Is this SID taken? Varonis Threat Labs Discovers Synthetic SID Injection Attack

varonis.com/blog/synthetic-sid



Varonis Threat Labs researchers have discovered a technique where threat actors with existing high privileges can inject synthetic SIDs into an Active Directory Access Control List (ACL). This creates a scenario where backdoors and hidden permission grants can occur when a new account is created with a matching legitimate SID.

This attack is made possible as:

- SIDs are easily guessable as they're predominantly consecutively assigned
- Active Directory does not verify if a SID applied to an ACL is valid

We're terming the SIDs which conform to the formatting rules of legitimate SIDs but don't actually yet reference an object to be "synthetic".

Background

Active Directory's permission system is composed of three parts:

- 1. **Trustees:** objects which have permissions applied. This most commonly includes user accounts, groups, and computer accounts.
- 2. Security Identifier (SID): Within Active Directory, security principals are identified by a security identifier (SID). The SID is a unique identifier used to represent any entity that can be authenticated by the operating system. It can be loosely compared to a social security number or a citizen ID but for a domain object. The SID is issued by a Domain Controller and is assigned to an object at the time of its creation. It cannot be reused or used to identify another entity.
- 3. Access Control List (ACL): the mapping between an object (SID) and permissions within Active Directory.

No SID Verification

When an ACL is created the trustees' SID is not verified to exist on the domain. Because no validity check is done for the SID, with sufficient permissions, it's possible to add a non-existent "synthetic" SID to an ACL.

These non-existing (Synthetic) SIDs with ACL permissions persist innocuously on the ACLs until a new user or computer account is created that is assigned the previously synthetic SID. These new accounts instantly inherit the previously granted ACL permissions.

How to examine an ACL

We can see the ACL of an object by going to its security tab:

General	Operating System	Member	Of Dele	gation	Pass	sword Replication				
Location	Managed By	Object	Security	Dia	l-in	Attribute Editor				
Group or us	Group or user names:									
Sert P	Sert Publishers (EVIE\Cert Publishers)									
🚨 Enterp	Enterprise Admins (EVIE\Enterprise Admins)									
🎎 Key A	See Key Admins (EVIE\Key Admins)									
Sector: Enterp	orise Key Admins (EVI	E\Enterprise	e Key Admin	s)		2				
See Admin	istrators (EVIE\Admin	istrators)								
Secon Accor	unt Operators (EVIE\A	Account Ope	erators)							
K myAco	count (EVIE\myAccou	unt)				~				
	<u> </u>	<u> </u>								
				Add		Remove				
Permissions	s for myAccount				Allow	Deny				
Full cont	rol					□ ^				
Read					\checkmark					
Write										
Create a	ll child objects									
Delete a	Il child objects									
Allowed	to authenticate									
Change	password									
For special	permissions or advan	ced settinas	, click Adva	inced.		Advanced				
		-	-			Auvanceu				
	0	К	Cancel		Apply	Help				

Windows resolves the entry's SID and presents the username for readability. However, behind the scenes, the ACL identifies the user via their SID as defined by the SDDL (more on SDDLs here <u>https://docs.microsoft.com/en-us/windows/win32/secauthz/security-descriptor-string-format</u>).

Injecting a synthetic SID into an ACL

As Windows doesn't verify that the SIDs exist on the domain when an ACL is created it's possible to insert our Synthetic SID into any object's ACL we have privileges over:

General	Members	Membe	er Of	Managed I	By
Object	Se	curity	Attri	bute Editor	
Group or user na	ames:				
SELF					^
🚨 Authentica	ted Users				
SYSTEM 🕺					
Account U	nknown(S-1-5-2	1-1337-1337-1	337-123)		
a test1				₽	
👗 sidtest1					~
			Add	Remove	•
^o emissions for J nknown(S-1-5	Account -21-1337-1337-1	337-123)	Allow	Deny	
Full control			\checkmark		^
Read			\checkmark		
Write			\checkmark		
Create all chil	d objects		\checkmark		
Delete all chil	d objects		\checkmark		~
or special perm	nissions or advan	ced settings, o	click	Advanced	
Advanced					
advanced					

