MWR INFOSECURITY

Pragmatic Automation

Nick Jones - 15th August 2019

LABS

Have you ever found yourself…

MWR LABS

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

MWR LABS

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?

MWR LABS

- Make everyone's lives easier
- Reduce human error
- Improves efficiency
- Scale across larger environments

- (Usually more interesting than doing things manually)

Whoami

MWR LABS

Nick Jones

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

Research interests:

- Cloud
- Attack Detection
- DevOps/Automation

Categories of Automation

MWR LABS

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

Quick Hacks

MWR LABS

- 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

MWR LABS

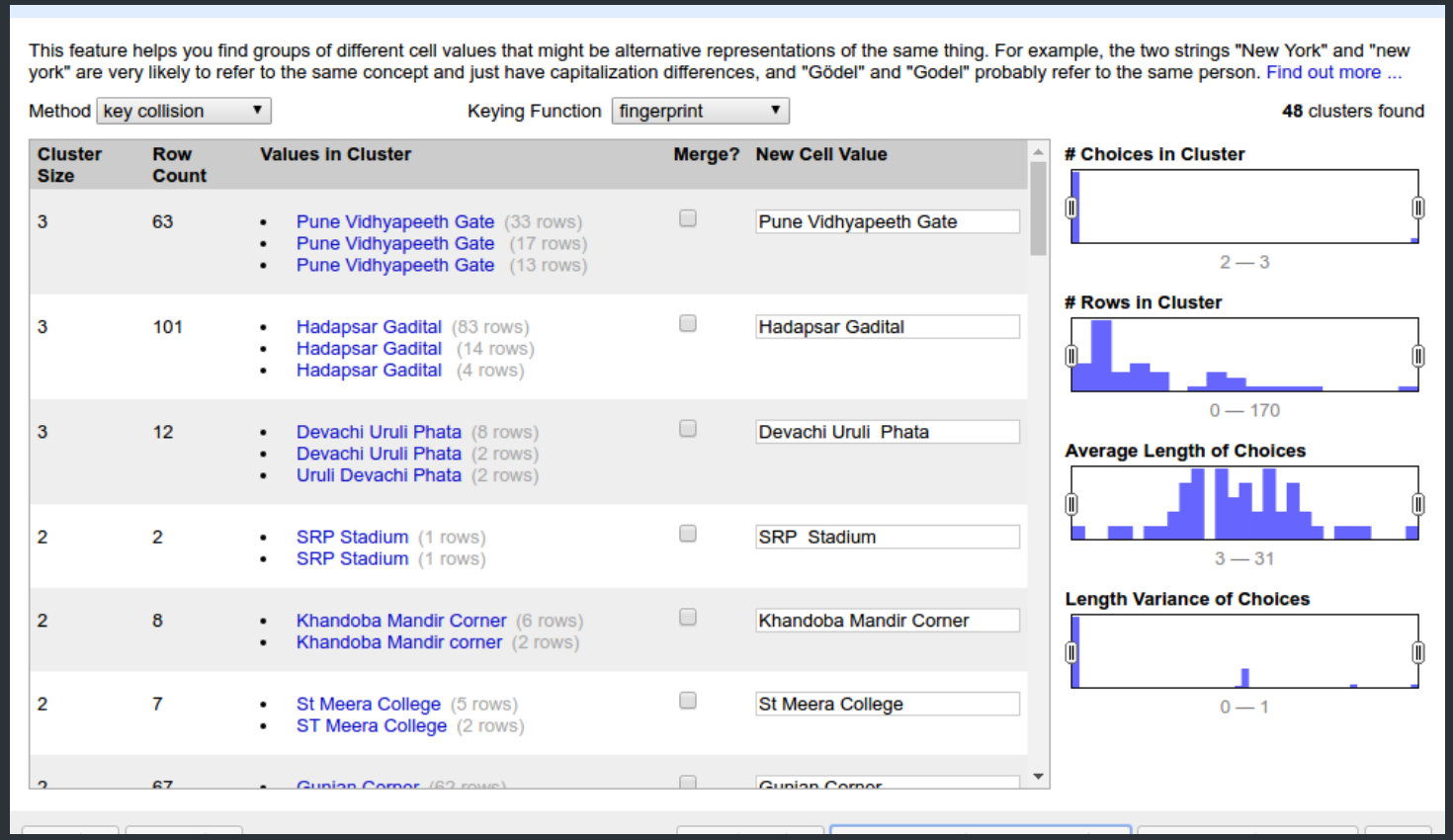
- Python/Ruby/Powershell etc
- Great for:
  - Things too big for a quick hack
  - Things you're likely to reuse
- Bad for:
  - Learning curve

Automation Tooling

MWR LABS

- 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



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

Data Normalisation

Great for:

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

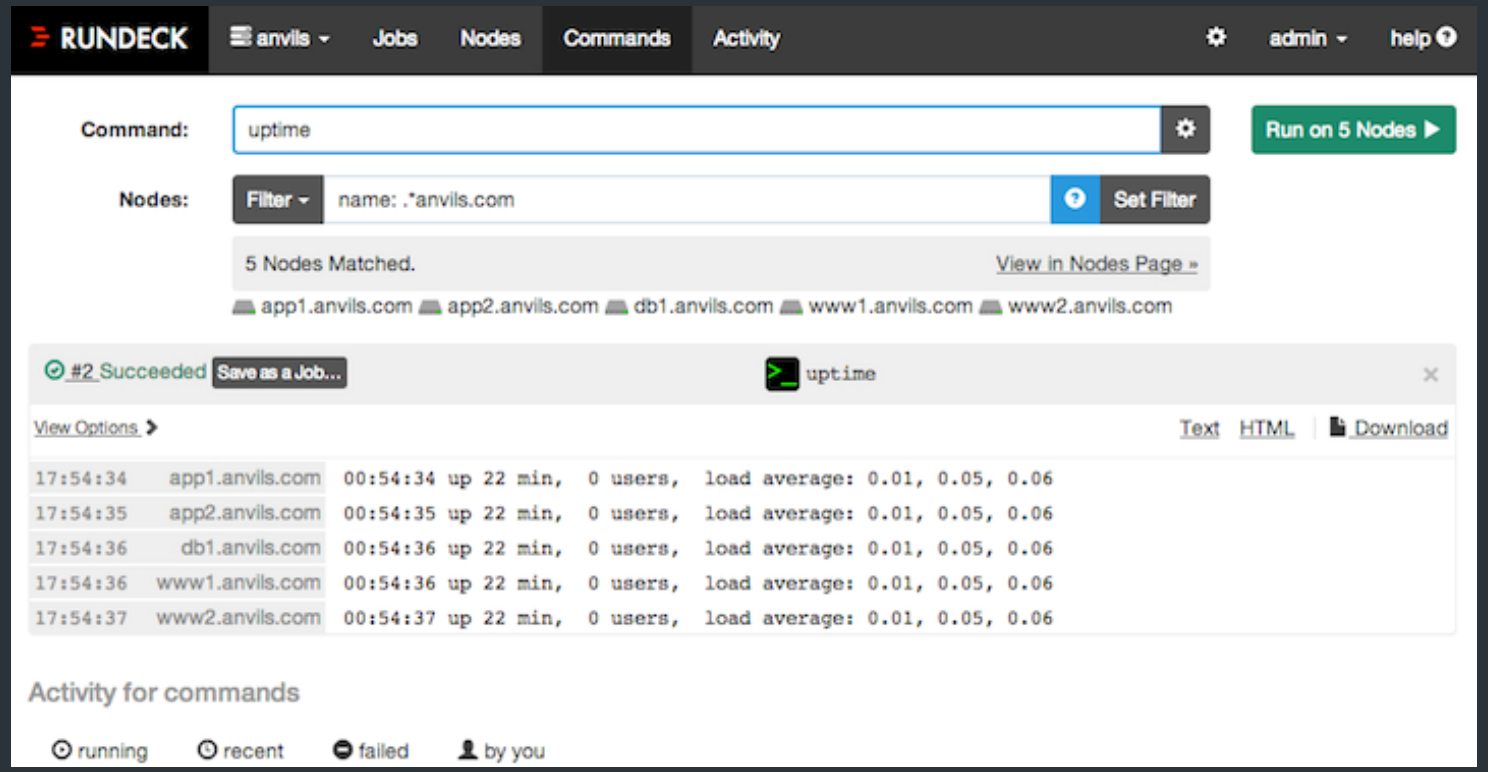
RunDeck

MWR LABS

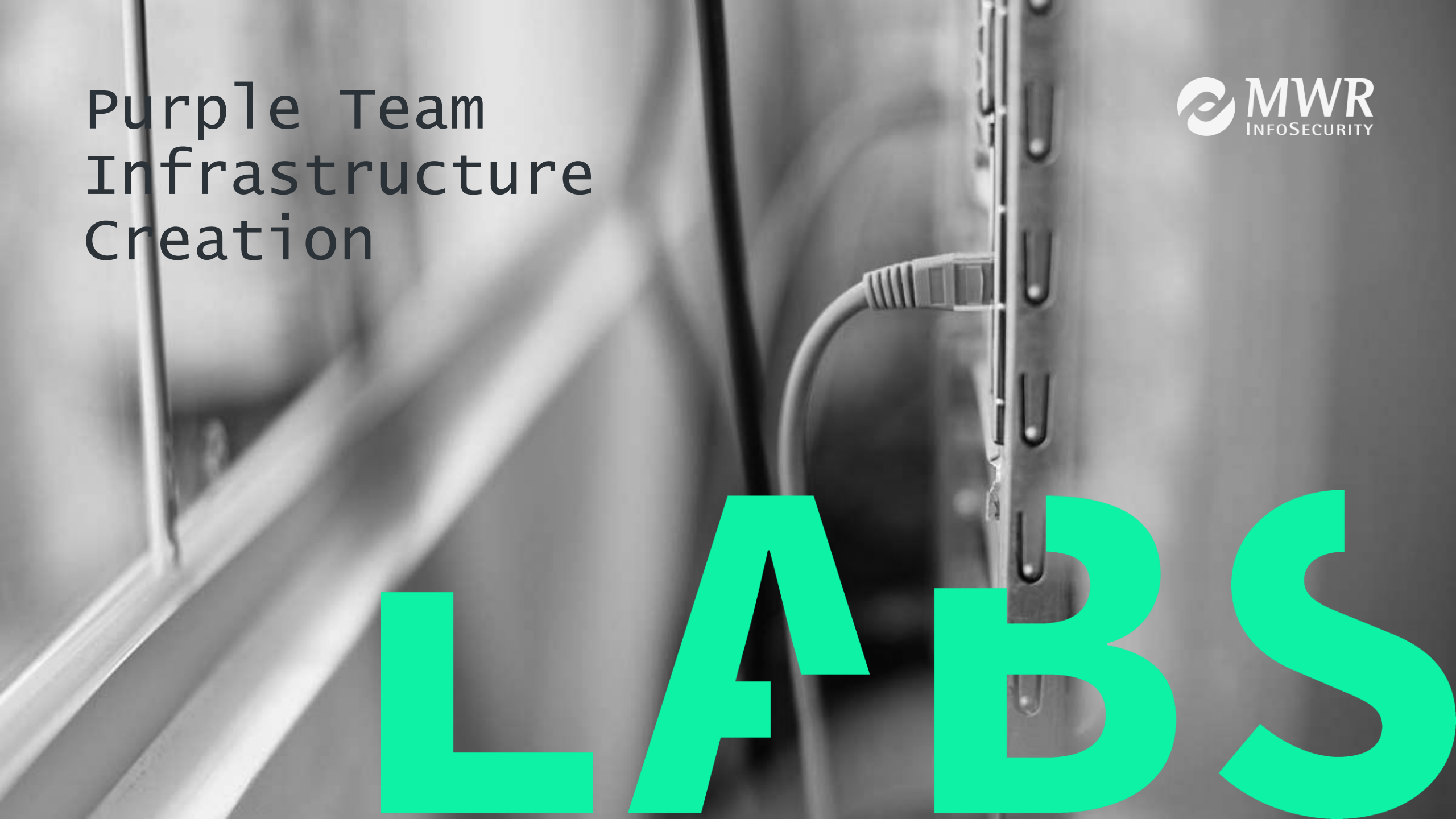
Runbook Automation

Great for:

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



Purple Team Infrastructure Creation



MWR InfoSecurity

LABS

Purple Teaming

MWR LABS

+ ‘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?

