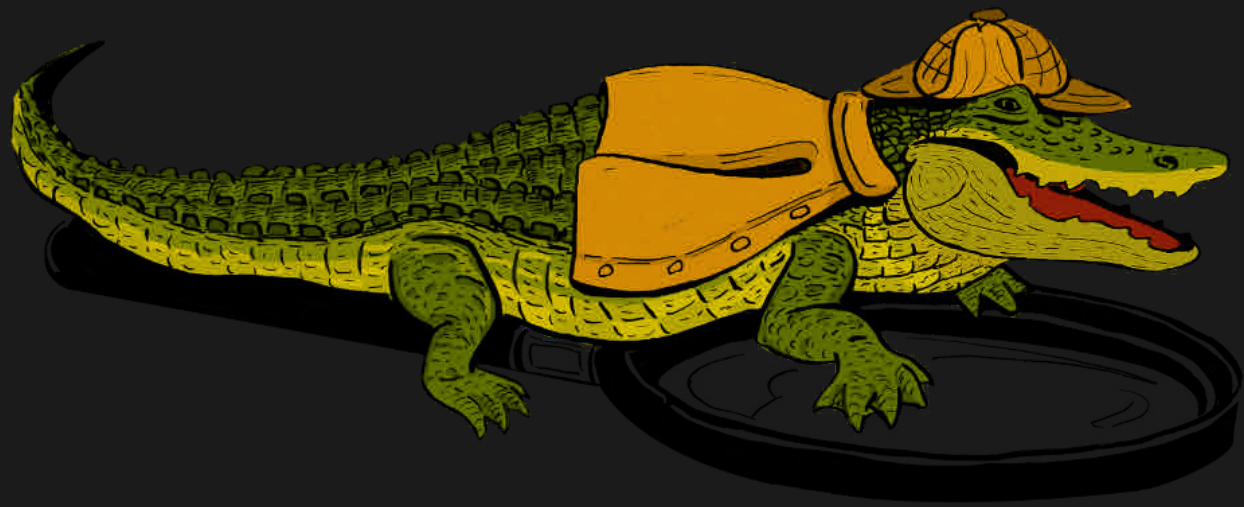
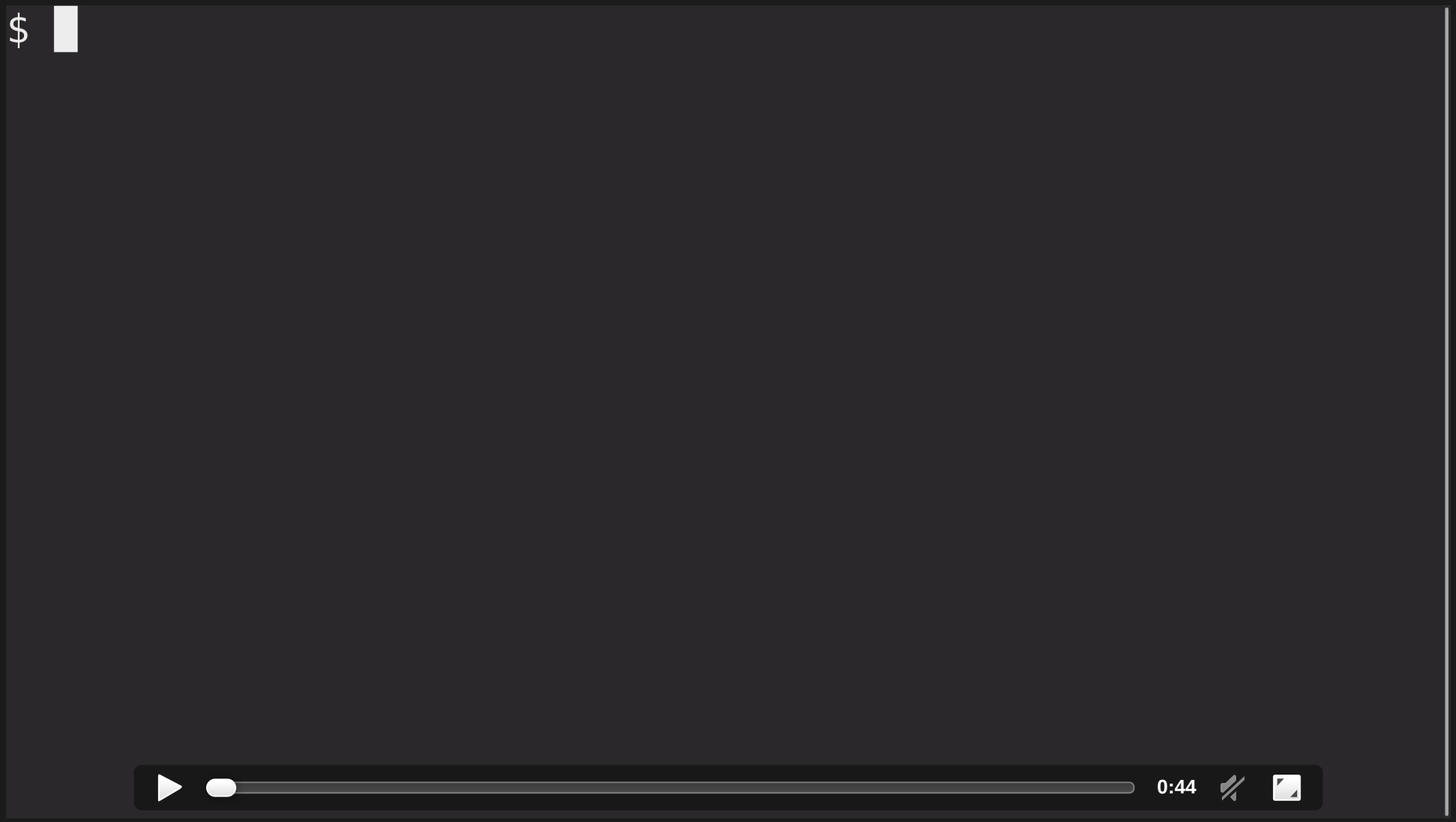
Mozilla InvestiGator



