

Pragmatic Automation

Nick Jones – 15th August 2019

LABS

Have you ever found yourself...

- ...repeating the same task over and over?
- ...manually pulling lots of things out of spreadsheets?
- ...wanting more people in your team?

A wise man once said...

“[Automation] is the art of spending 4 hours working out how to do a 2 hour job in 10 minutes.

That way, the next time you have to do it, you do it in 10 minutes and spend the other hour and 50 down the pub”

Why Automate?

- Make everyone's lives easier
 - Reduce human error
 - Improves efficiency
 - Scale across larger environments
-
- (Usually more interesting than doing things manually)

whoami



Nick Jones

- Senior consultant, cloud team lead
- Ex–software developer

Research interests:

- Cloud
- Attack Detection
- DevOps/Automation

Categories of Automation

- Quick hacks and one-liners
- Scripting
- Automation tooling
- ~~Bespoke software~~

Quick Hacks

- Excel Macros
- Grep/sed/awk one-liners
- Great for:
 - Speeding little things up
- Bad for:
 - Bigger things

```
grep "Status: Up" nmap-scan.gnmap | cut -d' ' -f2 | sort -u > livehosts.txt
```

Scripting

- Python/Ruby/Powershell etc
- Great for:
 - Things too big for a quick hack
 - Things you're likely to reuse
- Bad for:
 - Learning curve

Automation Tooling

- Anything domain-specific – config management, orchestration, data analysis etc
- Good for:
 - Getting things done well, quickly
- Bad for:
 - Anything the tooling wasn't designed for
 - Learning curve

OpenRefine

This feature helps you find groups of different cell values that might be alternative representations of the same thing. For example, the two strings "New York" and "new york" are very likely to refer to the same concept and just have capitalization differences, and "Gödel" and "Godel" probably refer to the same person. [Find out more ...](#)

Method: key collision Keying Function: fingerprint 48 clusters found

Cluster Size	Row Count	Values in Cluster	Merge?	New Cell Value
3	63	<ul style="list-style-type: none"> Pune Vidhyapeeth Gate (33 rows) Pune Vidhyapeeth Gate (17 rows) Pune Vidhyapeeth Gate (13 rows) 	<input type="checkbox"/>	Pune Vidhyapeeth Gate
3	101	<ul style="list-style-type: none"> Hadapsar Gadital (83 rows) Hadapsar Gadital (14 rows) Hadapsar Gadital (4 rows) 	<input type="checkbox"/>	Hadapsar Gadital
3	12	<ul style="list-style-type: none"> Devachi Uruli Phata (8 rows) Devachi Uruli Phata (2 rows) Uruli Devachi Phata (2 rows) 	<input type="checkbox"/>	Devachi Uruli Phata
2	2	<ul style="list-style-type: none"> SRP Stadium (1 rows) SRP Stadium (1 rows) 	<input type="checkbox"/>	SRP Stadium
2	8	<ul style="list-style-type: none"> Khandoba Mandir Corner (6 rows) Khandoba Mandir corner (2 rows) 	<input type="checkbox"/>	Khandoba Mandir Corner
2	7	<ul style="list-style-type: none"> St Meera College (5 rows) ST Meera College (2 rows) 	<input type="checkbox"/>	St Meera College
2	67	<ul style="list-style-type: none"> Gurjan Corner (62 rows) 	<input type="checkbox"/>	Gurjan Corner

Choices In Cluster

Rows In Cluster

Average Length of Choices

Length Variance of Choices

Data Normalisation

Great for:

- Combining spreadsheets
- Cleaning data up
- Similar data/different formats

<https://schoolofdata.org/2013/07/26/using-openrefine-to-clean-multiple-documents-in-the-same-way/>

RunDeck

Runbook Automation

Great for:

- Running ad-hoc and scheduled tasks
- Self-service access to scripts

The screenshot displays the RunDeck web interface. At the top, there's a navigation bar with 'RUNDECK', a dropdown menu for 'anvils', and tabs for 'Jobs', 'Nodes', 'Commands', and 'Activity'. On the right of the navigation bar are links for 'admin' and 'help'. Below the navigation bar, the 'Commands' tab is active. It shows a 'Command' input field with 'uptime' and a 'Run on 5 Nodes' button. Below this, there's a 'Nodes' section with a 'Filter' dropdown set to 'name: *.anvils.com' and a 'Set Filter' button. It indicates '5 Nodes Matched' and lists the nodes: 'app1.anvils.com', 'app2.anvils.com', 'db1.anvils.com', 'www1.anvils.com', and 'www2.anvils.com'. A status bar shows '#2_Succeeded' and a 'Save as a Job...' button. Below this, there's a table of command execution results for the 'uptime' command. The table has columns for time, node name, and uptime details. At the bottom, there's a section for 'Activity for commands' with filters for 'running', 'recent', 'failed', and 'by you'.

