HashiCorp

Security in a DevOps World

DevOpsPro 2019

Peter Souter

Technical Account Manager - HashiCorp

Introductions - Who is this guy?

Technical Account Manager at HashiCorp
Peter Souter

Based in…
London, UK

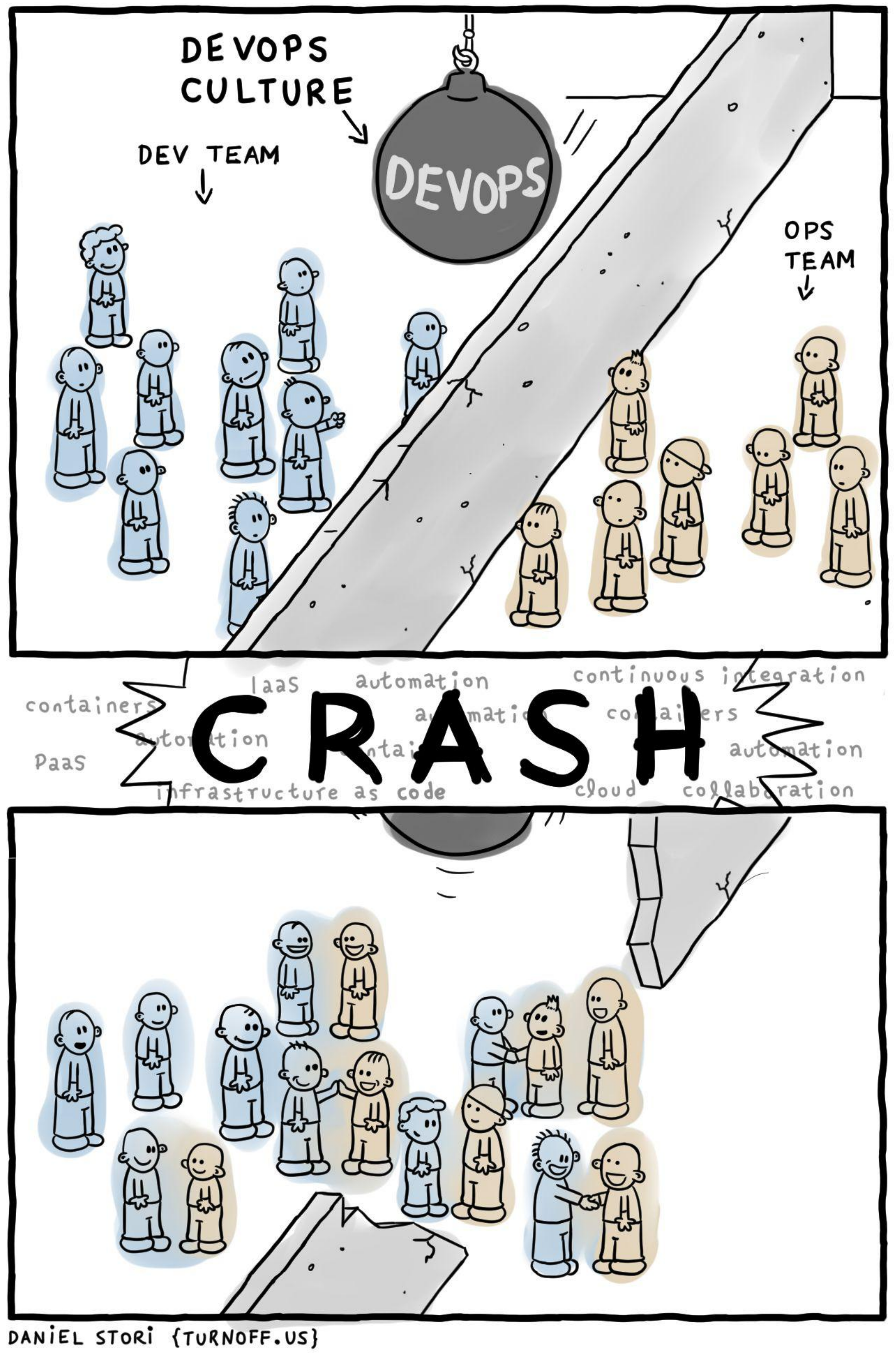
First time in Lithuania
Vilinus is an awesome city!

Worn a lot of hats in my time…
Developer, Consultant, Pre-Sales, TAM

Interested in…
Making people's operational life easier and more secure

DEVOPS ALL THE THINGS

So what is DevOps?

