# {SecDev,Rugged,Cloud} Ops

~~Where Security and Operations meet~~

# There is no cloud

## it's just someone else's computer

# $ whoami

- Blue teamer (party of one)
- Done the attack stuff
- Worked for one of the “big Four”
- Head of Security for $company
- Likes long walks on the beach

# Agenda

- AWS Accounts 101
- Defend
- Defend some more
- Q&A
- ???
- Profit

# Pizza as a Service 2.0

http://www.paulkerrison.co.uk

| Tradition On-Premises (legacy) | Infrastructure as a Service (IaaS) | Containers as a Service (CaaS) | Platform as a Service (PaaS) | Function as a Service (FaaS) | Software as a Service (SaaS) |
|---|---|---|---|---|---|
| Conversation | Conversation | Conversation | Conversation | Conversation | Conversation |
| Friends | Friends | Friends | Friends | Friends | Friends |
| Beer | Beer | Beer | Beer | Beer | Beer |
| Pizza | Pizza | Pizza | Pizza | Pizza | Pizza |
| Fire | Fire | Fire | Fire | Fire | Fire |
| Oven | Oven | Oven | Oven | Oven | Oven |
| Electric / Gas | Electric / Gas | Electric / Gas | Electric / Gas | Electric / Gas | Electric / Gas |
| Homemade | Communal Kitchen | Bring Your Own | Takeaway | Restaurant | Party |

- Configuration
- Functions
- Scaling...
- Runtime
- OS
- Virtualisation
- Hardware

You Manage

Vendor Manages

# AWS Security 101

- Protect your account
- Segregate your accounts
- Use “Organisations”
- Use roles and minimise IAM users (access keys)
- Config
- Security Hub
- Inspector (nothing in the UK yet)
- Monitor everything (CloudTrail + CloudWatch)


S.A.P.D.
S.A.P.D.

# Tooling

- **ScoutSuite**
- **CloudMapper**
- **Terraform + Packer**
- **Python + Boto3**
- #brexit
- Frontal Lobotomy
- **SecurityMonkey**

# ScoutSuite
# https://github.com/nccgroup/ScoutSuite

Scout2 Analytics Compute Database Management Messaging Network Security Storage Regions Filters Help