Note: the domain section of the SID is changeable, but the "S-1-5-21" is not. The Synthetic SID in the screenshot both:

- Cannot be resolved ("Account Unknown") because it is not assigned
- Valid for the ACL entry

Getting control over an existing SID is not easily achieved as SIDs can't be taken from other users or reused. However, by mapping what SIDs currently exist in the domain we can

predict what SIDs new users will be created with allowing us to create a scenario where a newly created account inherits our injected permissions. We can map the currently existing SIDs with PowerShell:

(([adsisearcher]"(objectSid=*)").FindAll()).Properties.objectsid | ForEach-Object {(New-Object System.Security.Principal.SecurityIdentifier(\$_,0)).Value}

The SID in the following image has no account related to it and is the next available SID in the domain. It was granted Full Control on the "Remote Management Users" object:

Advanced S	Security Settings for Remote Management Users		- 0
wner:	Administrators (EVIE\Administrators) Change		
ermission	Auditing Effective Access		
or addition	al information, double-click a permission entry. To modify a permission entry, select the	e entry and click	Edit (if available).
ermission e	ntries:		
Туре	Principal	Access	Inherit 1
Allow	S-1-5-21-143722562-1117806217-3041158659-5105	Full control	None
Allow Allow	S-1-5-21-143722562-1117806217-3041158659-5105 S-1-5-21-143722562-1117806217-3041158659-5106	Full control Full control	None None
Allow Allow Allow	S-1-5-21-143722562-1117806217-3041158659-5105 S-1-5-21-143722562-1117806217-3041158659-5106 Domain Admins (EVIE\Domain Admins)	Full control Full control Full control	None None None
Allow Allow Allow Allow	S-1-5-21-143722562-1117806217-3041158659-5105 S-1-5-21-143722562-1117806217-3041158659-5106 Domain Admins (EVIE\Domain Admins) Account Operators (EVIE\Account Operators)	Full control Full control Full control Full control	None None None None
Allow Allow Allow Allow Allow	S-1-5-21-143722562-1117806217-3041158659-5105 S-1-5-21-143722562-1117806217-3041158659-5106 Domain Admins (EVIE\Domain Admins) Account Operators (EVIE\Account Operators) Authenticated Users	Full control Full control Full control Full control Send to	None None None None None
Allow Allow Allow Allow Allow Allow Allow	S-1-5-21-143722562-1117806217-3041158659-5105 S-1-5-21-143722562-1117806217-3041158659-5106 Domain Admins (EVIE\Domain Admins) Account Operators (EVIE\Account Operators) Authenticated Users Windows Authorization Access Group (EVIE\Windows Authorization Access Group)	Full control Full control Full control Full control Send to	None None None None None None
Allow Allow Allow Allow Allow Allow Allow Allow	S-1-5-21-143722562-1117806217-3041158659-5105 S-1-5-21-143722562-1117806217-3041158659-5106 Domain Admins (EVIE\Domain Admins) Account Operators (EVIE\Account Operators) Authenticated Users Windows Authorization Access Group (EVIE\Windows Authorization Access Group) Enterprise Admins (EVIE\Enterprise Admins)	Full control Full control Full control Full control Send to Full control	None None None None None Parent
