ManageEngine Log360 Cloud

PROACTIVE ADMONITORING with Log360 Cloud

5 CRITICAL USE CASES

Enterprises rely on Active Directory (AD) because of its ability to manage and organize resources such as users, computers, and services in a centralized, secure manner. As a result, there is always the possibility that threat actors will target AD and make modifications and configuration changes to gain unauthorized access, leading to data breaches, service disruptions, and other security incidents. In this document, we will look at five critical use cases that IT administrators and security teams should consider when it comes to securing their AD environment.

1. Auditing GPO modifications

A group policy object (GPO) defines various settings for users and computer accounts inside an AD environment. Any unauthorized GPO change related to privileges, access to information or services, or security settings can lead to outages as well as security challenges. Auditing GPO modifications in AD is crucial because of the following reasons:

- **1.** Auditing critical policy changes like changes to account lockout policy and password change policy helps in detecting and responding to malicious activities instantly.
- 2. Monitoring any unauthorized change or modification to GPO security changes is crucial. Some modifications—like reducing the password complexity or length requirements, disabling Windows firewalls, or allowing remote desktop services on insecure networks—make the organization vulnerable to potential security breaches.
- **3.** Auditing GPOs is also crucial, as it is used to manage the policy settings for Windows Updates across organizational units. Monitoring these changes would ensure that these policies are configured properly, preventing any unapproved changes that may pose a threat to their security.

PROBLEM:

Imagine a scenario where a malicious actor gains unauthorized access to the AD environment and modifies GPO settings. The attacker might weaken password policies, disable critical security configurations, or grant unauthorized access to sensitive files.

Let's take the example of an attacker who wants to weaken the password policies so that they can have unauthorized access to the user accounts.

In a native AD environment, the password policy settings are configured through GPO settings, usually found in the Default Domain Policy.

<u></u>		Group Policy Manager	nent	_ 0 ×
Kile Action View Window Help				_ 8
🗢 🔿 🙎 🗊 💫 🖬 🗶 🧟 🗊				
	Group Policy Management Editor	_ 0	x	
File Action View Help	, , ,			
	2 🖬			
A IN Computer Configuration	Policy A Po	licy Setting		*
a 📔 Policies	Enforce password history 0 p	passwords remembered		
Software Settings	Maximum password age 42	days		
Mindows Settings	Minimum password age 0 c	lavs	10Notdelete	
Scripts (Startu	Minimum password length 5 c	haracters	estdeena	
🖌 🗟 Security Settin	Password must meet complexity requirements Dis	sabled		
🔺 🏭 Account P	ing store passwords using reversible encryption Dis	sabled		
Passwe	Minimum password length Properties	? X		
▶ 🧾 Accou II	inimitant passificita lenger roperaes			
p in Kerber	Security Policy Setting Explain			
b 🗿 Event Log	Minimum password length			
Restricted				
System Se	Define this policy setting			
▶ A Registry	Pressured as ut he at least:			
p A File System	A chamatan			
b ≦ Windows I				
Network L				
Wireless N				
Public Key				
b Software P				
gpo test 1				
II Gpo\$				
GPO_Hypnen				
GPO_Test23				
gpo1				
gpo10				
gpo11	OK Cancel	Apply		
apo12				
gpo14	WMI Hittering			
	This GPO is inked to the following twin inter.	M Onen		
C 00021	<pre>cnone></pre>	• Upen		
	📸 🔅 📧 🔤 🤉 🖾			ENG 15:35
	💗 👒 👺 💻 🗐 🕷 1			NS UNTL 06-01-2024

One of the settings associated with password policies is Minimum Password Length.

Fig. 1: Modifying the minimum password length property

The attacker might modify this configuration to weaken the password policy by reducing the minimum password length, thus increasing the vulnerability of user accounts.

SOLUTION:

GPO Setting Changes > Password Policy Changes

In Log360 Cloud (See Figure 2):

- 1. Go to the **Reports** tab.
- 2. Navigate to **Devices** in the dropdown, then the **Active Directory** menu.
- 3. Go to GPO Setting Changes > Password Policy Changes.

