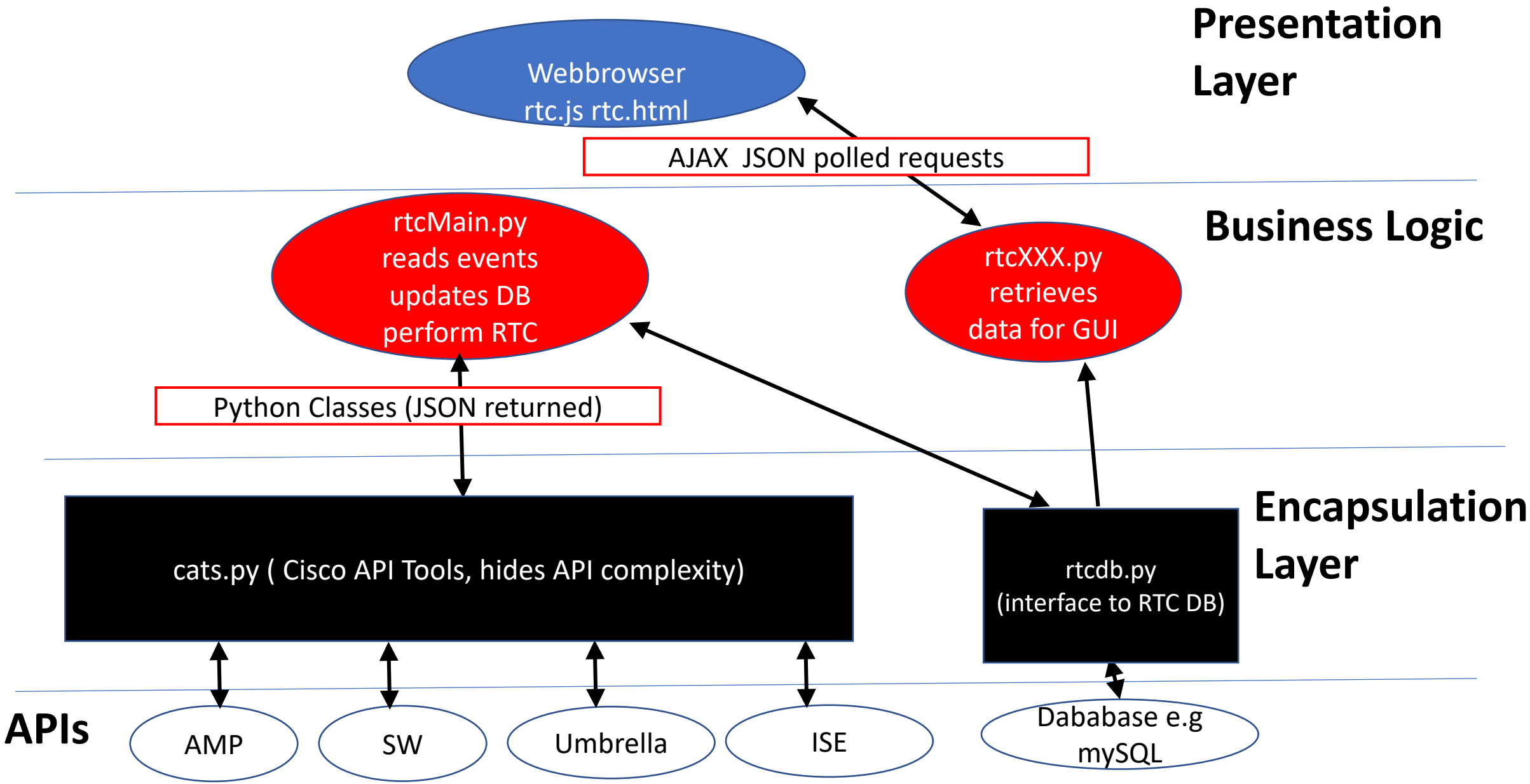