Investigate 1,000 endpoints in 10s from the command line

slides at mig.ninja/rmllsec16

Real-Time systems investigation



AUG
1
2014

MDN Database Disclosure

Stormy

We have just concluded an investigation into a disclosure affecting members of M
Developer Network. We began investigating the incident as soon as we learned of
disclosure. The issue came to light ten days ago when one of our web developers
discovered that, starting on about June 23, for a period of 30 days, a data sanitizati
process of the Mozilla Developer Network (MDN) site database had been failing, re
the accidental disclosure of MDN email addresses of about 76,000 users and encry
passwords of about 4,000 users on a publicly accessible server. As soon as we lear
the database dump file was removed from the server im

Mozilla says hacker compromised Bugzilla an used stolen 'security-sensitive' info to attack Firefox users

EMIL PROTALINSKI SEPTEMBER 4, 2015 9:42 AM

TAGS: BUGZILLA, FIREFOX, MOZILLA FIREFOX, MOZILLA FOUNDATION

SEP

oving Security for Bugzilla

a major part of how we accomplish our mission of openness at
inating among our many contributors, and a focal point for
hile most information in Bugzilla is public, Bugzilla restricts
information, so that only certain privileged users can access it.

penness that we are disclosing today that someone was able to

Mozilla Cloud Services

Engineering the information superhighway

APR
9
2016

Stolen Passwords Used to Break into Firefox Accounts

Mark Mayo

We recently discovered a pattern of suspicious logins to Firefox Accounts. It appears t
attacker with access to passwords from data breaches at other websites has been
attempting to use those passwords to log into users' Firefox Accounts. In some cases

Goal #1: Detecting IOCs

```
<indicatoritem id="1f3aff31-1155-4003-968c-40e5bd11e46e" condition="i
    <context document="FileItem" search="FileItem/Md5sum" type="mir">
    <content type="md5">3ce55c6994101faec00b5b7c2fee494f</content>
</context></indicatoritem>
```

Is that botnet IP connected anywhere?

