Merou
A decentralised audit framework
Luke Faraone
Dropbox
What is it?

authorisation service

open source

decentralised

audited
Before we continue...
Interns, man.
Naming is hard
A decentralised audit framework

Luke Faraone
Dropbox
Why does it matter?

Granularity
Usable software means users won't hate interacting with it.

Scalability
Reduces choke-points, removes central teams from the critical path

Visibility
Membership and access control are all in one place
Why does it matter?
"Who gave a sales engineer access to prod?!"
"OK, fine, we'll implement a process"
In the beginning...

Request for production access

* Required

Username *

Your answer

What type of access do you require *

- Production access to a specific set of machines
- Puppet Access
- Amazon Shell Access
- Production Root Access
- Other:

Why do you need access? *

Your answer
Which, quickly we realised...

Effort
Approval and actioning tracked manually

SPOF
Small number of approvers / actioners
Which, quickly we realised...

Automation???
What, are we going to write Google Apps Script?

Truth?
How is access reviewed?
Let's do a little more work...
Access Requests

Username: 
Reason: 

Additional Instructions:

Requested By: 
Requested At: 2014-08-29

Production Shell Access
- Datacenter: both
- Machine Groups: all
- Last Approver Change: 2014-08-29
- Approver: 
- Last Actioner Change: 2014-08-29
- Actioner: 

Sudoers
- Sudo User: root
- Group (if known): 
- Group (if not present): 
- Last Approver Change: 2014-08-29 05:22 PM
- Approver: 
- Last Actioner Change: 2014-08-29 05:40 PM
- Actioner: 

Nagios (Thruk)
- Last Approver Change: 2014-08-29
- Approver: 
- Last Actioner Change: 2014-08-29
- Actioner: 

actioned
Small improvements...
Automation
Report generation
What we quickly realized...

Teams of users often need the same set of permissions
Teams often share a core set of permissions
flanket

Solution: Templates?
### Users

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:travis_ci@svec.localhost">travis_ci@svec.localhost</a></td>
<td>np-owner</td>
</tr>
<tr>
<td>audit-managers</td>
<td>np-owner</td>
</tr>
<tr>
<td>storage-team</td>
<td>owner</td>
</tr>
</tbody>
</table>

### Public Keys

<table>
<thead>
<tr>
<th>Age</th>
<th>Type</th>
<th>Size</th>
<th>Fingerprint</th>
</tr>
</thead>
</table>

### Permissions

<table>
<thead>
<tr>
<th>Permission</th>
<th>Argument</th>
<th>From Group</th>
<th>Granted</th>
</tr>
</thead>
<tbody>
<tr>
<td>production.shell</td>
<td>hwrole=magic_pocket</td>
<td>storage-team</td>
<td>40 minutes ago</td>
</tr>
</tbody>
</table>

### Access Tokens

<table>
<thead>
<tr>
<th>Name</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyFirstAccessToken</td>
<td>55 minutes ago</td>
</tr>
</tbody>
</table>

### Shell

<table>
<thead>
<tr>
<th>Name</th>
<th>Shell</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>/bin/false</td>
</tr>
</tbody>
</table>

### Passwords

<table>
<thead>
<tr>
<th>Name</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>LegacySvc1</td>
<td>55 minutes ago</td>
</tr>
</tbody>
</table>

### Recent Activity

<table>
<thead>
<tr>
<th>Date</th>
<th>Actor</th>
<th>Action</th>
<th>Description</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Distributed management of groups, permissions, and permission grants
Distributed management

Securely?
Transparent record of activity

<table>
<thead>
<tr>
<th>Date</th>
<th>Actor</th>
<th>Action</th>
<th>Description</th>
<th>Extra</th>
</tr>
</thead>
</table>
| 2016-07-05 05:45 PM | harb@dropbox.com | grant_permission | Granted permission with argument: blahblahback | Group: 🚀 group1  
Permission: ⚙ grouper.admin.permissions |
"Who gave a sales engineer access to prod?!"
"Why does that sales engineer *still* have access to prod?!"
Distributed auditing
Permissions can be marked as *audited*.
Permissions can be marked as *audited*.

Groups that have been granted audited permissions become **audited groups**.
Permissions can be marked as *audited*.

Groups that have been granted audited permissions become **audited groups**.
Permissions can be marked as audited.

Groups that have been granted audited permissions become audited groups.

Owners of audited groups first undergo audit training.
Submitting this form will create a new global audit. This will start new reviews for all audited groups.

**Ends At**  
06/06/2017

Set the above date to be the due date for the audit. Users will receive email notifications immediately, and will periodically receive updates about the state of their groups and work they need to do.

**ONLY DO THIS IF YOU ARE VERY SURE.**

Yes, Start Global Audit
Audit Group

Your group has an outstanding audit that needs to be completed before **2017-06-05 05:00 PM**, giving you 13 days to complete the audit.

<table>
<thead>
<tr>
<th>Member</th>
<th>role</th>
<th>Audit Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:admin@example.com">admin@example.com</a></td>
<td>owner</td>
<td>approved</td>
</tr>
<tr>
<td><a href="mailto:alice@example.com">alice@example.com</a></td>
<td>member</td>
<td>pending</td>
</tr>
<tr>
<td><a href="mailto:jacob@example.com">jacob@example.com</a></td>
<td>np-owner</td>
<td>pending</td>
</tr>
<tr>
<td><a href="mailto:lisa@example.com">lisa@example.com</a></td>
<td>member</td>
<td>pending</td>
</tr>
<tr>
<td><a href="mailto:luke_wf@example.com">luke_wf@example.com</a></td>
<td>member</td>
<td>pending</td>
</tr>
</tbody>
</table>

[Complete Audit]
## Recent Activity

<table>
<thead>
<tr>
<th>Date</th>
<th>Actor</th>
<th>Action</th>
<th>Description</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-10-21 01:10 PM</td>
<td>@<a href="mailto:herb@dropbox.com">herb@dropbox.com</a></td>
<td>complete_audit</td>
<td>Completed group audit.</td>
<td>Group: disabled_group1</td>
</tr>
<tr>
<td>2016-10-21 11:50 AM</td>
<td>@<a href="mailto:herb@dropbox.com">herb@dropbox.com</a></td>
<td>start_audit</td>
<td>Started global audit.</td>
<td></td>
</tr>
</tbody>
</table>

## Group

<table>
<thead>
<tr>
<th>Group</th>
<th>Started</th>
<th>Ends</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>🦄 aws.billing</td>
<td>2016-10-21 11:50 AM</td>
<td>1 month</td>
<td>in progress</td>
</tr>
<tr>
<td>🦄 securityauditors</td>
<td>2016-10-21 11:50 AM</td>
<td>1 month</td>
<td>in progress</td>
</tr>
</tbody>
</table>
(content cut for time)
Takeaways
Merou!

Transparency and democracy work
... when paired with process and tools.

Let other people do your work for you
... but make their jobs' easy.
Thanks for listening!

*Epinephelus malabaricus*, a.k.a. the **Malabar Grouper**
(Image: Jon Hanson from London, UK; [CC-BY-SA 2.0](https://creativecommons.org/licenses/by-sa/2.0/))

[github.com/dropbox/merou](https://github.com/dropbox/merou)
luke@dropbox.com