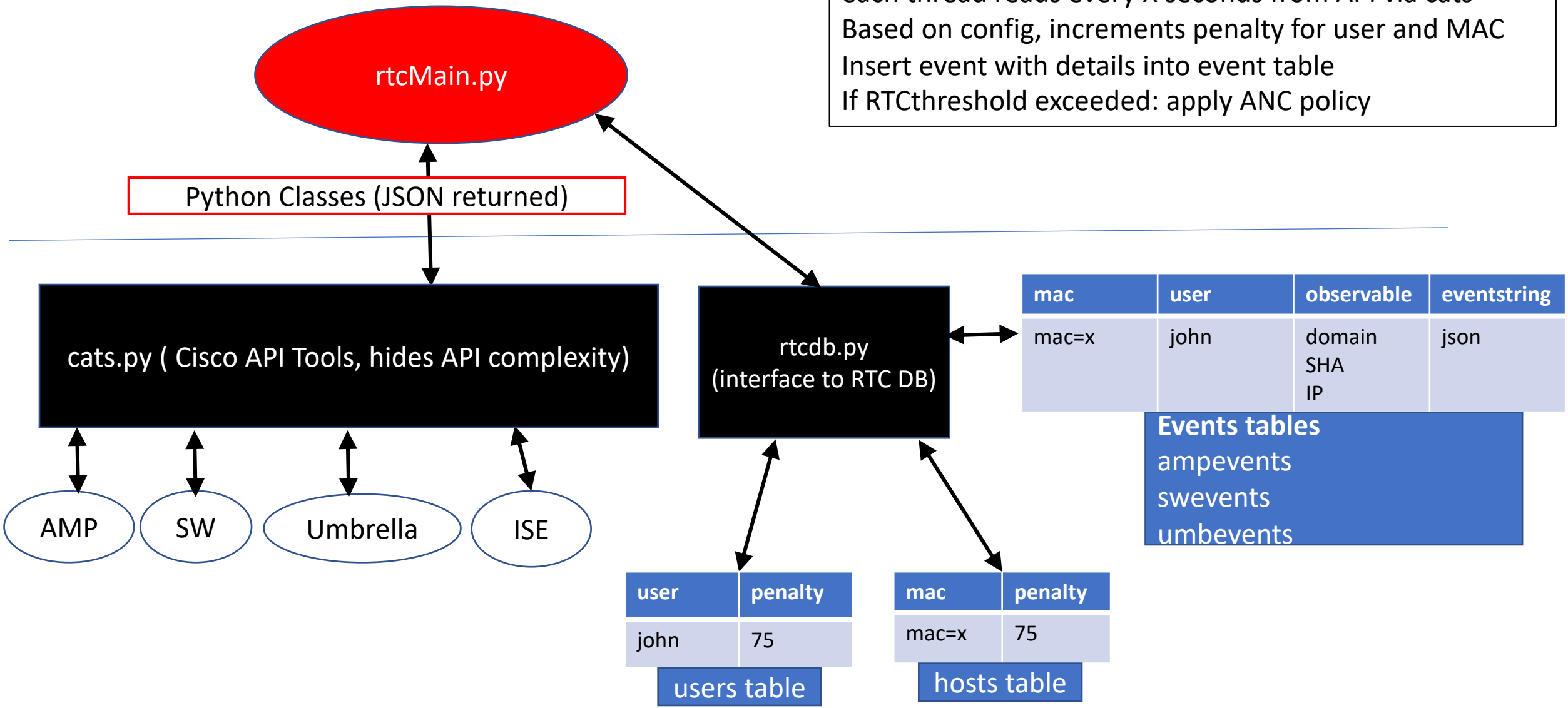
High Level Design

