aws

COMMUNITY DAY

AOTEAROA

aws

COMMUNITY DAY

AOTEAROA

AWS Security Faux Pas

Blaise St-Laurent | Sept 2023

Who am I?

- Director of Cloud Security, team of 8
- 25 years in the security field
- Came from a network security background
- Cloud agnostic, but primarily AWS and Azure focused
- Have worked in many sectors, Govt, ICS, Financial, Telco

ZX Security – What we do

- Web based security testing (API, website etc)
- Internal and external penetration testing
- Specialist work (hardware, red team, physical access)
- Security design and architecture reviews
- vCISO, SLT security advice and consulting
- And of course, cloud security reviews

All this results in a wide range of customers that all are looking to Cloud for very different reasons. All these types of engagements can have a cloud component.

aws

COMMUNITY DAY

AOTEAROA

Security in a nutshell

- CIA Triad
  - Confidentiality – Not disclosing your customers’ data
  - Integrity – not allowing your customer’s data to be changed
  - Availability – Ensuring everyone who is allowed to can get to the data.
- Identity as the primary gate and source of truth about a person
  - Authentication
  - Metadata about the identity
  - Types of identities
    - Public!
    - Users
    - Non-human users / identities
- Access control – what the identities can do
- Audit – how do you know you’ve got a problem
- Defence in depth – security is like an ogre.

AWS Security – Across our customer base:

- AWS is its own world, not just a handy alternative to VMWare
- Lots of “failed” first attempts
- Control Tower has taken hold, we see about 50% of the accounts using it
- DevOps is driving a lot of excitement
  - Infrastructure as Code is a thing now, with AWS more popular than other clouds
  - Cloud Dev Kit is driving development
- Serverless is sexy but scary, still being digested as a concept

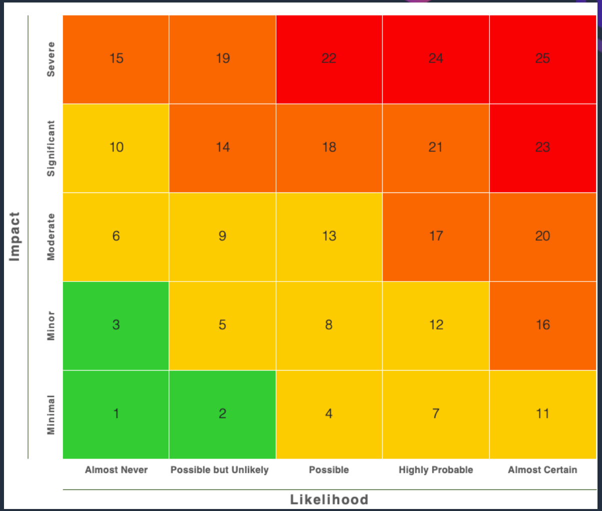
aws
COMMUNITY DAY
AOTEAROA

Impact and Likelihood for non-security people

Impact: The effect exploiting the vulnerability will have on the environment
Likelihood: The relative chance that an attacker will be able to exploit the vulnerability

Risk = Impact X likelihood (kinda)

Assumptions:
Users are likely to choose poor passwords
The target is generally data, or to compromise the entire environment
Email accounts are compromisable



Impact

	Almost Never	Possible but Unlikely	Possible	Highly Probable	Almost Certain
Severe	15	19	22	24	25
Significant	10	14	18	21	23
Moderate	6	9	13	17	20
Minor	3	5	8	12	16
Minimal	1	2	4	7	11