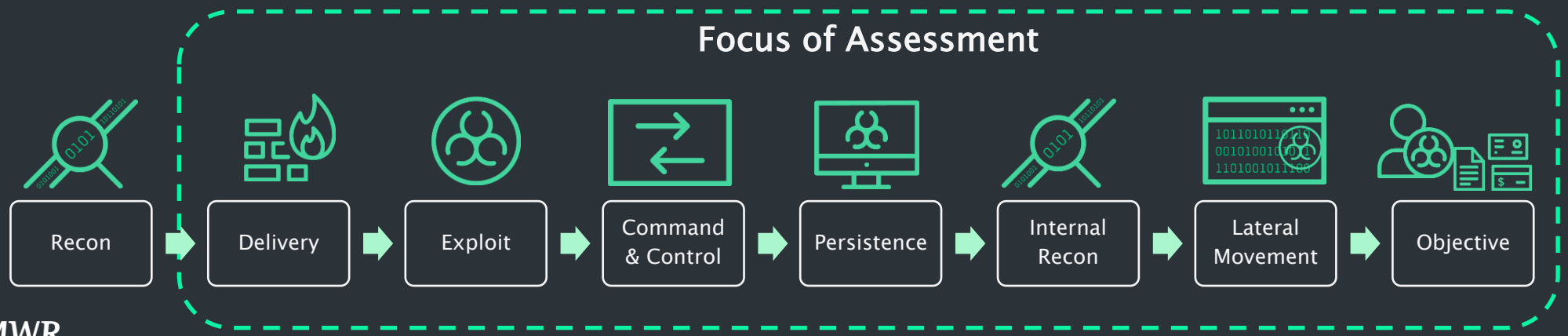
Methodology

MWR LABS

Cyber kill chain

- 400+ test cases.
- AttackSim.

MWR ATTACKSIM



Infrastructure Setup

MWR LABS

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

Before Automation?