Goal #2: covering the small mistakes

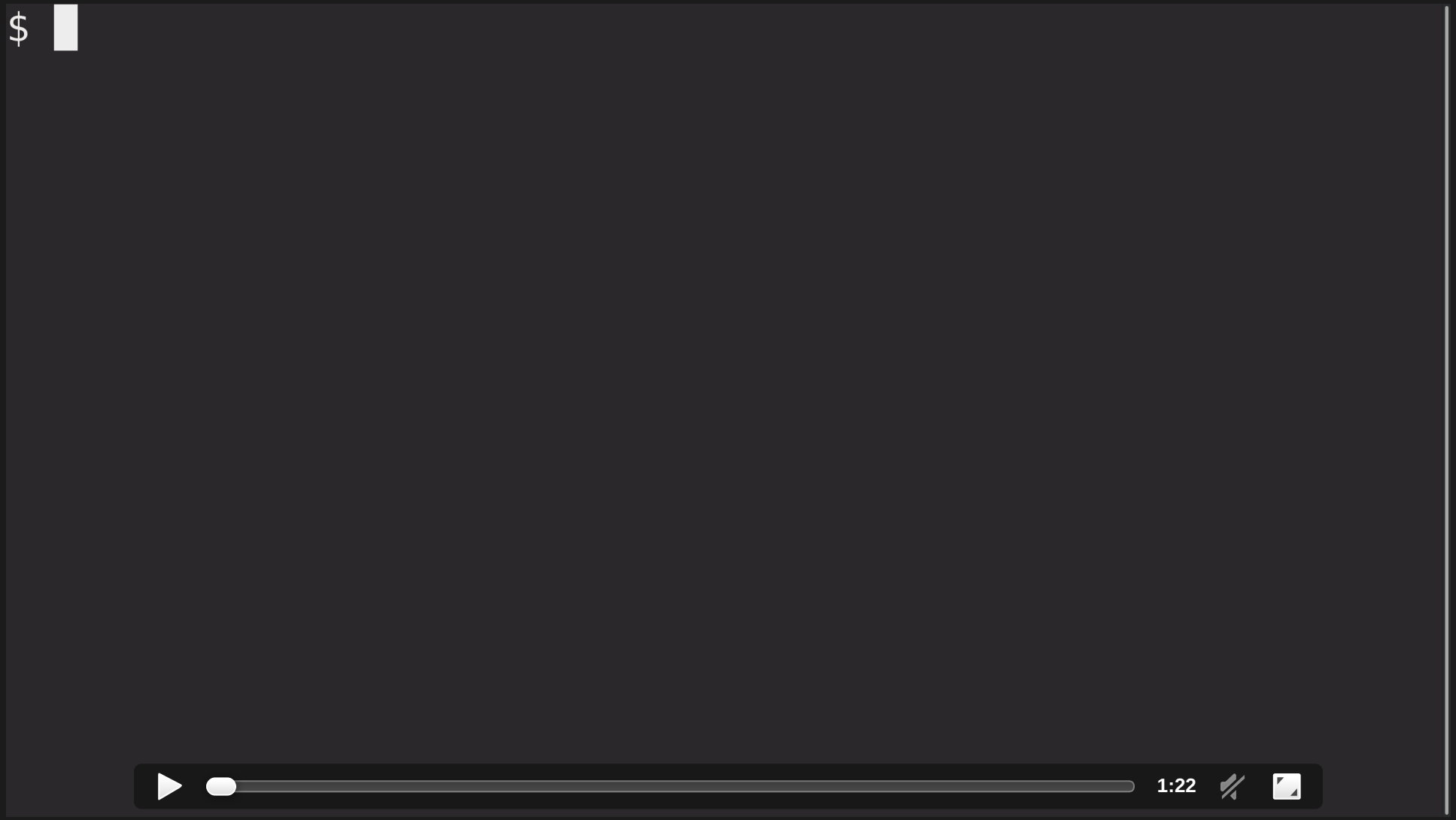
git commit -a . && git push github master