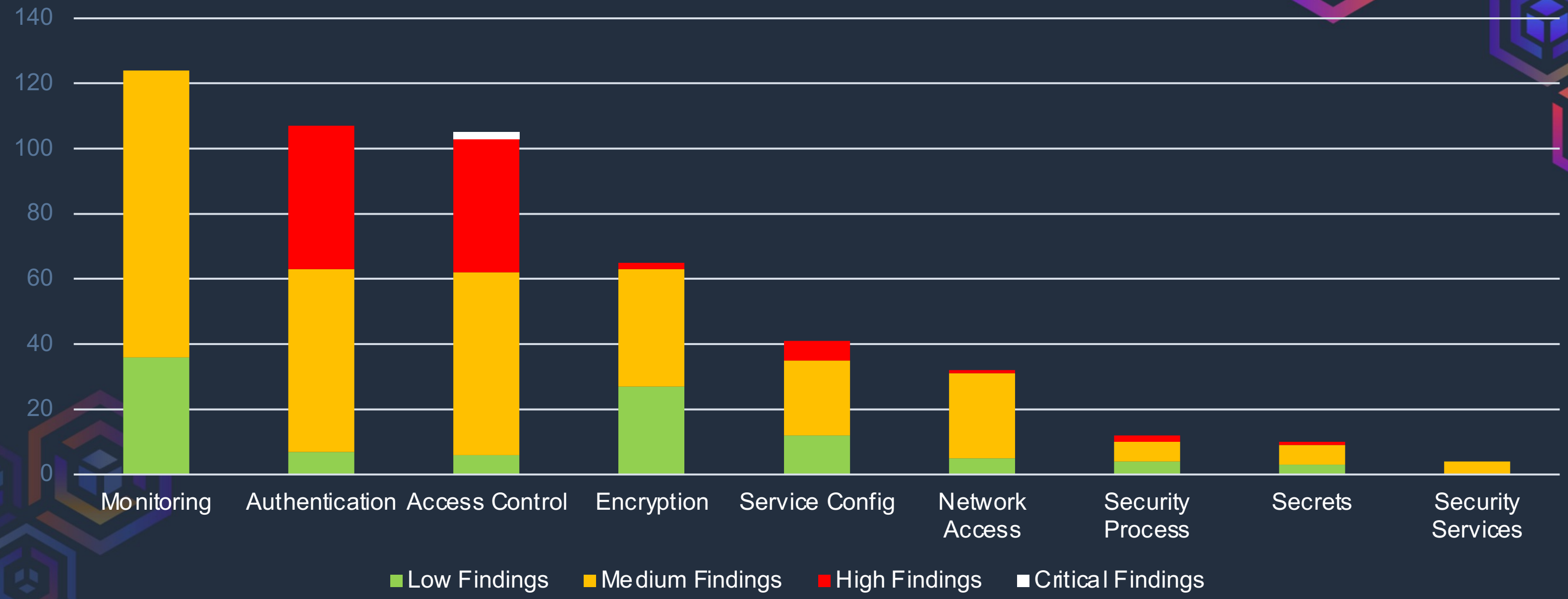
Likelihood

The Data

- The result of automated and manual testing:
  - Automated to perform reconnaissance and get the low hanging fruit
  - Manual testing / examinations to confirm and dive deeper
- Also examine any source code, externally facing resources
- Pulled from 50+ reports over the last 4 years
- ZX uses normalized findings for many common issues so we can compare across customers
- Note we are looking primarily at how common an issue is
  - Easy to pick up programmatically
  - Not a default setting

