SCRIPT #16 · CYBER SECURITY

Log eventi di sicurezza critici

Estrae dal log di sicurezza gli eventi corrispondenti a Event ID considerati critici per un audit.

AUTORE	COPYRIGHT	PREREQUISITI
Francesco Larossa	© 2026 SysAdmin Italia	Permessi di lettura sul log di sicurezza

Cosa fa questo script

Lo script interroga il log di sicurezza filtrando su un elenco di Event ID considerati particolarmente rilevanti per un audit di sicurezza: creazione utenti, modifiche a gruppi privilegiati, cancellazione dei log di audit, e altri eventi sensibili, producendo un report consolidato.

Come si usa

Esegui lo script specificando quante ore indietro analizzare. L'elenco di Event ID monitorati e personalizzabile modificando l'array all'interno dello script.

```
.\Audit-EventiSicurezzaCritici.ps1 -OreIndietro 24
```

In quale contesto usarlo

Pensato per essere eseguito quotidianamente, magari con invio automatico del report via email al team di sicurezza: raccoglie in un unico posto eventi che, sparsi nel log generale, sarebbero facilmente persi tra migliaia di voci meno rilevanti generate ogni giorno da un sistema in normale funzionamento.

Codice completo

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

```
<#
.SYNOPSIS
    Estrae dal log di sicurezza gli eventi corrispondenti a Event ID considerati critici per un audit.
#>
param(
    [int]$OreIndietro = 24,
    [string]$PercorsoCSV = "C:\Report\EventiSicurezzaCritici.csv"
)

# Event ID monitorati: 4720=creazione utente, 4726=eliminazione utente,
# 4728/4732/4756=aggiunta membro a gruppo privilegiato, 1102=log di audit cancellato,
# 4740=account bloccato, 4767=account sbloccato
$eventIdCritici = @(4720, 4726, 4728, 4732, 4756, 1102, 4740, 4767)

$dataLimite = (Get-Date).AddHours(-$OreIndietro)

$eventi = Get-WinEvent -FilterHashtable @{LogName='Security'; Id=$eventIdCritici; StartTime=$dataLimite} `
    -ErrorAction SilentlyContinue

$risultati = $eventi | Select-Object TimeCreated, Id,
```

```
    @{N="Descrizione";E={$_.Message.Split("`n")[0]}}

$risultati | Export-Csv -Path $PercorsoCSV -NoTypeInformation -Encoding UTF8 -Delimiter ";"
Write-Host "Trovati $($risultati.Count) eventi critici nelle ultime $OreIndietro ore." -ForegroundColor $(if($risultati.Count `
    -gt 0){"Yellow"}else{"Green"})
```