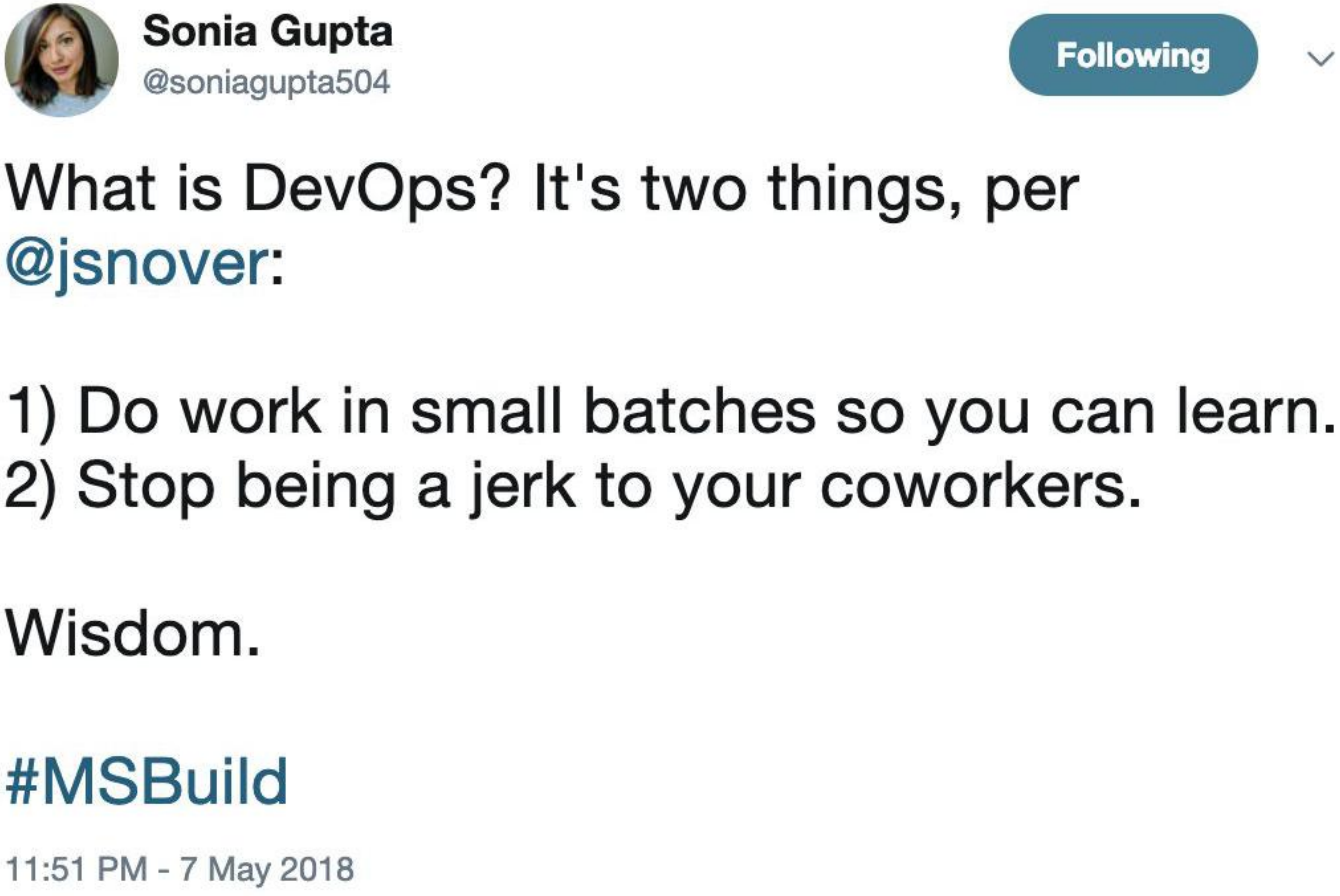


http://turnoff.us/geek/devops-explained/

- Agile/lean principles
- CALMS
- Removing silos
- Iterative delivery of software
- Delivering customer value

@petersouter

Summarised...



Sonia Gupta
@soniagupta504

What is DevOps? It's two things, per @jsnover:

1) Do work in small batches so you can learn.
2) Stop being a jerk to your coworkers.

Wisdom.

#MSBuild

11:51 PM - 7 May 2018

The old way of doing things...

Winston Royce's "Managing The Development of Large Software Systems" - 1976.

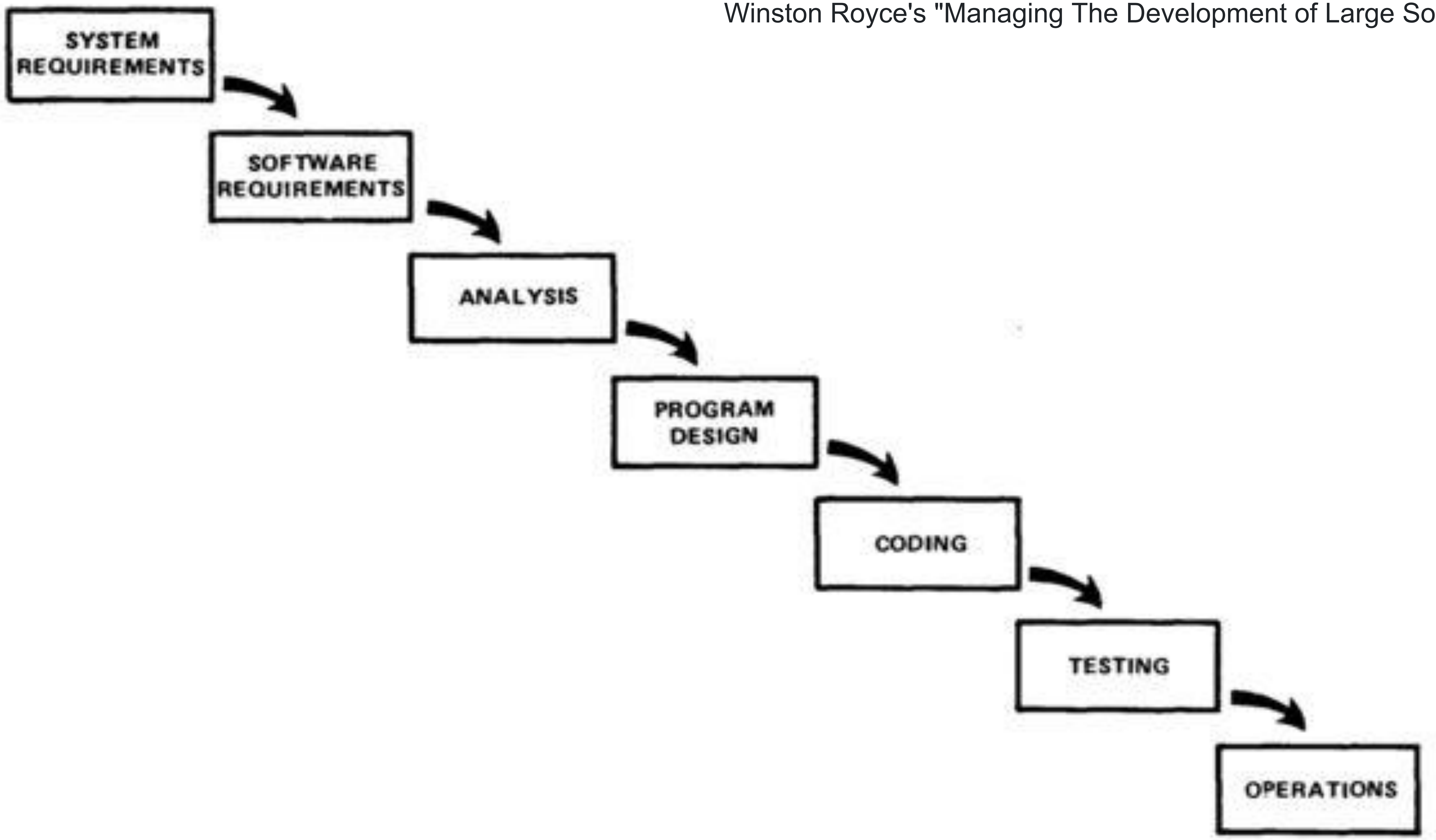
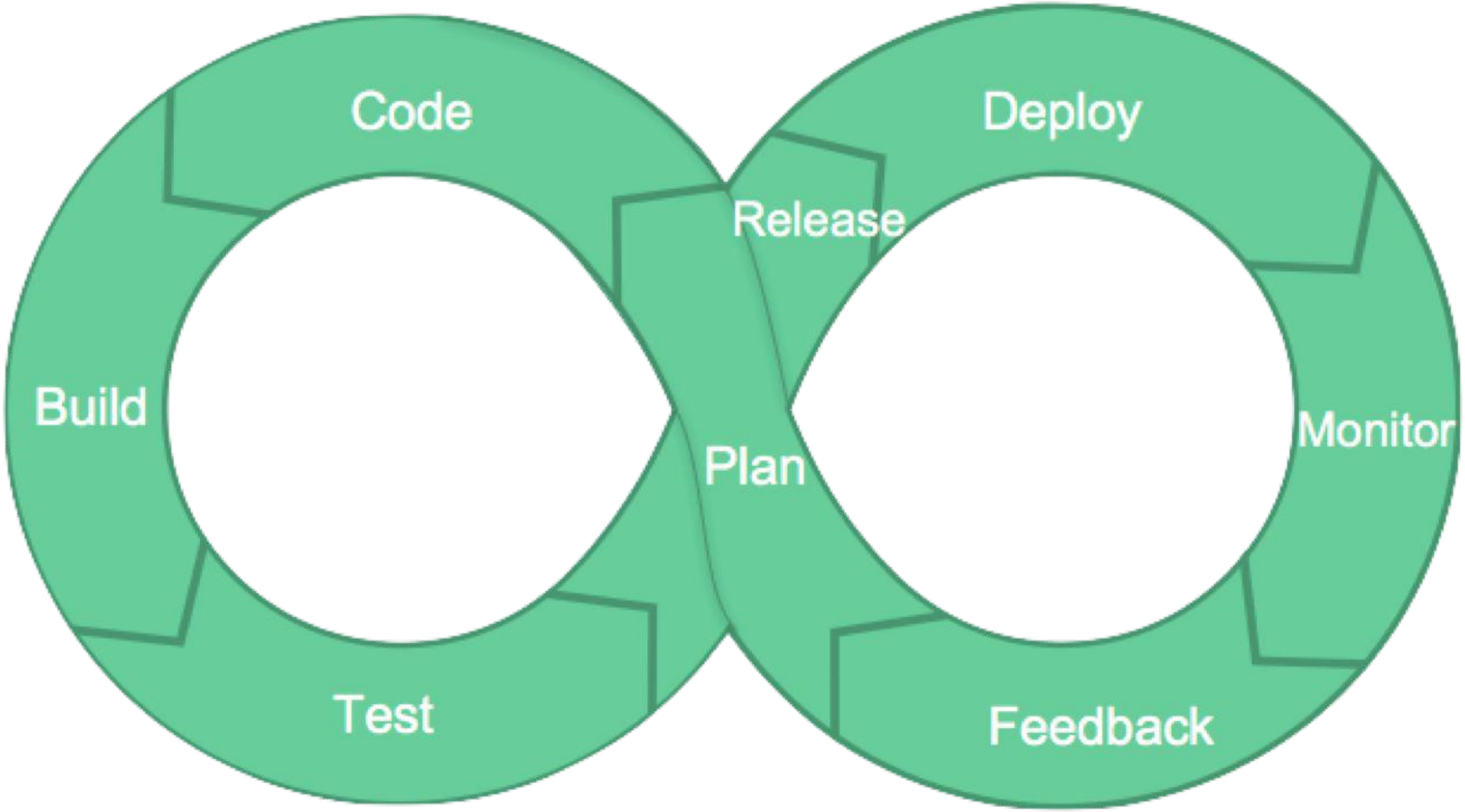