COMMUNITY DAY
AOTEAROA

Broad Trends

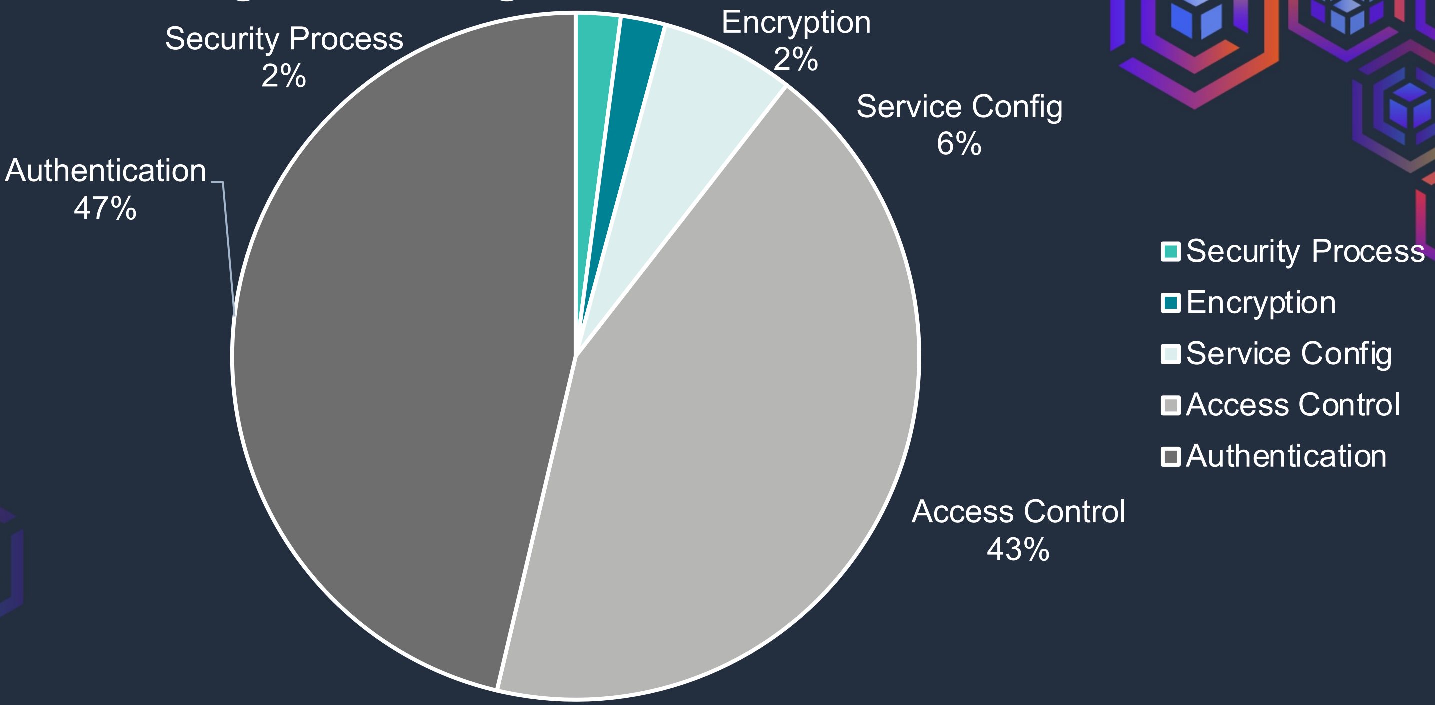


aws

COMMUNITY DAY

AOTEAROA

Breakdown of High Findings



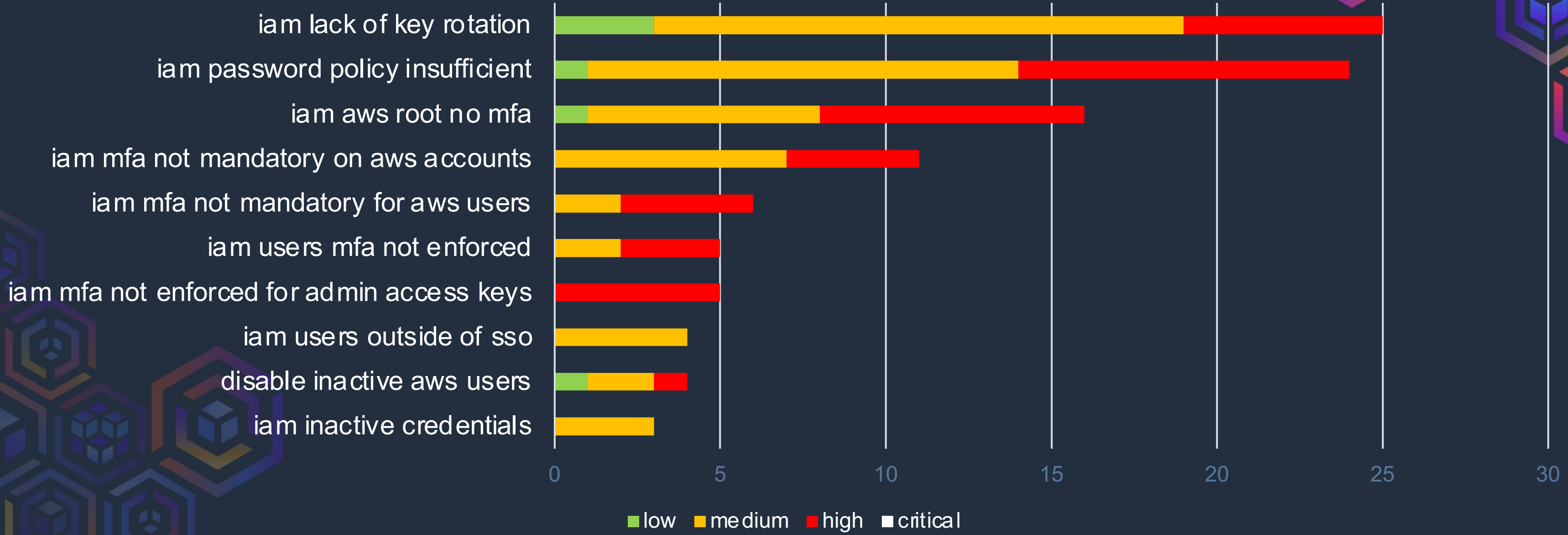
aws COMMUNITY DAY AOTEAROA

Some Notable Findings

- Critical: World writeable bucket
  - Better: it had root creds stored in a file
- Critical: Incorrect IAM configuration made root compromise on 14 ec2 servers trivial
- Super common: SSRF leads to metadata server in EC2
- Lack of key rotation (especially important on CI/CD)
  - Keys copied into github
- SNS Publishing open to public

