

Noroff

# CND 2025

SOC Log Pre-Processing Script

Tobias Axelson | tobaxe01194@stud.noroff.no  
09/11/2025

## Contents

Overview .....	2
Task.....	2
Security .....	2
Logging and output.....	2
Dependencies.....	2
Installation .....	3
How to run the script .....	3
Testing evidence.....	4
Fig.1.....	4
Fig.2.....	5
Fig.3.....	5
Potential Problems .....	6

## Overview

This script automates the daily SOC pre-processing workflow. It securely downloads and validates configuration files, processes Apache logs, audits system integrity, generates reports, packages results and signs them for upload to a remote server defined by the operator. This method ensures traceability, data validation and operational security.

## Task

The structure of the script is based on the provided tasks in the provided assignment, ranging from T1-24, while adhering to the K1-11 requirements.

## Security

- HTTPS enforced for config and CTI downloads
- GPG signatures verified before usage
- Lockfile and cleanup function to prevent concurrent runs of the script
- SHA256 checksum ensure package integrity after transfer
- Audit logging at every step

## Logging and output

- Main log: /opt/security/logs/socscript.log
- Reports: /opt/security/tmp/socscript-<date>/report.txt
- Validation: /opt/security/validation/validation.txt
- Uploads stored and verified on remote submission server

## System requirements

- Operating system: Linux (tested on Ubuntu 24.04.3 LTS)
- Web Server: Apache2 (The script needs /var/log/apache2/access.log to function)
- Internet access: Required to download configuration and threat lists
- GPG Keys: [soc-sign@dragur.no](mailto:soc-sign@dragur.no) and [soc-ingest@dragur.no](mailto:soc-ingest@dragur.no)
- Tools:
  - Curl

- Gnupg
- Rsync
- Iptables
- Net-tools
- Findmnt
- awk

## Installation

To replicate this project, one would need to:

- Copy the script to /opt/security/
- Make the script executable
- Import SOC signing keys
- Ensure the Apache server is running
  - Folder structure used in this project:
    - /var/www/html/soc-hub.no/socscript/sigs
    - Sigs need to be included. -C parameter points to “soc-hub.no/socscript”, and requires a subdirectory named sigs

## How to run the script

Manual execution:

- `sudo /opt/security/socscript-tobaxe01194.sh -C <URL> -r <REMOTE_HOST> -u <REMOTE_USER>`
- Example: `./socscript-tobaxe01194.sh -C https://soc-hub.no/socscript -r 192.168.111.128 -u toby`

Automated via system cron:

- `sudo crontab -e`
- Hit 1 for nano
- Add line:
  - `30 0 * * * opt/security/socscript-tobaxe01194.sh -C https://soc-hub.no/socscript -r 192.168.111.128 -u toby`
- This ensures that the script is run at 02:30 AM daily

# Testing evidence

Fig.1

```
axe-server@ubuntu-headless:/opt/security$ sudo ./socscrip.sh -C https://soc-hub.no/socscrip -r 192.168.111.128 -u toby
Parameters validated:
URL = https://soc-hub.no/socscrip
REMOTE_HOST = 192.168.111.128
REMOTE_USER = toby
HTTPS check passed: https://soc-hub.no/socscrip
Configuration file ready: /opt/security/tmp/socscrip-20251109/f7732518b3a230ba9a5d9d22356c2ab8e3d5a7968c017b79bdf73557df81af90.conf
STAGE10=GOOD

Top 10 URLs by unique hosts (404 errors):
/robots.txt, 51975, 3652
/images/frontpagepics/0000/0077/Risenfront.jpg, 721, 549
/about-us/contact-details, 539, 288
/images/trailers/cityhunter.mpg, 890, 179
/images/filmpics/0000/6231/MBF014_Cannibal_3D.jpg/img%5Drnrn%5Bimg%5Dhttp://www.visualprezz.net/images/tp.jpg%5B/img%5Drnrn%5Bimg%5Dhttp://www.visualprezz.net/img_post/Style_10/info.film.png, 1632, 140
/videos/Video_Ong.php, 360, 130
/images/filmpics/0000/6231/MBF014_Cannibal_3D.jpg/img]rnrn[img]http://www.visualprezz.net/images/tp.jpg[/img]rnrn[img]http://www.visualprezz.net/img_post/Style_10/info.film.png, 759, 123
/show_film.php?id=697, 135, 95
/images/trailers/myluckystars.mpg, 327, 92
/index.php3, 127, 88

STAGE11=GOOD

Audit summary:
- Modified last 48h: 1 files
- Not accessed 60d+: 1 files
- Executables in /tmp or /var/tmp: 2 files

STAGE12=GOOD
STAGE13=WARNING
STAGE14=WARNING
STAGE15=WARNING
STAGE16=GOOD
STAGE17=GOOD
STAGE18=GOOD
STAGE19=WARNING
STAGE20=GOOD
STAGE21=GOOD
STAGE22=GOOD
STAGE23=GOOD
Upload file: socscrip-ubuntu-headless-20251109-18.tar.gz (53MB)
socscrip Check ubuntu-headless 20251109-18:44 OK
STAGE24=GOOD
axe-server@ubuntu-headless:/opt/security$
```

This screenshot shows the script executed from command line. The script takes three arguments, `-C <URL>`, `-r <REMOTE_HOST>`, `-u <REMOTE_USER>`. Further the script outputs information about the process, and indicating if things are working as intended.

