ManageEngine Log360 Cloud

MONITOREO DE AD PROACTIVO con Log360 Cloud

5 CASOS DE USO **CRÍTICOS**

Las empresas confían en Active Directory (AD) por su capacidad para gestionar y organizar recursos como usuarios, computadores y servicios de forma centralizada y segura. Como resultado, siempre existe la posibilidad de que los actores de amenazas ataquen AD y realicen modificaciones y cambios de configuración para obtener acceso no autorizado, lo que conduce a violaciones de datos, interrupciones del servicio y otros incidentes de seguridad. En este documento, analizaremos cinco casos de uso críticos que los administradores de TI y los equipos de seguridad deben tener en cuenta a la hora de proteger su entorno de AD.

1.Auditar las modificaciones en GPO

Un objeto de directiva de grupo (GPO) define varios ajustes para las cuentas de equipos y usuarios dentro de un entorno de AD. Cualquier cambio no autorizado en un GPO relacionado con privilegios, acceso a información o servicios, o ajustes de seguridad puede provocar interrupciones y problemas de seguridad.

- Auditar los cambios críticos en las políticas, como los cambios en la política de bloqueo de cuenta y la política de cambio de contraseña, ayuda a detectar y responder a actividades maliciosas al instante.
- 2. Monitorear cualquier cambio o modificación no autorizada en los ajustes de seguridad del GPO es crucial. Algunas modificaciones (como reducir los requisitos de complejidad o longitud de las contraseñas, desactivar los firewalls de Windows o permitir servicios de desktop remoto en redes inseguras) hacen que la organización sea vulnerable a posibles brechas de seguridad.
- 3. Auditar los GPO también es crucial, ya que se utilizan para gestionar los ajustes de las políticas de actualización de Windows en todas las unidades organizativas. Monitorear estos cambios garantiza que estas políticas estén configuradas correctamente, previniendo cualquier cambio no aprobado que pueda representar una amenaza a su seguridad.

PROBLEMA:

Imagine un escenario en el que un actor malicioso obtiene acceso no autorizado al entorno de AD y modifica los ajustes del GPO. El atacante podría debilitar las políticas de contraseñas, desactivar configuraciones de seguridad críticas o conceder acceso no autorizado a archivos confidenciales.

Tomemos el ejemplo de un atacante que quiere debilitar las políticas de contraseña para poder tener acceso no autorizado a las cuentas de usuario.

En un entorno de AD nativo, las políticas de contraseña se configuran a través de GPO, normalmente en la política de dominio predeterminada.

Action View Window Help				
2 📰 🖻 🖆 🗙 🍳 🖬				
<i></i>	Group Policy Management Edito	or 🔤		
File Action View Help				
🔷 🔿 🖄 📰 🔒	2 10			
🔺 👰 Computer Configuration	Policy	Policy Setting		
a 🧾 Policies	- Enforce password history	0 passwords remembered		
Software Settings	Antimum password age	42 days		
A Windows Settings	Minimum password age	0 days	ONotdelete	
Scripts (Startu	Minimum password length	5 characters	astdeena	
A Security Settin	Representation of the second s	Disabled		
Account P	al Store passwords using reversible encryption	Disabled		
Passwitz	Minimum paceword long	th Properties ? ×		
Accou	Minimum password leng			
þ 🗿 Kerber	Security Policy Setting Explain			
b 📓 Local Polic	Silver Main an annual locath			
Event Log	Minimum password length			
b System Se				
Registry	 Define this policy setting 			
File System	Password must be at least:			
Wired Net	4 characters			
Windows				
Network L				
p 🔐 wireless in				
Software F				
Network A				
<				
gpo test 1				
Gpo\$				
GPO_Hyphen				
GPO_Test1				
apo1				
gpo10				
gpo11	OK	Cancel Annhy		
gpo12	- OK	Carlos Appy		
gpo13	WMI Filtering			
gpo14	This GPO is linked to the following WMI fil	ter:		
gpors	v (none>	✓ Open		
ш				
				ENG

Una de las configuraciones asociadas con las políticas de contraseña es la longitud mínima de la contraseña.

Fig. 1: Modificar la propiedad de longitud mínima de la contraseña

El atacante podría modificar esta configuración para debilitar la política de contraseña reduciendo la longitud mínima de la contraseña, y aumentando así la vulnerabilidad de las cuentas de usuario.

