SCRIPT #04 · CYBER SECURITY

# Stato Windows Defender su piu endpoint

Verifica lo stato di protezione Defender su un elenco di computer remoti.

| AUTORE | COPYRIGHT | PREREQUISITI |
| --- | --- | --- |
| Francesco Larossa | © 2026 SysAdmin Italia | PowerShell Remoting abilitato sui computer target |

## Cosa fa questo script

Lo script si collega a un elenco di computer e recupera lo stato di Windows Defender su ciascuno: protezione in tempo reale attiva, data ultimo aggiornamento firme, e stato generale dei servizi.

## Come si usa

Prepara un file di testo con un computer per riga, poi esegui lo script indicandone il percorso.

```
.\Verifica-DefenderMultiplo.ps1 -ListaComputer "C:\Dati\computer.txt"
```

## In quale contesto usarlo

Controllo di base ma essenziale per assicurarsi che la protezione antivirus sia realmente attiva su tutti gli endpoint, non solo installata: un servizio disabilitato per errore, o firme non aggiornate da settimane, sono scenari piu comuni di quanto si pensi in ambienti con molti dispositivi.

## Codice completo

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

```
<#
.SYNOPSIS
    Verifica lo stato di protezione Windows Defender su un elenco di computer remoti.
#>
param(
    [Parameter(Mandatory=$true)]
    [string]$ListaComputer,
    [string]$PercorsoCSV = "C:\Report\StatoDefender.csv"
)

$computer = Get-Content -Path $ListaComputer

$risultati = foreach ($pc in $computer) {
    try {
        $stato = Invoke-Command -ComputerName $pc -ScriptBlock {
            Get-MpComputerStatus | Select-Object RealTimeProtectionEnabled, AntivirusSignatureLastUpdated, AntivirusEnabled
        } -ErrorAction Stop

        [PSCustomObject]@{
            Computer              = $pc
            ProtezioneRealTime    = $stato.RealTimeProtectionEnabled
            AntivirusAttivo       = $stato.AntivirusEnabled
            UltimoAggiornamento   = $stato.AntivirusSignatureLastUpdated
            Stato                 = "OK"
```

```
        }
    }
    catch {
        [PSCustomObject]@{
            Computer            = $pc
            ProtezioneRealTime  = "N/D"
            AntivirusAttivo     = "N/D"
            UltimoAggiornamento = "N/D"
            Stato               = "NON RAGGIUNGIBILE: $_"
        }
    }
}

$risultati | Export-Csv -Path $PercorsoCSV -NoTypeInformation -Encoding UTF8 -Delimiter ";"
$problemi = ($risultati | Where-Object {$_.ProtezioneRealTime -ne $true}).Count
Write-Host "Controllati $($computer.Count) computer. Con protezione non attiva: $problemi" -ForegroundColor $(if($problemi `
    -gt 0){"Red"}else{"Green"})
```