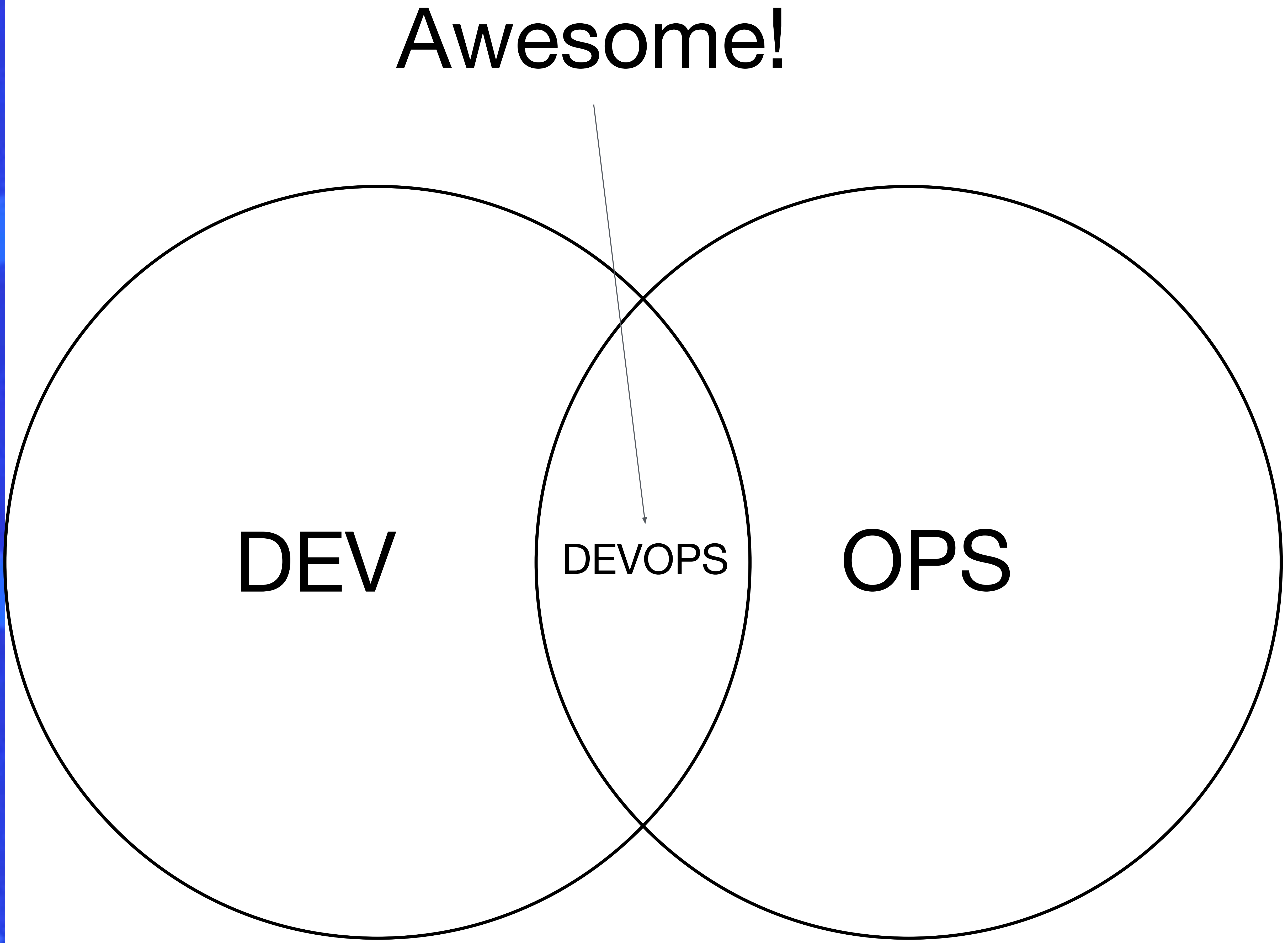
Figure 2. Implementation steps to develop a large computer program for delivery to a customer.