•	_	_	_	_		_		_	_	_	_	_	_			_	_		License	2-	A-
Log360 Cloud																					
Home Reports Co	mplance	Search	Correlation	Alerts	Cloud Protection	Settings	Support														
Devices 👻 Windo	ws A	tive Directory	Unix/Linux	Cisco	SonicWall Fortine	t Juniper	Meraki	Sophos	PakAlto	WatchGuard	Barracuda	Huawei	Arista	NetScreen	-						
	ρ	Descent																			
User Logon Reports	•	Password	Policy Changes																	pon va 🔹	69
Local Logon-Logoff	•	Domain	testdomain.com		~ т												Period	2024-01-01 00:00:00 - 2024-01-05	23:59:59		Ξ.
Account Management	•		E Incident																1 - 1 of 1	50 🕶	115
User Management	•	GPO Name			Modified Time 👻		Domain Com	troller		Who Modified			Summary						Linked GPOs		
Group Management		default don	ain policy		2024-01-05 02:18:07		win-7ug5oka	tosv		testdomainiad	ministrator		Added	(0) O M	fodified (1)	Removed (0)			testdomain		_
Computer Management																					
OU Management																					
GPO Management																					
GPO Setting Changes	-																				
Group Policy Setting Chan	1																				
Computer Configuration Ch	1																				
User Configuration Change																					
Password Policy Changes																					
Account Lockout Policy Ch																					
Security Settings Changes																					
Administrative Template C																					
Wodows 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

- 4. Click on the change reported.
- 5. View the changed GPO setting (as shown in Figure 3)

Log360 Cloud				Showing GPO Changes of	f default domain policy			×		Lice	150 🐥	?- (9 -
Home Reports				Computer Configuration/Poli	cies/Windows Settings/Security Settings/Account Policies	Password Policy		(*)					
Devices 🗸 W	rindows A	ctive Directory	Unix/Linux Cisco										
Search available reports	Q			ChangeType	Policy Name	Old value	New value						
User Logon Reports	•	Password	Policy Changes	Modified	Minimum password length	7 characters	3 characters				Expor	t As 🔻 🔞	
Local Logon-Logoff	•	Domain	testdomain.com					_	Period	2024-01-01 00:00:00 - 2024-01-05 23:59:59		i i i	
Account Management	•		Incident							1	- 1 of 1	50 - 0	
User Management	•	GPO Name	2						1000	Linked	GPOs		
Group Management	•	default dom	nain policy					- 1		testdor	nain		
Computer Management	•												
OU Management	•												
GPO Management	•												
GPO Setting Changes	•					Cince							
Group Policy Setting Chan						ciose							
Computer Configuration Ch													
User Configuration Change													
Password Policy Changes													
Account Lockout Policy Ch													
Security Settings Changes													
Administrative Template C													
User Rights Assignment Ch													
Crear Online Dedecements													
Other AD Object Changes													
Permission Changes	,												
Configuration Augisting	,												
DNS Changes													
AzureAD Password Protectio													
Domain Object Changes													
LAPS Audit	,												
Do 5 Mar													
													-
													Þ

Fig. 3: GPO Changes to default domain policy

2. Auditing recently created users

A user, with the right account permissions, can make almost any change to the AD environment.

PROBLEM:

Consider a scenario where an intruder creates a new user account and adds this user to a privileged group. User creation can be a part of the kill chain the attacker uses to navigate within the network. This user might gain unrestricted access to sensitive data, depending on the group they were added to.

SOLUTION:

User Management > Recently Created Users In Log360 Cloud (See Figure 4):

- 1. Go to the **Reports** tab.
- 2. Navigate to **Devices** in the dropdown, then the **Active Directory** menu.
- 3. Go to User Management > Recently Created Users.
- 4. View the recently created users.



Fig. 4: Recently Created Users

3. Auditing recently enabled users

Malicious actors may attempt to enable user accounts that have remained in the stale or disabled state for extended time periods to avoid detection. Instances where the disabled account has administrative privileges can lead to privilege escalation, granting the attackers elevated permissions.