MWR LABS

- 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

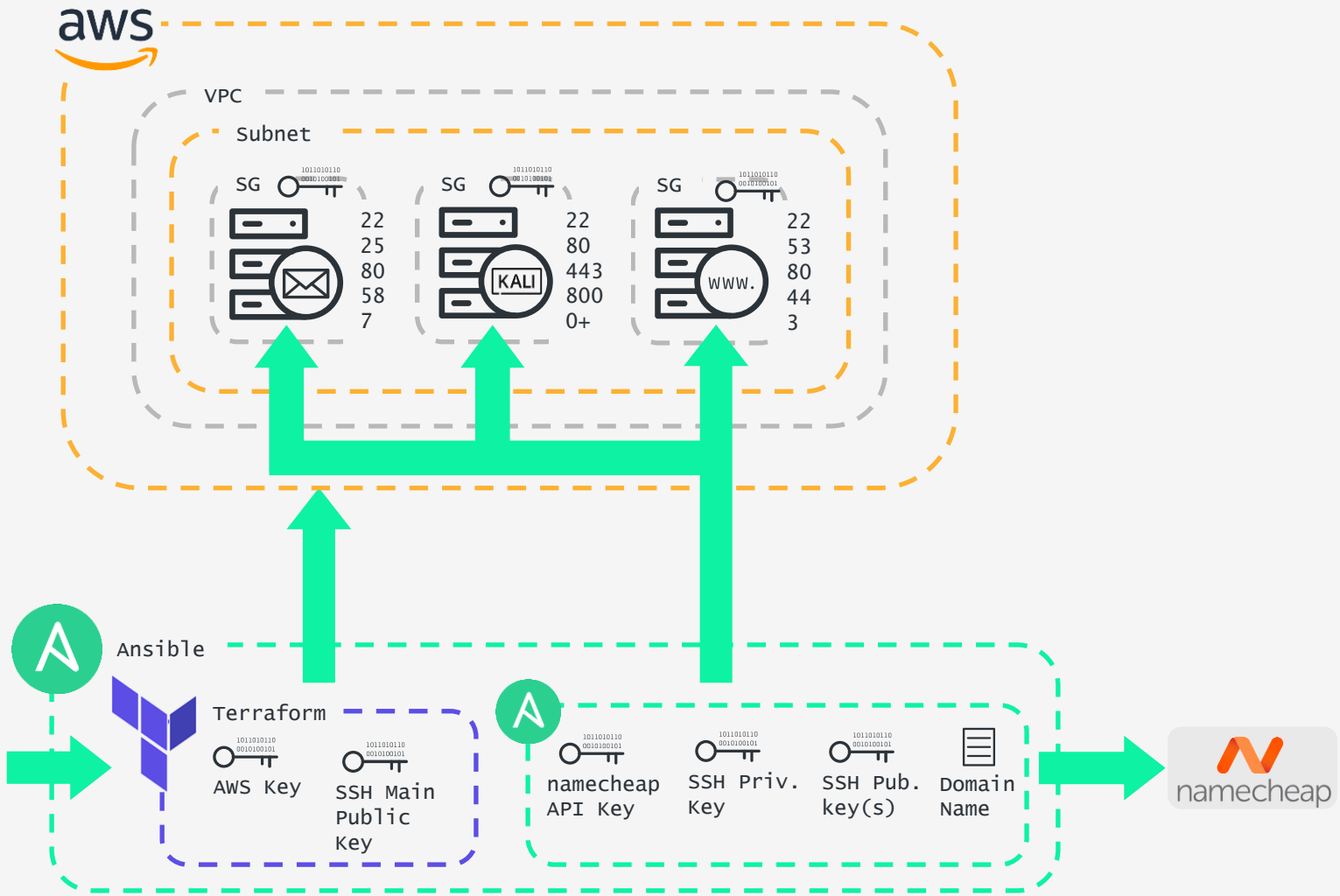
MWR LABS

- Terraform
  - Infrastructure Orchestration
  - Cloud as code

- Ansible
  - ‘IT Automation’
  - OS-level configuration ++

Infrastructure Creation

MWR LABS



AWX

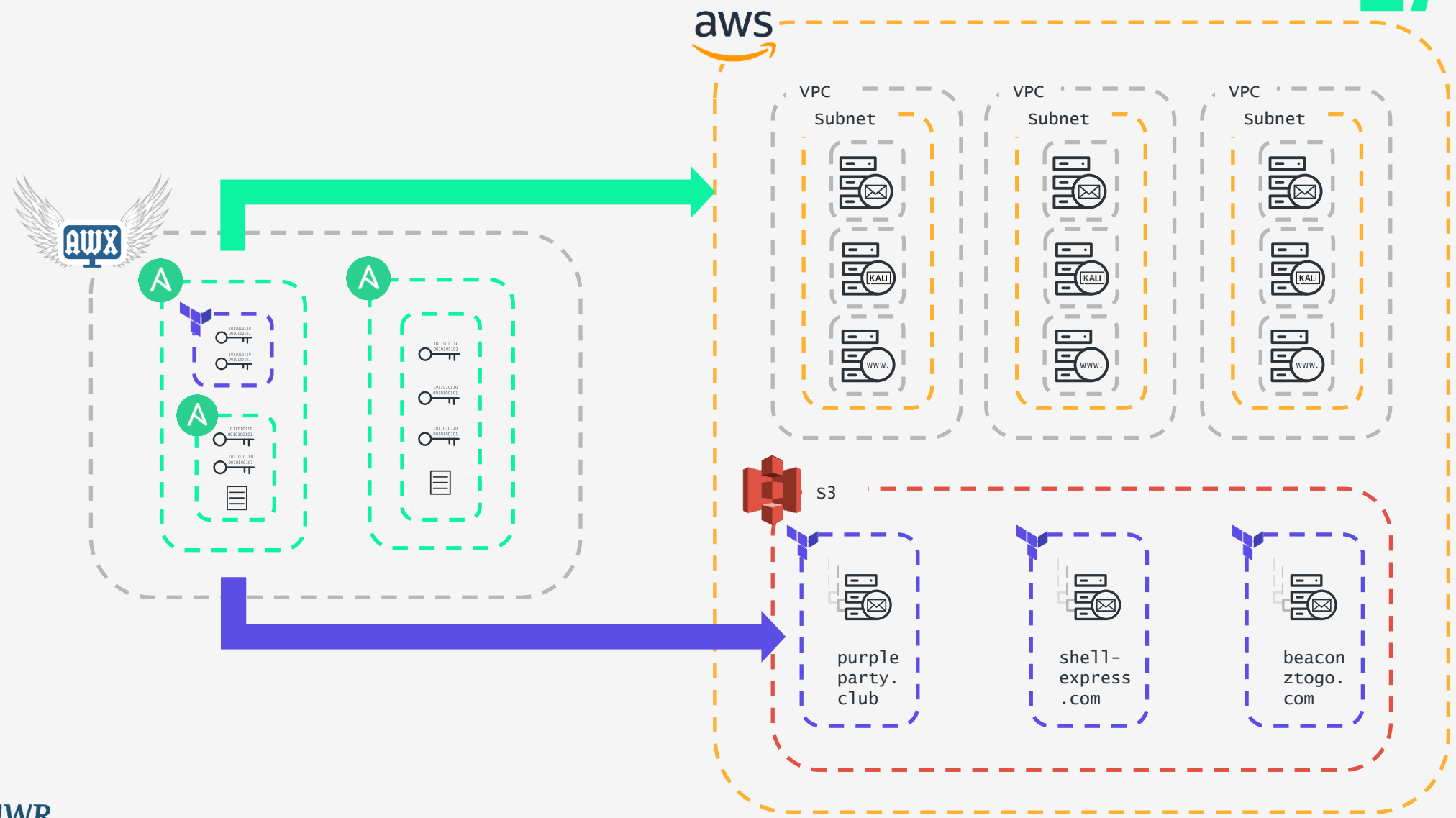
MWR LABS

- Web Interface + API
- RBAC

Allows you to manage:

- Credentials
- Inventory

MWR LABS


aws
AWX
VPC
Subnet
VPC
Subnet
VPC
Subnet
KALI
KALI
KALI
www.
www.
www.
S3
purple party. club
shell-express.com
beaconztogo.com

End result?

