Please perform the following steps to capture the requested data:

1. Please ensure that the Sensor is in Active state.
2. Create a "temp" folder under C:\
3. Please document exact steps taken to reproduce the issue in the case notes, along with the Time Stamp capture (example is included at the bottom of this document).
4. Please ensure that the following files have been downloaded:
	1. Cbc-sensor-capture.ps1
	2. ProcmonLowAlt.zip (extract the contents of the archive)
5. Download and install the Procmon SDK installer:
	1. <https://developer.microsoft.com/en-us/windows/downloads/windows-10-sdk>
6. Copy cbc-sensor-capture.ps1, ProcmonLowAlt.exe and winsdksetup.exe to C:\temp
7. Open Command Prompt using the "Run As Administrator" option, Change Directory to C:\temp
8. Run the following command to reset sensor counters and retain PSC events:

Powershell -ExecutionPolicy bypass -f cbc-sensor-capture.ps1 keepevents
	1. When the "Enter the uninstall code to unlock restricted RepCLI commands.:" prompt is presented, enter the uninstall code.
	2. When "Hit enter to stop trace and collect logs.:" presents, start to reproduce the behavior.
	3. Note local machine time when testing started, and timezone of machine.
	4. Note local time when issue occurred.
	5. Once behavior is fully reproduced, press Enter to exit the capture.
9. Run the following command to start wpr trace (Collect data approximately for 4 minutes while the issue reproduces).

Powershell -ExecutionPolicy bypass -f c:\temp\cbc-sensor-capture.ps1 minifilter

(perform the above listed steps from "b to e", and add this entry "wpr-active-hostname-" in the file name, so the file name should look like "wpr-active-hostname-YYYYDDMMHHMMSS.zip")
10. Run the following command to start procmon capture: (Collect data approximately for 4 minutes while the issue reproduces:

powershell -executionpolicy bypass -f c:\temp\cbc-sensor-capture.ps1 procmon

(perform the above listed steps from "b to e", and add this entry "procmon-active-hostname-" in the file name, so the file name should look like "procmon-active-hostname-YYYYDDMMHHMMSS.zip")
11. Now place the Sensor is in Bypass state". (Collect data approximately for 4 minutes while the issue reproduces)
12. Run the following command to capture WPR with the issue reproduced in Sensor Bypass State:

powershell -ExecutionPolicy bypass -f c:\temp\cbc-sensor-capture.ps1 minifilter bypass

(perform the above listed steps from "b to e", and add this entry "wpr-bypass-hostname-" in the file name, so the file name should look like "wpr-bypass-hostname-YYYYDDMMHHMMSS.zip")
13. Run the following command to capture procmon with the issue reproduced in Sensor Bypass State: (Collect data approximately for 4 minutes while the issue reproduces)

powershell -executionpolicy bypass -f c:\temp\cbc-sensor-capture.ps1 procmon bypass

(perform the above listed steps from "b to e", and add this entry "procmon-bypass-hostname-" in the file name, so the file name should look like "procmon-bypass-hostname-YYYYDDMMHHMMSS.zip")

Additional Notes:

Example of Time stamp capture:

Time stamp for reset counters: 10:19 AM PST

Time stamp for WPR trace with Sensor active: 10:29 AM PST

Time stamp for Procmon capture with Sensor active: 10:50 AM PST

Time stamp for WPR trace with Sensor bypass: 11:03 AM PST

Time stamp for Procmon capture with Sensor bypass: 11:14 AM PST