aws COMMUNITY DAY AOTEAROA

Authentication Deep Dive

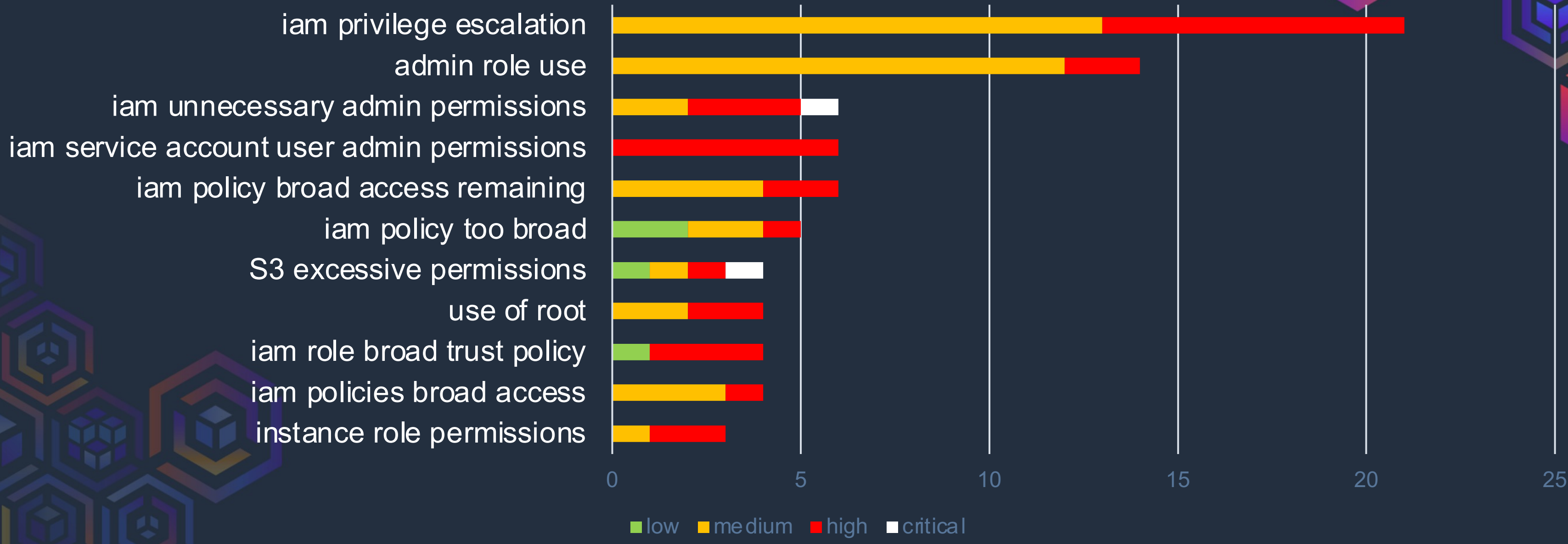


Authentication Major Risks

- Password policy
  - Over-represented thanks to NZISM / Audit / Compliance
- General account hygiene:
  - Lack of Key Rotation
  - Ancient / unused accounts
- MFA!!
  - Root accounts with either weak or no MFA
  - Users not requiring MFA for general login, even privileged accounts
  - No MFA for API / CLI access!
- IAM Identity Access Center (SSO) Included with Control Tower makes this MUCH easier

aws COMMUNITY DAY AOTEAROA

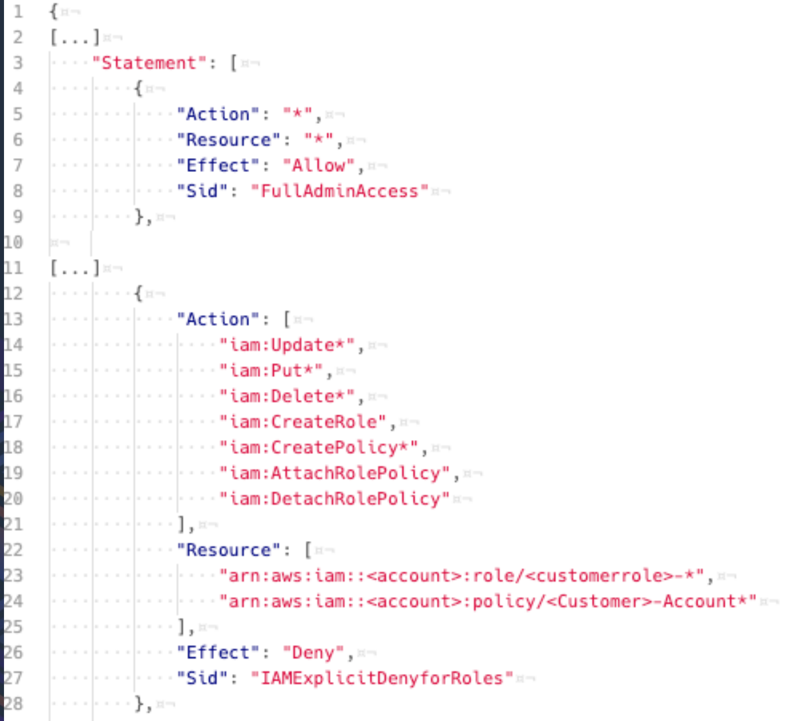
Access Control Deep Dive



Authentication Major Risks

- Privilege escalation station!
  - PassRole / AssumeRole
  - Allowing entities to modify IAM
  - CloudFormation / Lambda – services that create resources
- Policy Configuration issues:
  - NotActions
  - General Sloppiness
- Server-Side Request Forgery!
  - CapitalOne
  - Major Networking Vendor
- IAM Policy complexity – blocking Delete* doesn’t block Detach or Remove!

Defining Permissions is Hard



```
{
[...]
    "Statement": [
        {
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "FullAdminAccess"
        },

[...]
        {
            "Action": [
                "iam:Update*",
                "iam:Put*",
                "iam:Delete*",
                "iam:CreateRole",
                "iam:CreatePolicy*",
                "iam:AttachRolePolicy",
                "iam:DetachRolePolicy"
            ],
            "Resource": [
                "arn:aws:iam::<account>:role/<customerrole>-*",
                "arn:aws:iam::<account>:policy/<Customer>-Account*"
            ],
            "Effect": "Deny",
            "Sid": "IAMExplicitDenyforRoles"
        },
```

DetachRolePolicy != DetachUserPolicy

DeleteUserPermissionsBoundary not sufficient to prevent a user from modifying their permissions.