MWR LABS

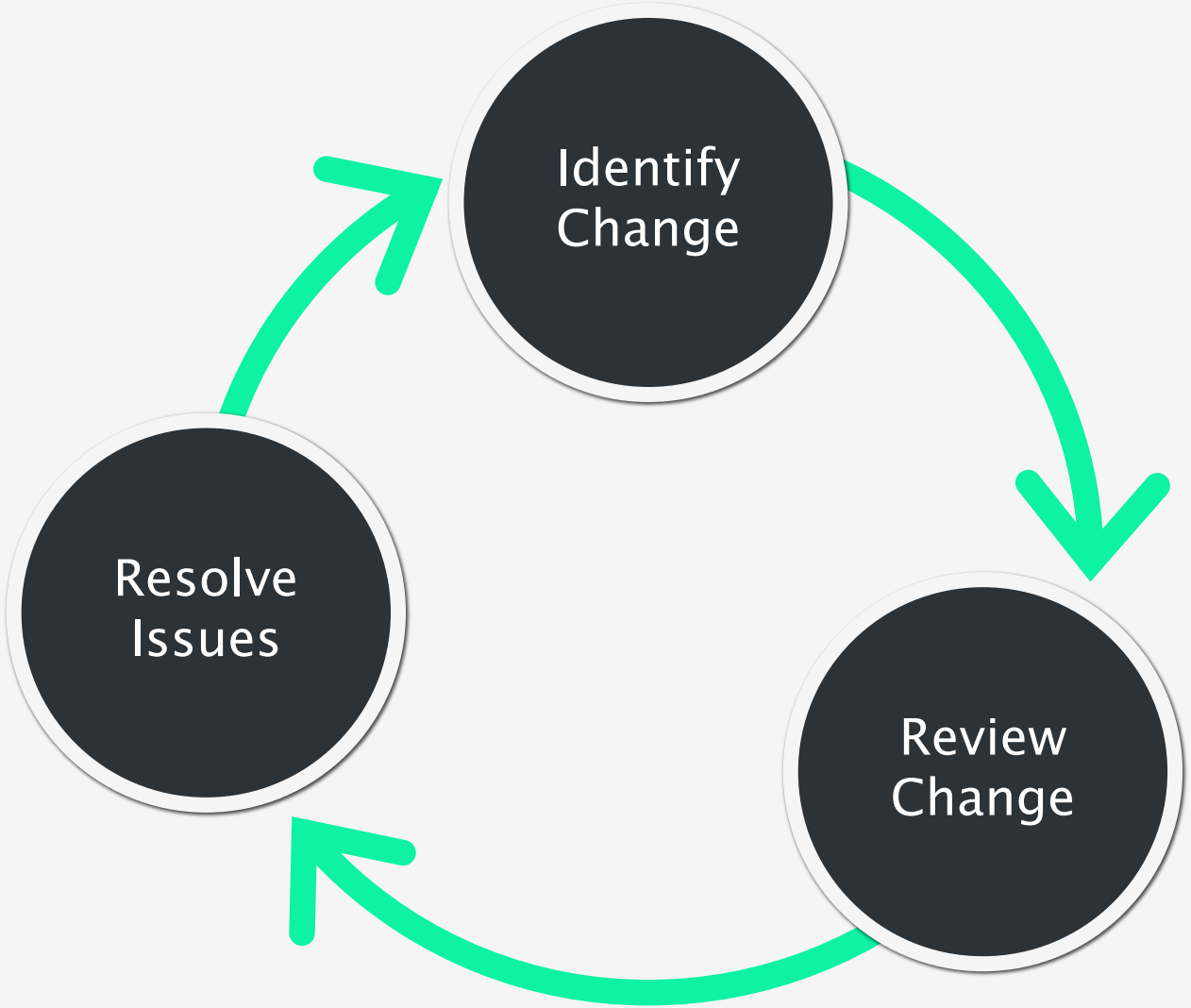
- Fully-automated purple team deployment
- Standardised, centralised, reproducible