PROBLEM:

Consider a case where a disabled user account has been enabled and misused by malicious agents. This can facilitate lateral movement within the network. Since disabled accounts attract less attention, re-enabling one may help an attacker maintain a stealthier presence in the network. Auditing recently enabled users is especially important when it comes to changes in user privileges. Sudden modifications to user accounts, such as enabling administrative access, could indicate a security incident or an attempt to escalate privileges.

SOLUTION:

User Management > Recently Enabled Users In Log360 Cloud (See Figure 5):

- 1. Go to the **Reports** tab.
- 2. Navigate to **Devices** in the dropdown, then the **Active Directory** menu.
- 3. Go to User Management > Recently Enabled Users.
- 4. View the recently enabled users.



Fig. 5: Recently Enabled Users

4. Auditing recently modified OUs

It is critical to audit changes to organizational units (OUs) because they are an administrative boundary. They can contain users, computers, groups, and other OUs within them. Policy settings may be applied at an OU level by linking a GPO to an OU. Any unauthorized modification such as adding a user to an OU can pose a threat to the organization's security posture, as all the settings applied to the OU will also be applicable to the newly added OU.

PROBLEM:

Imagine that an attacker blocks a specific OU from inheriting the security policies the admin has deployed by manipulating the Group Policy Inheritance settings of the OU. This would mean that the users and computers within that OU are vulnerable to malicious activity.

SOLUTION:

OU Management > Recently Modified OUs In Log360 Cloud (See Figure 6):

- 1. Go to the **Reports** tab.
- 2. Navigate to **Devices** in the dropdown, then the **Active Directory** menu.
- 3. Go to **OU Management > Recently Modified OUs.**
- 4. View the recently modified OUs.

Log360 Cloud																				License 🔒	?• `0 •
Home Reports	Complia	nce Se	arch Co	rrelation	Alerts	Cloud Protect	ion Settings	Support													
Devices 🗸	Windows	Active Dire	ctory Uni	o'Linux C	isco	SonicWall Fe	ortinet Juniper	Meraki	Sophos	PaloAlto	WatchGuard	Barracuda	Huawei	Arista	NetScreen	-					
		P																		Constitution - D	E. March
User Logon Reports		> Rece	nuy Modille	000s																Export As + E0	C More
Local Logon-Logoff		• Do	main All Do	mains		~	т										1	Period 2024-01-0	1 00:00:00 - 2024-01-1	3 23:59:59	iii
Account Management		•	Mho Channed																		
User Management		÷	into citangea																		
Group Management		•							Chart	Summan											
Computer Management		•							d -	Summary											
OU Management		-															\sim				
Recently Created OUs									3 -												
Recently Deleted OUs									tun 2												
Recently Moved OUs									0 1												
Recently Modified OUs									1 -												
Renamed OUs									0												
Ol History	e											all a									
Recently Undeleted OUs												adminu									
GPO Management		•										🔵 UserNan	ie								
GPO Setting Changes		•																			
Other AD Object Changes	5																				
Permission Changes		•	1 = 8	Incident																1 - 3 of 3	50 - 10
Configuration Auditing		, ou	Name	Iodified Time			Domain Controller	Message	•								ibutes EventId	Object Class	Primary Domain	Remarks	
DNS Changes		• oule	w16 2	024-01-05 06:3	1:07	administrator	win-7ug5okatosv	Organiza	ational Unit 'o	ulev16' was mo	dified by 'testdoma	in\administrator'.N	odified Proper	ies : 'gpoptio	ns', Values	gpoptions	5136	organizationaluni t	testdomain.com	Write Property : orga it	anizationalUn
AzureAD Password Protec	ction	* oule	rv12 2	024-01-05 06:2	2:12	administrator	win-7ug5okatosv	Organiza	ational Unit 'o	ulev12' was mo	dified by 'testdoma	in\administrator'.N	odified Proper	ies : 'gpoptio	ns', Values	gpoptions	5136	organizationaluni	testdomain.com	Write Property : org	anizationalUn
Domain Object Changes		<u>۲</u>						: T										t		it	
LAPS Audit		• oute	w1 2	024-01-05 06:2	2:02	administrator	win-7ug5okatosv	Organiza '1'	ational Unit 'o	ulev1' was mod	ified by 'testdomain	\administrator'.Mo	dified Properti	s : 'gpoption	s', Values :	gpoptions	5136	organizationaluni t	testdomain.com	Write Property : orgi it	anizationalUn

