~~Broadmap~~
Zeekpeek

Seth Hall / Robin Sommer

~~Broadmap~~
Zeekpeek

Seth & Robin's Ideas for 2.7

Seth Hall / Robin Sommer

Renaming

Renaming

Renaming

Move to GitHub, RTD

Supervisor Model

```
|  |    \-+= 12810 seth bro supervisor.bro
|  |      |--= 12814 seth bro Cluster::node=manager
|  |      |--= 12815 seth bro Cluster::node=logger
|  |      |--= 12816 seth bro -i en0 Cluster::node=worker-01
|  |      |--= 12817 seth bro Cluster::node=worker-02
|  |      |--= 12818 seth bro Cluster::node=worker-03
|  |      \--= 12834 seth bro Cluster::node=worker-04
```

Spicy is coming

```
# cat http-request.spicy
module HTTP;

const Token      = /[^ \t\r\n]+/;
const WhiteSpace = /[ \t]+/;
const NewLine    = /\r?\n/;

export type RequestLine = unit {
  method:  Token;
  :        WhiteSpace;
  uri:     Token;
  :        WhiteSpace;
  version: Version;
  :        NewLine;

  on %done {
    print self.method, self.uri, self.version.number;
    }
};

type Version = unit {
  :        /HTTP\//;
  number: /[0-9]+\.[0-9]+/;
};


# echo "GET /index.html HTTP/1.0" | spicy-driver http-request.spicy
GET /index.html 1.0
```

Osquery Integration

```
event bro_init() {
  local query = [
        $ev=host_process_events,
        $query="SELECT pid,path,cmdline,cwd,uid,gid,time,parent
                FROM process_events"
  ];

   osquery::subscribe(query);
}
```

```
event host_process_events(resultInfo: osquery::ResultInfo,
    pid: int, path: string, cmdline: string, cwd: string,
    uid: int, gid: int, start_time: int, parent: int) {

  print fmt("UID %d executed %s", uid, path);
}
```

https://github.com/bro/bro-osquery

Broker: Next Steps

- Collect experience
- Add higher-level cluster abstractions
- Asynchronous script functions (maybe …)

Begin Modernizing Code Base

- New I/O loop
- Investigate replacing regexp library
- Remove old communication & serialization
- Investigate replacing manual memory mgmt
- Adapt newer C++ features