This technically follows AWS’s recommendations.

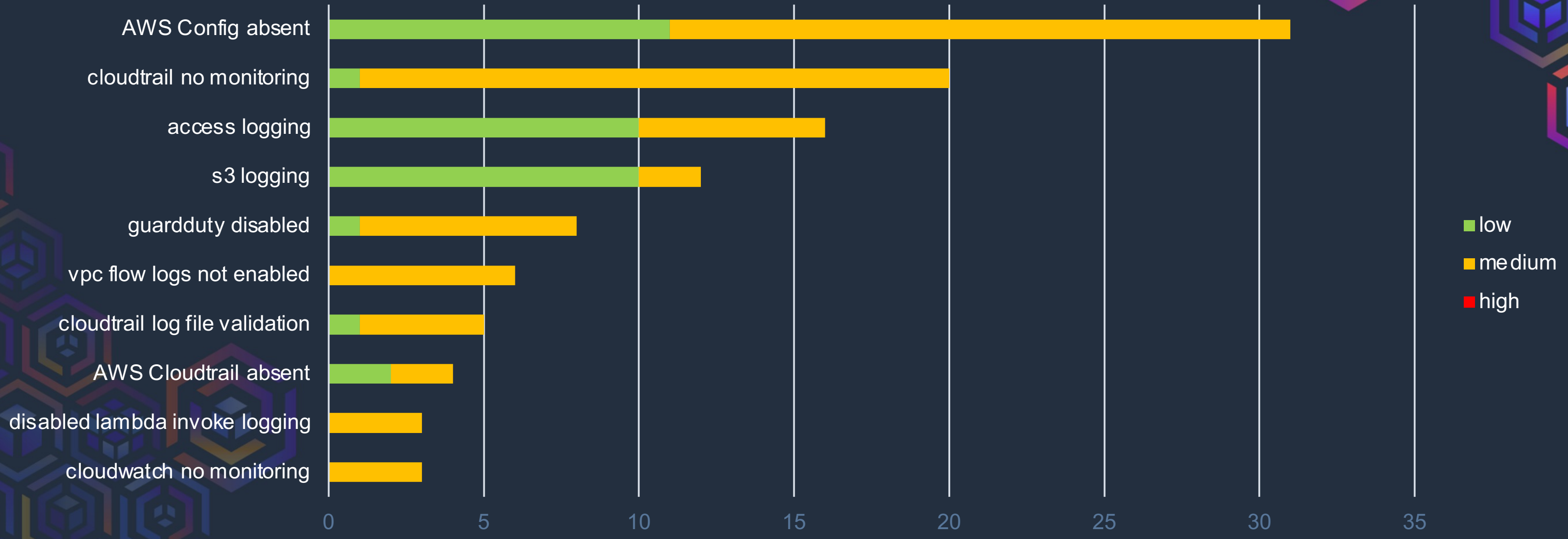
Every API permission has its own resource requirements and naming conventions

aws

COMMUNITY DAY

AOTEAROA

Monitoring Deep Dive



Monitoring Major? Risks

- So many places to configure
- All come at a cost
- What do you do with them once you have them
- What is your plan once you detect badness

aws

COMMUNITY DAY

AOTEAROA

AWS Security Services

Almost too many of them – Idea – scrolling the giant page
https://aws.amazon.com/products/security/

Critical ones to understand fully:

- IAM (!!!)
- CloudTrail / CloudWatch / Config
- Inspector / GuardDuty
- SecurityHub
- AWS Shield and WAF
- AWS KMS, Cert Mger and Secrets Mger

Free Tools

Current opensource toolset takes a little effort to get running.

General tools for CIS benchmarks and more:

- Prowler
- ScoutSuite

Manages all the different roles / auth you're likely to do

- Awsume
- AWS-Vault

Deep dive on IAM:

- Cloudsplaining
- Pmapper

Firefox with Multi-Container plugin (to manage different logins to the console)

aws

COMMUNITY DAY

AOTEAROA