Title: Enrich web server logs Description: Access Watch, Logagent's output filter, deploys and easily plugs into any existing data pipeline as the industry's most precise robot intelligence used to detect malicious bots, threat detection, geoip, and the key for devops teams to stay in control of what is happening on their infrastructure and web assets

Access Watch output filter

Web traffic insights and robot detection are key for teams to stay in control of what is happening on their infrastructure and web assets. Automated robotic traffic now represents a larger share of website activity over human customers. These bots have a significant impact, with many working hard to disguise their identity and activity, thereby increasing risk and costs while harming performance for online businesses. Access Watch deploys the industry's most precise robot intelligence to be easily plugged into any existing data pipeline.

This plugin provides a seamless integration with the Access Watch service to all Sematext clients.

Example config to enrich Nginx web server logs with Access Watch robot information (requires Access Watch API key and Sematext Logsene Token):

```
options:
  includeOriginalLine: false # don't log original log line
  printStats: 60             # print stats every minute
  maxInputRate: 1mb          # per second

input:
  files:
      - '/var/log/nginx/access_log'

outputFilter:
  - module: access-watch
    config:
      apiKey: 'YOUR_REVEAL_API_KEY_HERE'


output:
  sematext:
    module: elasticsearch
    url: 'https://logsene-receiver.sematext.com'
    index: 'YOUR_LOGSENE_TOKEN_HERE'
```

Run Logagent with your config:

```
logagent --config logagent-example-config.yml
```