Account ID: 179374595322

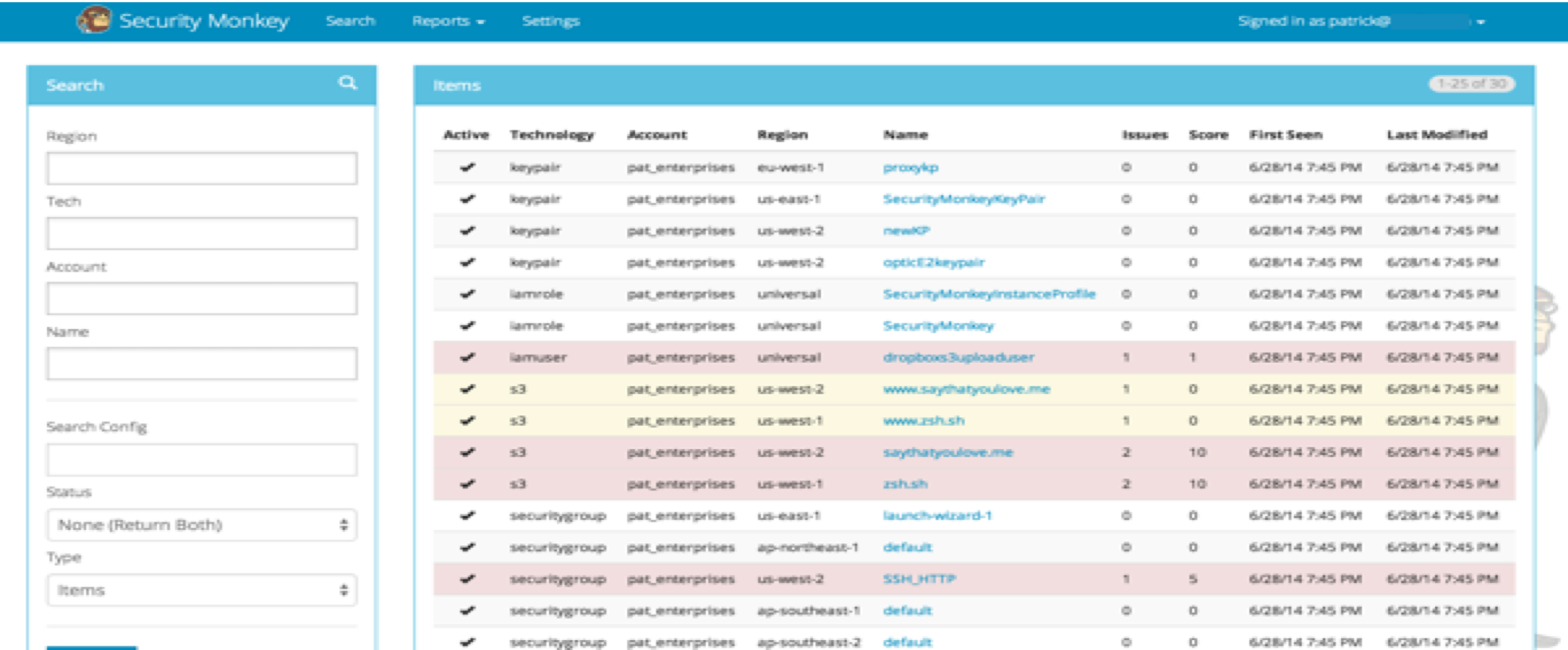
## Dashboard

Summary:

| Service | # of Resources | # of Rules | # of Findings | # of Checks |
|---|---|---|---|---|
| Lambda | 1 | 0 | 0 | 0 |
| Cloudformation | 22 | 1 | 2 | 22 |
| CloudTrail | 44 | 5 | 5 | 104 |
| CloudWatch | 2 | 1 | 1 | 2 |
| Directconnect | 0 | 0 | 0 | 0 |
| EC2 | 60 | 22 | 116 | 1465 |

