**List Of Datasets Selected For RnD**

**(To be Confirmed by Sir)**

1. AWSCTD (Attack-Caused Windows OS System Calls Traces Dataset)

Focus: Windows system call traces triggered by various attacks.

Data Type: System calls captured during attack and normal scenarios.

Use Case: Ideal for HIDS research based on system call analysis.

Year: 2018.

Link: <https://link.springer.com/chapter/10.1007/978-3-031-35190-7_6>

2. ISOT Cloud Intrusion Detection Dataset (ISOT CID)

Focus: Cloud-based intrusion detection with Windows logs.

Data Type: System logs, performance metrics (CPU usage), system calls.

Use Case: Can be used for Windows HIDS in virtualized environments.

Size: 8TB+ of real cloud data.

Link: <https://github.com/gfek/Real-CyberSecurity-Datasets>

3. COMIDDS (Comprehensive Overview of Datasets for Intrusion Detection Systems)

Focus: Repository listing various HIDS/NIDS datasets, including Windows-based ones.

Data Type: Multiple datasets covering logs, system calls, behavioral data.

Use Case: Great for finding more datasets tailored to HIDS research.

Link: <https://github.com/fkie-cad/COMIDDS>

4. OSSEC (Open Source HIDS SECurity - Self-Generated Data)

Focus: Open-source HIDS capable of monitoring Windows logs and registry changes.

Data Type: Self-generated logs from real-world system activity.

Use Case: Not a pre-made dataset, but useful for creating your own Windows HIDS dataset.

Link: <https://www.ossec.net/>