One consultant, one day


MWR
INFOSECURITY
Scaling Cloud Security
LABS

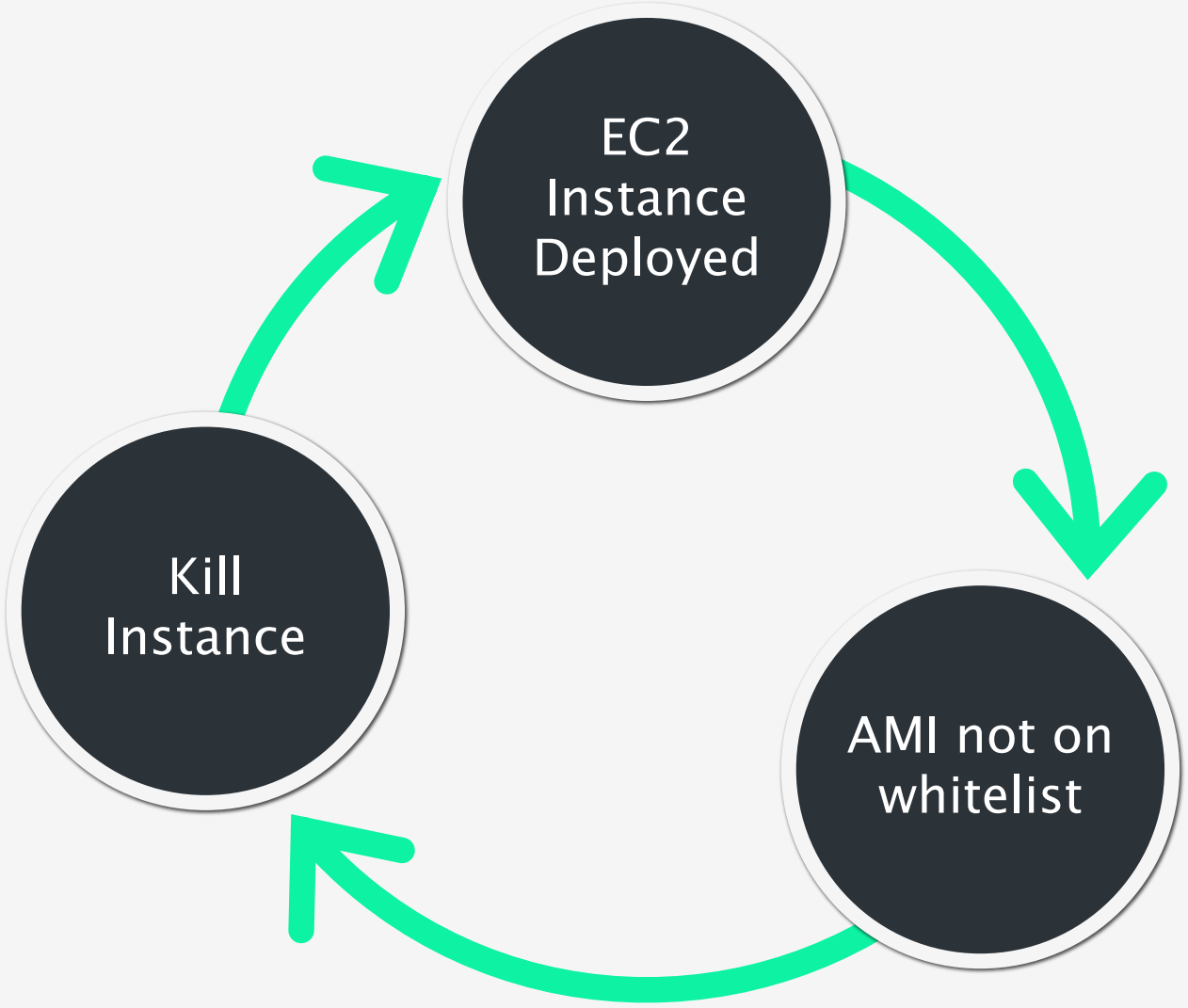
Continuous Configuration Review

Continuous Configuration Enforcement



Remediation time: 30 minutes

Continuous Configuration Enforcement



Remediation time: 30 minutes

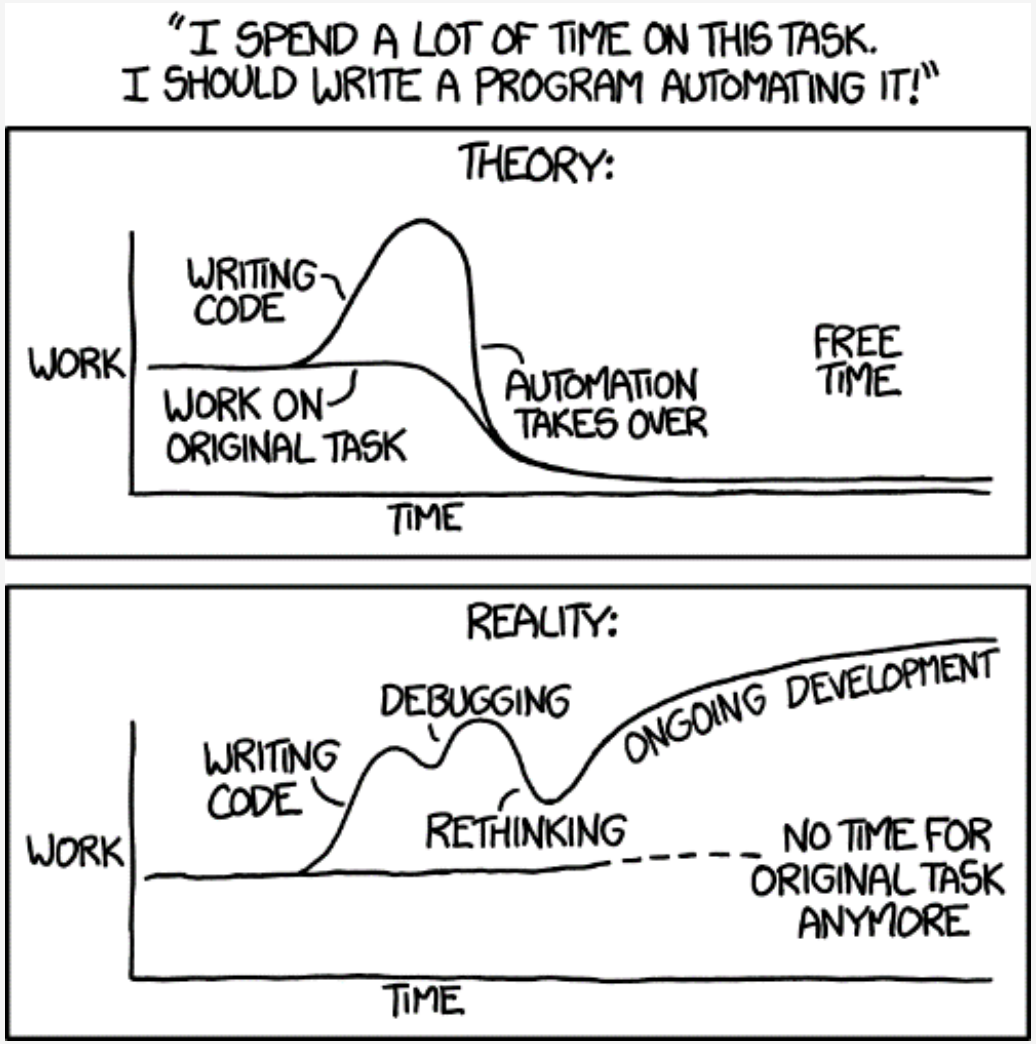
Existing Work

MWR LABS

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

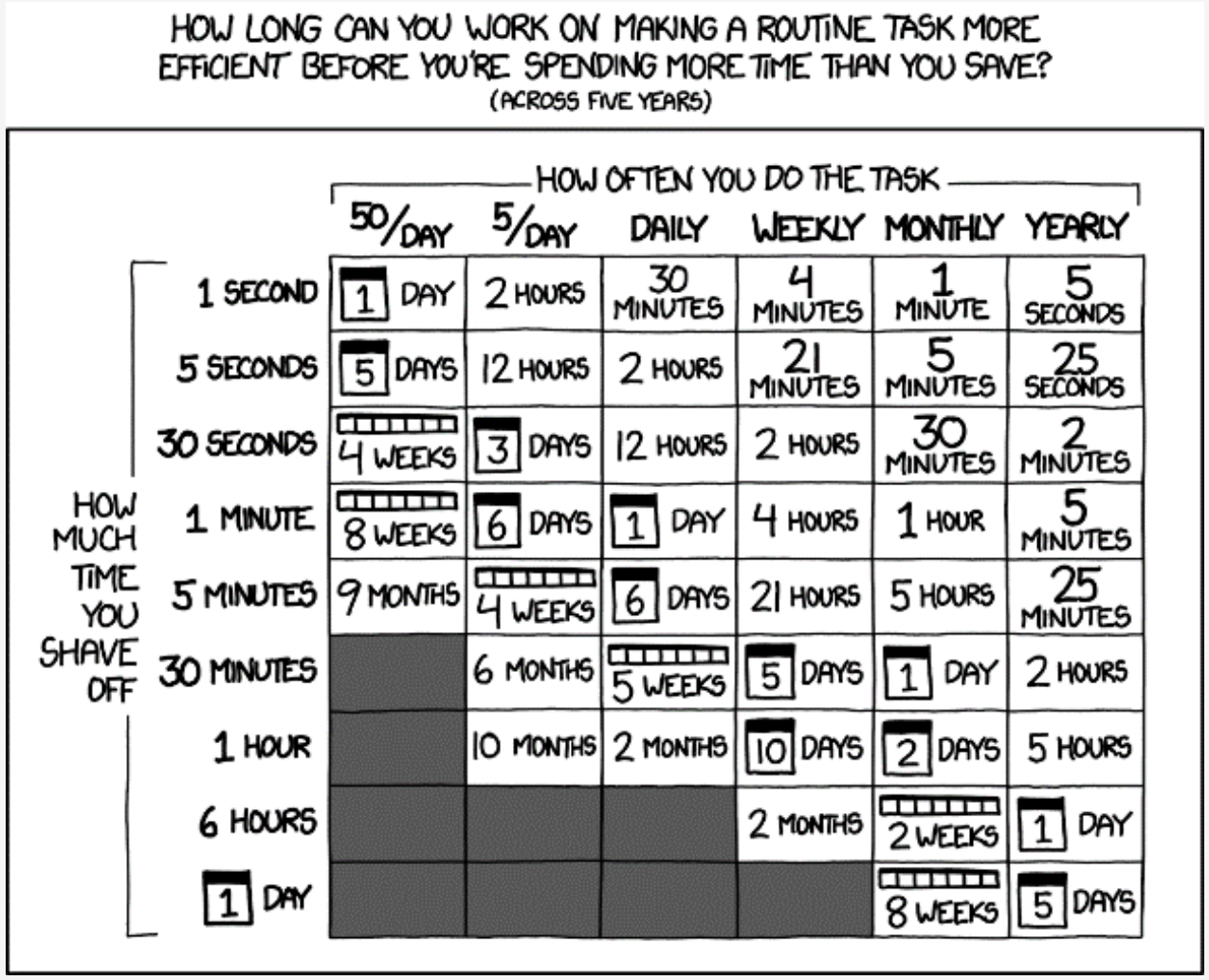

MWR
INFOSECURITY
Gotchas
LABS