Fig. 6: Recently Modified OUs

5. Auditing new members added to the Domain Admins security group

The Domain Admins group in AD is used to assign administrative roles to users in the domain. By default, this group is a member of the Administrators group and therefore carries a set of privileges associated with it.

Members of the Domain Admins group have unrestricted access to shared resources and AD objects.

PROBLEM:

Consider a scenario where a malicious actor adds a new user to the Domain Admins group. This would provide the new member with unrestricted access to shared resources and AD objects.

SOLUTION:

Group management > Recently Added Members to Security Groups In Log360 Cloud (See Figure 7):

- 1. Go to the **Reports** tab.
- 2. Navigate to **Devices** in the dropdown, then the **Active Directory** menu.
- 3. Go to Group Management > Recently added Members to Security Groups.
- 4. View the recently modified OUs.



Log360 Cloud																			License 🔔	?- 🛛 -
Home Reports Com																				
Devices 🗸 Window	ns Ac	tive Directory	Unix/Linux	Cisco	SonicWall Fortinet	Juniper	Meraki	Sophos	PaloAlto	WatchGuard	Barracuda	Huawei	Arista	NetScreen	•					
	Q																			
User Logon Reports	•	Recently Ac	Ided Member	s to Securit	y Groups													E	xport As 👻 🕞	E: More
Local Logon-Logoff	•	Domain	All Domains		~ т											Period 20	24-01-01 00:00:00	- 2024-01-13 23:5):59	Ê
Account Management	•																			
User Management		Top Grou	ps Modified																	
Group Management	-																			
Recently Created Security							-	Chart	Summary											
Recently Created Distribu								2								~				
Recently Deleted Security																				
Recently Deleted Distribu								ti I												
Recently Moved Groups								00 1												
Renamed Groups	1																			
Recently Modified Groups																				
Recently Added Members to								0			~									
Recently Added Members to											diministic.									
Pecently Removed Members											· ·									
Extended Attribute Change											Groupnam	le								
Recently Undeleted Groups																				
Group Object History																				
Computer Management	•		B, Incident			_	_	_		_			_	_	_				1 - 1 of 1	50 - 10
OU Management		Groupname	SID			Caller U	lser Name	Membr	er Name		Modified Time	- D	omain Contro	ller Rer	narks		Domain	Group Scope	Caller User	Domain
GPO Management		administrato	rsgroup s-1-5	-21-14537270	047-977783198-1234243547-81	14 adminis	trator	cn=tes	stuser,dc=testdom	ain,dc=com	2024-01-05 02:2	2:38 w	in-7ug5okatos	av Am	ember was	s added to a security-enabled global group.	testdomain	global	testdomain	
GPO Setting Changes	•																			
Other AD Object Changes	•																			
Permission Changes	•																			
Configuration Auditing	•																			
DNS Changes	•																			
AzureAD Password Protection																				
Domain Object Changes	,																			

Fig. 7: Recently Added Members to Security Groups

About Log360 Cloud

ManageEngine Log360 Cloud, a unified cloud SIEM solution with integrated CASB capabilities, helps enterprises secure their network from cyberattacks. With its security analytics, threat intelligence, and incident management capabilities, Log360 Cloud helps security analysts spot, prioritize, and resolve threats in both on-premises and cloud environments. The solution is highly scalable and helps drive down infrastructure and storage costs.

For more information about Log360 Cloud, visit www.manageengine.com/cloud-siem/.

Sign up for free

Q Personalized Demo