Allow	S-1-5-21-143722562-1117806217-3041158659-5105 S-1-5-21-143722562-1117806217-3041158659-5106 Domain Admins (EVIE\Domain Admins) Account Operators (EVIE\Account Operators) Authenticated Users Windows Authorization Access Group (EVIE\Windows Authorization Access Group) Enterprise Admins (EVIE\Enterprise Admins) Administrators (EVIE\Administrators)	Full control Full control Full control Send to Full control Special	None None None None None Parent Parent
Allow	S-1-5-21-143722562-1117806217-3041158659-5105 S-1-5-21-143722562-1117806217-3041158659-5106 Domain Admins (EVIE\Domain Admins) Account Operators (EVIE\Account Operators) Authenticated Users Windows Authorization Access Group (EVIE\Windows Authorization Access Group) Enterprise Admins (EVIE\Enterprise Admins) Administrators (EVIE\Administrators) Pre-Windows 2000 Compatible Access (EVIE\Pre-Windows 2000 Compatible Access)	Full control Full control Full control Send to Full control Special List contents	None None None None None Parent Parent Parent
Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow	S-1-5-21-143722562-1117806217-3041158659-5105 S-1-5-21-143722562-1117806217-3041158659-5106 Domain Admins (EVIE\Domain Admins) Account Operators (EVIE\Account Operators) Authenticated Users Windows Authorization Access Group (EVIE\Windows Authorization Access Group) Enterprise Admins (EVIE\Enterprise Admins) Administrators (EVIE\Administrators) Pre-Windows 2000 Compatible Access (EVIE\Pre-Windows 2000 Compatible Access)	Full control Full control Full control Send to Full control Special List contents	None None None None Parent Parent Parent
Allow Allow Allow Allow Allow Allow Allow Allow Allow	S-1-5-21-143722562-1117806217-3041158659-5105 S-1-5-21-143722562-1117806217-3041158659-5106 Domain Admins (EVIE\Domain Admins) Account Operators (EVIE\Account Operators) Authenticated Users Windows Authorization Access Group (EVIE\Windows Authorization Access Group) Enterprise Admins (EVIE\Enterprise Admins) Administrators (EVIE\Administrators) Pre-Windows 2000 Compatible Access (EVIE\Pre-Windows 2000 Compatible Access)	Full control Full control Full control Send to Full control Special List contents	None None None None None Parent Parent Parent
Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow	S-1-5-21-143722562-1117806217-3041158659-5105 S-1-5-21-143722562-1117806217-3041158659-5106 Domain Admins (EVIE\Domain Admins) Account Operators (EVIE\Account Operators) Authenticated Users Windows Authorization Access Group (EVIE\Windows Authorization Access Group) Enterprise Admins (EVIE\Enterprise Admins) Administrators (EVIE\Administrators) Pre-Windows 2000 Compatible Access (EVIE\Pre-Windows 2000 Compatible Access) Remove Edit	Full control Full control Full control Send to Full control Special List contents	None None None None None Parent Parent Parent Restore defaults