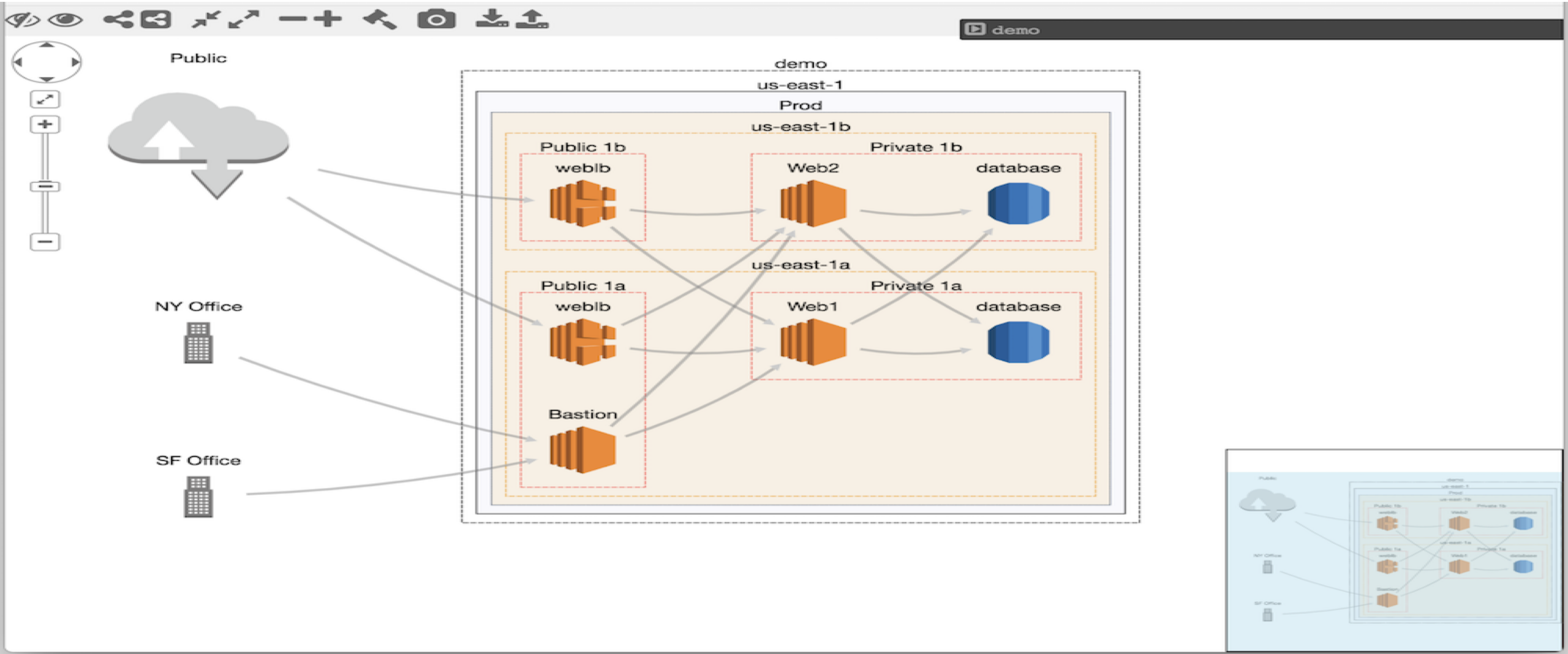
# Security Monkey

# https://github.com/Netflix/security_monkey



# Cloudmapper

# https://github.com/duo-labs/cloudmapper



# Python + Boto3

# AWS-InfoSec

https://github.com/znb/AWS-Information-Security-Environment

# Defend some more

- TheHive + Cortex
- Google Rapid Response
- MISP
- Fleet + Launcher

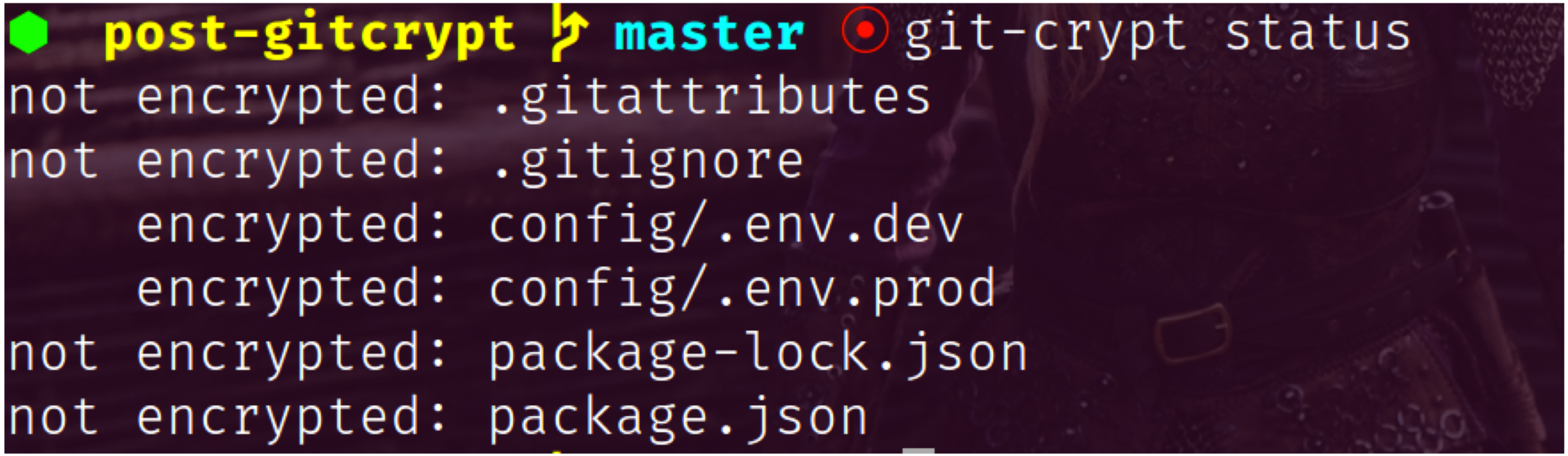
YOU GET

ALL THE BONUS POINTS

# Make life hard^H^H^H**easier**

- Git-crypt - https://github.com/AGWA/git-crypt
- Aws-vault - https://github.com/99designs/aws-vault