Fig.2

```
[Sun Nov 9 06:44:27 PM UTC 2025] Created /opt/security/tmp/socscript-20251109/recent_modified.txt
find: '/opt/web/sites/r': No such file or directory
[Sun Nov 9 06:44:27 PM UTC 2025] Created /opt/security/tmp/socscript-20251109/old_unaccessed.txt
[Sun Nov 9 06:44:27 PM UTC 2025] Created /opt/security/tmp/socscript-20251109/tmp_executables.txt
[Sun Nov 9 06:44:27 PM UTC 2025] Filecheck and audit completed successfully.
[Sun Nov 9 06:44:27 PM UTC 2025] WARNING: /data/webstatic not mounted.
[Sun Nov 9 06:44:27 PM UTC 2025] Starting T14: Comparing live config /etc/apache2/apache2.conf to reference /opt/security/ref/httpd.conf-20251020
not found. 06:44:27 PM UTC 2025] ERROR: Reference config /opt/security/ref/httpd.conf-20251020
[Sun Nov 9 06:44:27 PM UTC 2025] T14 Status: WARNING
[Sun Nov 9 06:44:27 PM UTC 2025] Starting T15: Checking firewall and listening ports integrity...
[Sun Nov 9 06:44:27 PM UTC 2025] Firewall rules have changed. Diff saved to /opt/security/tmp/socscript-20251109/firewall.diff
[Sun Nov 9 06:44:27 PM UTC 2025] Listening ports unchanged.
[Sun Nov 9 06:44:27 PM UTC 2025] T15 status: WARNING
[Sun Nov 9 06:44:27 PM UTC 2025] Starting T16: Saving validation outputs...
[Sun Nov 9 06:44:27 PM UTC 2025] Validation summary written to /opt/security/validation/validation.txt
[Sun Nov 9 06:44:27 PM UTC 2025] Copied current webserver config to /opt/security/validation/webconfig-20251109
[Sun Nov 9 06:44:27 PM UTC 2025] Copied current firewall rules to /opt/security/validation/firewall-20251109
[Sun Nov 9 06:44:27 PM UTC 2025] T16 completed successfully
[Sun Nov 9 06:44:27 PM UTC 2025] Starting T17: Checking disk space utilisation...
[Sun Nov 9 06:44:27 PM UTC 2025] WARNING: /run is low on space: 1% used, 386MB free.
[Sun Nov 9 06:44:27 PM UTC 2025] WARNING: / is low on space: 78% used, 2170MB free.
[Sun Nov 9 06:44:28 PM UTC 2025] WARNING: /dev/shm is low on space: 0% used, 1935MB free.
[Sun Nov 9 06:44:28 PM UTC 2025] WARNING: /run/lock is low on space: 0% used, 5MB free.
[Sun Nov 9 06:44:28 PM UTC 2025] WARNING: /boot is low on space: 12% used, 1446MB free.
[Sun Nov 9 06:44:28 PM UTC 2025] Disk space check complete. Status: GOOD
[Sun Nov 9 06:44:28 PM UTC 2025] Starting T18: Detecting error IPs...
[Sun Nov 9 06:44:30 PM UTC 2025] Created /opt/security/tmp/socscript-20251109/403errors.txt (threshold 20).
[Sun Nov 9 06:44:32 PM UTC 2025] Created /opt/security/tmp/socscript-20251109/401errors.txt (threshold 20).
[Sun Nov 9 06:44:34 PM UTC 2025] Created /opt/security/tmp/socscript-20251109/404errors.txt (threshold 20).
[Sun Nov 9 06:44:36 PM UTC 2025] T18 complete. Status: GOOD
[Sun Nov 9 06:44:36 PM UTC 2025] Starting T19: Checking for high risk path accesses...
[Sun Nov 9 06:44:36 PM UTC 2025] Checking for paths: /admin,/wp-admin/,/backups
[Sun Nov 9 06:44:37 PM UTC 2025] Found 174 access attempts to high risk paths.
[Sun Nov 9 06:44:37 PM UTC 2025] T19 complete. Status: WARNING
[Sun Nov 9 06:44:37 PM UTC 2025] Starting T20: Checking IPs against threat intelligence list...
[Sun Nov 9 06:44:37 PM UTC 2025] Threat list downloaded successfully.
[Sun Nov 9 06:44:43 PM UTC 2025] No threat IP matches found.
[Sun Nov 9 06:44:43 PM UTC 2025] T20 Complete. Status: GOOD
[Sun Nov 9 06:44:43 PM UTC 2025] Starting T21: Packaging and signing report...
[Sun Nov 9 06:44:43 PM UTC 2025] Creating archive: /opt/security/socscript-ubuntu-headless-20251109-18.tar.gz
[Sun Nov 9 06:44:52 PM UTC 2025] Archive created successfully.
[Sun Nov 9 06:44:52 PM UTC 2025] Signing tar.gz with soc-ingest@dragur.no...
[Sun Nov 9 06:44:52 PM UTC 2025] GPG signature created: /opt/security/socscript-ubuntu-headless-20251109-18.tar.gz.gpg
[Sun Nov 9 06:44:52 PM UTC 2025] Generating SHA256 checksum...
[Sun Nov 9 06:44:52 PM UTC 2025] SHA256 checksum saved to /opt/security/socscript-ubuntu-headless-20251109-18.tar.gz.sha256
[Sun Nov 9 06:44:52 PM UTC 2025] T21 completed successfully. Archive ready for upload.
[Sun Nov 9 06:44:52 PM UTC 2025] Starting T22: Uploading to server...
[Sun Nov 9 06:44:52 PM UTC 2025] Connecting to 192.168.111.128 on port 31337 ...
sending incremental file list
socscript-ubuntu-headless-20251109-18.tar.gz
socscript-ubuntu-headless-20251109-18.tar.gz.gpg
socscript-ubuntu-headless-20251109-18.tar.gz.sha256

sent 54,882,130 bytes received 121 bytes 21,952,900.40 bytes/sec
total size is 54,869,467 speedup is 1.00
[Sun Nov 9 06:44:55 PM UTC 2025] Upload completed successfully to 192.168.111.128:/submission/ubuntu-headless/2025/11/
[Sun Nov 9 06:44:55 PM UTC 2025] T22 completed with status: GOOD
[Sun Nov 9 06:44:55 PM UTC 2025] Starting T23: Validating uploaded archive integrity...
[INFO] Found remote SHA file: /submission/ubuntu-headless/2025/11/socscript-ubuntu-headless-20251109-18.tar.gz.sha256
socscript-ubuntu-headless-20251109-18.tar.gz: OK
[Sun Nov 9 06:44:57 PM UTC 2025] SHA256 validation successful on remote host 192.168.111.128
[Sun Nov 9 06:44:57 PM UTC 2025] T23 completed with status: GOOD
[Sun Nov 9 06:44:57 PM UTC 2025] Starting T24: Generating final upload summary...
[Sun Nov 9 06:44:57 PM UTC 2025] Upload summary: File 'socscript-ubuntu-headless-20251109-18.tar.gz' size 53MB
[Sun Nov 9 06:44:57 PM UTC 2025] T24 completed with status: GOOD
[Sun Nov 9 06:44:57 PM UTC 2025] Cleaning up and restoring environment
[Sun Nov 9 06:44:58 PM UTC 2025] Removed lockfile: /var/run/socscript.ubuntu-headless.lock
[Sun Nov 9 06:44:58 PM UTC 2025] Removed working directory: /opt/security/tmp/socscript-20251109
[Sun Nov 9 06:44:58 PM UTC 2025] Returned to starting directory: /opt/security
[Sun Nov 9 06:44:58 PM UTC 2025] Environment restored successfully
axe-server@ubuntu-headless:/opt/security$
```