Balance of Effort



Some things just aren't worth automating

MWR LABS

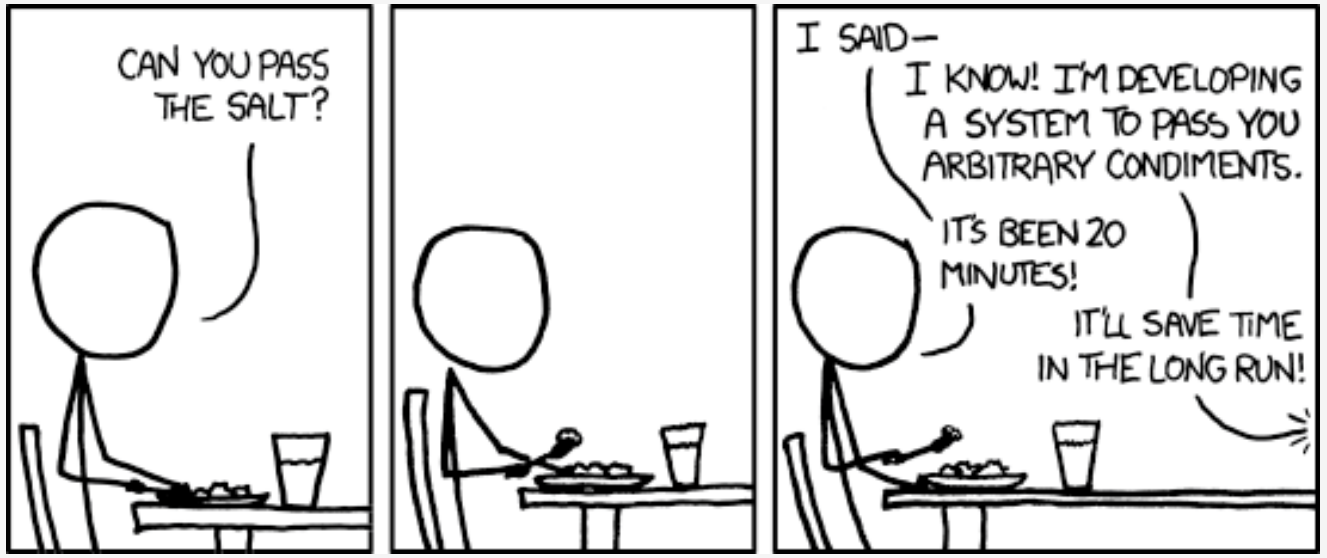

HOW LONG CAN YOU WORK ON MAKING A ROUTINE TASK MORE EFFICIENT BEFORE YOU'RE SPENDING MORE TIME THAN YOU SAVE?
(ACROSS FIVE YEARS)
HOW OFTEN YOU DO THE TASK
50/DAY
5/DAY
DAILY
WEEKLY
MONTHLY
YEARLY
HOW MUCH TIME YOU SHAVE OFF
1 SECOND
1 DAY
2 HOURS
30 MINUTES
4 MINUTES
1 MINUTE
5 SECONDS
5 SECONDS
5 DAYS
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