We created an account called "ThisIsMySid" and it took over the SID:

· ·					Guest S			06017 2044450	DELO
General		Members	Member Of	Managed By	administrator	-1-5-21-143/2250	52-111/86	00217-3041158	3059-
Obje	ect	Securty		Attribute Editor			52-111786	00217-3041150 06217-3041150	8650_3
aroup or u	user na	ames:			testi -	-1-5-21-14372256	52-111786	00217-3041138 06217-3041158	8659-
atest1	I (EVIE	E\test 1)		~	sidtest1 S	5-1-5-21-14372250	52-111786	06217-3041158	8659-9
sidtes	st1 (E\	VIE\sidtest1)			ThisIsMySID S	5-1-5-21-14372250	52-111780	06217-3041158	8659-5
Advanc	red Se	curity Settings for Re	mote Mana	agement Users				×	
				· · · · · · · · · · · · · · · · · · ·			_		
Owner:		Administrators (EV	/IE\Admini	strators) Change					
D		A	F//						
Permissi	sions	Auditing	Effective A	ccess					
or addit	tional	information, double-	-click a per	mission entry. To modify	a permission entry, select	the entry and click Edit	(if available).		
er adam	cional	and the second second	ener a per		a permission energy select	the entry and ener car	(available).		
ermissio)	on en	tries:							
Туре	e	Principal		Access	Inherited from	Applies to		^	
Type	oe ow	Principal ThislsMySID		Access Full control	Inherited from None	Applies to This object only		^	
Type	ow ow	Principal ThislsMySID Account Unknown(S	-1-5-21	Access Full control Full control	Inherited from None None	Applies to This object only This object only			
Type Allo 2 Allo 2 Allo	oe ow ow ow	Principal ThisIsMySID Account Unknown(S Account Operators (E	-1-5-21 EVIE\Acc	Access Full control Full control Full control Full control	Inherited from None None None	Applies to This object only This object only This object only			
Type Allo Allo Allo Allo Allo	oe ow ow ow	Principal ThisIsMySID Account Unknown(S Account Operators (E SELF	-1-5-21 EVIE\Acc	Access Full control Full control Full control Special	Inherited from None None None None	Applies to This object only This object only This object only This object only			
Typ Allo Allo Allo Allo Allo	oe ow ow ow ow	Principal ThisIsMySID Account Unknown(S Account Operators (E SELF Authenticated Users	-1-5-21 EVIE\Acc	Access Full control Full control Full control Special Special	Inherited from None None None None None	Applies to This object only This object only This object only This object only This object only			
Typ	be bw bw bw bw bw bw bw	Principal ThisIsMySID Account Unknown(S Account Operators (E SELF Authenticated Users SYSTEM	-1-5-21 EVIE\Acc	Access Full control Full control Full control Special Special Full control	Inherited from None None None None None None	Applies to This object only This object only This object only This object only This object only This object only			
Typ	ow ow ow ow ow ow ow	Principal ThisIsMySID Account Unknown(S Account Operators (E SELF Authenticated Users SYSTEM Pre-Windows 2000 C	-1-5-21 EVIE\Acc ompatib	Access Full control Full control Full control Special Full control Special	Inherited from None None None None None CN=Builtin,DC=EVIE,D	Applies to This object only This object only This object only This object only This object only This object only This object only Output Descendant InetOrg	Person o		
Type Allo Allo Allo Allo Allo Allo Allo All	ove ow ow ow ow ow ow ow ow	Principal ThisIsMySID Account Unknown(S Account Operators (E SELF Authenticated Users SYSTEM Pre-Windows 2000 C Pre-Windows 2000 C	-1-5-21 EVIE\Acc ompatib ompatib	Access Full control Full control Special Special Full control Special Special	Inherited from None None None None CN= Builtin, DC=EVIE, D CN= Builtin, DC=EVIE, D	Applies to This object only This object only This object only This object only This object only This object only One Descendant InetOrg Descendant Group of	jPerson o objects		
Type Type	be bw bw bw bw bw bw bw bw bw bw bw bw bw	Principal ThisIsMySID Account Unknown(S Account Operators (E SELF Authenticated Users SYSTEM Pre-Windows 2000 C Pre-Windows 2000 C	-1-5-21 EVIE\Acc ompatib ompatib ompatib	Access Full control Full control Special Special Special Special Special Special Special Special	Inherited from None None None None CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D	Applies to This object only This object only This object only This object only This object only This object only Chine O	Person o objects ojects		
