Hands-On

Forwarding logs via Sysmon & Winkogbeat:

- Go to Security Onion Terminal.
- Type sudo so-allow
- Select Logtash Beat
- Type windows server IP & press enter.

Installing Sysmon:

- [ ] Go to windows server and Download Sysmon from microsoft.

Link: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Or https://download.sysinternals.com/files/Sysmon.zip

Then for the configuration Please follow this git.

Link: https://github.com/SwiftOnSecurity/sysmon-config

- [ ] Go Powershell of your windows server &
- Go to the directory where you download sysmon
- You can command .\Sysmon64.exe --help for instruction
- Type .\sysmon64.exe -i .\sysmonconfig-export.xml and press enter.

Here we install sysmon.

Installing winlogbeat:

- Go to Security Onion Console from the windows server.
- Then Downloads
- And download Winlogbeat.
- Then install the winlogbeat on your windows server.
- Create a file with winlogbeat.yml on your windows server.
- Go to the Link: https://github.com/elastic/beats/blob/main/winlogbeat/winlogbeat.yml
- Copy the raw code from this git and paste it on winlogbeat.yml file.
- Modify where you need. Such as go to logtrash portion and remove the comment sign '#' from 1st and 3rd lines. And set the local host or your server IP.

- Copy the winlogbeat.yml file then Go to Local disk(c)>ProgramData>Elastic>Beats>winlogbeat and past here.
- Open the services menu which you can search from the search bar.
- Look for the Elastic Winlogbeat-Oss, Press that, and then press start

Here We install winlogbeat.

Visualization or Monitoring:

- Go to Security Onion Console from the windows server.
- And then goto hunt.
- There You found sysmon
- And there also found you all windows logs.