MISP CLI

AUTOMATE ALL THE THINGS

CIRCL / TEAM MISP PROJECT



MISP PROJECT

MISP CLI 5054-04-12

MISP CLI Automate all the things CRCL / Taxi MSP Project

MISP CLI FUNCTIONALITIES

MISP CLI 5054-04-12

└─MISP CLI functionalities

- The MISP API is great for remotely executing administrative tasks
- But sometimes we want to simplify the process / avoid
- MISP also has an extensive CLI sub-system for this reason

- The MISP API is great for remotely executing administrative tasks
- But sometimes we want to simplify the process / avoid having to deal with authentication
- MISP also has an extensive CLI sub-system for this reason

TYPES OF OBJECTIVES FOR THE SCRIPTS

MISP CLI 2024-15

└─Types of objectives for the scripts

Automating recurring tasks
 Recovery from loss of access
 Updates / initialisation
 Background worker management

- Automating recurring tasks
- Recovery from loss of access
- Updates / initialisation
- Background worker management

CLI DOCUMENTATION

CLI DOCUMENTATION

https://path.to.your.misp/events/automation

Administering the background workers via the APL

ander 1919 - Considerat ABA Server's Yopper for Sparrad (part) alter and Tells / Considerat ABA Server's Spatializations
ministering MISP eta the CU
n anneniste one en espect a la cit, ban las els estimatores en ordere (ACP) con accessioner en esteration. Anna XDA hastlande care tanon protector ((estima)
Characteristics and particular particular (
And An Annotation Install (Annot)
Produce And Provide Annual and a second
a 18 2008 Department #109-14-0 Toronda Toron Adulty applications
a barry between AMA up for a top Anna and an an anna an
a Bana Pangkan Willings Statement and a generation Pangation

https://path.to.your.misp/events/automation

Administering the background workers via the API.

You can start/stop and view the bacground workers via the API. Add worker: http://localhost:5001/servers/startWorker/[queue_name] Stop worker: http://localhost:5001/servers/stopWorker/[worker_pid] Get worker into: http://localhost:5001/servers/getWorkers

Administering MISP via the CLI

Certain administrative tasks are exposed to the API, these help with maintaining and configuring MISP in an automated way / via external tools. Get Setting: MISP/app/Console/cake Admin getSetting [setting] Set Setting: MISP/app/Console/cake Admin getAuthkey [email] Set Authkey: MISP/app/Console/cake Baseur1 [baseur1] Change Password: MISP/app/Console/cake Baseur1 [mex_password] [--override_password_change] Clear Bruteforce Entries: MISP/app/Console/cake Admin update0atbase Update All SON Structures: MISP/app/Console/cake Admin update0atbase Update All SON Structures: MISP/app/Console/cake Admin update0atbase Update Galaxy Definitions: MISP/app/Console/cake Admin update0atbase MISP/app/Console/



/var/www/MISP/app/Console/cake [Shell] [Command] [parameters] Example:

- /var/www/MISP/app/Console/cake Password "andras.iklody@gmail.com" "Nutella"
- Change password to "Nutella" for my user
 Some shells are single use and don't need a comm
- parameter Also used by the background processing
- Automation is meant to be used via cron jobs

/var/www/MISP/app/Console/cake [Shell] [Command]
[parameters]

Example:

- /var/www/MISP/app/Console/cake Password "andras.iklody@gmail.com" "Nutella"
- Change password to "Nutella" for my user
- Some shells are single use and don't need a command parameter
- Also used by the background processing
- Automation is meant to be used via cron jobs

MISP CLI

5

2024-04

 Editcontab of www-data user
 Crontab of www-data -e
 0 3,0;5;2;4 + *.
 Your / maw/MISF/app/Coale Server pull 1 9 full
 Paliserer ID ipp as user it every 6 hours
 Bjourly / urs/maw/MISF/app/Coale /cake Server cacheFed 1 csv full
 Cacheal Lev Greds user it every hour

- Edit crontab of www-data user
- ∎ crontab -u www-data -e
- 0 3,9,15,21 * * *
 /var/www/MISP/app/Console/cake Server pull 1
 30 full
- Pull server ID #30 as user #1 every 6 hours
- @hourly /var/www/MISP/app/Console/cake Server cacheFeed 1 csv full
- Cache all csv feeds as user #1 every hour