Time	Node	Uptime Details
17:54:34	app1.anvils.com	00:54:34 up 22 min, 0 users, load average: 0.01, 0.05, 0.06
17:54:35	app2.anvils.com	00:54:35 up 22 min, 0 users, load average: 0.01, 0.05, 0.06
17:54:36	db1.anvils.com	00:54:36 up 22 min, 0 users, load average: 0.01, 0.05, 0.06
17:54:36	www1.anvils.com	00:54:36 up 22 min, 0 users, load average: 0.01, 0.05, 0.06
17:54:37	www2.anvils.com	00:54:37 up 22 min, 0 users, load average: 0.01, 0.05, 0.06

Purple Team Infrastructure Creation



LABS

Purple Teaming

+ 'We've brought lots of security toys'

Do they actually prevent/detect anything?

+ We've got all the dashboards

Can analysts respond effectively to an alert?

+ Logs

Are the correct things being monitored?

MWR
LABS



MACHINE
LEARNING



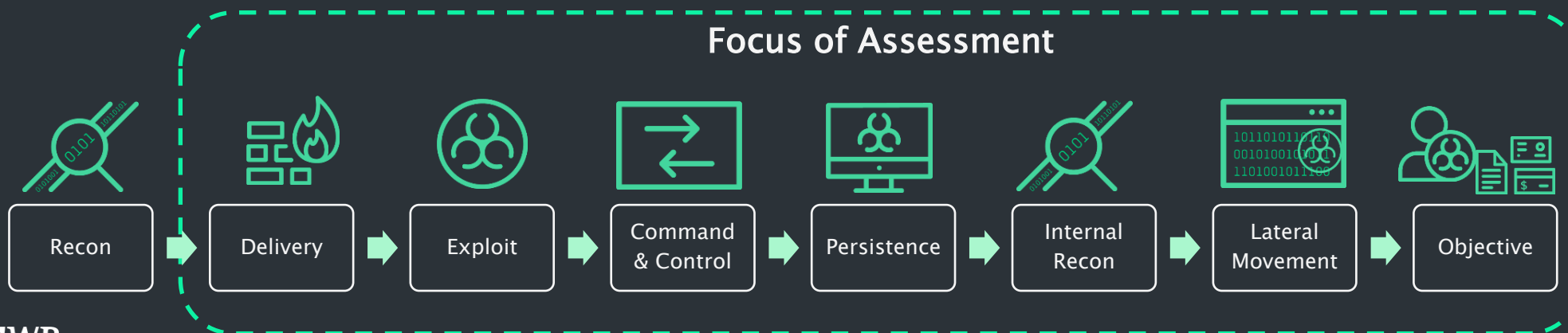
BLOCKCHAIN



Methodology

Cyber kill chain

- 400+ test cases.
- AttackSim.



MWR
ATTACKSIM

Infrastructure Setup

- Email delivery
- Web delivery
- Hosted payloads / tools
- Malware command and control (C2)

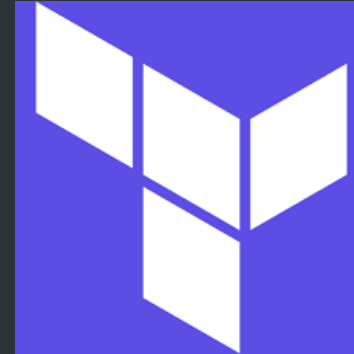
Before Automation?

- By hand:
 - Spin up EC2 instances
 - Install/configure software
 - Find / buy suitable domains
 - Configure DNS
 - Test it all

