Why?
Leverage existing tools and framework
Goals

Let Operations drive.
Let Security navigate.
Goals

COMPLY

WITH ALL THE THINGS!

meme generator.net
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.

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

File Integrity Monitoring (FIM)
osquery : Performant Endpoint Visibility
(https://osquery.io)
Custom Salt Modules

CIS execution module
(https://github.com/cedwards/saltstack-cis-module)
CIS module demo
CIS Execution Module Benefits

1. Fast
2. Flexible
3. Collaborative
FIM execution module
(https://github.com/cedwards/saltstack-fim-module)
Orchestration as Code

```plaintext
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: csl1.orl1.omniture.com
    - sls:
        - fim.diff
    - require:
        - salt: cp_push_new

fim.rotate:
salt.function:
    - tgt: csl1.orl1.omniture.com
    - require:
        - salt: fim_diff
```
FIM module demo
<table>
<thead>
<tr>
<th>target</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>/usr/bin/ab</td>
<td>2</td>
</tr>
<tr>
<td>/usr/bin/agentxtrap</td>
<td>2</td>
</tr>
<tr>
<td>/usr/bin/aria_chk</td>
<td>2</td>
</tr>
<tr>
<td>/usr/bin/aria_dump_log</td>
<td>2</td>
</tr>
<tr>
<td>/usr/bin/aria_fddump</td>
<td>2</td>
</tr>
<tr>
<td>/usr/bin/aria_pack</td>
<td>2</td>
</tr>
<tr>
<td>/usr/bin/aria_read_log</td>
<td>2</td>
</tr>
<tr>
<td>/usr/bin/cobbler</td>
<td>2</td>
</tr>
<tr>
<td>/usr/bin/htdocs</td>
<td>2</td>
</tr>
<tr>
<td>/usr/bin/htdigest</td>
<td>2</td>
</tr>
</tbody>
</table>
# Rare Permissions

<table>
<thead>
<tr>
<th>mode</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0655</td>
<td>4</td>
</tr>
<tr>
<td>0744</td>
<td>8</td>
</tr>
<tr>
<td>0775</td>
<td>12</td>
</tr>
<tr>
<td>0510</td>
<td>24</td>
</tr>
<tr>
<td>04510</td>
<td>76</td>
</tr>
<tr>
<td>02111</td>
<td>136</td>
</tr>
<tr>
<td>0500</td>
<td>156</td>
</tr>
<tr>
<td>0111</td>
<td>408</td>
</tr>
<tr>
<td>02555</td>
<td>408</td>
</tr>
<tr>
<td>02711</td>
<td>408</td>
</tr>
</tbody>
</table>
Custom Salt Modules

osquery execution module
(available in 2015.8.x)
osquery module demo
What’s coming?
Lastly…

We’re hiring!
Contact

Christer Edwards
cedwards@adobe.com

https://github.com/cedwards/