



GUIDE

Monitoring Windows Processes with Procmon

v1.0.0

Author:

Eldon Gabriel

August 29, 2025

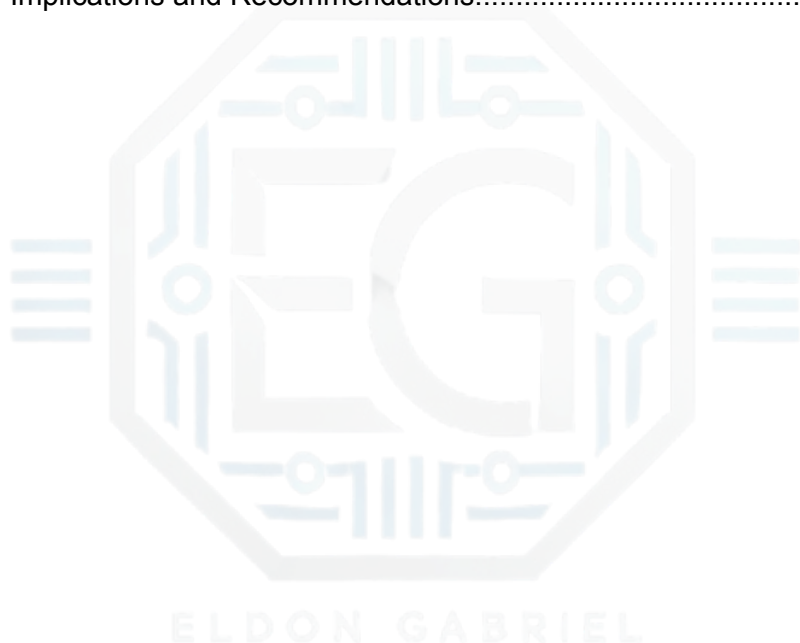
This guide is based on my independent practice and understanding of Windows process monitoring using Procmon, intended for portfolio demonstration.



Cybersecurity Professional | IT Security Consultant

TABLE OF CONTENTS


REVISION HISTORY	2
1.0 SECURING FOLDERS WITH ACCESS PERMISSIONS	3
1.1 Project Description	3
1.2 Capture Procmon Events	3
1.3 Apply Filters for Specific Processes	3
1.4 Review Registry Activity for a Selected Process	4
1.5 Filter Out File Read Events	4
1.6 Save Events to CSV	4
2.0 TESTING AND VERIFICATION	5
2.1 Key Takeaways	5
2.2 Security Implications and Recommendations	5





Cybersecurity Professional | IT Security Consultant

REVISION HISTORY

Version	Date	 Author	Description of Changes
v1.0.0	08/29/2025	Eldon G.	Initial draft.





1.0 SECURING FOLDERS WITH ACCESS PERMISSIONS

1.1 Project Description

This guide provides a step-by-step walkthrough for using Process Monitor (Procmon) on Windows to capture and analyze process activity.

1.2 Capture Procmon Events

- Launch Procmon as Administrator.
 - Allow Procmon to capture activity for a few minutes.
 - Stop capture with **Ctrl+E**.
-

1.3 Apply Filters for Specific Processes

- Go to **Filter > Filter...**
- Add:

Process Name is [Target Process] → Include

Process Name is [Another Target Process] → Include



Generate visible activity in monitored processes:

For any command-line tool, script, or application:

- Perform basic system or application actions.
 - Open programs or tools.
 - Run simple commands or scripts.
 - Interact with applications or services using normal workflows.
 - Stop capture with **Ctrl+E**.
-

1.4 Review Registry Activity for a Selected Process

- Clear filters (**Ctrl+Shift+C**).
 - Add filter: **Process Name is [Target Process]** → Include.
 - Open a File Explorer window (e.g., C:) and monitor registry-related events such as keys being opened or values being checked.
-

1.5 Filter Out File Read Events

- Add filter: **Operation is [Unnecessary Operation]** → Exclude.
 - This reduces noise in the log and keeps the view focused.
-

1.6 Save Events to CSV

- Go to **File > Save...**
 - Choose **CSV format**.
 - Save all or displayed events as **[Filename].csv**.
-



2.0 TESTING AND VERIFICATION

2.1 Key Takeaways

- Procmon shows live details of what processes are doing on the system.
 - Filters allow you to focus on the activity of specific processes.
 - Excluding heavy, repetitive operations such as file reads makes the data easier to analyze.
 - Exporting logs to CSV keeps a permanent copy of the events for later review.
-

2.2 Security Implications and Recommendations

- Watching how processes interact with files and the registry can reveal unusual or unwanted behavior.
 - Investigators and defenders can rely on Procmon during incident response to trace suspicious activity across a Windows endpoint.
-