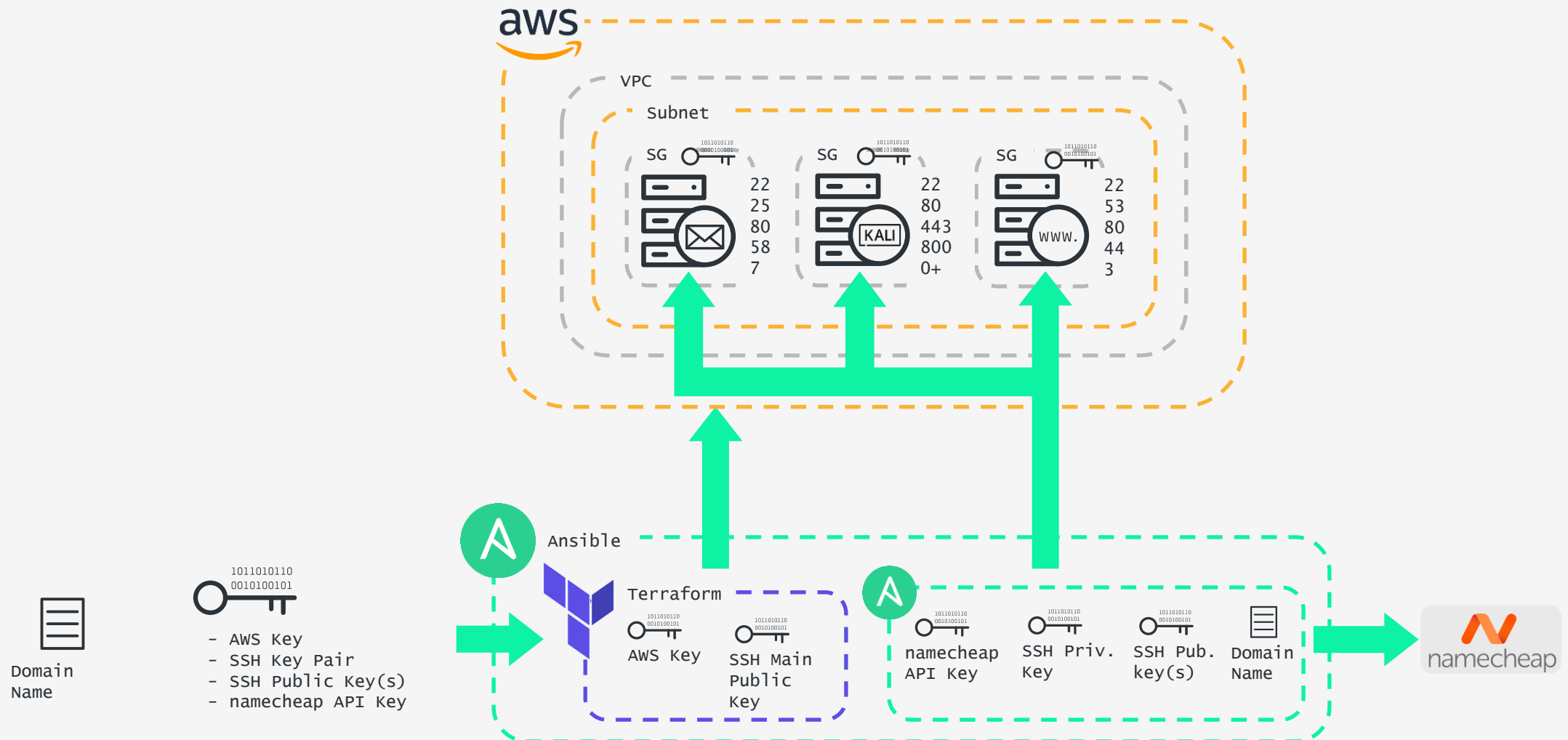
One consultant, two weeks

Infrastructure-as-Code

- Terraform
 - Infrastructure Orchestration
 - Cloud as code
- Ansible
 - ‘IT Automation’
 - OS-level configuration ++



