From *Metabrik* to *Sisyphe.io* (1/3)

All IP data in one place

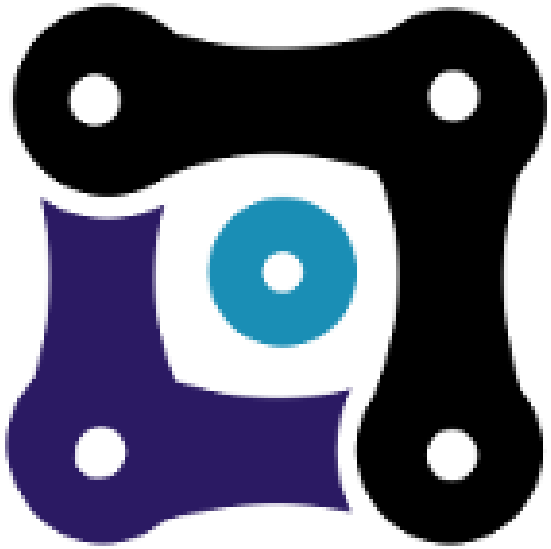
- Playing with full IPv4 address space
  - *address::generate*
- Port scanning + fingerprinting
  - *network::portscan*, *network::sinfp3*
- Mass reverse DNS all IPv4 addresses
  - *network::dns*
- Netblock + geo-IP location informations
  - *database::ripe*, *lookup::iplocation*
- Threalist lookups (SANS, iBlocklist, EmergingThreats, ...)
  - *lookup::threatlist*

From *Metabrik* to *Sisyphe.io* (2/3)

All IP data in one place

- Distributed architecture with multiple source IP addresses
  - *client::openssh*
- Distributed log collection
  - *server::syslogng*, *log::syslog*
- Store all data into an *ElasticSearch* cluster
  - *client::elasticsearch*
- Render that on a Web site (in *Perl* with *Mojolicious*)
  - *https://www.sisyphe.io/*

https://www.sisyphe.io (3/3)



- Twitter: @SisypheIo
- Twitter: @Metabrik
- Twitter: @PatriceAuffret