Carnegie Mellon University
Software Engineering Institute

CONFIGURATION FILE OVERVIEW

Silent Sentinel Development Team

22 April 2025

Silent Sentinel Configuration File Format

The Silent Sentinel configuration file contains a JSON object that can be modified before running Silent Sentinel with the `-c` option. Each section heading below is a key in the configuration file.

Note: There are slight differences between the command line option names and the fields/values in the configuration file.

volumeMountDirectory

This is a local directory that is volume mounted inside the testharness and listeningpost containers making the directory contents accessible to the containers as the /vol directory. It will be created when silentsentinel.sh is invoked, if it does not already exist on the host system.

Place all files that do not exist on the testharness container and that are required to analyze the tool under test here.

All output data and reports will be saved to this directory.

Example

```
    "volumeMountDirectory": "data_dir",
```

toolUnderTest

This is an array of strings specifying the tool under test and any required arguments. The tool under test with arguments is run within the testharness container.

This can spawn a subshell or run a utility in the regular shell of the testharness container.

Example

```
    "toolUnderTest": [
        "/vol/example2.sh",
        "listeningpost"
    ],
```

tag

This is the Linux distribution of the container image to use for the testharness and listentingpost containers. Please see the Tags section of the README for all possible options.

When not specified, `"debian"` is the default choice.

Example

```
    "tag": "debian",
```

ipv6

This is a Boolean value used to enable or disable IPv6 addresses. Setting this value to true with Docker v27 or older will cause unexpected networking behavior. When not specified, IPv6 support is disabled (false).

Example

```
    "ipv6": true,
```

analysisTools

This is a Boolean value used to enable or disable each analysis tool in the testharness container. When not specified, the default behavior is to run each analysis tool (true). The only exception to this rule is that core dumps are disabled by default (false). Core dumps are disabled by default (false), because core dumps and strace cannot be enabled simultaneously.

Example

```
    "analysisTools":
    {
        "clamscan": true,
        "coreDumps": false,
        "pspy": false,
        "strace": false,
        "suricata": true
    },
```

analysisToolTargets

This is an array of strings that tells Silent Sentinel where to perform static analysis techniques. A string can specify an absolute path to a file or a directory. Directories are recursively searched. File paths that do not exist are skipped with a warning when running static analysis techniques.

When no file paths are provided here, Silent Sentinel will perform static analysis techniques against the first argument of the tool under test. For example, a tool under test of `ls -a /vol/my-directory` without any analysisToolTargets specified will run static analysis technique against `ls`.

Example

```
    "analysisToolTargets": [
        "/vol/new-file.txt",
        "/etc/cron.d"
    ],
```

reportFormat

This is the format(s) of the Silent Sentinel report. Possible options are as follows:

- `"none"`: Silent Sentinel runs and exits without generating any reports
- `"markdown"`: Silent Sentinel generates a Markdown (.md) report
- `"all"`: Silent Sentinel generates both a Markdown (.md) and a PDF (.pdf) report

Example

```
    "reportFormat": "all"
```

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612
Phone: 412.268.5800 | 888.201.4479
Web: www.sei.cmu.edu
Email: info@sei.cmu.edu

Silent Sentinel

DM25-0550