Infrastructure Creation



AWX

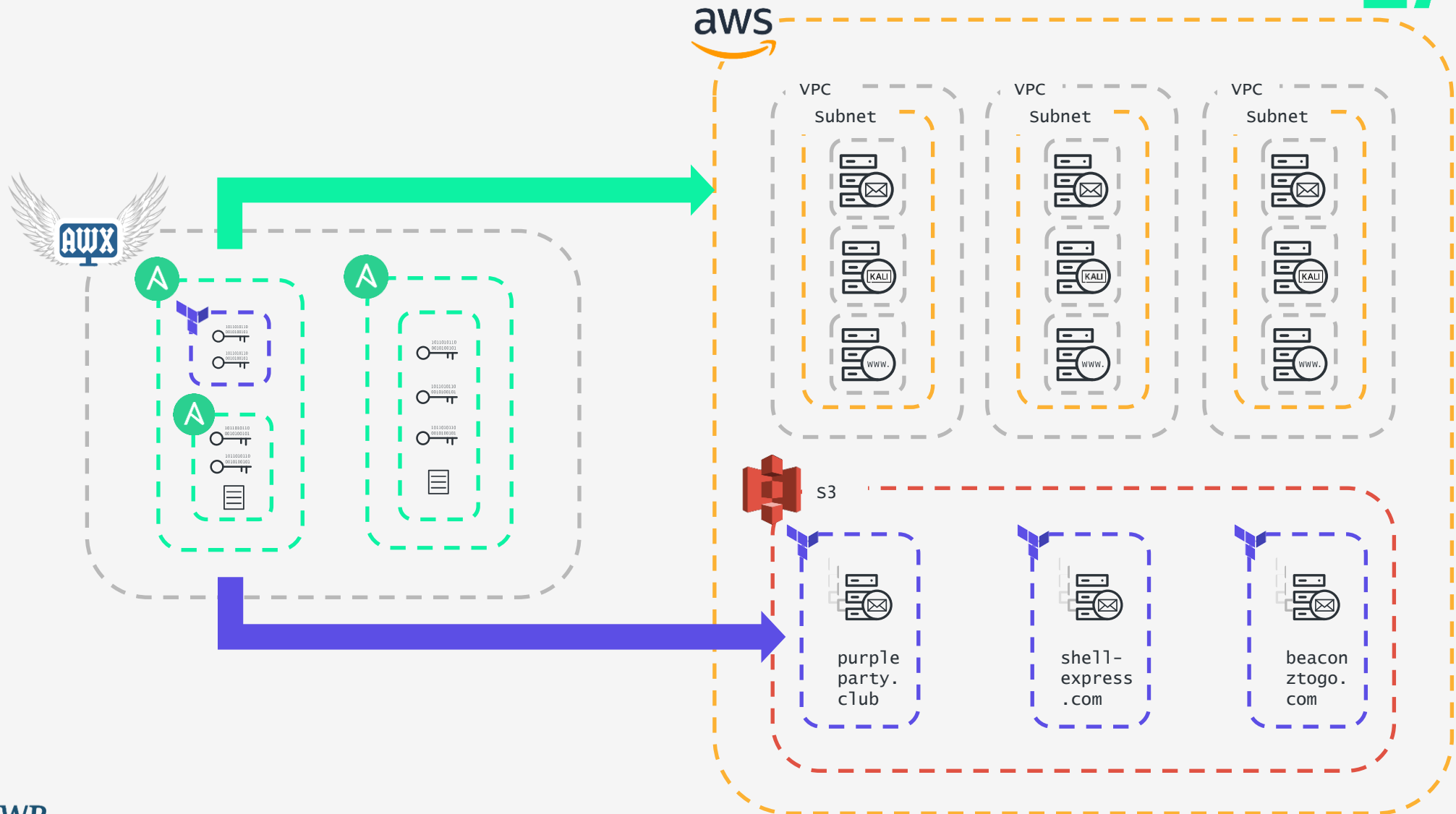


- Web Interface + API
- RBAC

Allows you to manage:

- Credentials
- Inventory





End result?

- Fully-automated purple team deployment
- Standardised, centralised, reproducible