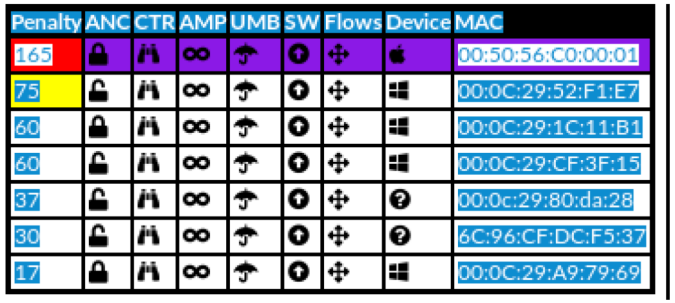


rtcMain.py - details

rtcMain multithreaded process, 3 threads AMP, SW, UMB
each thread reads every X seconds from API via cats
Based on config, increments penalty for user and MAC
Insert event with details into event table
If RTCthreshold exceeded: apply ANC policy



rtcGetHosts.py, rtcGetUsers.py



Penalty	ANC	CTR	AMP	UMB	SW	Flows	Device	MAC
165								00:50:56:C0:00:01
75								00:0C:29:52:F1:E7
60								00:0C:29:1C:11:B1
60								00:0C:29:CF:3F:15
37								00:0c:29:80:da:28
30								6C:96:CF:DC:F5:37
17								00:0C:29:A9:79:69

Webbrowser
rtc.js

AJAX Javascript polls at regular intervals updates GUI

rtcGetHosts.py

rtcGetUsers.py

CGI script - serves requests from presentation layer
Gathers information on hosts, users, penalties, events from DB but also some realtime info via APIs

cats.py (Cisco API Tools, hides API complexity)

rtcdb.py
(interface to RTC DB)

