Local System Threat Analyzer

Generated on 2025-04-29 14:06:08

Introduction

The Local System Threat Analyzer is a Python-based tool designed to monitor system processes and identify potentially malicious or resource-intensive activity. It utilizes psutil to inspect process details and flags suspicious behavior based on heuristics such as high CPU/memory usage, missing execution paths, and user-defined signatures.

Local System Threat Analyzer

Generated on 2025-04-29 14:06:08

Features

- Real-time and one-time scanning modes

- Suspicious behavior detection using process attributes

- CSV logging for detailed analysis

- CLI interface with tabulated output

- Easy conversion into a standalone executable

Local System Threat Analyzer

Generated on 2025-04-29 14:06:08

System Architecture

The tool is structured around three primary components:

1. process_monitor.py - Handles process enumeration and scanning logic

2. main.py - User interface and menu system for initiating scans

3. Log Writer - Writes output to timestamped CSV files for later review

Additional modules may include malware signature scanning and API-based validation.

Local System Threat Analyzer

Generated on 2025-04-29 14:06:08

Implementation Details

The tool relies heavily on the psutil library to retrieve system process details, while tabulate is used for user-friendly CLI output formatting. Suspicious processes are logged with PID, name, CPU%, memory usage, and file path into a timestamped CSV file.

Future enhancements include signature-based detection using hash comparisons and integration with online services such as VirusTotal for real-time reputation checks.

Local System Threat Analyzer

Generated on 2025-04-29 14:06:08

Future Improvements

- Integrate VirusTotal or other reputation APIs

- Add GUI with PyQt or Tkinter

- Enable persistent monitoring as a background service

- Export logs to remote storage or SIEM tools