One consultant, one day

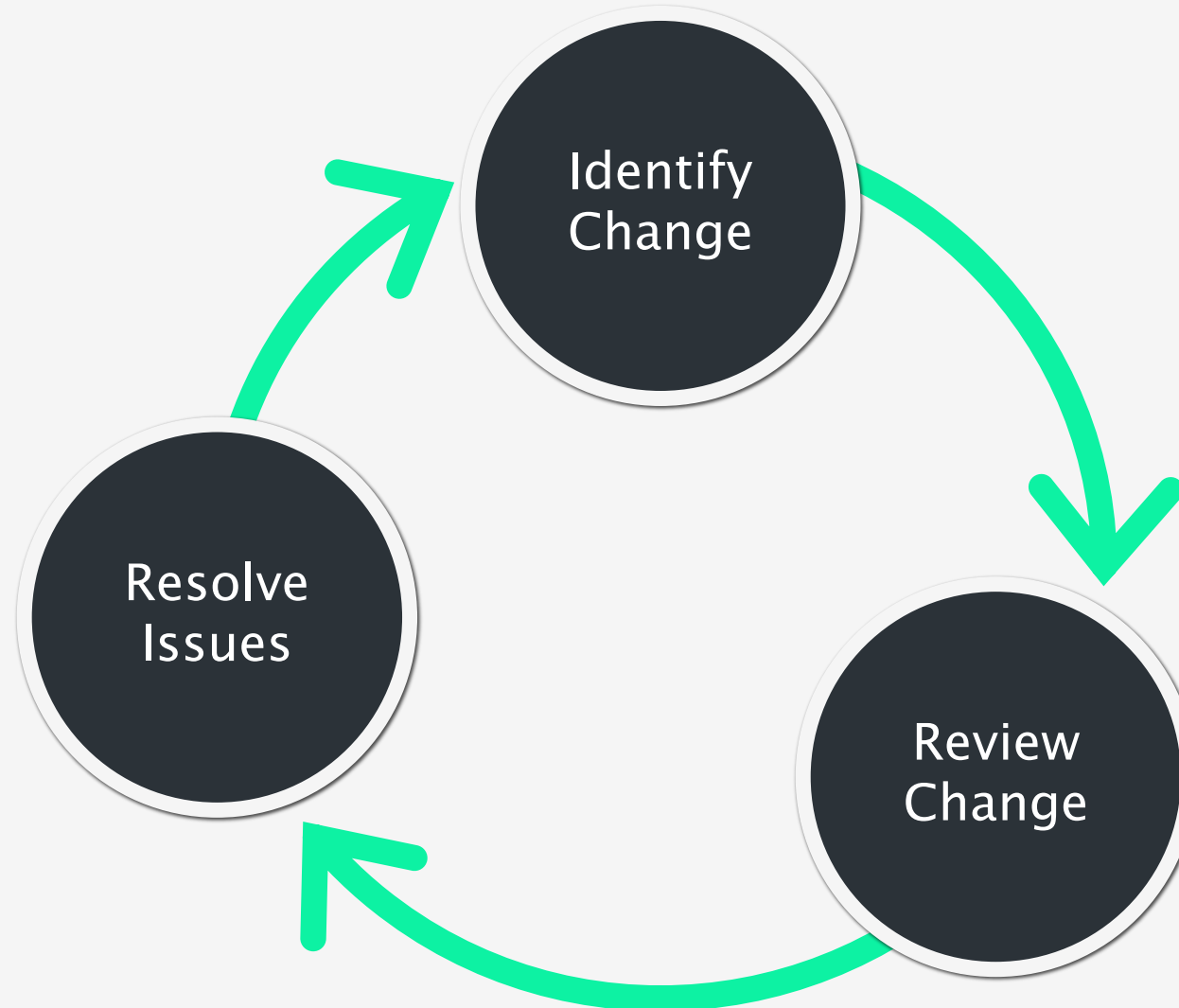
Scaling Cloud Security

LABS

Continuous Configuration Review

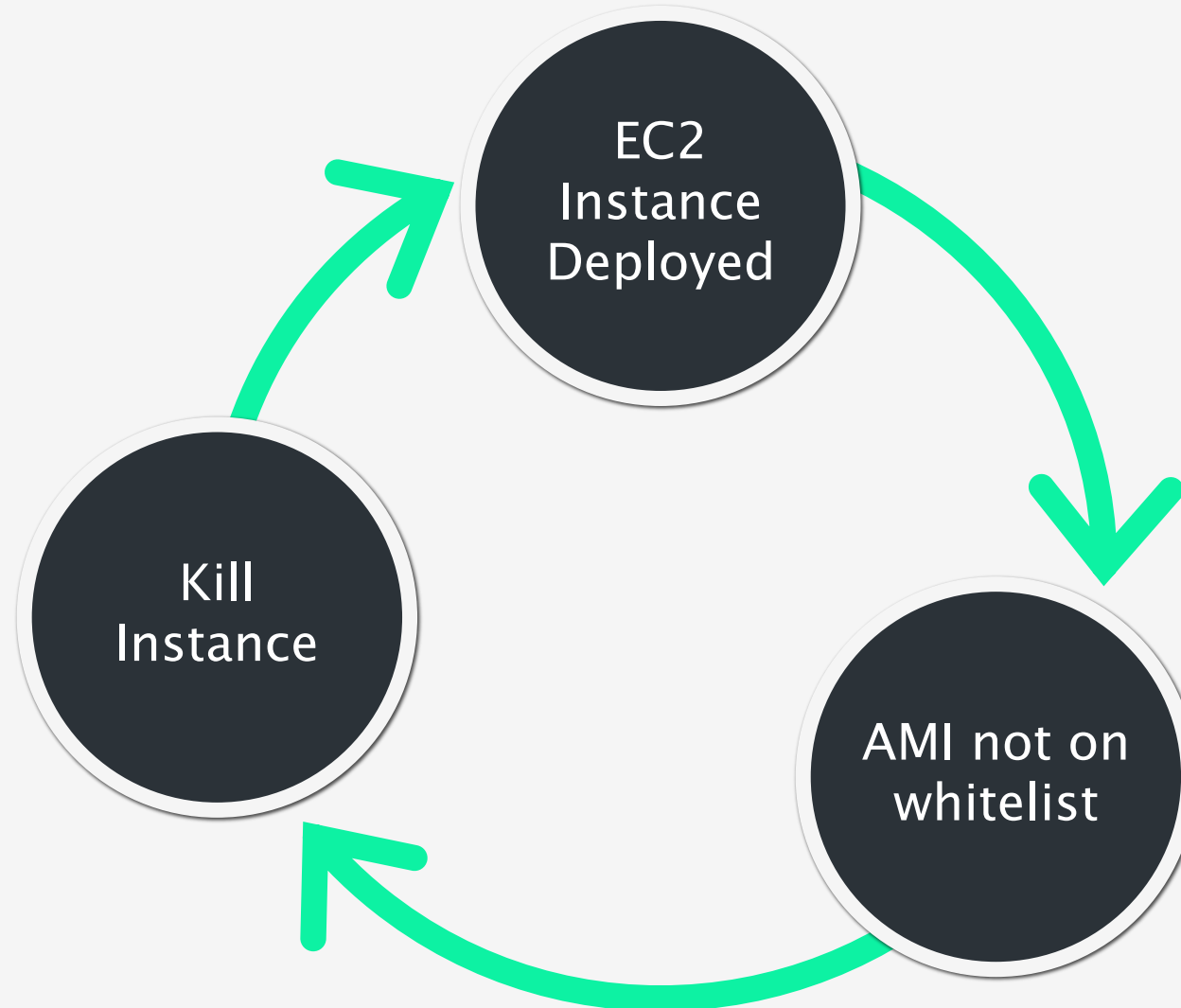


Continuous Configuration Enforcement



Remediation
time: 30
