1. Suspicious PowerShell Execution

process_name:powershell.exe AND (cmdline:Invoke OR cmdline:-e OR cmdline:-enc OR cmdline:DownloadString)

2. Command Prompt Suspicious Activity

process_name:cmd.exe AND (cmdline:/c OR cmdline:/k)

3. Unsigned Processes Executed from User Folders

process_name:* AND filemod_path:c:\users** AND NOT signed:true

4. Processes Connecting to Known Malicious IPs

netconn_ipv4:192.168.* OR netconn_ipv6:*:: OR netconn_port:4444

5. Unusual Parent-Child Process Relationships

parent_name:explorer.exe AND (process_name:cmd.exe OR process_name:powershell.exe OR process_name:wmic.exe OR process_name:mshta.exe)

6. Scheduled Task Creation

process_name:schtasks.exe AND (cmdline:create OR cmdline:/create)

7. Registry Key Modifications for Persistence

regmod_name:*\\Software\\Microsoft\\Windows\\CurrentVersion\\Run*

8. RDP Connections (Remote Desktop Protocol)

netconn_port:3389

9. Suspicious WMI Activity

process_name:wmic.exe AND (cmdline:process OR cmdline:/node OR cmdline:/format)

10. Mimikatz Process Execution

process_name:mimikatz.exe OR process_name:sekurlsa.exe OR cmdline:mimikatz

11. Suspicious Remote Tools

process_name:* (dns_request:*teamviewer.com OR dns_request:*anydesk.com OR dns_request:*logmein.com OR dns_request:*splashtop.com)

12. Binary Execution from Temp Directory

process_name:*.exe AND filemod_path:c:\users*\AppData\Local\Temp*

13. MSHTA Execution (JavaScript/VBScript)

process_name:mshta.exe

14. Processes Executing with Escalated Privileges

process_name:* AND (cmdline:* -nopr OR cmdline:* -nop OR cmdline:* bypass)

15. Suspicious Network Connections to External IPs

netconn_ipv4 NOT (netconn_ipv4:10.* OR netconn_ipv4:172.16.* OR netconn_ipv4:192.168.*)

16. Abnormal Script Execution

process_name:wscript.exe OR process_name:cscript.exe OR process_name:*.bat OR process_name:*.vbs OR process_name:*.js

17. Suspicious Use of BITSAdmin

process_name:bitsadmin.exe AND (cmdline:addfile OR cmdline:transfer)

18. File Deletion by Process

filemod_name:* AND filemod_action:DELETE

19. Common Lateral Movement Techniques

process_name:psexec.exe OR process_name:smbexec.exe OR process_name:wmiexec.exe

20. Suspicious Application Execution via LOLBins

process_name:regsvr32.exe OR process_name:msbuild.exe OR process_name:schtasks.exe OR process_name:msiexec.exe