Project Argos

Christer Edwards | Adobe Salt Master

Bē
Evolution Bureau

History

Why?

Magic

Goals

Leverage existing tools and framework

Goals

Let Operations drive.

Let Security navigate.

Goals

Argos

And set a watcher upon her, great and strong Argos, who with four eyes looks every way. And the goddess stirred in him unwearying strength: sleep never fell upon his eyes; but he kept sure watch always.

- https://en.wikipedia.org/wiki/Argus_Panoptes

Components

CIS benchmarks

(https://benchmarks.cisecurity.org/)

Components

File Integrity Monitoring

(FIM)

Components

osquery : Performant Endpoint Visibility

(https://osquery.io)

Custom Salt Modules

CIS execution module

(https://github.com/cedwards/saltstack-cis-module)

Letting Ops Drive…

CIS module demo

CIS Execution Module Benefits

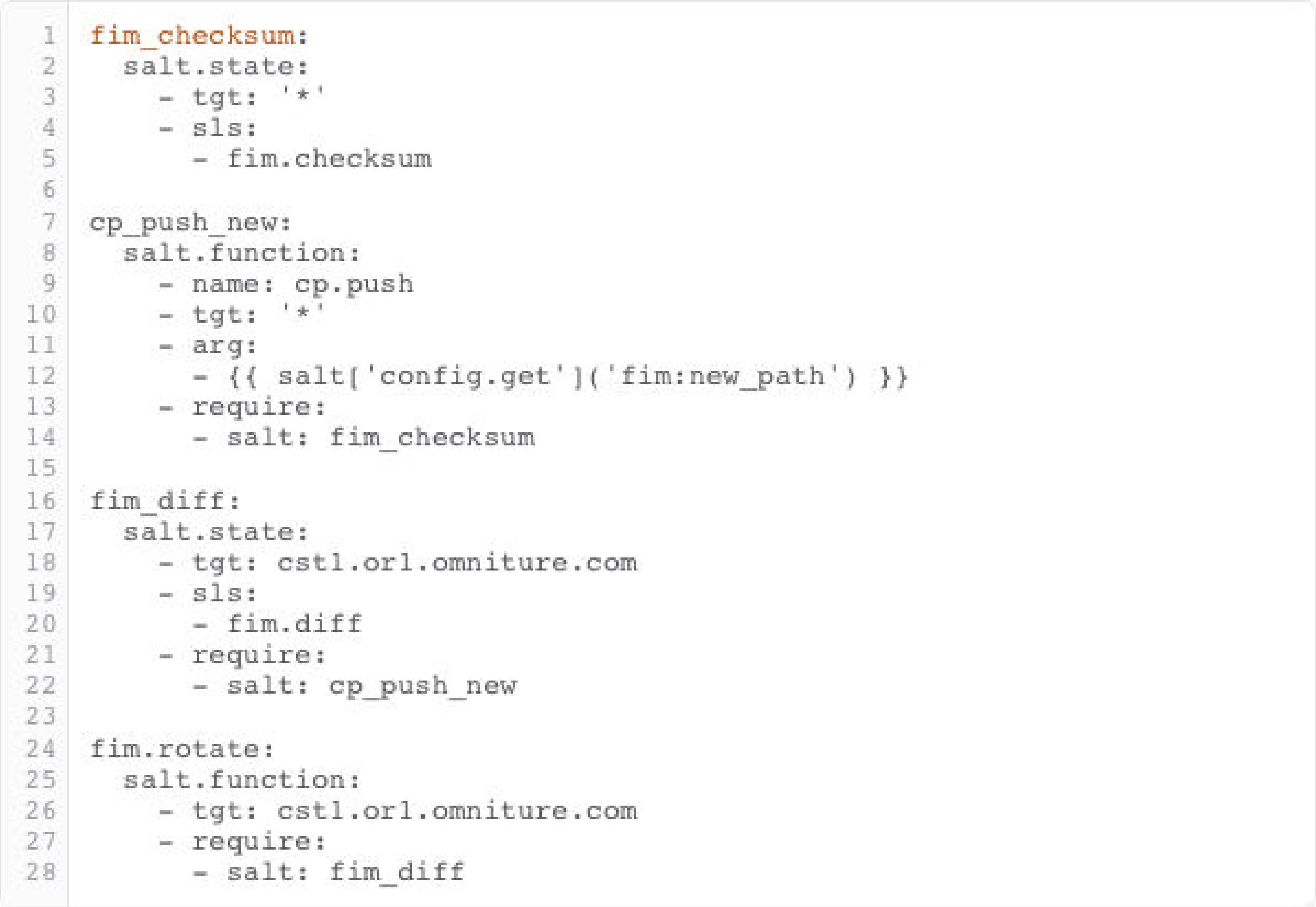
1. Fast
2. Flexible
3. Collaborative

Custom Salt Modules

FIM execution module

(https://github.com/cedwards/saltstack-fim-module)

Orchestration as Code

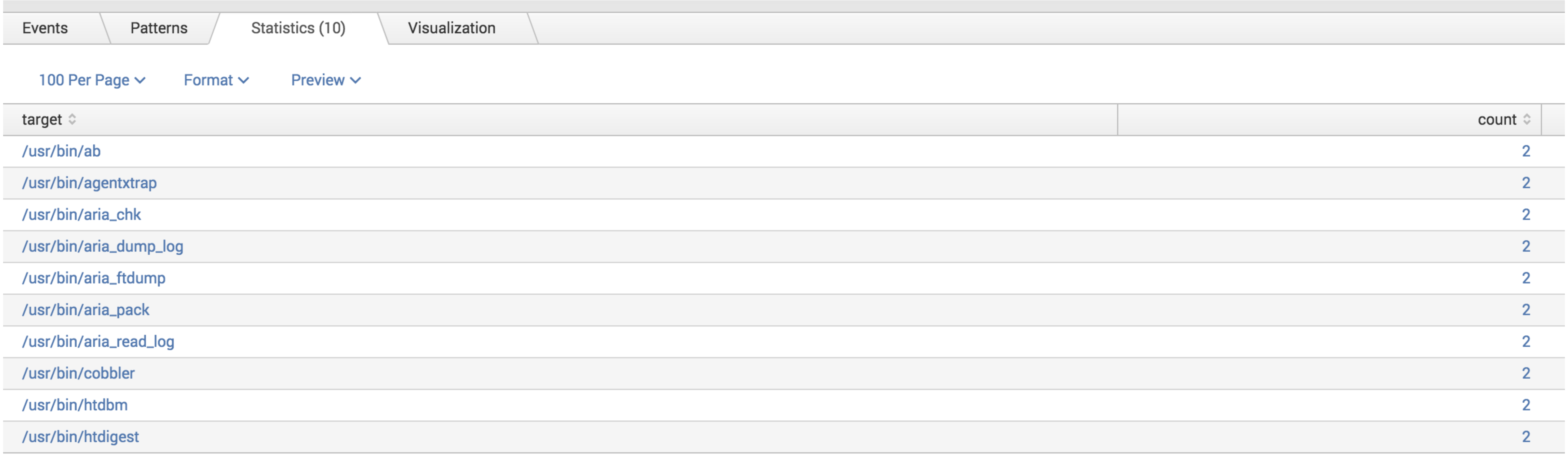


```
fim_checksum:
  salt.state:
    - tgt: '*'
    - sls:
      - fim.checksum

cp_push_new:
  salt.function:
    - name: cp.push
    - tgt: '*'
    - arg:
      - {{ salt['config.get']('fim:new_path') }}
    - require:
      - salt: fim_checksum

fim_diff:
  salt.state:
    - tgt: cstl.orl.omniture.com
    - sls:
      - fim.diff
    - require:
      - salt: cp_push_new

fim.rotate:
  salt.function:
    - tgt: cstl.orl.omniture.com
    - require:
      - salt: fim_diff
```