minutes

Continuous Configuration Enforcement



Remediation
time: 30
minutes

Existing work

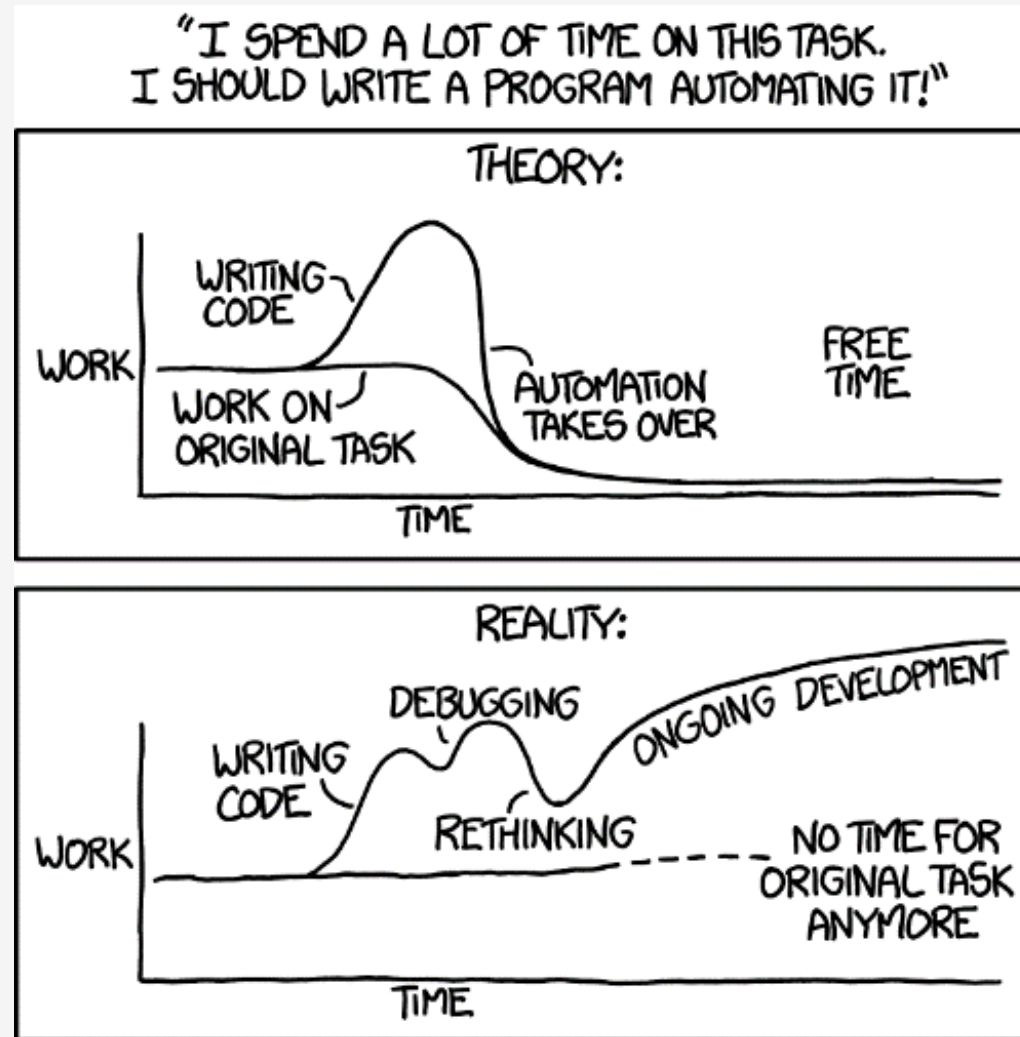
- AWS Whitepaper – Automating Governance on AWS
- OSS Frameworks:
 - Cloud Custodian
 - Security Monkey