@petersouter

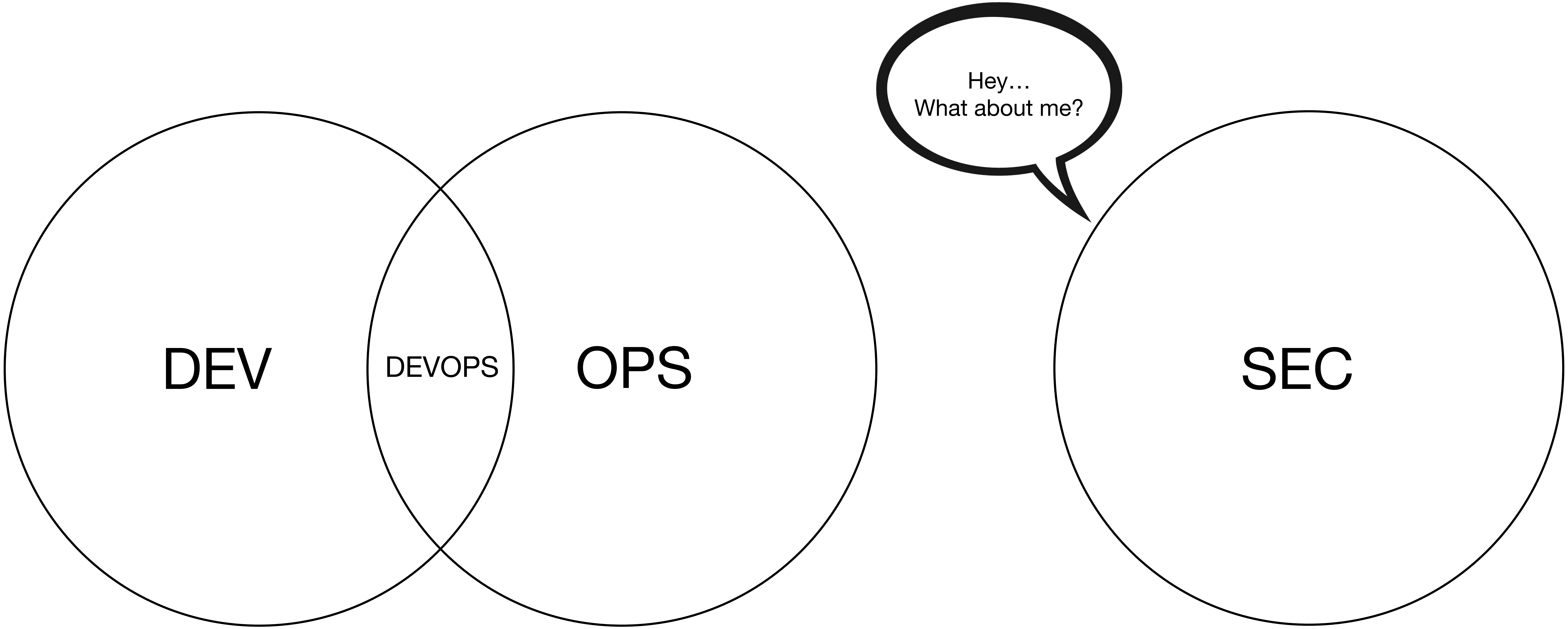
The new way of doing things...



Ok, so we've enabled a DevOps culture

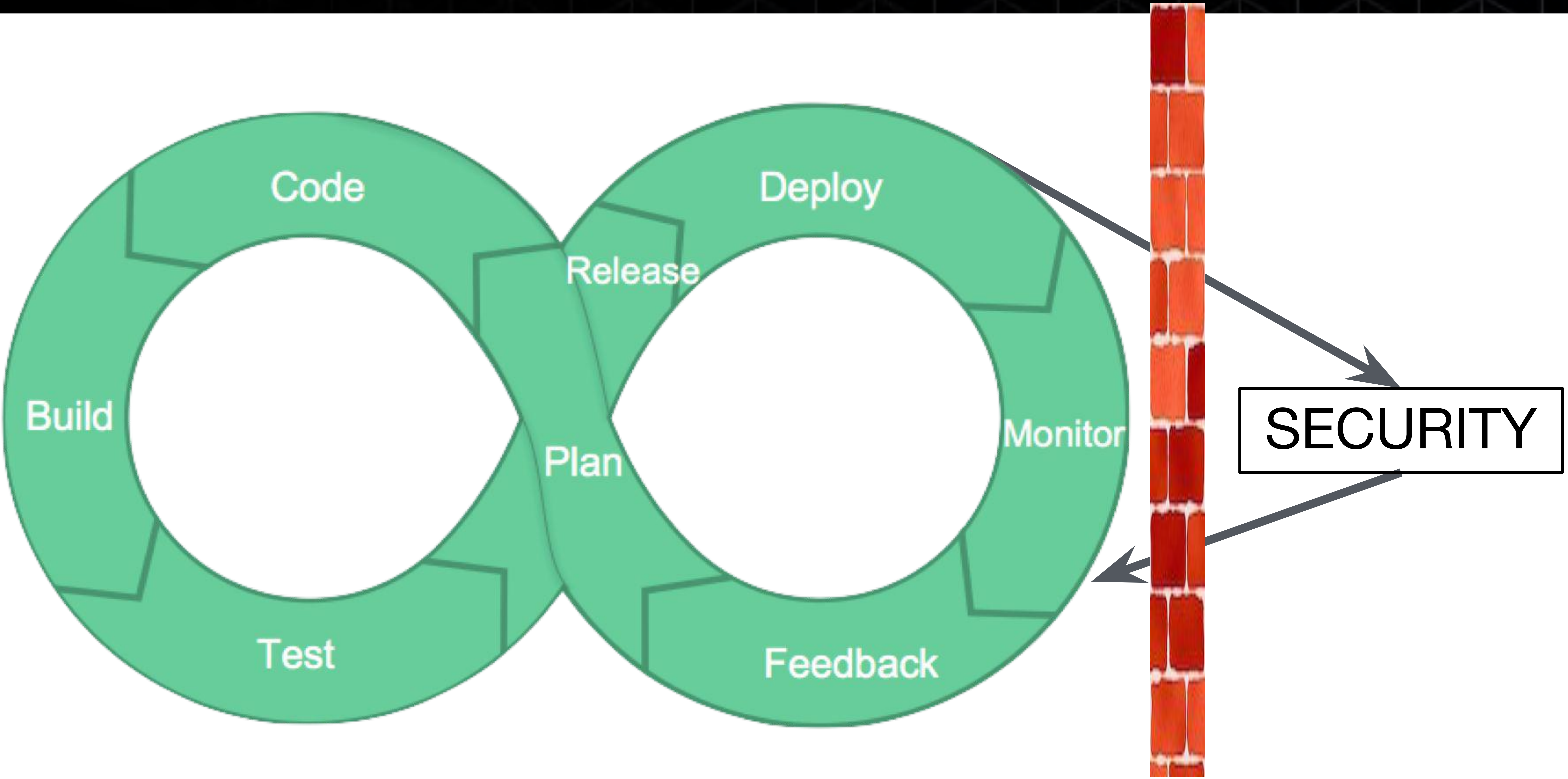


Wait...A new silo appears!