3 lines (3 sloc) | 0.119 kb — Raw | Blame | History

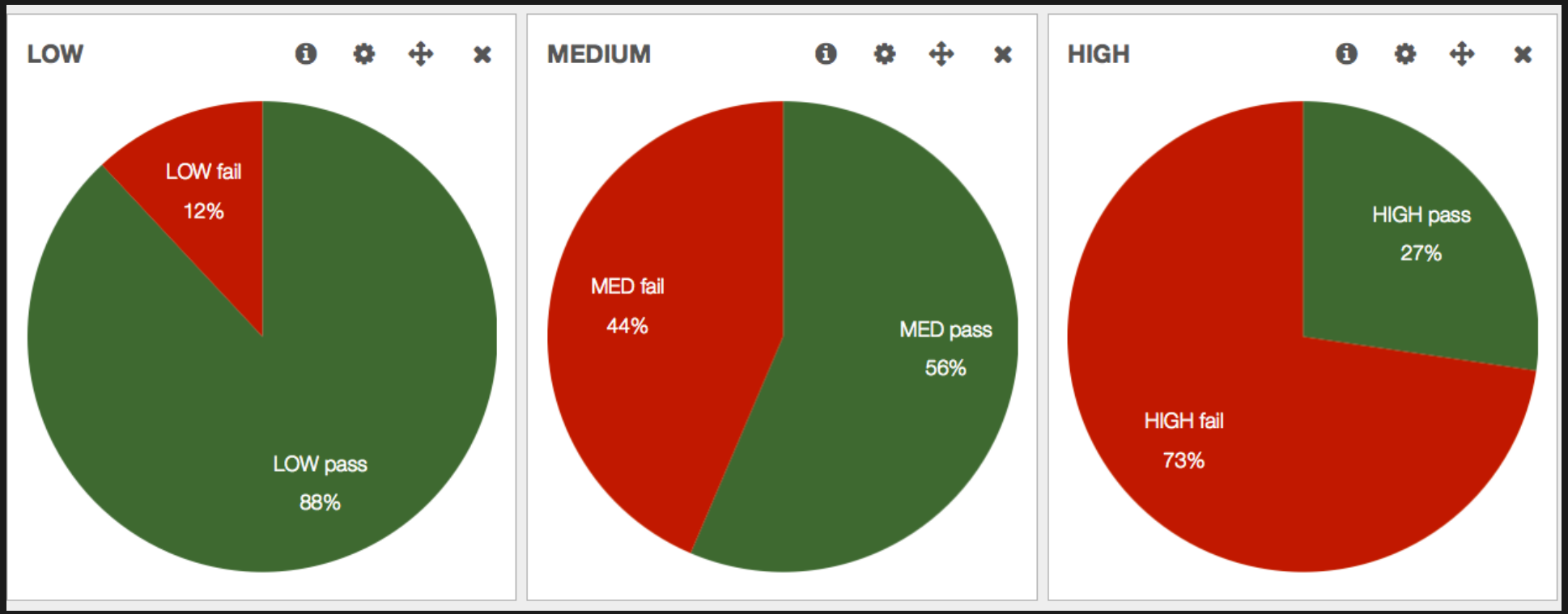
```
1  [Credentials]
2  aws_access_key_id = AKIAI
3  aws_secret_access_key = /                                    Gev6
```

$ mig file -path / -name "^\.boto$" -content "abcdef123456"

Got any private keys in those home folders?



Goal #3: Measuring security compliance



```
{
    "module": "file",
    "parameters": {
        "searches": {
            "checkforverboselogging": {
                "paths": [
                    "/etc/ssh/sshd_config"
                ],
                "contents": [
                    "(?i)^loglevel verbose$"
                ]
            },
            "checkpasswordusageisoff": {
                "paths": [
                    "/etc/ssh/sshd_config"
                ],
                "contents": [
                    "(?i)^passwordauthentication no$"
                ]
            }
        }
    }
}
```

Mozilla's startup mindset

- Experiment & fail fast
- Minimalistic centralization
- Everyone can write and host a website...
- ...sometimes using operational standards