Gotchas

LABS

Balance of Effort



Some things just
aren't worth
automating

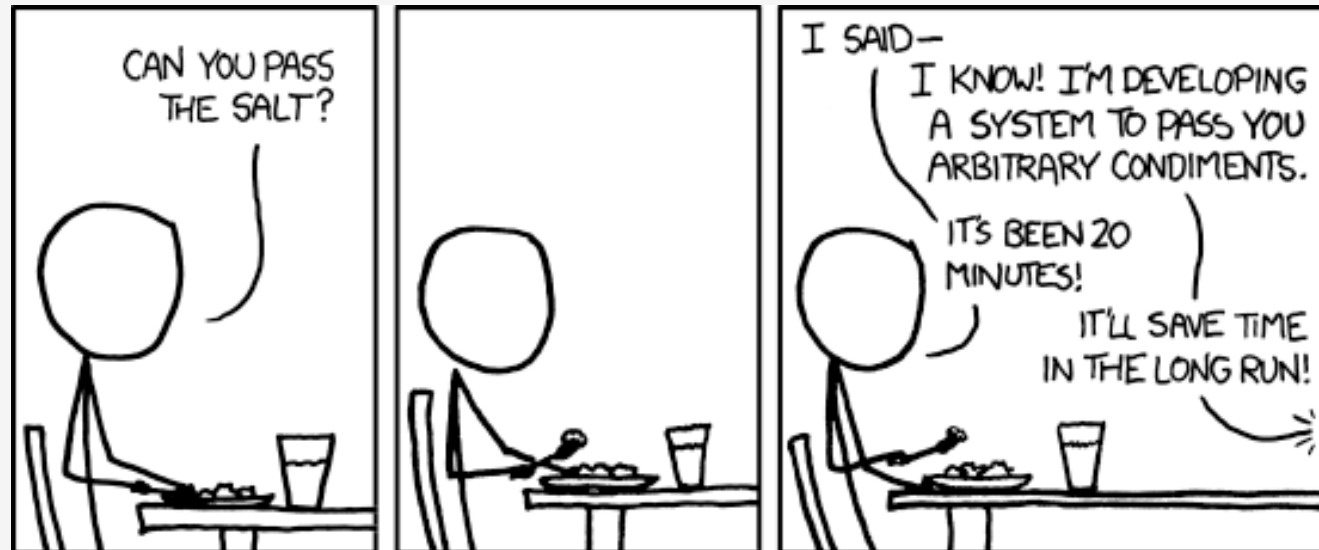
HOW LONG CAN YOU WORK ON MAKING A ROUTINE TASK MORE
EFFICIENT BEFORE YOU'RE SPENDING MORE TIME THAN YOU SAVE?
(ACROSS FIVE YEARS)

		HOW OFTEN YOU DO THE TASK					
		50/DAY	5/DAY	DAILY	WEEKLY	MONTHLY	YEARLY
HOW MUCH TIME YOU SHAVE OFF	1 SECOND	1 DAY	2 HOURS	30 MINUTES	4 MINUTES	1 MINUTE	5 SECONDS
	5 SECONDS	5 DAYS	12 HOURS	2 HOURS	21 MINUTES	5 MINUTES	25 SECONDS
	30 SECONDS	4 WEEKS	3 DAYS	12 HOURS	2 HOURS	30 MINUTES	2 MINUTES
	1 MINUTE	8 WEEKS	6 DAYS	1 DAY	4 HOURS	1 HOUR	5 MINUTES
	5 MINUTES	9 MONTHS	4 WEEKS	6 DAYS	21 HOURS	5 HOURS	25 MINUTES
	30 MINUTES		6 MONTHS	5 WEEKS	5 DAYS	1 DAY	2 HOURS
	1 HOUR		10 MONTHS	2 MONTHS	10 DAYS	2 DAYS	5 HOURS
	6 HOURS				2 MONTHS	2 WEEKS	1 DAY
	1 DAY					8 WEEKS	5 DAYS