Type Type Allo	e ow ow ow ow ow ow ow ow ow ow ow	Principal ThisIsMySID Account Unknown(S Account Operators (E SELF Authenticated Users SYSTEM Pre-Windows 2000 C Pre-Windows 2000 C SELF	-1-5-21 EVIE\Acc ompatib ompatib ompatib	Access Full control Full control Special Special Special Special Special Special	Inherited from None None None None CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D	Applies to This object only This object only This object only This object only This object only This object only Chine Descendant InetOrg Chine Descendant User ob Chine Descendant User ob Chine Object and all of Chine Object and Chine Object and Chine Object and All of Chine Object and Chine Object	iPerson o objects ojects iescendan		
Type Allo	be bw bw bw bw bw bw bw bw bw bw	Principal ThisIsMySID Account Unknown(S Account Operators (E SELF Authenticated Users SYSTEM Pre-Windows 2000 C Pre-Windows 2000 C SELF	-1-5-21 EVIE\Acc ompatib ompatib ompatib	Access Full control Full control Special Special Special Special Special Special	Inherited from None None None None CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D	Applies to This object only This object only This object only This object only This object only This object only This object only Descendant InetOrg Descendant User ob Descendant User ob This object and all of	JPerson o objects ojects descendan		
Type Allo	be bw bw bw bw bw bw bw bw bw bw	Principal ThisIsMySID Account Unknown(S Account Operators (E SELF Authenticated Users SYSTEM Pre-Windows 2000 C Pre-Windows 2000 C SELF Remove	-1-5-21 EVIE\Acc ompatib ompatib ompatib Edit	Access Full control Full control Special Special Special Special Special Special	Inherited from None None None None CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D	Applies to This object only This object only This object only This object only This object only This object only This object only Descendant InetOrg Descendant User ob Descendant User ob This object and all of Res)Person o objects ojects descendan store defaults	S	
Type Allo	be bw bw bw bw bw bw bw bw bw bw bw bw bw	Principal ThisIsMySID Account Unknown(S Account Operators (E SELF Authenticated Users SYSTEM Pre-Windows 2000 C Pre-Windows 2000 C SELF Remove Remove	-1-5-21 EVIE\Acc ompatib ompatib ompatib Edit	Access Full control Full control Special Special Special Special Special Special	Inherited from None None None None CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D	Applies to This object only This object only This object only This object only This object only This object only Descendant InetOrg Descendant User ob Descendant User ob This object and all of Res)Person o objects jects Jescendan store defaults	s	
Type Allo	be bw bw bw bw bw bw bw bw bw bw	Principal ThisIsMySID Account Unknown(S Account Operators (E SELF Authenticated Users SYSTEM Pre-Windows 2000 C Pre-Windows 2000 C Pre-Windows 2000 C SELF Remove eritance	-1-5-21 EVIE\Acc ompatib ompatib ompatib Edit	Access Full control Full control Special Special Special Special Special Special	Inherited from None None None None CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D	Applies to This object only This object only This object only This object only This object only This object only Descendant InetOrg Descendant User ob Descendant User ob This object and all of Res	JPerson o objects jjects Jescendan store defaults	\$ 5	
Type Constant of the second s	ee bow bow bow bow bow bow bow bow bow bow	Principal ThisIsMySID Account Unknown(S Account Operators (E SELF Authenticated Users SYSTEM Pre-Windows 2000 C Pre-Windows 2000 C Pre-Windows 2000 C SELF Remove eritance	-1-5-21 EVIE\Acc ompatib ompatib ompatib Edit	Access Full control Full control Special Special Special Special Special Special	Inherited from None None None None CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D	Applies to This object only This object only This object only This object only This object only This object only Descendant InetOrg Descendant User ob Descendant User ob This object and all of Res	JPerson o objects ojects descendan store defaults	s	
Type Allo	be by by by by by by by by by by	Principal ThisIsMySID Account Unknown(S Account Operators (E SELF Authenticated Users SYSTEM Pre-Windows 2000 C Pre-Windows 2000 C Pre-Windows 2000 C SELF Remove eritance	-1-5-21 EVIE\Acc ompatib ompatib Edit	Access Full control Full control Special Full control Special Special Special Special	Inherited from None None None None CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D CN=Builtin,DC=EVIE,D	Applies to This object only This object only This object only This object only This object only This object only Descendant InetOrg Descendant User ob Descendant User ob This object and all of Res	person o objects ojects descendan store defaults	s	