SOLUCIÓN:

Cambios en los ajustes de GPO > Cambios en la política de contraseña

En Log360 Cloud (véase Figura 2):

- 1. Vaya a la pestaña Informes.
- 2. Vaya a Dispositivos en el menú desplegable y luego al menú Active Directory.
- 3. Vaya a Cambios en los ajustes de GPO > Cambios en la política de contraseña.

contrasenta.							
Log360 Cloud	Search Correlation	Alerts Cloud Protection	Settings Support				License 🌲 ?* 😁 *
Devices 🗸 Windows A	Active Directory Unix/Linux	Cisco SonicWall Fortinet	Juniper Meraki Sophos	PaloAto WatchGuard Barracuda	Huawei Arista NetScreen 🝷		
Search available reports							
User Logon Reports	Password Policy Changes						Export As 👻 [5]
Local Logon-Logoff	Domain testdomain.com	✓ T				Period	2024-01-01 00:00:00 - 2024-01-05 23:59:59
Account Management	🖽 := 🛞 Incident						1.1 of 1 50 - 000
User Management	GPO Name	Modified Time 🔹	Domain Controller	Who Modified	Summary		Linked GPOs
Group Management	default domain policy	2024-01-05 02:18:07	win-7ug5okatosv	testdomainladministrator	Added (0) O Modifier	(1) Removed (0)	testdomain
Computer Management							
OU Management							
GPO Management							
GPO Setting Changes							
Group Policy Setting Chan							
Computer Configuration Ch	(
User Configuration Change							
Password Policy Changes							
Account Lockout Policy Ch							
Security Settings Changes							
Administrative Template C							
User Rights Assignment Ch							
Windows Settings Changes							
Group Policy Preference c							
Other AD Object Changes							
Permission Changes +							
Configuration Auditing							
DNS Changes +							
AzureAD Password Protection							
Domain Object Changes							
LAPS Audit							

- 4. Haga clic en el cambio reportado.
- 5. Vea el ajuste del GPO modificado (como se muestra en la Figura 3)

Log360 Cloud				Showing GF	O Changes of def	ault domain policy					:	< l		License 🔒	?- 0-
Home Reports Gos				A Computer C	onfiguration/Policies/W	indows Settings/Security Set	tings/Account Policies/Pa	ssword Policy			(*)				
Devices Vindow	s Acti	we Directory	Unix/Linux Cis		-		-								
Search available reports	P			ChangeT	ype	Policy Name			Old value	New value					
User Logon Reports	•	Password F	Policy Changes	0 Mod	lified	Minimum password le	ngth		7 characters	3 characters				Expo	rt As 🔻 🔞
Local Logon-Logoff		Domain	testdomain.com									Period	2024-01-01 00:00:00 - 2024-0	1-05 23:59:59	
Account Management			(B. Incident											1.1.011	50 - 00
User Management	•	GPO Name	CC MARKED											Linked GPOs	
Group Management		default dom	ain policy											testdomain	
Computer Management															
OU Management															
GPO Management															
GPO Setting Changes				-											
Group Policy Setting Chan								Close							
Computer Configuration Ch															
User Configuration Change															
Password Policy Changes															
Account Lockout Policy Ch															
Security Settings Changes															
Administrative Template C															
User Rights Assignment Ch															
Windows Settings Changes															
Group Policy Preference c															
Other AD Object Changes	•														
Permission Changes	•														
Configuration Auditing	•														
DNS Changes	•														
AzureAD Password Protection	•														
Domain Object Changes	•														
LAPS Audit	•														
															P

Fig. 3: Cambios en el GPO de la política de dominio predeterminada

2. Auditar los usuarios creados recientemente

Un usuario, con los permisos de cuenta adecuados, puede realizar casi cualquier cambio en el entorno de AD.

PROBLEMA:

Considere un escenario en el que un intruso crea una nueva cuenta de usuario y añade este usuario a un grupo privilegiado. La creación de usuarios puede ser una parte de la secuencia de ataque que el atacante utiliza para navegar dentro de la red. Este usuario podría obtener acceso sin restricciones a datos sensibles, dependiendo del grupo al que haya sido añadido.

SOLUCIÓN:

Gestión de usuarios > Usuarios creados recientemente En Log360 Cloud (véase Figura 4):

- 1. Vaya a la pestaña **Informes**.
- 2. Vaya a **Dispositivos** en el menú desplegable y luego al menú **Active Directory**.
- 3. Vaya a Gestión de usuarios > Usuarios creados recientemente.
- 4. Vea los usuarios creados recientemente.



Fig. 4: Usuarios creados recientemente

3. Auditar los usuarios habilitados recientemente

Los actores maliciosos pueden intentar habilitar cuentas de usuario que han permanecido inactivas o deshabilitadas durante largos periodos de tiempo para evitar ser detectados. Los casos en los que la cuenta deshabilitada tiene privilegios administrativos pueden conducir a un escalamiento de privilegios, otorgando a los atacantes permisos elevados.