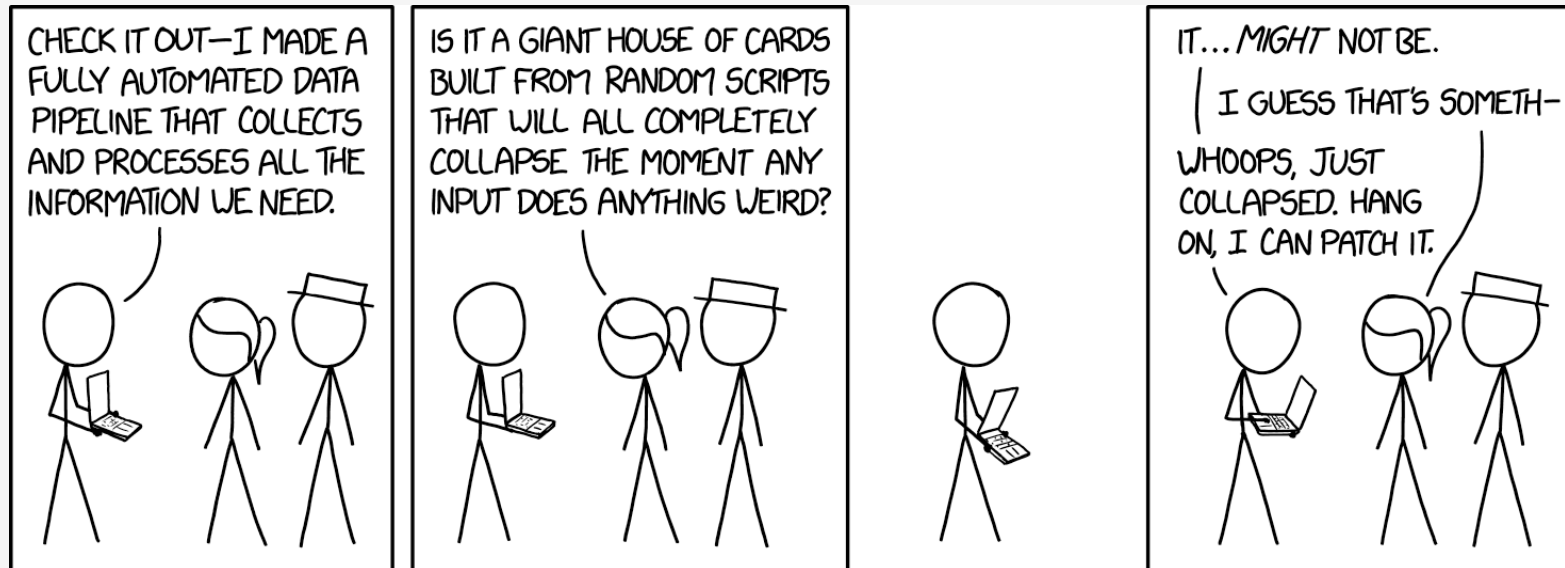
The Generalisation Problem

Don't try to generalise everything!

(try not to design yourself out of the general case, either)



Make It Maintainable



Error handling is important

Document it somewhere

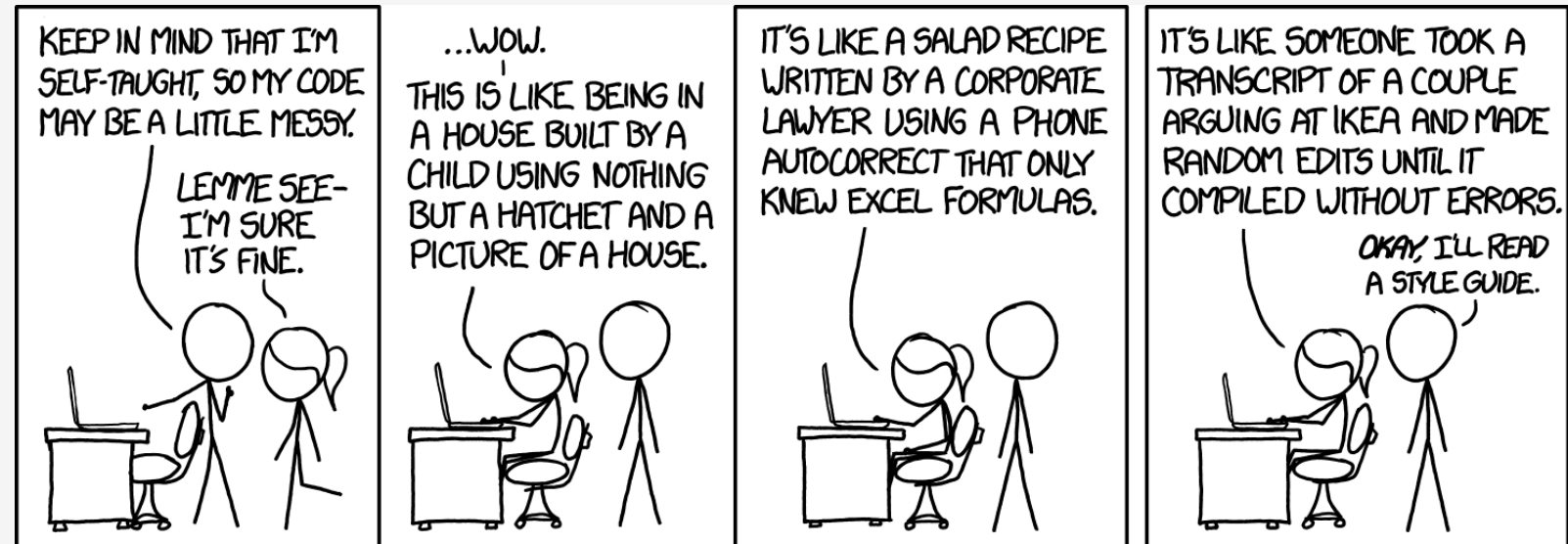
Version control is your friend

Know Your Limits

Understand what your skills allow you to do

Think through the business context

Know when to hand off to dedicated staff



where do I start?

- Never automated anything before?

Something small and simple

Something worthwhile

Something that irritates people

Conclusions

Automation is the
only way to secure
at scale

Efficiency
improvements
benefit everyone

Knowing how and
when to automate
will keep you
employed

Questions?

LABS