Incident Response at Mozilla

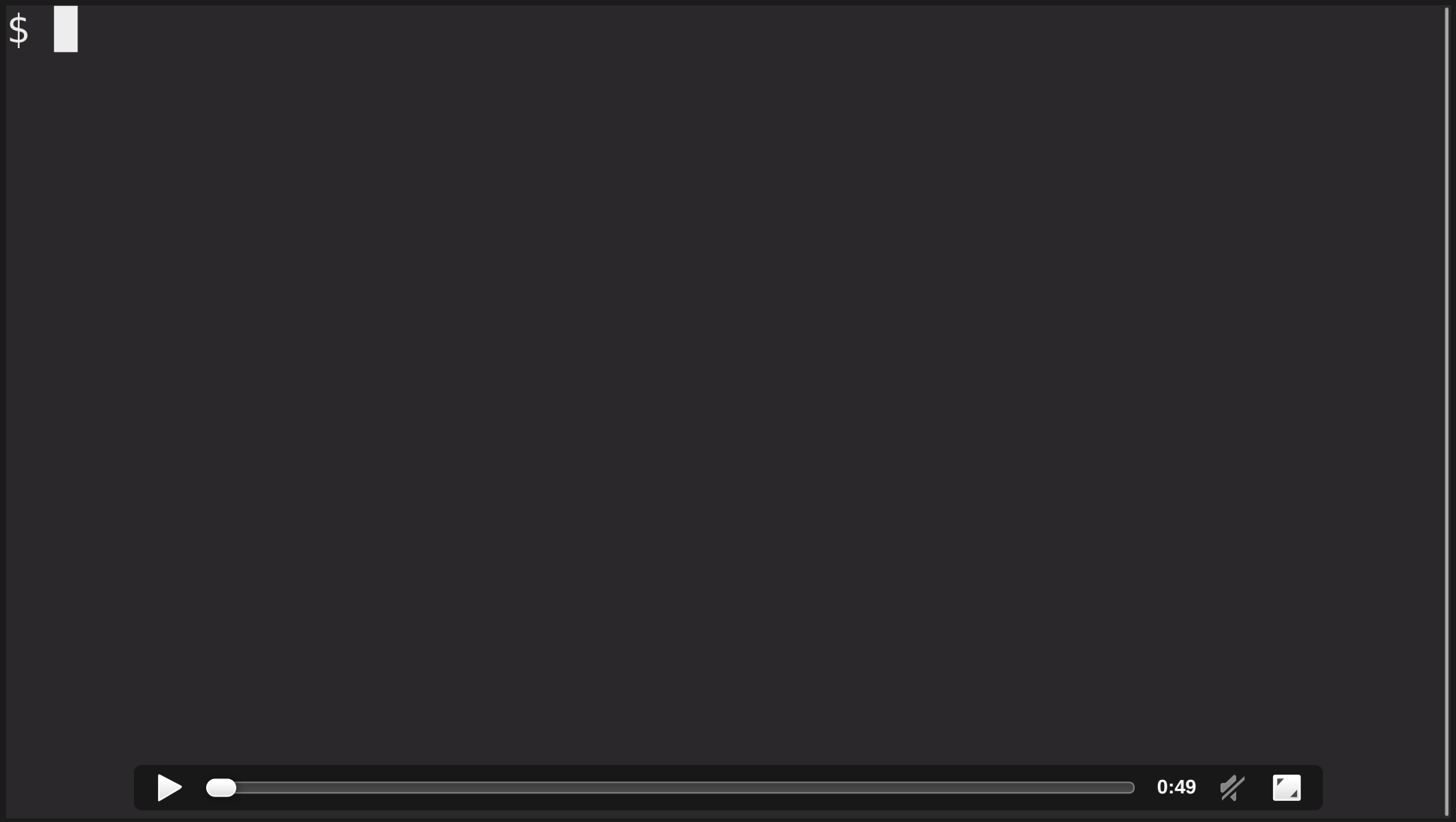
Security at the perimeter does not work

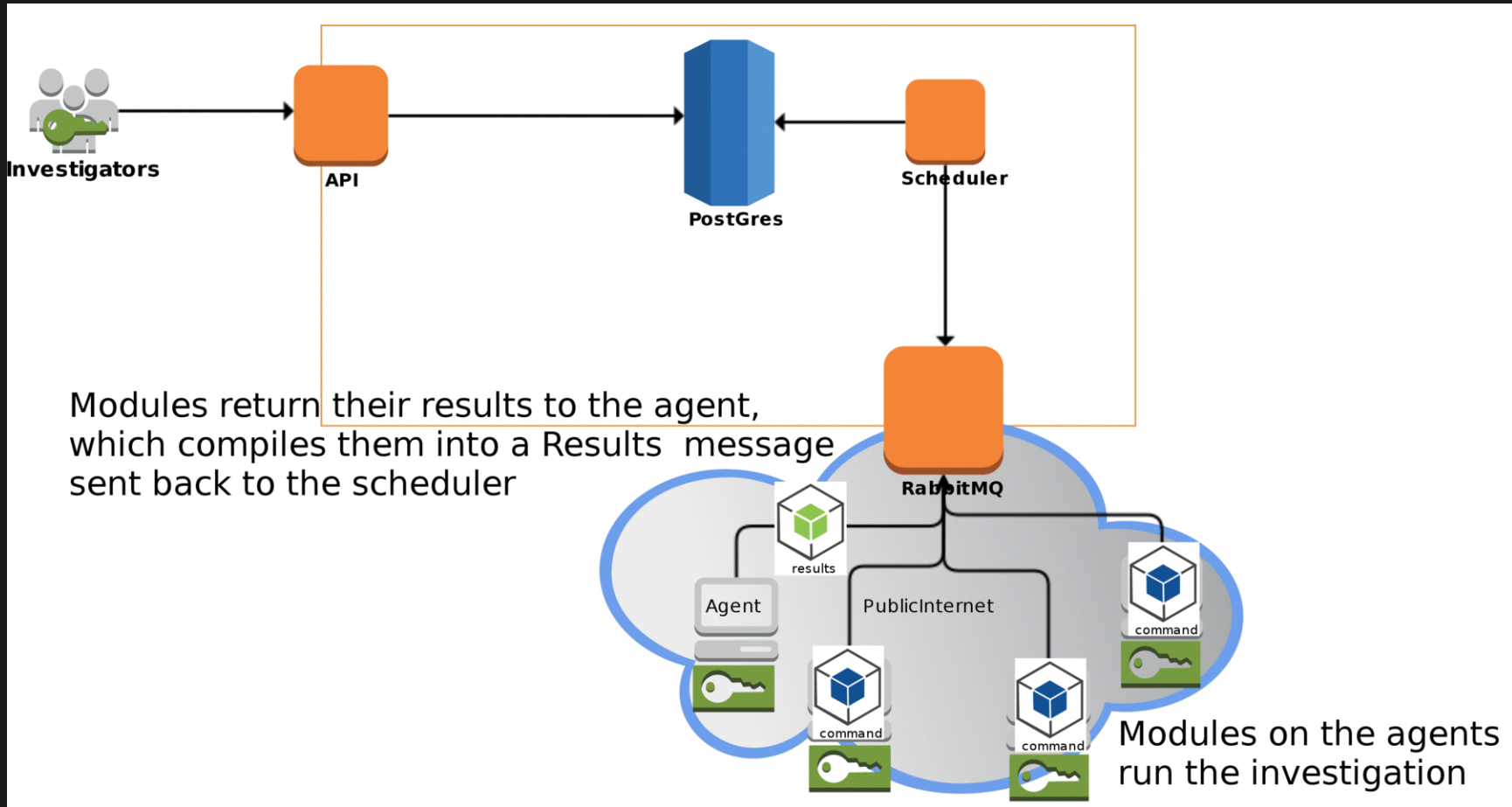
When your infrastructure lives all over the internet

