Active Directory Auditing Tool

https://www.manageengine.com/products/active-directory-audit/account-management-events/event-id-4729.html

Event ID 4729 - A member was removed from a security-enabled global group

Event ID	4729
Category	Account management
Sub category	Security group management
Description	A member was removed from a security-enabled global group

When Active Directory objects such as an user/group/computer is removed from a security group, event ID 4729 gets logged.

This log data gives the following information:

Subject: User who performed the action	Security ID Account Name Account Domain Logon ID
Member: Object removed from the security group	Security ID Account Name
Group: Security group from which the object was removed	Security ID Group Name Group Domain
Additional Information	Privileges

Why event ID 4729 needs to be monitored?

- Prevention of privilege abuse
- Detection of potential malicious activity
- Operational purposes like getting information on user activity like user attendance, peak logon times, etc.
- Compliance mandates

Pro tip:

ADAudit Plus audits, reports, and alerts group management actions performed on distribution and security groups making Active Directory auditing much easier.

Event 4729 applies to the following operating systems:

- Windows Server 2008 R2 and Windows 7
- Windows Server 2012 R2 and Windows 8.1
- Windows Server 2016 and Windows 10

Corresponding event ID for 4729 in Windows Server 2003 and older is 633

Revision #1
Created 5 January 2024 05:04:17 by ColtM
Updated 13 June 2024 01:28:01 by ColtM