The user "ThisIsMySID" now has full control over the group object.

It's worth noting that this trick also works for assigning Windows Privileges and rights such as SeDebugPrivilege, SeRemoteInteractiveLogonRight, or other <u>Privilege Constants</u>.

Exploitation





The main exploitation vector here is persistence. Threat actors with domain control can add permissions and privileges to future SIDs and regain a foothold by creating a user or computer account.

Creating an account is not much of an issue assuming you have control over a regular user account. Authenticated users can create up to 10 computer accounts by default, and computer accounts get SIDs assigned to them just like regular users which allows for this exploitation.

DCSync Exploitation Scenario

By adding a SID to the domain object and granting it synchronization privileges (which are required for the DCSync attack), the threat actor planted the backdoor. And of course, more than one SID can be added to make sure that it's not overwritten by regular activity.

To regain a foothold, the threat actor would have to gain control over a standard user account (possibly by phishing) and use that account to create a computer account:

The newly created account will replace one of the available SIDs and have DCSync permissions.



Remediation and Monitoring

Microsoft does not consider this a security issue, however, monitoring is still recommended as the assignment of synthetic SIDs is anomalous behavior.

Monitoring of the following is recommended to mitigate the risk of this technique.

- Alerts on abnormal privilege changes, rights assignments, and permission grants in Active Directory environments whether they are done automatically via scripts or malware, or manually by an active threat.
- Behavior-based modeling (as done by Varonis) on sensitive objects for ACL changes.

Changes on directory service objects in your organization (Windows event <u>5136</u>)
 Event Properties - Event 5136, Microsoft Windows security auditing.

A directory	service object was modified.			^
Subject:				
S	curity ID:			
A	ccount Name:			
A	count Domain:			
-				
Directory S	ervice:			
T	ame: /pe: Active Directory Domain Se	ervices		
	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
Object:	N. CN. Parrieta Dasletan Usar	CN- Puiltin		
G	UID: CN=Remote Desktop Users	, CN=Builtin		
C	ass: group			
Attributer				
L	DAP Display Name: nTSecuri	tyDescriptor		
S	ntax (OID): 2.5.5.15			
V	alue: O:BAG:BAD:AI(OA;;RP;46a9	b11d-60ae-405a-b7	7e8-ff8a58d456d2;;S-1-5-32-	
(A::CCDCL	CSWRPWPDTLOCRSDRCWDWO:::1	DA)(A::CCDCLCSWF	RPWPDTLOCRSDRCWDWO:::S	
1-5-21-378	1416057-1316462796-1760547704-4	192)		
(A;;CCDCL	CSWRPWPDTLOCRSDRCWDWO;;;	AO)(A;;LCRPLORC;;	PS)(A;;LCRPLORC;;;AU)	
(A;;CCDCL 00aa006e0	29.4828cc14-1437-45bc-9b07-add	615e5f28·RU)(OA;CIIOID;RP;40	c164200-20c0-11d0-a768- 1101D:RP:4c164200-20c0-11d0-	
a768-00aa	06e0529;bf967aba-0de6-11d0-a28	5-00aa003049e2;RU)	(OA;CIIOID;RP;5f202010-79a5-	
11d0-9020	00c04fc2d4cf;4828cc14-1437-45bc	-9b07-ad6f015e5f28	3;RU)(OA;CIIOID;RP;5f202010-	
(04-CIIOID	9020-00c04fc2d4cf;bf96/aba-0de6 •RP·bc0ac240-79a9-11d0-9020-00c	-11d0-a285-00aa00 04fc2d4cf+4828cc14	3049e2;KU) I-1437-45bc-9b07-	
ad6f015e5f	28;RU)(OA;CIIOID;RP;bc0ac240-79;	a9-11d0-9020-00c04	lfc2d4cf;bf967aba-0de6-11d0-	
a285-00aa(03049e2;RU)(OA;CIIOID;RP;59ba2f	42-79a2-11d0-9020-	00c04fc2d3cf;4828cc14-1437-	
45bc-9b07 0de6-11d0	ad6f015e5f28;RU)(OA;CIIOID;RP;59	9ba2f42-79a2-11d0-)-RD-027088f8-0ae1-	9020-00c04fc2d3cf;bf967aba-	
00a0c968f9	39;4828cc14-1437-45bc-9b07-ad6f	015e5f28;RU)(OA;Cl	IIOID;RP;037088f8-0ae1-11d2-	
b422-00a0	968f939;bf967aba-0de6-11d0-a285	-00aa003049e2;RU)	(OA;CIIOID;RP;b7c69e6d-2cc7-	-
11d2-854e	00a0c983f608;bf967a86-0de6-11d0	-a285-00aa003049e	2;ED)(OA;CIID;RP;b7c69e6d-	
(OA:CIIOID	:RP:b7c69e6d-2cc7-11d2-854e-00a	0c983f608:bf967aba	a-0de6-11d0-a285-	~
.og Name:	Security			
•	Microsoft Windows securi	ity Logged:	1/31/2022 9:29:31 AM	
ource:	5136	Task Category:	Directory Service Changes	
ource: event ID:	Information	Keywords:	Audit Success	
ource: Event ID: Level:	mornation	-		
ource: Event ID: .evel: Jser:	N/A	Computer:		
Source: Event ID: .evel: Jser: DpCode:	N/A Info	Computer:		