MIG's core principles

- Fast & Massively Distributed investigations.
- Simple to deploy across all operating systems.
- Strong Security! All actions are signed and recorded.
- Do not retrieve raw data, respect Privacy.

Scan processes memories for a regex





Modules return their results to the agent, which compiles them into a Results message sent back to the scheduler

Modules on the agents run the investigation

What else can you do?

Find which machines have a specific USB device connected

```
mig file -matchany -path /sys/devices/ -name "^uevent$" \
-content "PRODUCT=20a0/4107"
```

Locating a device by its mac address

```
mig netstat -nm 8c:70:5a:c8:be:50
```

List endpoints that cannot ping a destination

```
mig ping -t "name LIKE '%scl3%'" -show notfound \
-d 10.22.75.57 -p icmp
```

Find endpoints running ElasticSearch

```
mig file -path /proc -name "^cmdline$" -maxdepth 2 \
-content "[e]lasticsearch"
```

Writing actions by hand is easy

```
{
  "name": "Shellshock IOCs (nginx and more)",
  "target": "environment->>'os' IN ('linux','darwin') AND mode='daemo
  "operations": [
    {
      "module": "file",
      "parameters": {
        "searches": {
          "iocs": {
            "paths": [
              "/usr/bin",
              "/usr/sbin",
              "/bin",
              "/sbin",
              "/tmp",
              "/var/tmp"
            ],
            "sha256": [
              "73b0d95541c84965fa42c3e257bb349957b3be626dec9d55efcc6e
              "ae3b4f296957ee0a208003569647f04e585775be1f3992921af996
              "2d3e0be24ef668b85ed48e81ebb50dce50612fb8dce96879f80306
              "2ff32fcfee5088b14ce6c96ccb47315d7172135b999767296682c3
              "1f5f14853819800e740d43c4919cc0cbb889d182cc213b0954251e
              "2bc9a2f7374308d9bb97b8d116177d53eaca060b562f6f66f5dd1a
            ],
            "contents": [
```

```
contents": [

 "/bin/busybox;echo -e '\\\\147\\\\141\\\\171\\\\146\\\\
 "legend rocks"
```

The faster we run investigations, the more we will investigate.

- bob left the company, did we revoke all his accesses?
- massive libstuff1 vulnerability, is it used anywhere?
- found IP 13.37.66.66 brute forcing the VPN, check other nodes to see if it's connected
- jean-kevin put some AWS key on pastebin, is it configured anywhere?
- anyone remembers that weird host that was running an anonymous proxy?