This screenshot shows output from the logfile, which the script appends various messages depending on how the script executes.

Fig.3

```
toby@soc-machine:/submission/ubuntu-headless/2025/11$ ls -l
total 53592
-rw-r--r-- 1 toby toby 54869214 Nov 9 18:48 socscript-ubuntu-headless-20251109-18.tar.gz
-rw-r--r-- 1 toby toby 141 Nov 9 18:48 socscript-ubuntu-headless-20251109-18.tar.gz.gpg
-rw-r--r-- 1 toby toby 111 Nov 9 18:48 socscript-ubuntu-headless-20251109-18.tar.gz.sha256
toby@soc-machine:/submission/ubuntu-headless/2025/11$
```

This final figure shows the uploaded files at the remote location.

# Potential Problems

## Missing or incorrect configuration files

- If (hostname).conf or default.conf cannot be downloaded the script will terminate
- This happens if user supply wrong URL or without https:// prefix

## Missing GPG keys

- The script requires SPC signing keys ([soc-sign@dragur.no](mailto:soc-sign@dragur.no) and [soc-ingest@dragur.no](mailto:soc-ingest@dragur.no))
- If keys are not imported beforehand, signature validation and packaging will fail
- Use `gpg -import <key.pub>`

## Permission or ownership issues

- The script writes to /opt/security, /var/run and reads from /var/log/apache2
- Running as non-root will cause permission errors
- Always run as sudo

## Network connectivity issues

- The script relies on internet connectivity to download configuration files, threat lists and remote upload

## Missing dependencies

- The script relies on curl, gpg, rsync, iptables, findmnt and awk.
- Should already be installed

## Invalid parameter usage

- The script accepts 6 arguments -C, -r, -u followed by a value
- Not using those flags and values will cause error

## Log rotation timing

- If log rotation has not occurred, it may reuse access.log instead of access.log.1