mac	user	observable	eventstring
mac=x	john	domain SHA IP	json

Events tables
ampevents
swevents
umbevents

AMP

SW

Umbrella

ISE

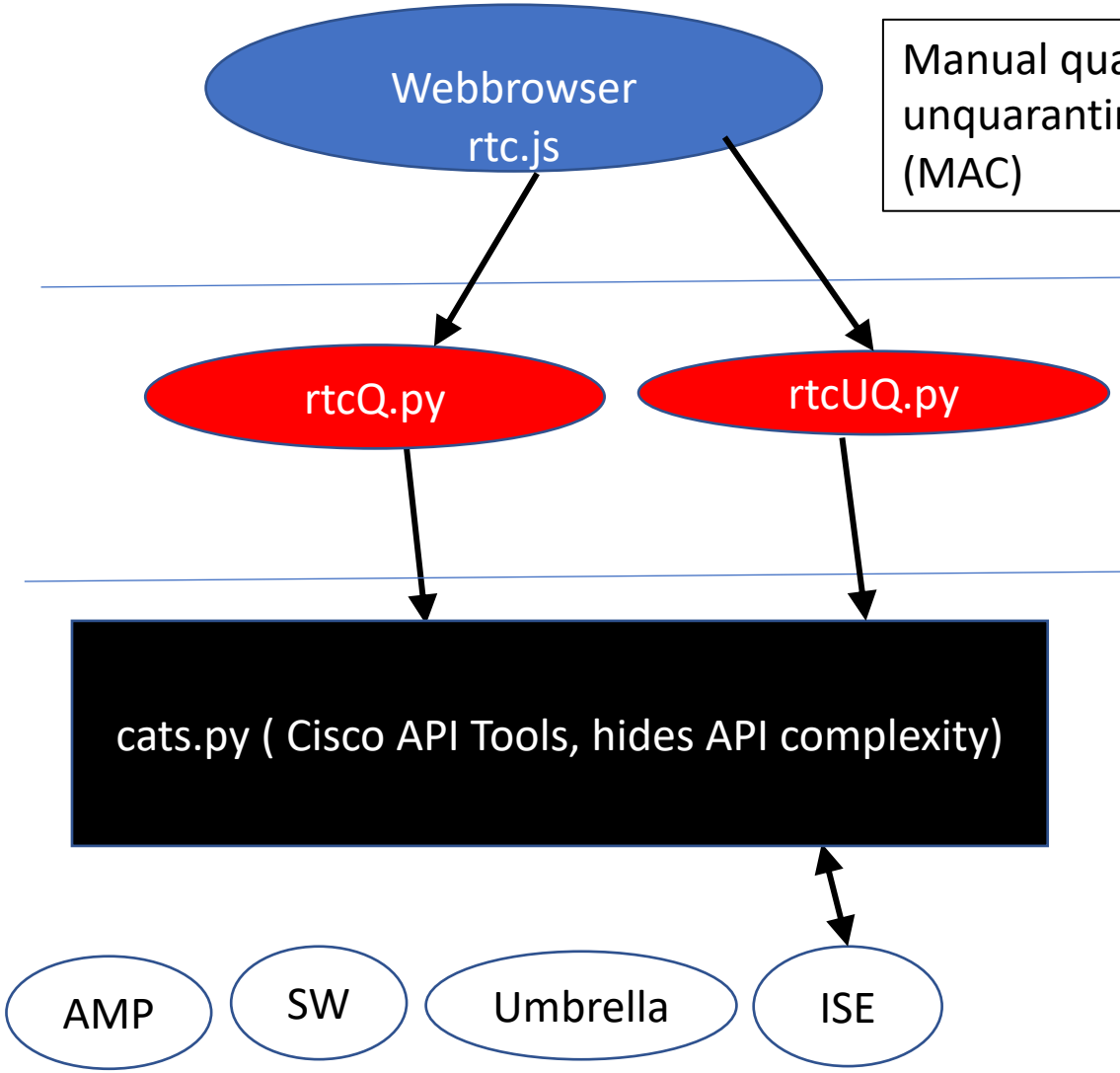
user	penalty
john	75

users table

mac	penalty
mac=x	75

hosts table

rtcQ.py, rtcUQ.py

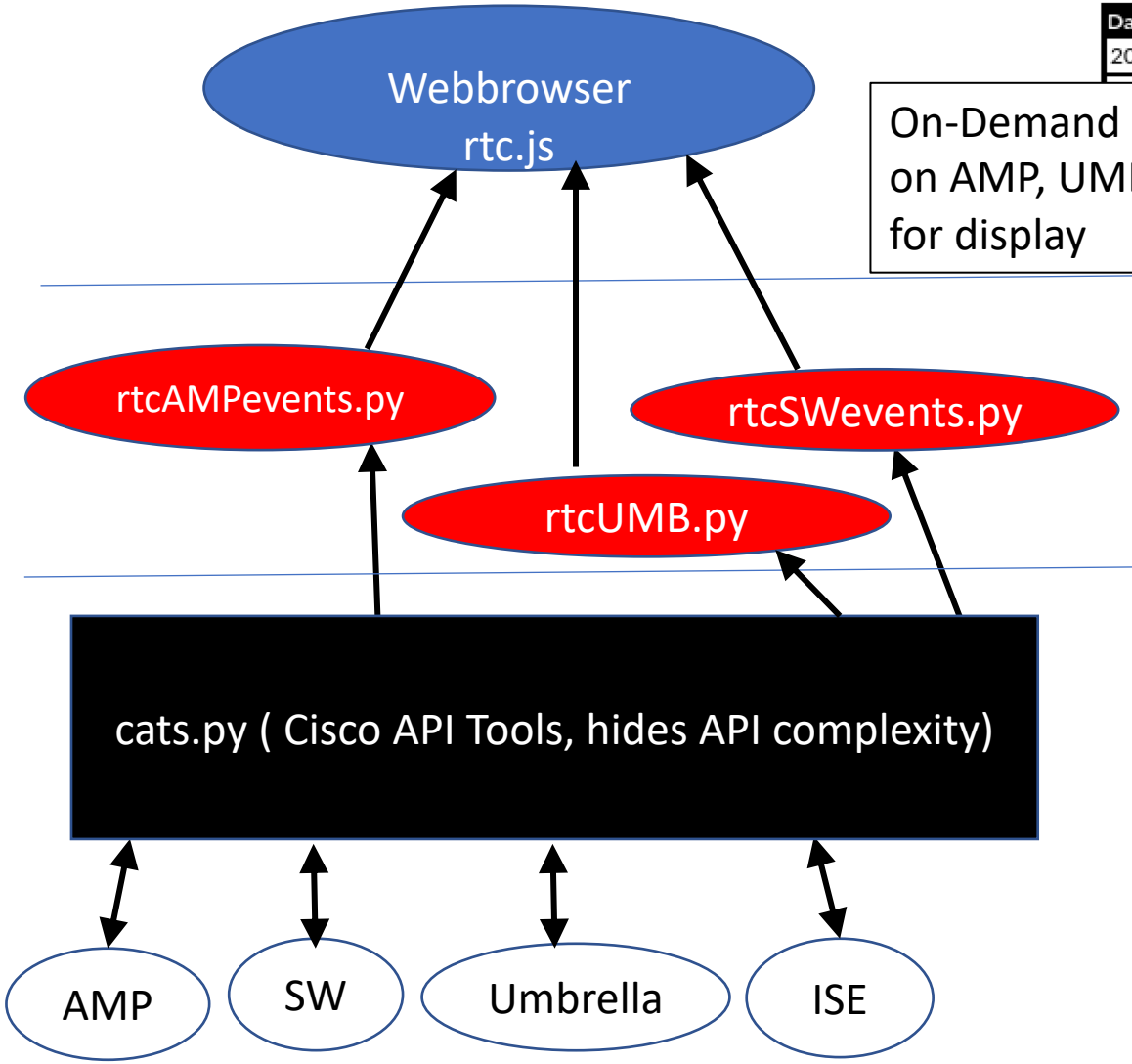


Manual quaratine or unquarantine of host (MAC)

Penalty	ANC	CTR	AMP	UMB	SW	Flows	Device	MAC
165								00:50:56:C0:00:01
75								00:0C:29:52:F1:E7
60								00:0C:29:1C:11:B1
60								00:0C:29:CF:3F:15
37								00:0c:29:80:da:28
30								6C:96:CF:DC:F5:37
17								00:0C:29:A9:79:69

CGI script - serves requests to perform manual quarantine or unquarantine of endpoint

