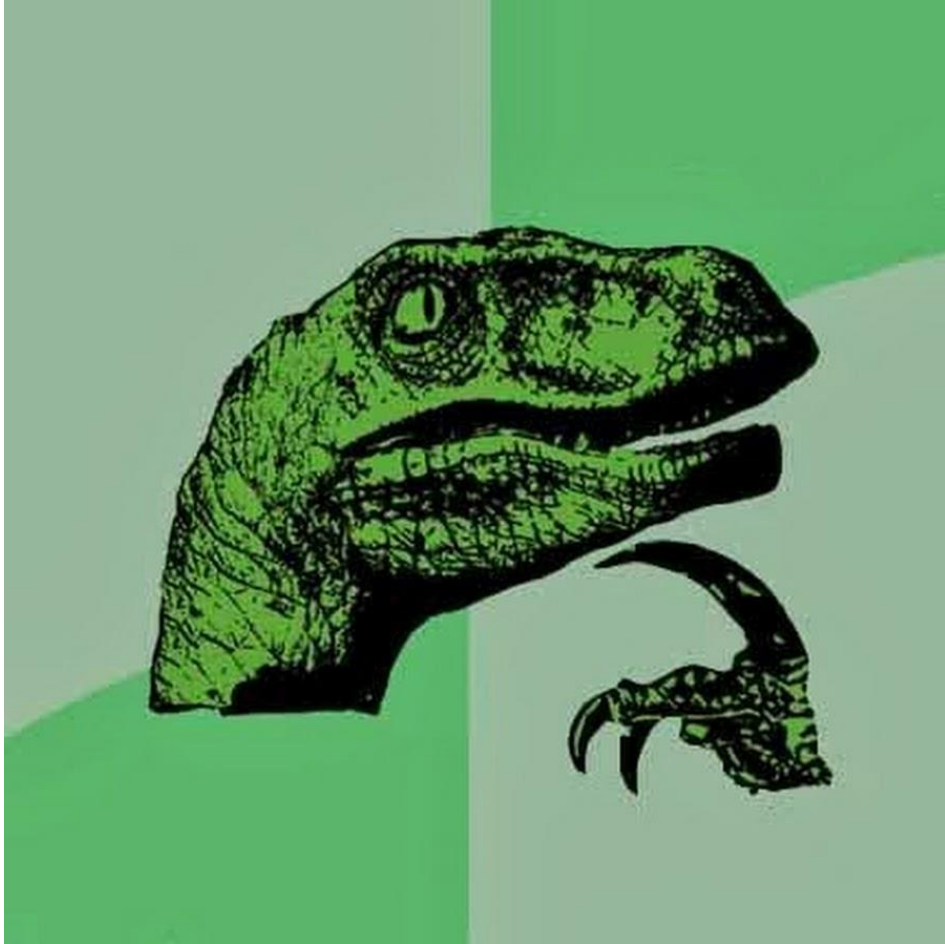
Register here:

[Trimarc.co/WebcastPanel2207](https://Trimarc.co/WebcastPanel2207)

[ @TrimarcSecurity | TrimarcSecurity.com ]



# Recommendations



Slides, Video & Security Articles:  
[Hub.TrimarcSecurity.com](https://Hub.TrimarcSecurity.com)

Active Directory security can be complicated, but there are a number of actions that can be taken in the near-term to improve the security posture.

Implementing the guidance in this webcast levels up you AD security.

Concerned about your AD Security Posture?

Contact Trimarc to perform a comprehensive **Active Directory Security Assessment** & find out why our customers return to Trimarc to assess their **Azure AD & VMware** environments (and **AD** again!).

[Trimarc.co/WebContact](https://Trimarc.co/WebContact)





# Questions







# Resources & References

---



# References

- LDAP Signing & Channel Binding:
  - <https://www.hub.trimarcsecurity.com/post/ldap-channel-binding-and-signing>
- Decentralized Name Resolution:
  - <https://www.blumira.com/integration/disable-llmnr-netbios-wpad-lm-hash/>
  - <https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/>
  - <https://techcommunity.microsoft.com/t5/networking-blog/mdns-in-the-enterprise/ba-p/3275777>
- Microsoft recommended Audit Policy:
  - <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>





# References

- KRBRelayup Tool:
  - <https://github.com/DecOne/KrbRelayUp>
- Kerberos Attack References:
  - <https://blog.redforce.io/windows-authentication-attacks-part-2-kerberos/>
  - <https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html>
  - <https://exploit.ph/defending-the-three-headed-relay.html>
  - <https://dirkjanm.io/worst-of-both-worlds-ntlm-relaying-and-kerberos-delegation/>
  - <https://posts.specterops.io/a-case-study-in-wagging-the-dog-computer-takeover-2bcb7f94c783>
  - <https://posts.specterops.io/another-word-on-delegation-10bdb3cd94a>
  - <https://github.com/Kevin-Robertson/Powermad>
  - <https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/resource-based-constrained-delegation-ad-computer-object-take-over-and-privileged-code-execution>
- Microsoft recommended krbrelay guidance:
  - <https://www.microsoft.com/security/blog/2022/05/25/detecting-and-preventing-privilege-escalation-attacks-leveraging-kerberos-relaying-krbrelayup/>



# KrbRelayUp Summary

- Simplified tooling to automate the process and techniques within krbrelay, powermad, Rubeus, and SCMUACBypass
- This is a no-fix local privilege escalation path for attackers
- By default works in most AD environments if LDAP Signing and/or Channel Binding is not enforced
- Uses the computer object to relay Kerberos to LDAP that can then abuse RBCD settings to impersonate (S4U2Self & S4U2Proxy) any user and obtain SYSTEM permissions on target host
- Many other variations on this attack; ADCS web enrollment, ShadowCreds, and MAQ.
- Attacker can target any workstation or server in the AD forest (once they have access) and depending on the configuration, across a trust!



# KrbRelayUp Overview

- Key Points

- In this scenario, attacker can create a new computer account in AD
- Trimarc has seen that ~75% of AD forests enable this
- There are 2 computers in this scenario: the target and a computer object in AD that the attacker controls (created)
- The attacker is logged onto the target computer
- Attacker has local logon rights to the target system
- Attacker creates new computer account which provides ability to set Resource Based Constrained Delegation (RBCD)
- Kerberos Delegation is impersonation
- Leverage Kerberos feature called S4U2Self to impersonate the user (AD account with admin rights on target, could be AD admin account)
- Leverage Kerberos feature called S4UProxy to impersonate the target computer account
- Once this is completed, the attacker has local SYSTEM rights on the target computer

