



# **GUIDE**

# **Monitoring Windows**

# **Processes with Procmon**

*v1.0.1*

Author:

**Eldon Gabriel**

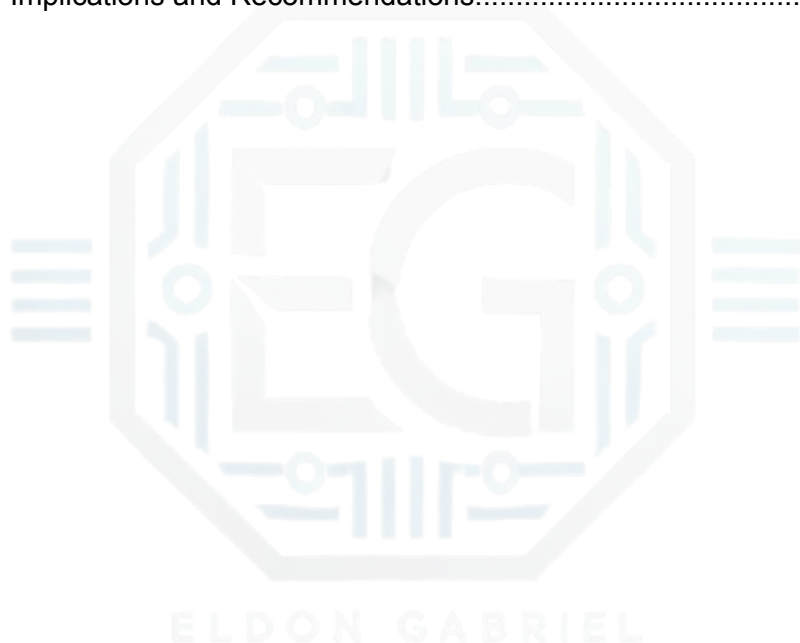
September 1, 2025



Cybersecurity Professional | IT Security Consultant

## TABLE OF CONTENTS


<b>REVISION HISTORY</b>	<b>2</b>
<b>1.0 SECURING FOLDERS WITH ACCESS PERMISSIONS</b>	<b>3</b>
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
<b>2.0 TESTING AND VERIFICATION</b>	<b>5</b>
2.1 Key Takeawys	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.
v1.0.1	09/01/2025	Eldon G.	Updated security implications and recommendations; refined Procmon steps for clarity





Cybersecurity Professional | IT Security Consultant

## 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.



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



## 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

#### Potential Risks Identified

- Unauthorized or unexpected access to sensitive folders or registry keys.
- Processes performing actions beyond their intended scope.

#### Recommendations

- Check folder and file permissions to ensure least-privilege access.
- Monitor critical processes for abnormal behavior using Procmon or similar tools.
- Regularly audit logs to detect suspicious activity.
- Apply security best practices such as role-based access control (RBAC) and account segregation.

#### Compliance Mapping

- Aligns with **NIST SP 800-53** control families (Audit and Accountability, Access Control).
- Supports **ISO 27001** practices for access management and activity monitoring.
- Helps satisfy **PCI-DSS** requirements for logging and monitoring access to sensitive data.