rtcAMPevents.py, rtcSWevents.py, rtcUMBevents.py, rtcFLOWS.py, rtcISEsessions.py

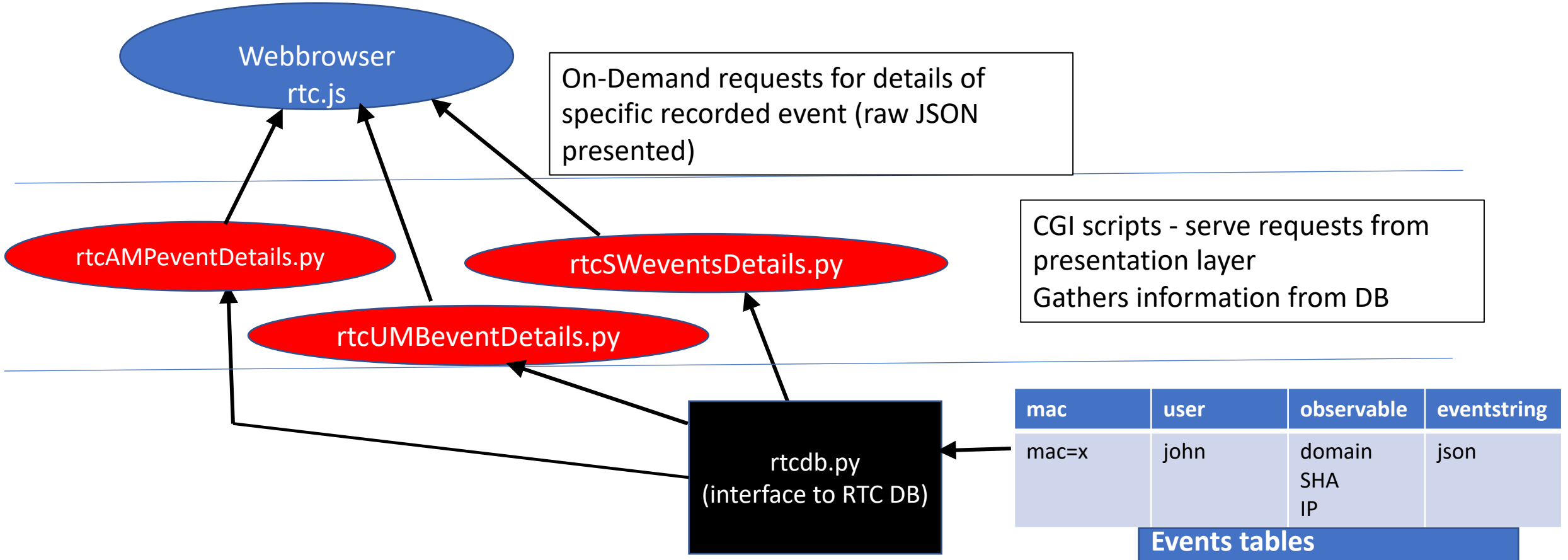


Date	Event Type	Hostname	Network addresses
2018-10-22T21:59:37+00:00	Threat Quarantined	vmrat13B.labrats.se	[{"ip":"192.168.22.13","mac":"00:0c:29:a9:79:69"
		vmrat13B.labrats.se	[{"ip":"192.168.22.13","mac":"00:0c:29:a9:79:69"