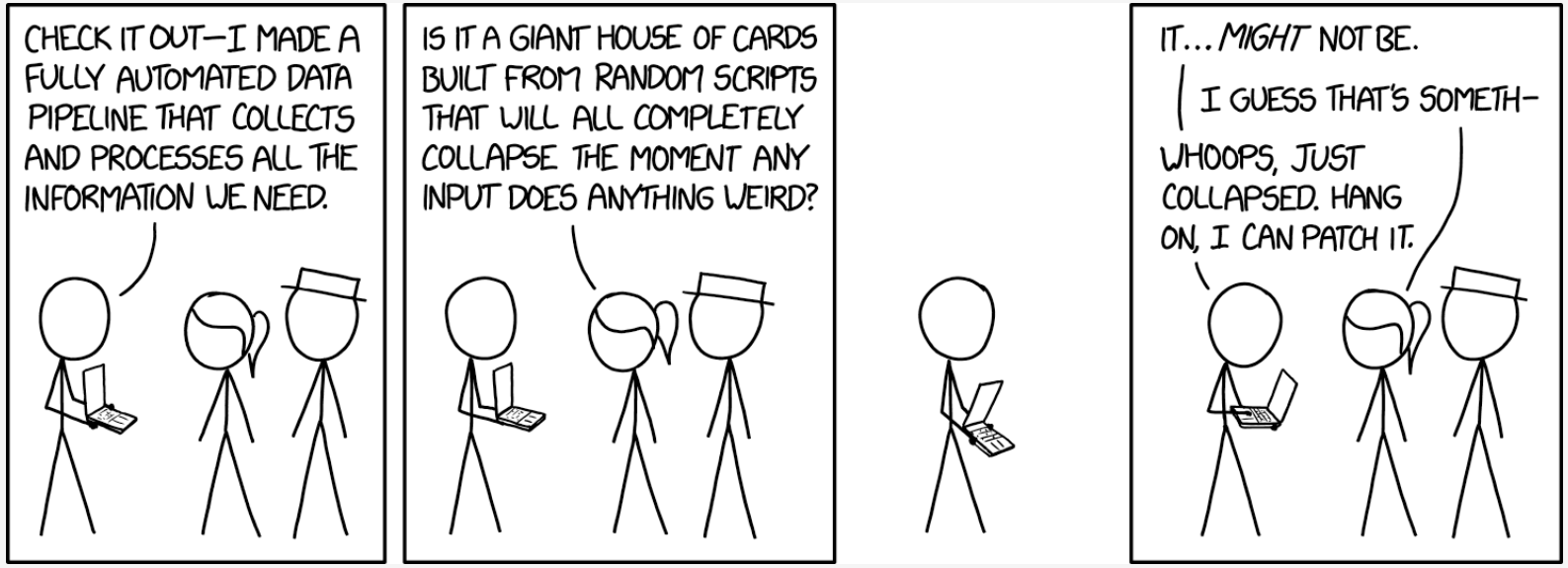
MWR LABS

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

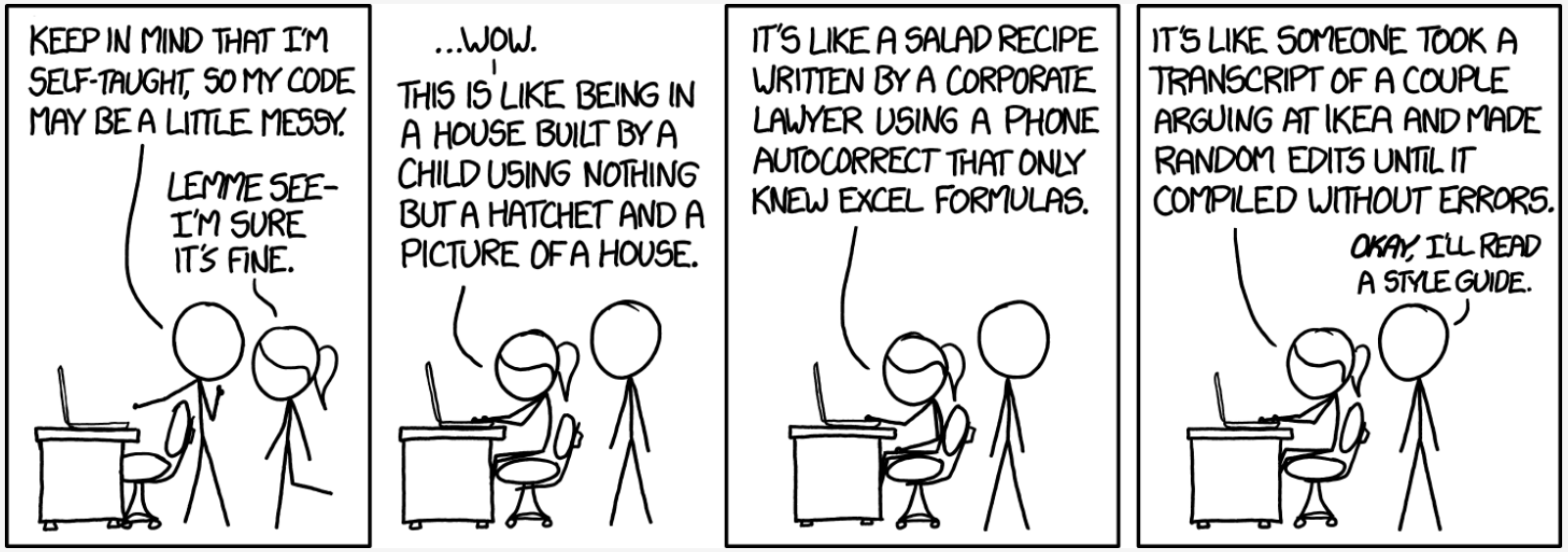
Know Your Limits

MWR LABS

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?

MWR LABS

- Never automated anything before?

Something small and simple	Something worthwhile	Something that irritates people

Conclusions

MWR LABS

Automation is the only way to secure at scale

Efficiency improvements benefit everyone

Knowing how and when to automate will keep you employed

MWR INFOSECURITY

Questions?

LABS