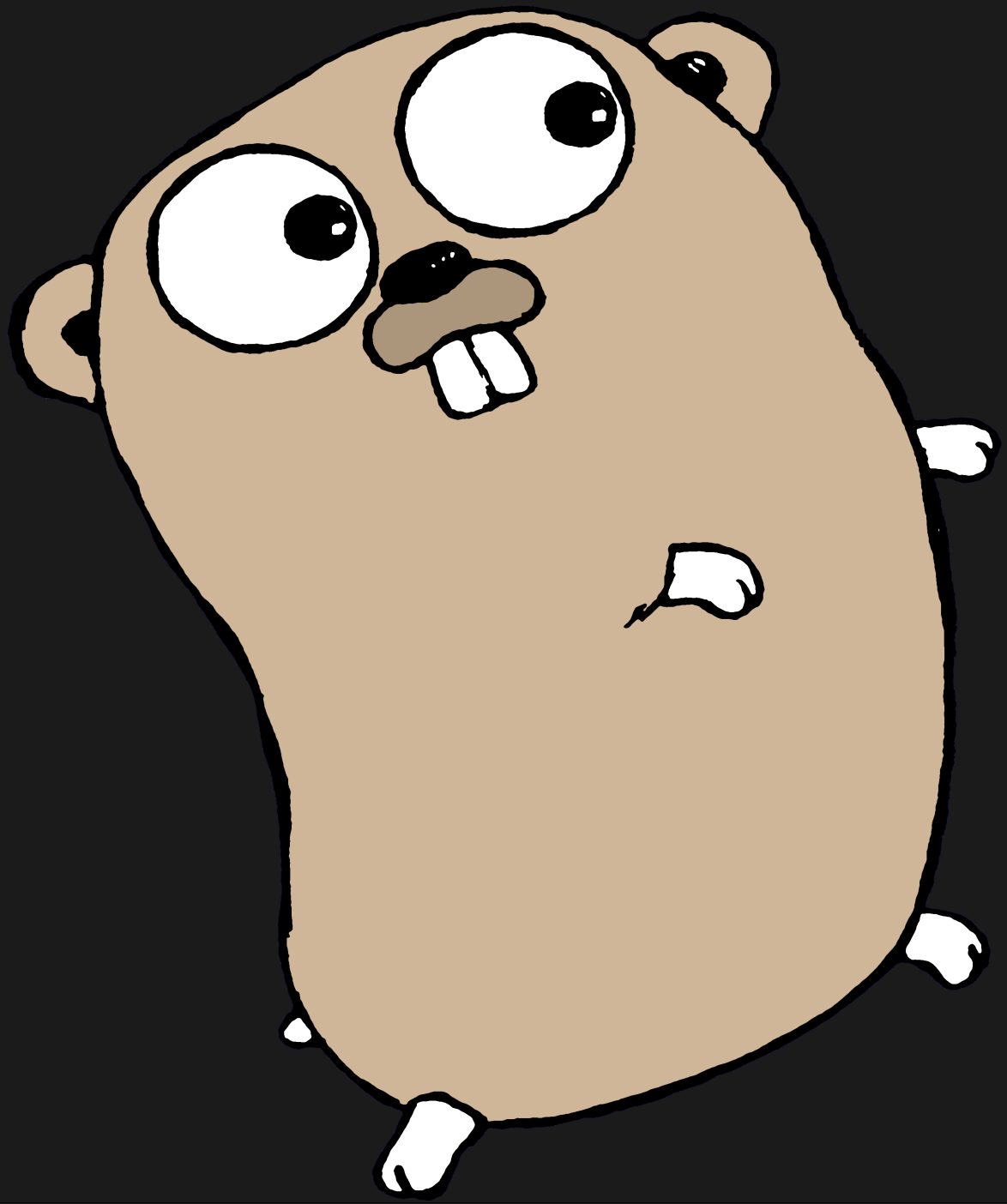
Internals

Go is Great!

Pleasant language to use, static typing catches most errors.

Compiles to a single static binary, no dependencies.

Configuration is built-in or deployed via provisioning.