Сору

Close

 \times

• Behavior-based modeling (like that provided by Varonis) to alert when a user is granted permissions over a sensitive object or to monitor a trustee that's added to the object and alert if it doesn't exist.

Drag columns to group						
Event Type (Event Details)	User Name (Event By Accou	Path (Event On Resource)	Account Name (Permission Change Detail			
DS object permission added	Evie.cat\Administrator	Evie.cat\Builtin\Remote Desktop Users	user5			

• Direct privilege assignments (Windows event <u>4704</u>) may indicate synthetic SID injection.

Event Properti	es - Event 4704, I	Microsoft Windo	ws security audit	ing.	×
General Details A user right wa Subject: Securi Accou Logor Target Accoun Accou New Right: User F	ity ID: unt Name: unt Domain: n ID: t: unt Name: Right:	S-1-5-21-37 SeSecurityP	781416057-13164 rivilege	52796-1760547704-1234	•
User Right: Log Name: Security Source: Microsoft Win Event ID: 4704 Level: Information User: N/A OpCode: Info More Information: <u>Event Log Or</u>		/indows security 1 <u>Online Help</u>	Logged: Task Category: Keywords: Computer:	2/2/2022 9:47:46 AM Authorization Policy Change Audit Success	
Сору					Close
ent Description					
e user right SeMa	nageVolumePrivil	ege was assigned <mark>t</mark>	o vrnslab.se\S-1-5-	21-3781416057-1316462796-176054770	04-1237
e user right SeSys	stemtimePrivilege	was assigned to vri	nslab.se\S-1-5-21-3	3781416057-1316462796-1760547704-1	238
e user right SeRes	storePrivilege was	assigned to vrnslal	b.se\S-1-5-21-3781	416057-1316462796-1760547704-1238	
e user right Selm	personatePrivilege	was assigned to v	rnslab.se\S-1-5-21-	3781416057-1316462796-1760547704-	1238

The user right SeCreatePagefilePrivilege was assigned to vrnslab.se\S-1-5-21-3781416057-1316462796-1760547704-1237

The user right SeCreateSymbolicLinkPrivilege was assigned to vrnslab.se\S-1-5-21-3781416057-1316462796-1760547704-1238

Removing Orphaned SIDs

Having a process to monitor and remove orphaned SIDs will prevent the attacker from gaining control over the synthetic SIDs as well.

Consider using <u>PowerShell, ICACLS</u>, or dedicated tools to find orphaned SIDs and remove them.

Sources



Eric Saraga