PROBLEMA:

Considere un caso en el que una cuenta de usuario deshabilitada ha sido habilitada y utilizada indebidamente por agentes maliciosos. Esto puede facilitar el movimiento lateral dentro de la red. Dado que las cuentas deshabilitadas atraen menos atención, volver a habilitar una puede ayudar al atacante a permanecer en la red sigilosamente. Auditar a los usuarios recientemente habilitados es especialmente importante cuando se realizan cambios en los privilegios de los usuarios. Las modificaciones repentinas en las cuentas de usuario, como habilitar el acceso administrativo, podrían indicar un incidente de seguridad o un intento de escalar privilegios.

SOLUCIÓN:

Gestión de usuarios > Usuarios habilitados recientemente En Log360 Cloud (véase Figura 5):

- 1. Vaya a la pestaña Informes.
- 2. Vaya a **Dispositivos** en el menú desplegable y luego al menú **Active Directory**.
- 3. Vaya a Gestión de usuarios > Usuarios habilitados recientemente.
- 4. Vea los usuarios habilitados recientemente.



Fig. 5: Usuarios habilitados recientemente

4. Auditar las unidades organizativas modificadas recientemente

Es crítico auditar los cambios en las unidades organizativas (OU) porque son un perímetro administrativo. Pueden contener usuarios, equipos, grupos y otras OU dentro de ellas. Los ajustes de la política se pueden aplicar a nivel de OU, vinculando un GPO a una OU. Cualquier modificación no autorizada, como añadir un usuario a una OU, puede suponer una amenaza para la postura de seguridad de la organización, ya que todos los ajustes que se aplican a la OU también se aplicarán a la OU recién añadida.

PROBLEMA:

Imagine que un atacante bloquea una OU específica para que no herede las políticas de seguridad que el administrador ha implementado, manipulando los ajustes de herencia de políticas de grupo de la OU. Esto significaría que los usuarios y equipos dentro de esa OU son vulnerables a actividades maliciosas.

SOLUCIÓN:

Gestión de OU > OU modificadas recientemente En Log360 Cloud (véase Figura 6):

- 1. Vaya a la pestaña Informes.
- 2. Vaya a **Dispositivos** en el menú desplegable y luego al menú **Active Directory**.
- 3. Vaya a Gestión de OU > OU modificadas recientemente.
- 4. Vea las OU modificadas recientemente.

Log360 Cloud																				License 🔔	?• @•
Home Reports Comp	liance	Search	Correlation	Alerts	Cloud Protect	on Settings	Support														
Devices Vindows	Ac	ive Directory	Unix/Linux	Cisco	SonicWall Fo	rtinet Juniper	Meraki	Sophos	PaloAlto	WatchGuard	Barracuda	Huawei	Arista	NetScreen	-						
	Q	Descetter																		Front As - D	E. Maria
User Logon Reports		Recently Mo	diffied OUs																	Export As + Eg	More
Local Logon-Logoff		Domain	All Domains		*	т											Period	2024-01-03	00:00:00 - 2024-01-1	3 23:59:59	iii i
Account Management		Miles Chara	had																		
User Management		who chan	Jeo																		
Group Management									-												
Computer Management								Chart	Summary												
OU Management	-							-								~					
Recently Created OUs								3													
Recently Deleted OUs								nut													
Recently Moved OUs								ů f													
Recently Modified OUs	l							1													
Renamed OUs																					
Extended Attribute Change								0			10										
DU History Recently Lindelated OLIX											administr										
GPO Management											UserNam	e									
GPO Setting Changes																					
Other AD Object Changes	ĺ.																				
Permission Changes	ĺ.		B Incident																	1,3013	50 - 100
Configuration Audition		OU Name	Modified Tim	e •	Who changed	Domain Controller	Message								Modified Attr	itutes Eve	ntid Ob	iect Class	Primary Domain	Remarks	
DNS Changer		oulev16	2024-01-05	06:31:07	administrator	win-7ug5okatosy	Organiza	tional Unit 'ou	lev16' was mor	dified by 'testdomai	n\administrator'.M	odified Propert	ies : 'apoptio	ns', Values	apoptions	513	6 ora	anizationaluni	testdomain.com	Write Property : on	sanizationalUn
AnumAD Paraword Protection	Ţ.					-	: T										t.			it	
Domain Object Changer	Č.	oulev12	2024-01-05	06:22:12	administrator	win-7ug5okatosv	Organiza	itional Unit 'ou	lev12' was moo	dified by 'testdomai	n\administrator'.M	odified Propert	ies : 'gpoptio	ns', Values	gpoptions	513	6 org	anizationaluni	testdomain.com	Write Property : or	ganizationalUn
LAPS Audit	ĺ.	oulev1	2024-01-05	06:22:02	administrator	win-7ug5okatosv	Organiza	tional Unit 'ou	lev1' was modi	fied by 'testdomain	\administrator'.Mo	dified Propertie	s : 'gpoption	s', Values :	gpoptions	513	5 org	anizationaluni	testdomain.com	Write Property : on	anizationalUn
Lou o Hudit							т										t			it	
																					e
																					- V