Security of the Agent

Agent only runs something if these conditions are met:

1. action has valid PGP signatures
2. issued by trusted investigators
3. with ACL accesses to a given module

multiple signatures required to run sensitive modules

Agent ACLs

The weights of each investigator providing a valid signature are summed, and if the total weight is equal or higher than the minimum weight, the operation is considered valid.

```
TotalWeight = Weight[Alice} + Weight[Bob]
if TotalWeight >= MinimumWeight { run module }
```

Mozilla/Scribe: Revisiting Vulnerability Management

```
{  "objects": [ {
            "object": "libnss3-package",
            "package": {
                "name": "libnss3:amd64"
            }
        }
    ],
    "tests": [ {
            "test": "libnss3 test",
            "object": "libnss3-package",
            "evr": {
                "operation": "<",
                "value": "2:3.19.2"
            }
        }
    ]
}
```

Scribe finds bad packages

A vulnerability database, such as Ubuntu USN, or OpenVAS NVT, is converted into a JSON Scribe policy.

Each MIG Agent runs the thousands of tests from the policy locally, and returns out-of-date package.

https://github.com/mozilla/mig/tree/master/actions/scribe

The Future: MIG 1.0

1.0

Edit Milestone | New issue

Due by December 31, 2016 **0%** complete

This is MIG 1.0. The real deal!

7 Open ✓ 0 Closed

Create an API endpoint for agents to retrieve PGP public keys agent api easy enhancement up-for-grabs
#240 opened on 6 Jun by jvehent

Simplify API responses api client enhancement up-for-grabs
#241 opened on 6 Jun by jvehent

Replace API X-PGP-Authorization with basic tokens api enhancement up-for-grabs 2
#239 opened on 6 Jun by jvehent

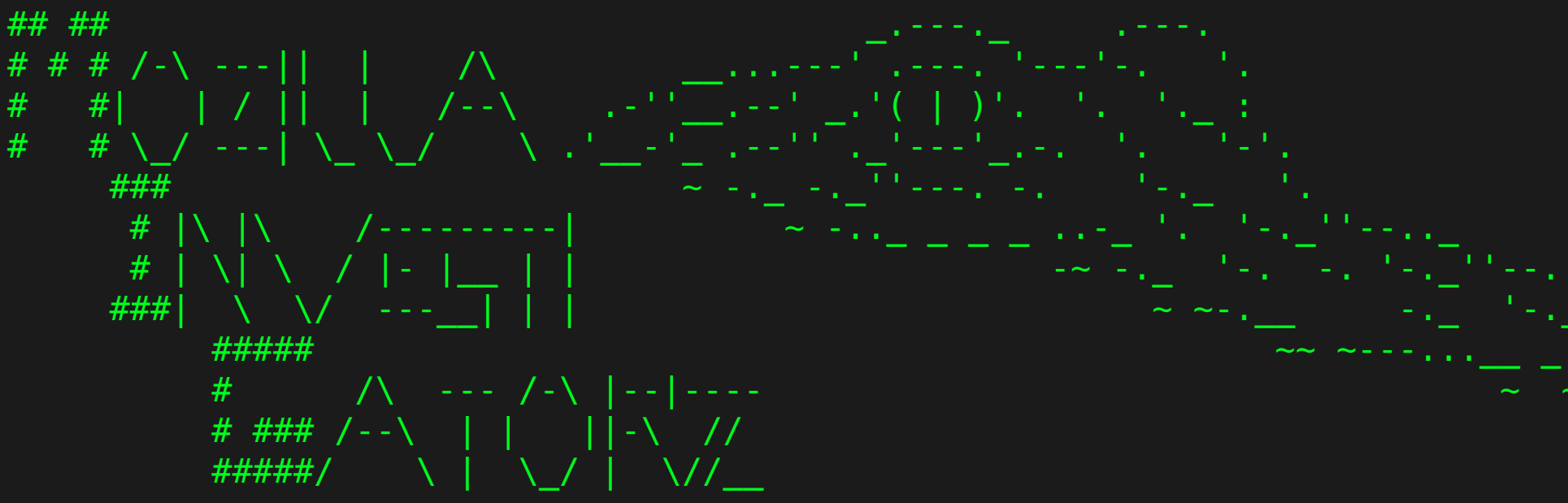
Remove RabbitMQ and scheduler agent scheduler up-for-grabs 2
#238 opened on 6 Jun by jvehent

Manage agent configuration in external configuration file agent enhancement up-for-grabs
#237 opened on 6 Jun by jvehent

Don't require ACLs in MIG Agent agent easy enhancement up-for-grabs
#236 opened on 6 Jun by jvehent

MIG 1.0 ✓ agent api client enhancement scheduler
#242 opened on 6 Jun by jvehent

Questions?



Check it out at https://mig.ninja

Link to these slides: mig.ninja/rmllsec16

Extra goodies: Visualizing results on a map