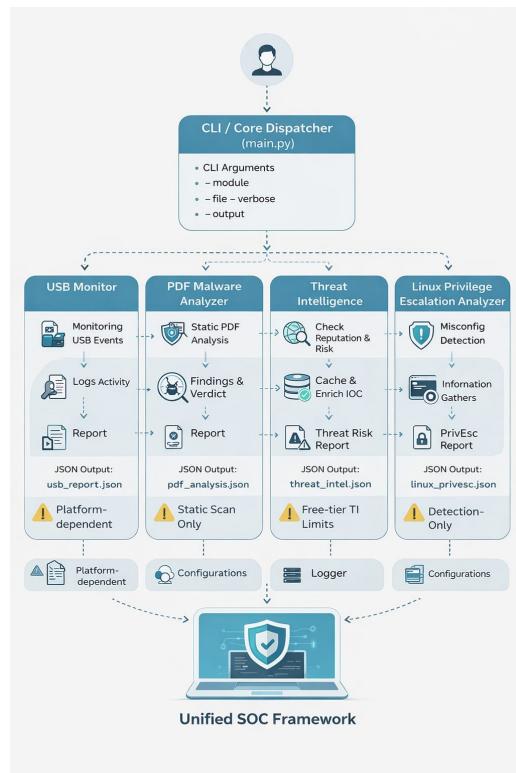


# Unified Security Operations Framework – Project Submission

## Overall Architecture Diagram



## CLI Help & Module Execution

The screenshot shows a Microsoft Visual Studio Code (VS Code) interface with the following details:

- File Explorer:** Shows the project structure under "UNIFIED-SECURITY-OPERATIONS-FRAMEWORK".
- Code Editor:** Displays the main.py file containing Python code for a security framework. The code includes logic for "usb\_monitor", "pdf\_malware", and "threat\_intel" modules.
- Terminal:** Shows two terminal sessions:
  - The first session shows the command: `python run.py -h` followed by usage information for the `run.py` script.
  - The second session shows the command: `Unified SOC Framework`.
- Bottom Status Bar:** Shows the current file is `main.py`, along with other status indicators like Pushpendarrinha (1 day ago), Ln 57, Col 76, Spaces: 4, UTF-8, LF, Python, and Finish Setup.

Linux Privilege Escalation Analyzer – Execution Output

The screenshot shows a terminal window with the title "Unified-Security-Operations-Framework". The terminal is displaying a log file named "linux\_privesc.log" with the following content:

```
data > logs > linux_privesc.log
1 2026-01-27 22:24:08,883 | INFO | System info collected: {'user': 'enp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Linux'}
2 2026-01-27 22:24:08,883 | INFO | Searching for SUID binaries
3 2026-01-27 22:25:03,418 | INFO | System info collected: {'user': 'enp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Linux'}
4 2026-01-27 22:25:03,419 | INFO | Searching for SUID binaries
5 2026-01-27 22:25:09,777 | INFO | Checking sudo permissions
6 2026-01-27 22:30:05,890 | INFO | System info collected: {'user': 'enp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Linux'}
7 2026-01-27 22:30:05,890 | INFO | Searching for SUID binaries
8 2026-01-27 22:38:11,448 | INFO | Checking sudo permissions
9 2026-01-29 12:40:45,933 | INFO | System info collected: {'user': 'enp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Linux'}
10 2026-01-29 12:40:45,936 | INFO | Searching for SUID binaries
11 2026-01-29 12:42:23,984 | INFO | System info collected: {'user': 'enp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Linux'}
12 2026-01-29 12:42:23,984 | INFO | Searching for SUID binaries
13
```

The terminal interface includes tabs for PROBLEMS, OUTPUT, DEBUG CONSOLE, TERMINAL (which is selected), and PORTS. Below the terminal, there is a command line input field with the following text:

```
(venv) (enp7s0d㉿Tor-connection) -[~/Desktop/Unified-Security-Operations-Framework]
$ python run.py --module linux_privesc --output privesc_report.json
```

## Privilege Escalation JSON Report

Unified-Security-Operations-Framework

```

File Edit Selection View Go ...
EXPLORER README.md privesc_report.json architecture.md limitations.md Preview README.md .gitignore utils.py constants.py ...
privesc_report.json ...
1 {
2     "summary": {
3         "risk_level": "LOW"
4     },
5     "system_info": {
6         "user": "enp7s0d",
7         "uid": 1000,
8         "kernel": "6.17.10+kali-amd64",
9         "os": "Description:\tKali GNU/Linux Rolling"
10    },
11    "suid_binaries_count": 0,
12    "dangerous_sudo": false,
13    "writable_cron": []
14 }

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```

[virtualenv] (venv) [enp7s0d@Tor-connection: ~] ~/Desktop/Unified-Security-Operations-Framework
$ jq . privesc_report.json
{
    "summary": {
        "risk_level": "LOW"
    },
    "system_info": {
        "user": "enp7s0d",
        "uid": 1000,
        "kernel": "6.17.10+kali-amd64",
        "os": "Description:\tKali GNU/Linux Rolling"
    },
    "suid_binaries_count": 0,
    "dangerous_sudo": false,
    "writable_cron": []
}

```

TERMINAL

Pushpenderrathore (1 day ago) Ln 14, Col 2 Spaces: 2 UTF-8 LF {} JSON Finish Setup AI Context: 1 file