Maybe not so awesome...

The old way of doing things… returns?

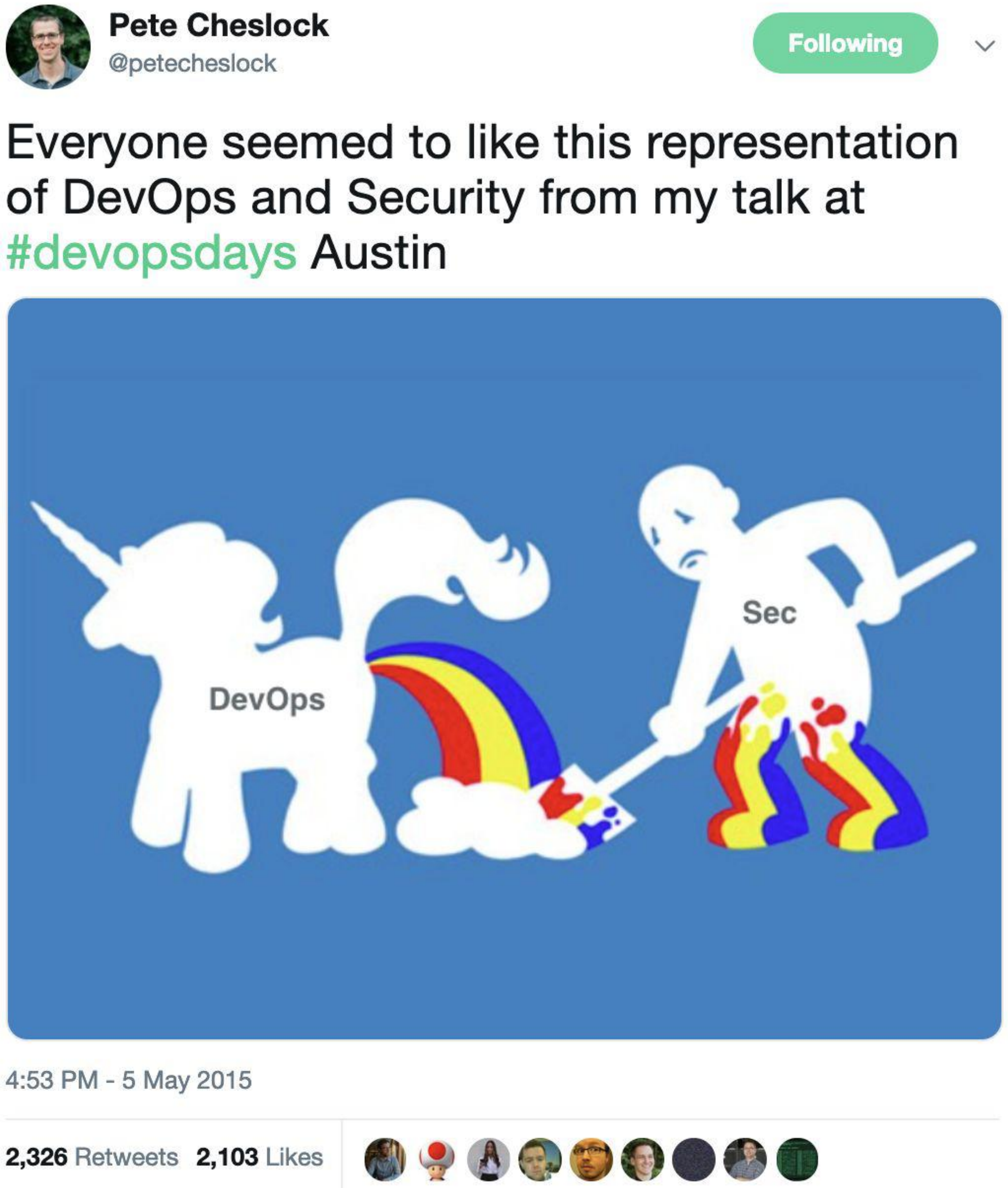


Security as the new silo…

https://flic.kr/p/uw9QRD

- Manual processes
- Dead-tree documents
- Defaulting to no
- Lack of automation
- Black box processes

Summarised...



Pete Cheslock
@petecheslock

Following

Everyone seemed to like this representation of DevOps and Security from my talk at #devopsdays Austin

