SCRIPT #07 · CYBER SECURITY

Audit dei membri del gruppo Domain Admins

Elenca i membri attuali di Domain Admins, confrontandoli con un elenco di riferimento atteso.

AUTORE	COPYRIGHT	PREREQUISITI
Francesco Larossa	© 2026 SysAdmin Italia	Modulo ActiveDirectory

Cosa fa questo script

Lo script recupera i membri attuali del gruppo Domain Admins e li confronta con un elenco di riferimento (definito manualmente nello script o passato come file), segnalando in rosso eventuali membri non previsti e in giallo membri previsti ma non piu presenti.

Come si usa

Definisci l'elenco atteso dei membri (o passalo tramite file), poi esegui lo script per il confronto.

```
.\Audit-DomainAdmins.ps1 -ElencoAtteso "C:\Dati\domain_admins_attesi.txt"
```

In quale contesto usarlo

Domain Admins e il gruppo con i privilegi piu elevati di tutto il dominio: qualsiasi aggiunta non pianificata merita un'indagine immediata. Schedulare questo controllo quotidianamente, con notifica automatica in caso di discrepanza, e una delle misure di sicurezza a piu alto rapporto valore/sforzo disponibili.

Codice completo

Il codice è lo stesso del file Audit-DomainAdmins-1.ps1: per usarlo scarica il file dalla pagina invece di copiarlo da questo PDF.

```
<#
.SYNOPSIS
    Elenca i membri attuali di Domain Admins, confrontandoli con un elenco di riferimento atteso.
#>
param(
    [Parameter(Mandatory=$true)]
    [string]$ElencoAtteso
)

Import-Module ActiveDirectory

$membriAttuali = (Get-ADGroupMember -Identity "Domain Admins" -Recursive).SamAccountName
$membriAttesi = Get-Content -Path $ElencoAtteso

$nonPrevisti = $membriAttuali | Where-Object { $_ -notin $membriAttesi }
$mancanti = $membriAttesi | Where-Object { $_ -notin $membriAttuali }

Write-Host "=== Membri attuali di Domain Admins: $($membriAttuali.Count) ===" -ForegroundColor Cyan
```

```
$membriAttuali | ForEach-Object { Write-Host "  - $_" -ForegroundColor Gray }

if ($nonPrevisti) {
    Write-Host "`n[ATTENZIONE] Membri NON previsti nell'elenco di riferimento:" -ForegroundColor Red
    $nonPrevisti | ForEach-Object { Write-Host "  ! $_" -ForegroundColor Red }
}
if ($mancanti) {
    Write-Host "`n[INFO] Membri attesi ma non piu presenti:" -ForegroundColor Yellow
    $mancanti | ForEach-Object { Write-Host "  - $_" -ForegroundColor Yellow }
}
if (-not $nonPrevisti -and -not $mancanti) {
    Write-Host "`nNessuna discrepanza rilevata." -ForegroundColor Green
}
```