# Git-crypt Demo



HashiCorp

# Vault


HashiCorp
Vault

http://flaws.cloud/

http://flaws2.cloud/

credentials — ~

Project

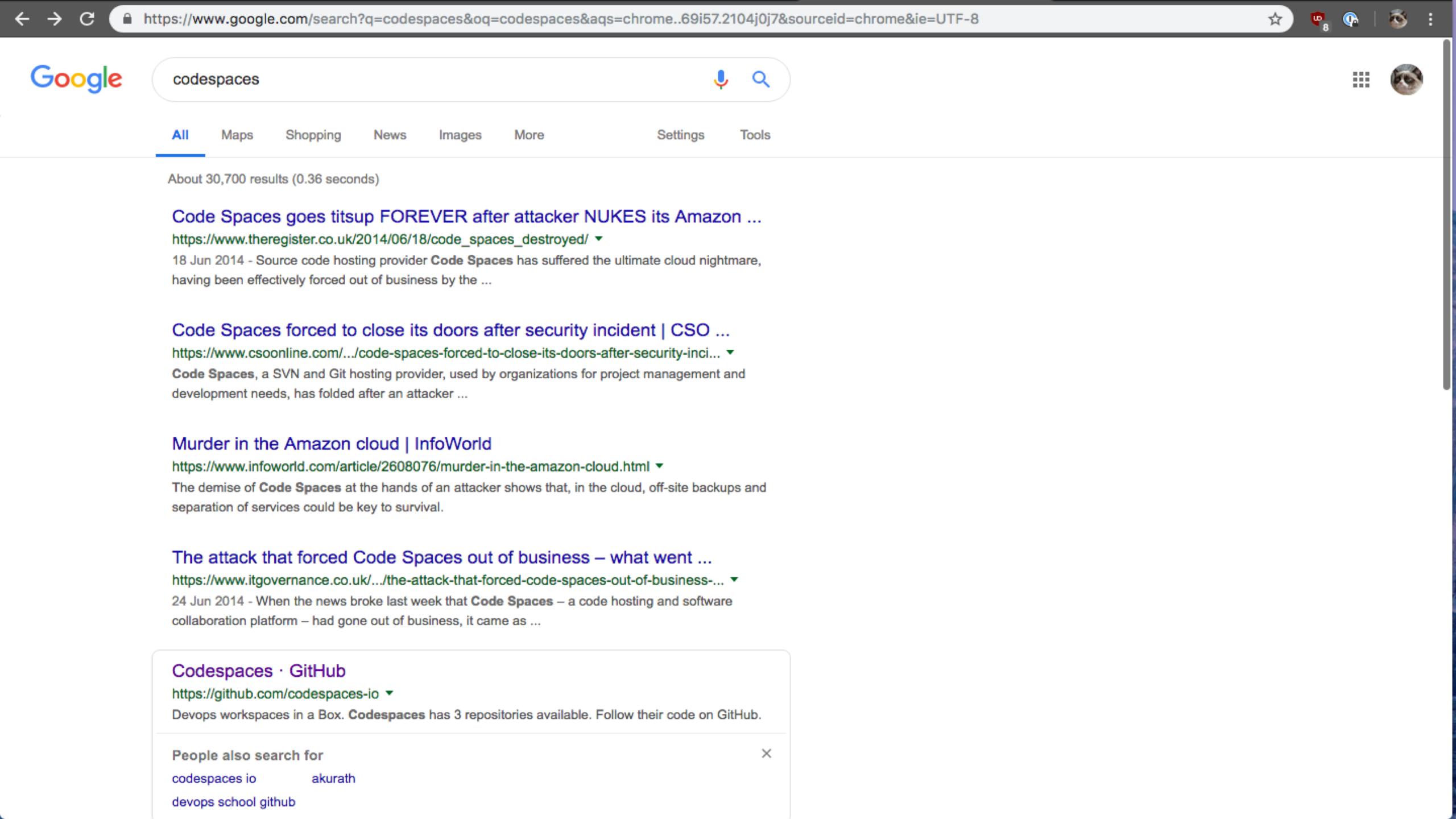
.aws

credentials

credentials

```
1  [default]
2  aws_access_key_id = AKIAJEZ_REST_KEY
3  aws_secret_access_key = Wemfb25Q2hWbFnGhP+MOSHARROF_RUBEL
4
5
```

https://github.com/carnal0wnage/weirdAAL


https://www.google.com/search?q=codespaces&oq=codespaces&aqs=chrome..69i57.2104j0j7&sourceid=chrome&ie=UTF-8
Google
codespaces
All
Maps
Shopping
News
Images
More
Settings
Tools
About 30,700 results (0.36 seconds)
Code Spaces goes titsup FOREVER after attacker NUKES its Amazon ...
https://www.theregister.co.uk/2014/06/18/code_spaces_destroyed/
18 Jun 2014 - Source code hosting provider Code Spaces has suffered the ultimate cloud nightmare, having been effectively forced out of business by the ...
Code Spaces forced to close its doors after security incident | CSO ...
https://www.csoonline.com/.../code-spaces-forced-to-close-its-doors-after-security-inci...
Code Spaces, a SVN and Git hosting provider, used by organizations for project management and development needs, has folded after an attacker ...
Murder in the Amazon cloud | InfoWorld
https://www.infoworld.com/article/2608076/murder-in-the-amazon-cloud.html
The demise of Code Spaces at the hands of an attacker shows that, in the cloud, off-site backups and separation of services could be key to survival.
The attack that forced Code Spaces out of business – what went ...
https://www.itgovernance.co.uk/.../the-attack-that-forced-code-spaces-out-of-business-...
24 Jun 2014 - When the news broke last week that Code Spaces – a code hosting and software collaboration platform – had gone out of business, it came as ...
Codespaces · GitHub
https://github.com/codespaces-io
Devops workspaces in a Box. Codespaces has 3 repositories available. Follow their code on GitHub.
People also search for
codespaces io
akurath
devops school github

https://github.com/stuhirst/awssecurity

kthxbinowaitquestions?!