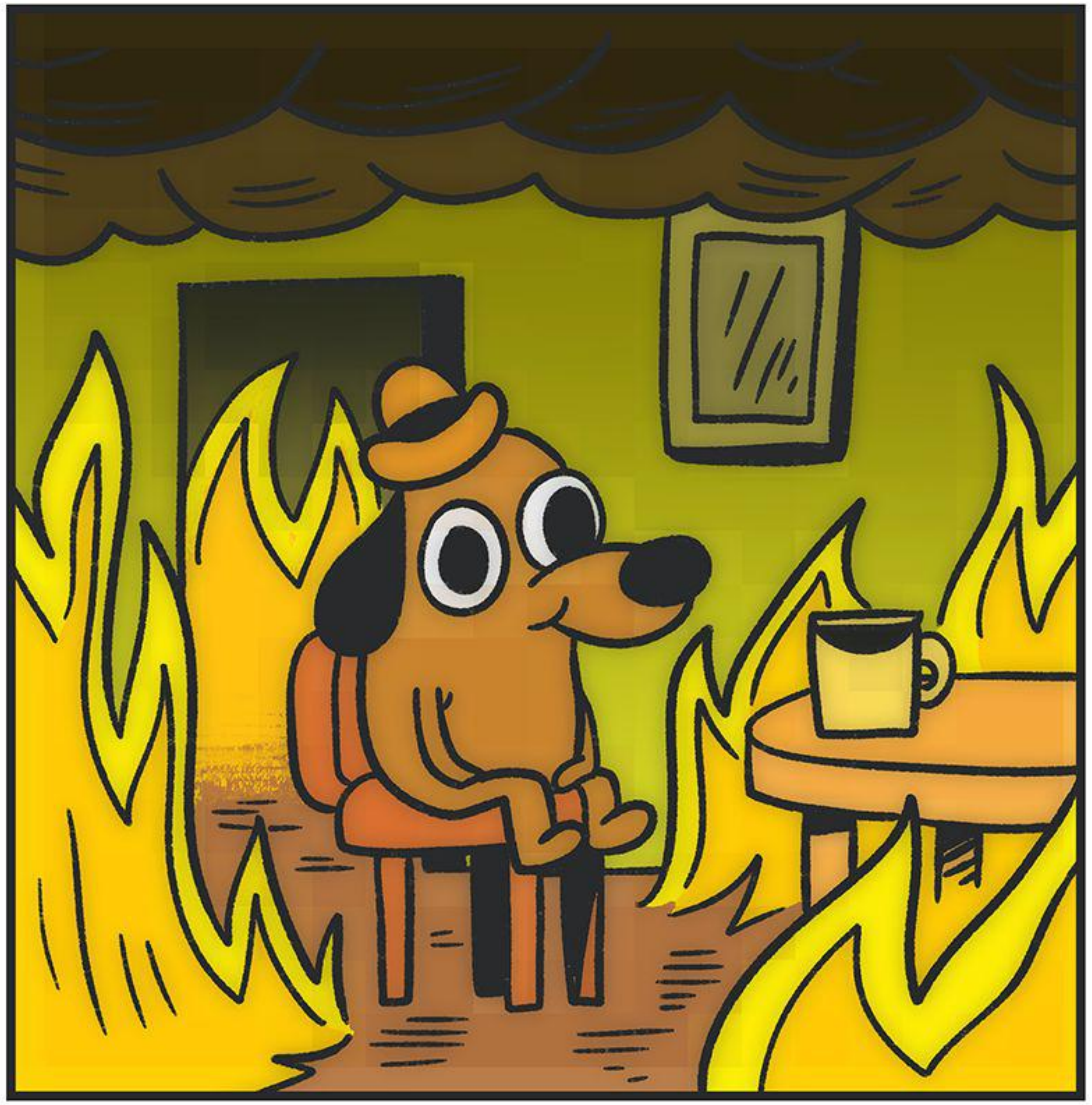
4:53 PM - 5 May 2015

2,326 Retweets 2,103 Likes

What happens with a silo’d/blocker Sec process?

- Shadow IT
- Slow delivery time
- Frustrated devs and PMs
- Unable to use new technologies and innovate

What happens with no Sec process?



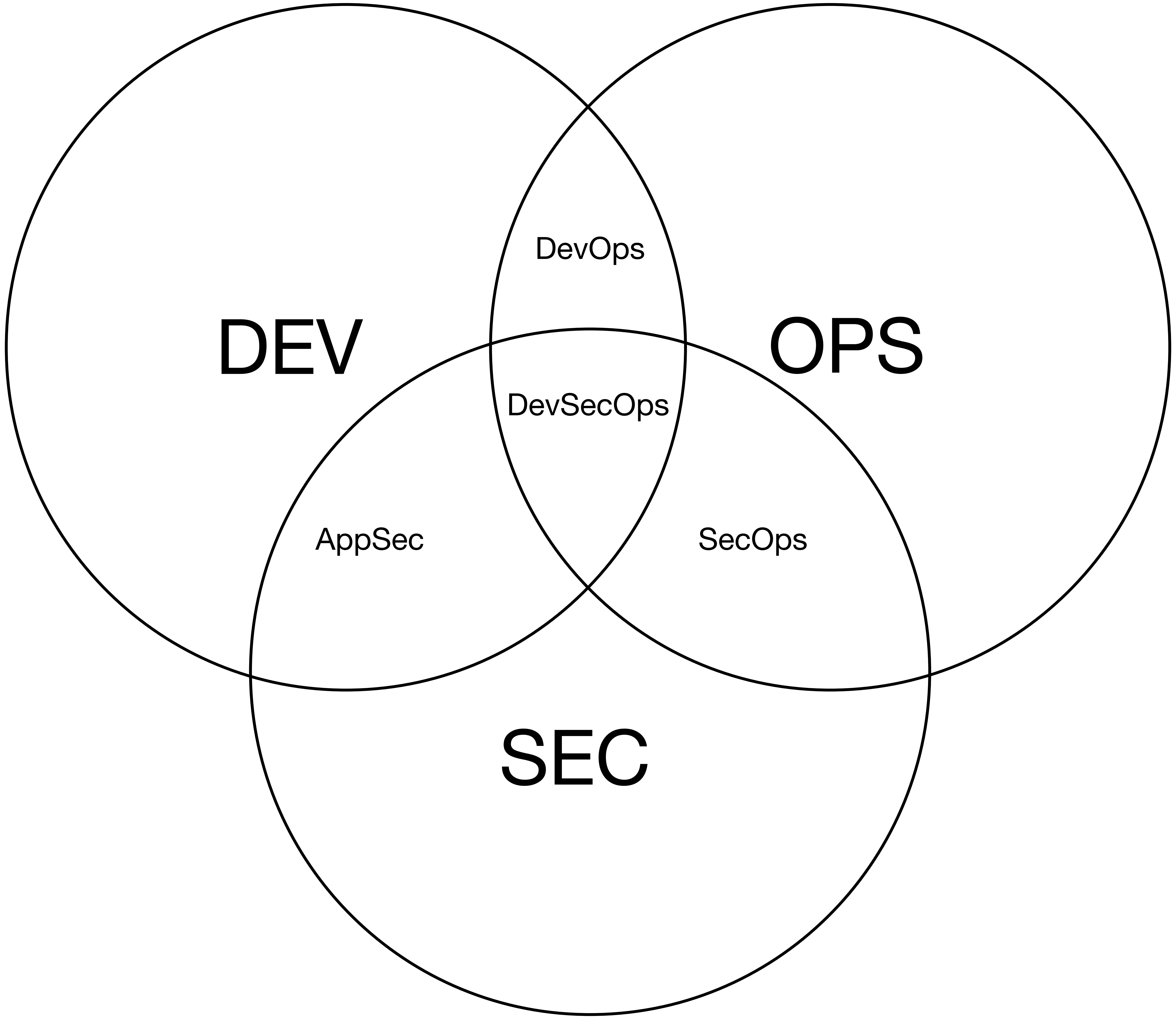
- Crypto Ransom
- Data theft
- Loss of Customers
- Legal and PR fires

You can't stop everything

- Blocking everything is impossible
- Defense in depth
- Reduce the blast radius
- Detect oddities and outliers

https://flic.kr/p/np68Q1

So… what do we do?



Aka

- DevSecOps
- Rugged Software,
- Rugged DevOps,
- SecDevOps,
- DevOpsSec
- DevOps (?!)

@petersouter

Sidebar: Isn’t this just DevOps?

Tl;dr… kinda?

Sidebar: Rugged Software

I am rugged and, more importantly, my code is rugged.

I recognize that software has become a foundation of our modern world.

I recognize the awesome responsibility that comes with this foundational role.

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic, and national security.