Fig. 6:Unidades organizativas modificadas recientemente

5. Auditar los nuevos miembros añadidos al grupo de seguridad de administradores de dominio

El grupo de administradores de dominio en AD se utiliza para asignar funciones administrativas a los usuarios del dominio. Por defecto, este grupo es miembro del grupo de administradores y, por tanto, lleva asociado un conjunto de privilegios.

Los miembros del grupo de administradores de dominio tienen acceso ilimitado a los recursos compartidos y a los objetos de AD.

PROBLEMA:

Consideremos un escenario en el que un actor malicioso añade un nuevo usuario al grupo de administradores de dominio. Esto proporcionaría al nuevo miembro acceso sin restricciones a los recursos compartidos y objetos de AD.

SOLUCIÓN:

Gestión de grupos > Miembros añadidos recientemente a un grupo de seguridad En Log360 Cloud (véase Figura 7):

- 1. Vaya a la pestaña Informes.
- 2. Vaya a **Dispositivos** en el menú desplegable y luego al menú **Active Directory**.
- 3. Vaya a Gestión de grupos > Miembros añadidos recientemente a un grupo de seguridad.
- 4. Vea las OU modificadas recientemente.



Log360 Cloud																			License 🔔	?- Ө-
Home Reports Co																				
Devices 🗸 Window	ws Ac	tive Directory	Unix/Linux	Cisco	SonicWall Fortine	Juniper	Meraki	Sophos	PaloAlto	WatchGuard	Barracuda	Huawei	Arista	NetScreen	-					
	Q																			
User Logon Reports		Recently Ac	dded Members	to Security	/ Groups													E	xport As 👻 👩	E: More
Local Logon-Logoff	•	Domain	All Domains		v т											Period 2	024-01-01 00:00:00	- 2024-01-13 23:5	9:59	#
Account Management																				
User Management		top Grou	ips Modined																	
Group Management	-																			
Recently Created Security								Chart	Summary											
Recently Created Distribu								2								~				
Recently Deleted Security																				
Recently Deleted Distribu								Ħ												
Recently Moved Groups								00 1 -												
Renamed Groups	1																			
Recently Modified Groups																				
Recently Added Members to								0												
Recently Added Members to											winish b.									
Recently Removed Members											80,									
Recently Removed Members											Groupnan	ne								
Decently Lindeleteri Groups																				
Group Object History																				
Computer Management	•		B, Incident																1 - 1 of 1	50 - III0
OU Management		Groupname	SID			Cal	ler User Name	Mem	iber Name		Modified Time	• D	omain Contro	ller Rer	marks		Domain	Group Scope	Caller Use	r Domain
GPO Management		administrato	rsgroup s-1-5	-21-14537270	47-977783198-12342435	47-8104 adr	ninistrator	cn=te	estuser,dc=testdi	omain,dc=com	2024-01-05 02:2	22:38 wi	in-7ug5okatos	w Aπ	nember was	added to a security-enabled global group	testdomain	global	testdomain	1
GPO Setting Changes																				
Other AD Object Changes																				
Dermission Changes																				
Configuration Audition																				
DNS Chapter																				
Annual Distantion																				
AzureAD Password Protection																				
Domain Object Changes	,																			
																				P

Fig. 7: Miembros añadidos recientemente a un grupo de seguridad

Acerca de log360 Cloud

ManageEngine Log360 Cloud, una solución SIEM unificada en la nube con funciones de CASB integradas, ayuda a las empresas a proteger su red de ataques cibernéticos. Con sus funciones de análisis de seguridad, inteligencia de amenazas y gestión de incidentes, Log360 Cloud ayuda a los analistas de seguridad a detectar, priorizar y resolver amenazas tanto en entornos on-premises como en la nube. La solución es altamente escalable y ayuda a reducir los costos de infraestructura y almacenamiento.

Para obtener más información sobre Log360 Cloud, visite www.manageengine.com/latam/cloud-logmanagement/

Registrarse gratis

R Demostración personalizada