	re	vmrat13B.labrats.se	[{"ip":"192.168.22.13","mac":"00:0c:29:a9:79:69"

On-Demand requests for live info on AMP, UMB, SW or ISE via API for display

CGI scripts - serve requests from presentation layer
Gathers information from API

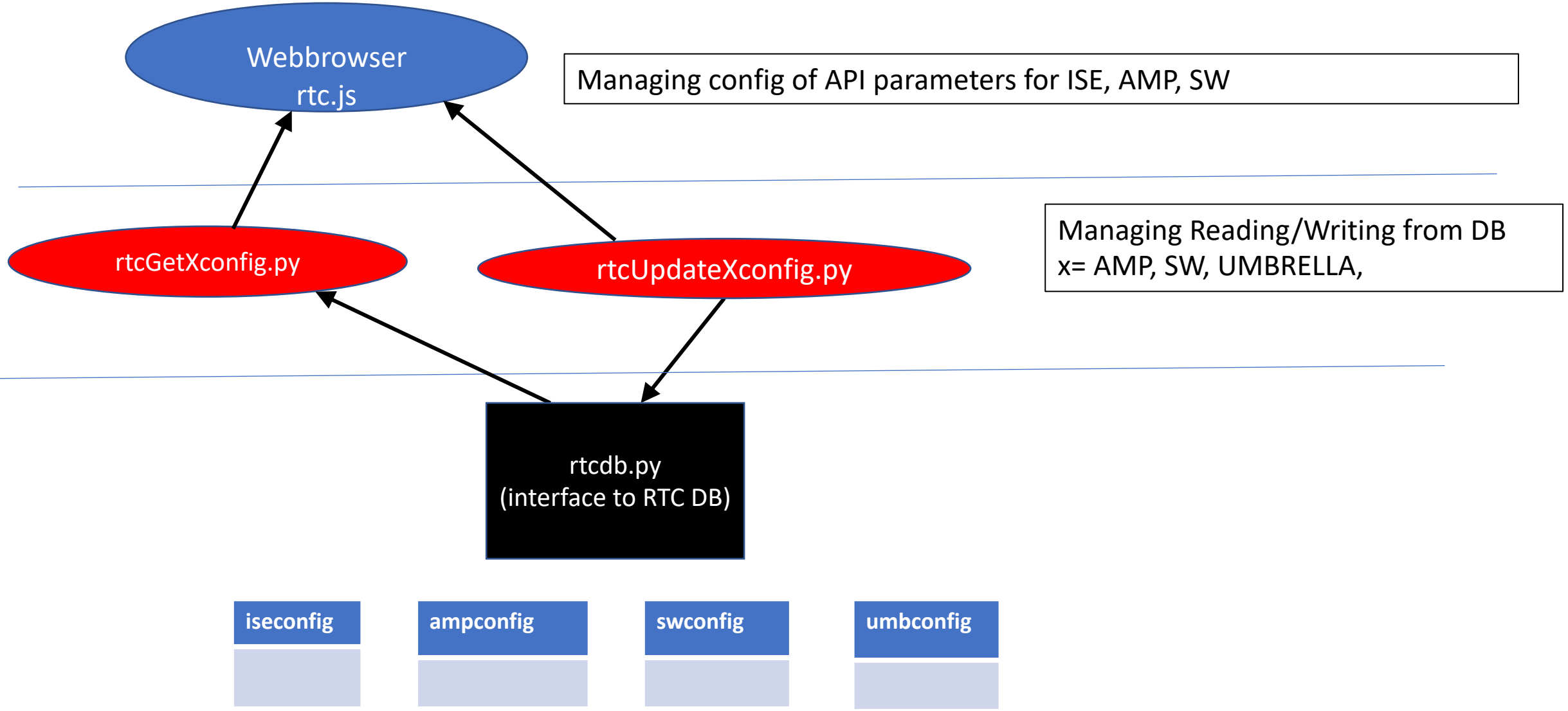
rtcAMPeventsdetails.py, rtcSWeventDetails.py, rtcUMBeventDetails.py,