## USB Monitoring Module – Verbose Mode

Unified-Security-Operations-Framework

```

File Edit Selection View Go ...
EXPLORER README.md usb_monitor.log architecture.md limitations.md Preview README.md .gitignore utils.py constants.py ...
usb_monitor.log ...
data > logs > usb_monitor.log
36 2026-01-28 23:29:56.564 | INFO | ID: MODEL_ID=0066
37 2026-01-28 23:29:56.565 | INFO | ID: VENDOR_ID=leat
38 2026-01-28 23:30:38.244 | INFO | ID: MODEL_ID=0066
39 2026-01-28 23:30:38.245 | INFO | ID: VENDOR_ID=leat
40 2026-01-28 23:30:38.253 | INFO | ID: MODEL_ID=e1f8
41 2026-01-28 23:30:38.254 | INFO | ID: VENDOR_ID=23a9
42 2026-01-28 23:30:38.273 | INFO | ID: MODEL_ID=0066
43 2026-01-28 23:30:38.273 | INFO | ID: VENDOR_ID=leat
44 2026-01-28 23:30:38.449 | INFO | ID: MODEL_ID=e1f8
45 2026-01-28 23:30:38.450 | INFO | ID: VENDOR_ID=23a9
46 2026-01-28 23:30:38.538 | INFO | ID: MODEL_ID=0066
47 2026-01-28 23:30:38.538 | INFO | ID: VENDOR_ID=leat
48 2026-01-28 23:30:38.221 | INFO | USB monitoring stopped by user
49 2026-01-28 23:30:38.221 | INFO | USB monitor process terminated cleanly
50 | 2026-01-29 12:45:23.142 | INFO | Starting USB device monitoring

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```

[virtualenv] (venv) [enp7s0d@Tor-connection: ~] ~/Desktop/Unified-Security-Operations-Framework
$ python run.py --module usb_monitor --verbose
[*] Verbose mode enabled
[VERBOSE] Use monitoring started
[VERBOSE] ID: MODEL_ID=e1f8
[VERBOSE] ID: VENDOR_ID=23a9
[VERBOSE] ID: VENDOR_ID=e1f8
[VERBOSE] ID: VENDOR_ID=0066
[VERBOSE] ID: MODEL_ID=0066
[VERBOSE] ID: VENDOR_ID=leat

```

TERMINAL

Ln 1, Col 1 Spaces: 4 UTF-8 LF {} Log Finish Setup AI Context: 1 file

## Generated Logs and Evidence

The screenshot shows a terminal window titled "Unified-Security-Operations-Framework" running on a Kali Linux system (emp7s0d@Tor-connection). The terminal displays the following content:

```
$ python run.py --help
usage: run.py [-h] --module {usb_monitor,pdf_malware,threat_intel,linux_privesc} [--file FILE]
              --output OUTPUT
              --verbose
Unified SOC Framework

options:
-h, --help            show this help message and exit
--module {usb_monitor,pdf_malware,threat_intel,linux_privesc}
                      Module to run
--file FILE          Input target (PDF file path for pdf_malware | IP/Domain for threat_in
--output OUTPUT       Save report to file (JSON format)
--verbose            Enable verbose output

[...]
$ tree data/logs -P "*.log"
data/logs
├── linux_privesc.log
└── pdf_malware.log
└── threat_intel.log
└── usb_monitor.log

1 directory, 4 files

[...]
$ ls
cli  data  modules  privesc_report.json  requirements.txt  tests
core  docs  Notes.txt  README.md        run.py        venv

[...]
$ file ./*
./cli:           directory
./core:          directory
./data:          directory
./docs:          directory
./modules:       directory
./Notes.txt:     Unicode text, UTF-8 text
./privesc_report.json: JSON text data
./README.md:    Unicode text, UTF-8 text, with very long lines (359)
./requirements.txt: ASCII text
./run.py:        Python script, ASCII text executable
./tests:         directory
./venv:          directory

[...]
$ ls data/logs
linux_privesc.log  pdf_malware.log  threat_intel.log  usb_monitor.log

[...]
$ tail -n 20 data/logs/linux_privesc.log
2026-01-27 22:24:08,083 | INFO | System info collected: {'user': 'emp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Description:\tKali GNU/Linux Rolling'}
2026-01-27 22:24:08,883 | INFO | Searching for SUID binaries
2026-01-27 22:24:08,883 | INFO | System info collected: {'user': 'emp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Description:\tKali GNU/Linux Rolling'}
2026-01-27 22:25:03,419 | INFO | Searching for SUID binaries
2026-01-27 22:25:03,419 | INFO | Checking sudo permissions
2026-01-27 22:30:05,890 | INFO | System info collected: {'user': 'emp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Description:\tKali GNU/Linux Rolling'}
2026-01-27 22:30:05,890 | INFO | Searching for SUID binaries
2026-01-27 22:30:11,448 | INFO | Checking sudo permissions
2026-01-29 12:40:45,933 | INFO | System info collected: {'user': 'emp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Description:\tKali GNU/Linux Rolling'}
2026-01-27 22:25:03,419 | INFO | Searching for SUID binaries
2026-01-27 22:25:03,419 | INFO | Checking sudo permissions
2026-01-29 12:42:23,984 | INFO | System info collected: {'user': 'emp7s0d', 'uid': 1000, 'kernel': '6.17.10+kali-amd64', 'os': 'Description:\tKali GNU/Linux Rolling'}
2026-01-29 12:42:23,984 | INFO | Searching for SUID binaries
2026-01-29 12:42:23,984 | INFO | Checking sudo permissions
2026-01-29 12:42:23,984 | INFO | Searching for SUID binaries
2026-01-29 12:42:23,984 | INFO | Checking sudo permissions

[...]
```