## Windows Server

## Ghost (Cring) Ransomware

## Security Compliance Plan

### Patch Management and Vulnerability Remediation

Objective: Ensure patching of Common Vulnerabilities and Exposures (CVE): CVE-2018-13379, CVE-2010-2861, CVE-2009-3960, CVE-202134473, CVE-2021-34523, CVE-2021-31207.

* Use SolarWinds Patch Manager to monitor missing patches and apply updates.
* Manually check and apply critical security updates if SolarWinds lacks coverage.
* Use PowerShell to verify patch status:

Get-HotFix | Where-Object { $PSItem.HotFixID -match "KB" } # Replace KB with specific ID

### Access Control

Objective: Prevent unauthorized access through privilege escalation and credential misuse.

* Limit remote access to authorized users only.
* Use PowerShell to list local admins and check unauthorized accounts:

Get-LocalGroupMember -Group "Administrators"

### PowerShell Hardening and Logging

Objective: Detect and prevent abuse of PowerShell for ransomware execution.

* Enable PowerShell Script Block Logging (Logs viewable in EventViewer) via GPO:

Computer Configuration > Administrative Templates > Windows PowerShell > Enable Logging

* Monitor logs for suspicious commands:

Get-WinEvent -LogName "Microsoft-Windows-PowerShell/Operational" | Select-Object -First 10

* Enable **PowerShell Transcription** (Logs written to file) via the Registry:

**EXAMPLE**  
$regPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription"

# Create the registry path if it doesn't exist

if (-not (Test-Path $regPath)) {

New-Item -Path $regPath -Force

}

# Enable PowerShell Transcription

Set-ItemProperty -Path $regPath -Name "EnableTranscripting" -Value 1 -Type DWord

# Set the output directory for logs

$logPath = "C:\PowerShellLogs"

Set-ItemProperty -Path $regPath -Name "OutputDirectory" -Value $logPath -Type String

Write-Output "PowerShell Transcription enabled. Logs will be stored in $logPath"

### Network Security and Segmentation

Objective: Restrict lateral movement and minimize attack surface.

* Disable SMBv1:

Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force

* Restrict unnecessary ports using Windows Firewall.
* Monitor network traffic using SolarWinds NetFlow.

### Application Control and Execution Prevention

Objective: Prevent unauthorized execution of ransomware binaries.

* Implement AppLocker or Software Restriction Policies (SRP) to allowlist trusted applications.
* Use PowerShell to list running processes for suspicious executables:

Get-Process | Where-Object { $PSItem.Path -match "Temp|AppData" }

### Incident Detection and Response

Objective: Identify and respond to suspicious activity.

* Use SolarWinds Security Event Manager for real-time alerts on failed logins, privilege escalation, and lateral movement.
* Use PowerShell to detect failed login attempts:

Get-EventLog -LogName Security -InstanceId 4625 -Newest 10

### Backup and Recovery

Objective: Ensure ransomware resilience by maintaining secure backups.

* Coordinate with Storage Admins to confirm backup health status.
* Verify backups regularly.