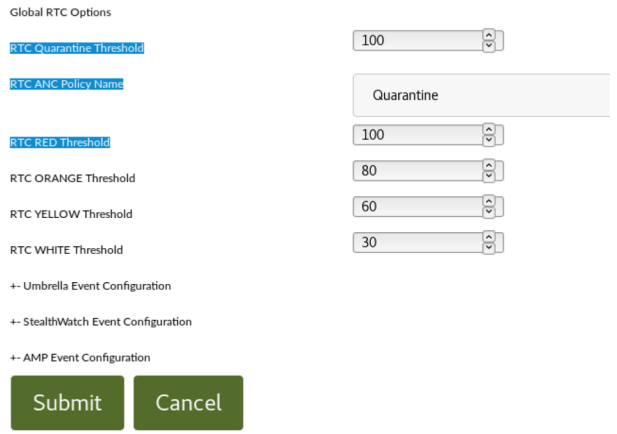
mac	user	observable	eventstring
mac=x	john	domain SHA IP	json

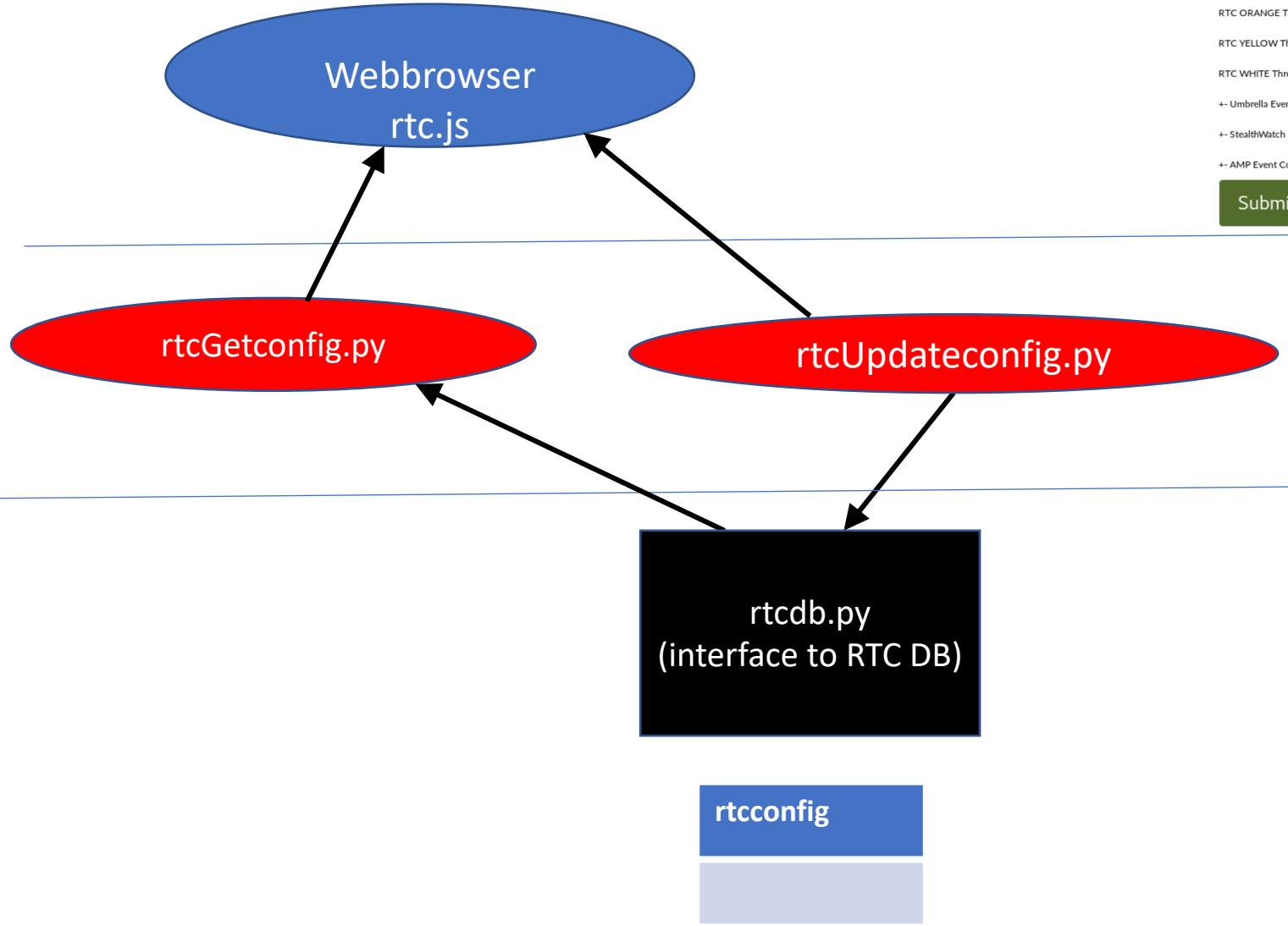
Events tables
ampevents
swevents
umbevents

rtcGetXconfig.py, rtcUpdateXconfig.py,



rtcGetconfig.py, rtcUpdateconfig.py,





Managing rtC global config options

To consider

- Currently a host or user will only get a penalty once for the same observable
  - e.g. If SHA256 observed N times on host/user will only get 1*penalty
  - e.g. if host/user connects to the same CNC domain many times, only 1*penalty
- This should be configurable? Depending on type of IOC, penalty should accumulate for the same observable

Known Issues/Challenges

- Umbrella API rate-limiting
  - have observed status code 429 with no data (API rate limit exceeded) when polling every minute
- ISE pxGrid request for specific host returns empty
  - sometimes failed if subsequent requests, e.g. in loop
- Retrieving events within specific time window
  - issues observed with Umbrella API and SW API (returns events waaay outside window).... still works because we don’t let the same observable accrue penalty more than once (see predvious slide). still irritating because it clutters logs.

Must fix

- Security! No login to app ☺ and No input validation
- Errorhandling, logging need improving
- Some redundancies can be removed by adding library functions

Requirements (1)

- python3
- webserver, mysql
- python3 mysqlconnector
- websockets

Where to put files

- rtc.js, rtc.html, rtc.css put in web server directory (e.g. /var/www/html)
- rtc*.py put in cgi-bin directory (e.g. /usr/lib/cgi-bin)
- rtcMain.py can be in any directory since not cgi-script, but cgi-bin will work
- *.json (contains username password for mysql connection) in same directory as cgi-bin