Deeper Insight

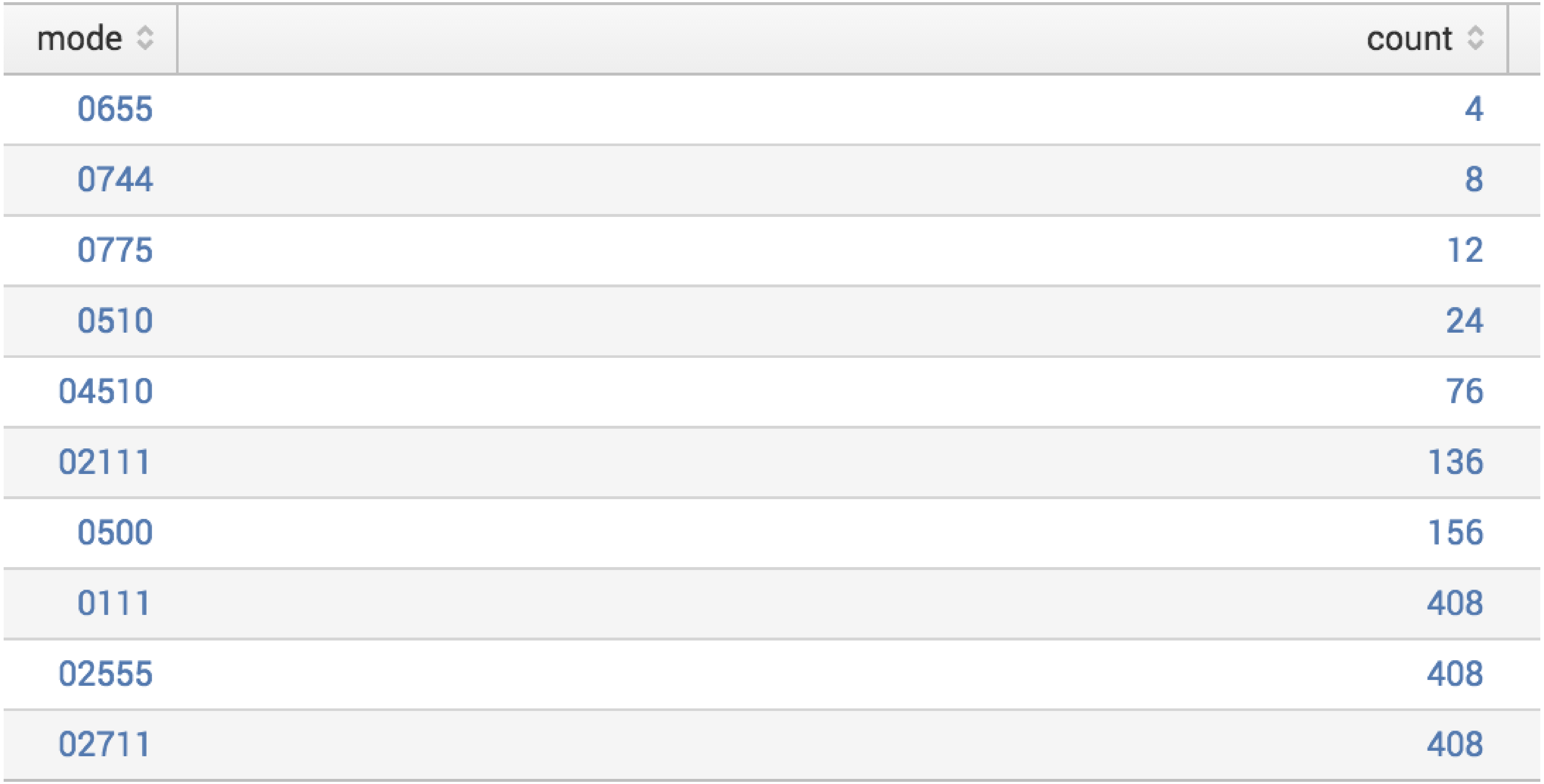
FIM module demo

Rare Targets



target	count
/usr/bin/ab	2
/usr/bin/agentxtrap	2
/usr/bin/aria_chk	2
/usr/bin/aria_dump_log	2
/usr/bin/aria_ftdump	2
/usr/bin/aria_pack	2
/usr/bin/aria_read_log	2
/usr/bin/cobbler	2
/usr/bin/htdbm	2
/usr/bin/htdigest	2

Rare Permissions



mode	count
0655	4
0744	8
0775	12
0510	24
04510	76
02111	136
0500	156
0111	408
02555	408
02711	408

Custom Salt Modules

osquery execution module

(available in 2015.8.x)

Performant Endpoint Visibility

osquery module demo

The Future

What’s coming?

Lastly…

We’re hiring!

Contact

Christer Edwards

cedwards@adobe.com

https://github.com/cedwards/

Adobe