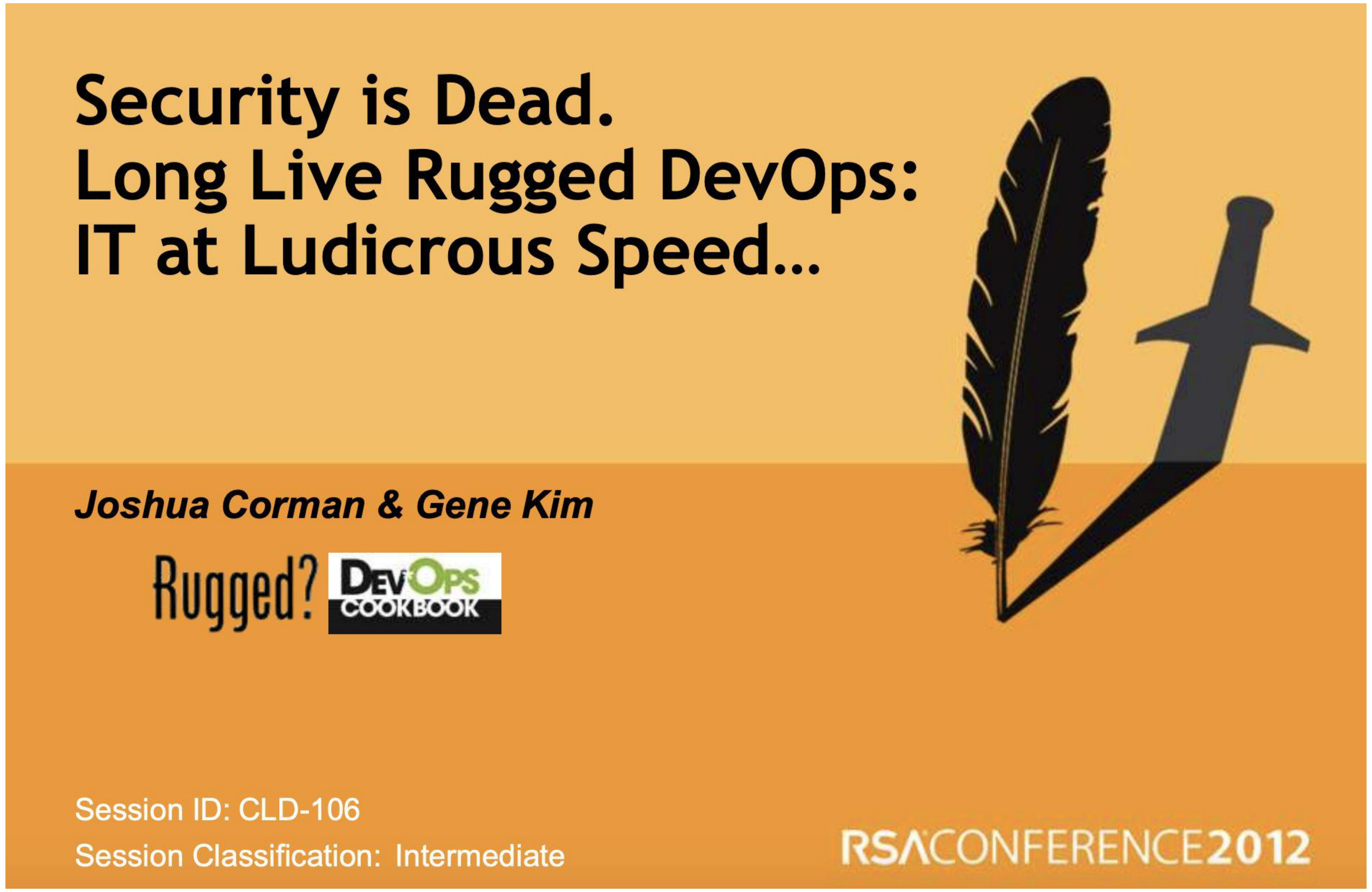
I recognize these things - and I choose to be rugged.

I am rugged because I refuse to be a source of vulnerability or weakness.

I am rugged because I assure my code will support its mission.

I am rugged because my code can face these challenges and persist in spite of them.

I am rugged, not because it is easy, but because it is necessary and I am up for the challenge.



Security is Dead.
Long Live Rugged DevOps:
IT at Ludicrous Speed…

Joshua Corman & Gene Kim

Rugged?
DevOps Cookbook

Session ID: CLD-106
Session Classification: Intermediate

RSA CONFERENCE 2012

Whatever the name, what is the core principle?

Shift
Security
Left

What does shifting security left mean?

“Security must “shift left,” earlier into design and coding and into the automated test cycles, instead of waiting until the system is designed and built and then trying to fit some security checks just before release”

- **DevOpsSec: Delivering Secure Software Through Continuous Delivery, Jim Bird**

Examples of shifting it left

Plan	Develop	Test	Deploy	Operate
‘Evil user’ stories	Hardened Software Frameworks	Static Code Analysis	System Hardening	Observability
Security Requirements	Sec Focused Code Review	Pentesting	Patching	Anomaly and Threat detection
		Game Days - Red Teams		

Shifting left leads to sub-goals being achieved

The more security shifted left the more security:

...stops being an afterthought

...becomes embedded in processes

...starts being a shared responsibility

Security is everyone’s responsibility!

Like fire safety...

Security becomes everyone's responsibility!

This doesn’t mean only non-Sec people do security

This doesn’t mean you don’t need a Security team

How does this look in teams?

Similar to DevOps approach:

Security Champions and SME’s

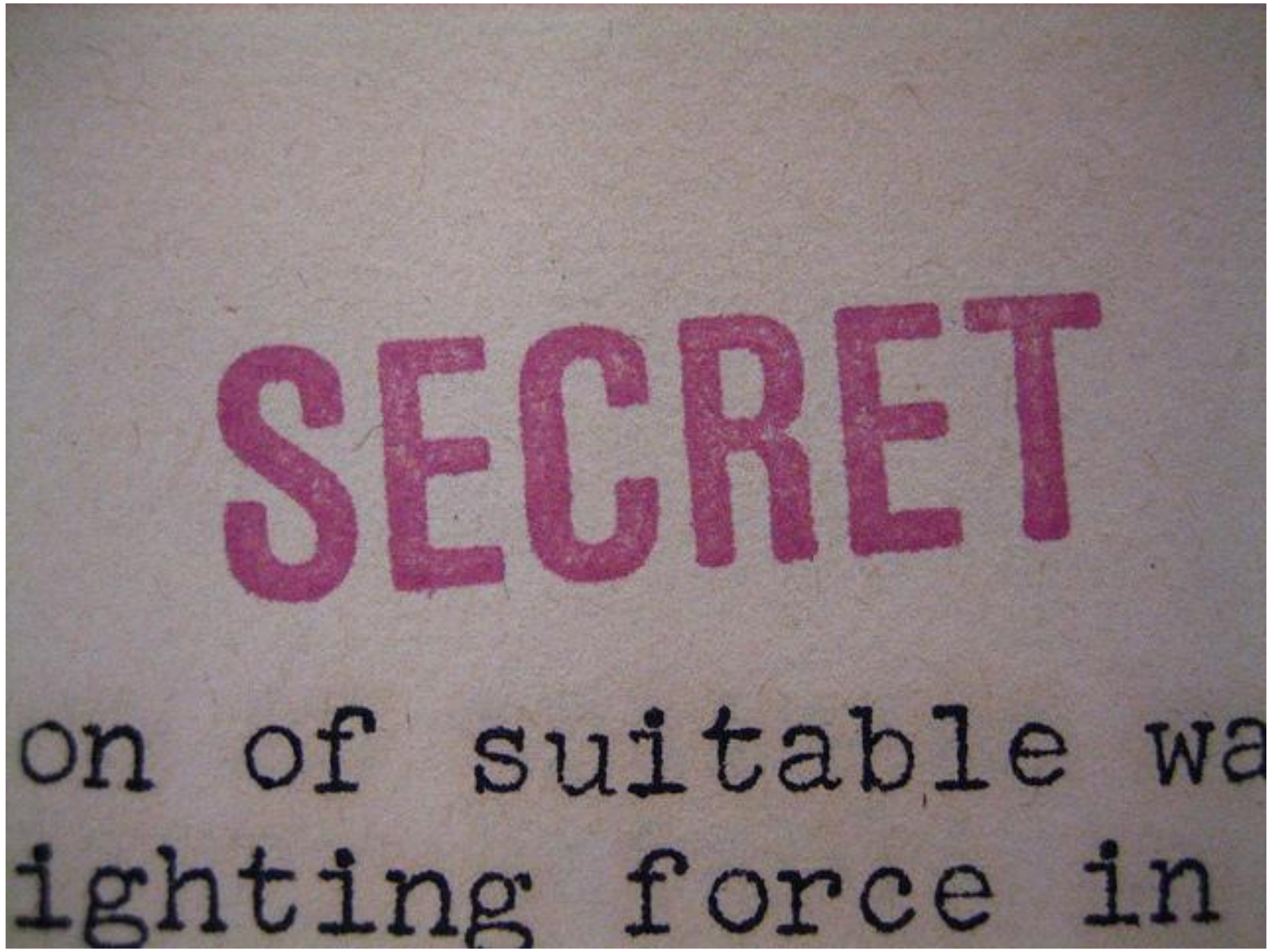
Embedded Security Engineers in squads

Dedicated Security tasks within the larger Sec team

“Where do we even begin?”

- Pick a particular area that's causing pain
- Set a baseline
- Iterate and make it better
- No big bang changes!

Secret management as an example...



- Something I’ve had a lot of experience in my career
- Reflects a lot of the changes that have come up in operations and sec
  - ○ Static -> Dynamic
  - ○ Pets -> Lifestock
- New solutions are needed!

What are Secrets?

Small
A few kb
at most

Required
Software won't
work without
them!

Radioactive
Consequences
are dire if leaked

Examples
Passwords,
API Keys,
SSH Keys,
SSL Certs

https://flic.kr/p/dHrwpb

Different Teams = Different requirements

I want to be able to use a database for my app

Dev

I want to be able to provide database credentials for running applications

Ops

I want database credentials stored in a safe way and provided following our policies

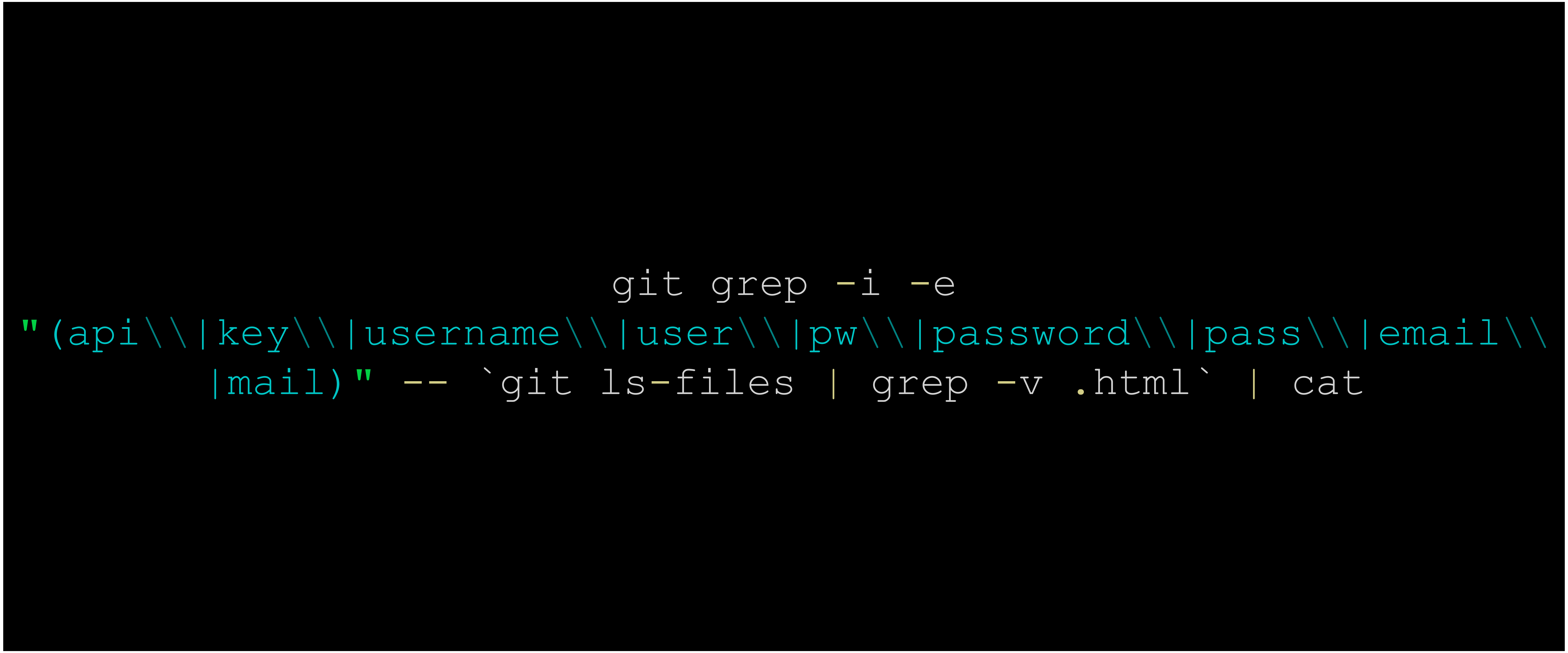
Sec

@petersouter

Begin - Set a Secrets Baseline: Iteration 1

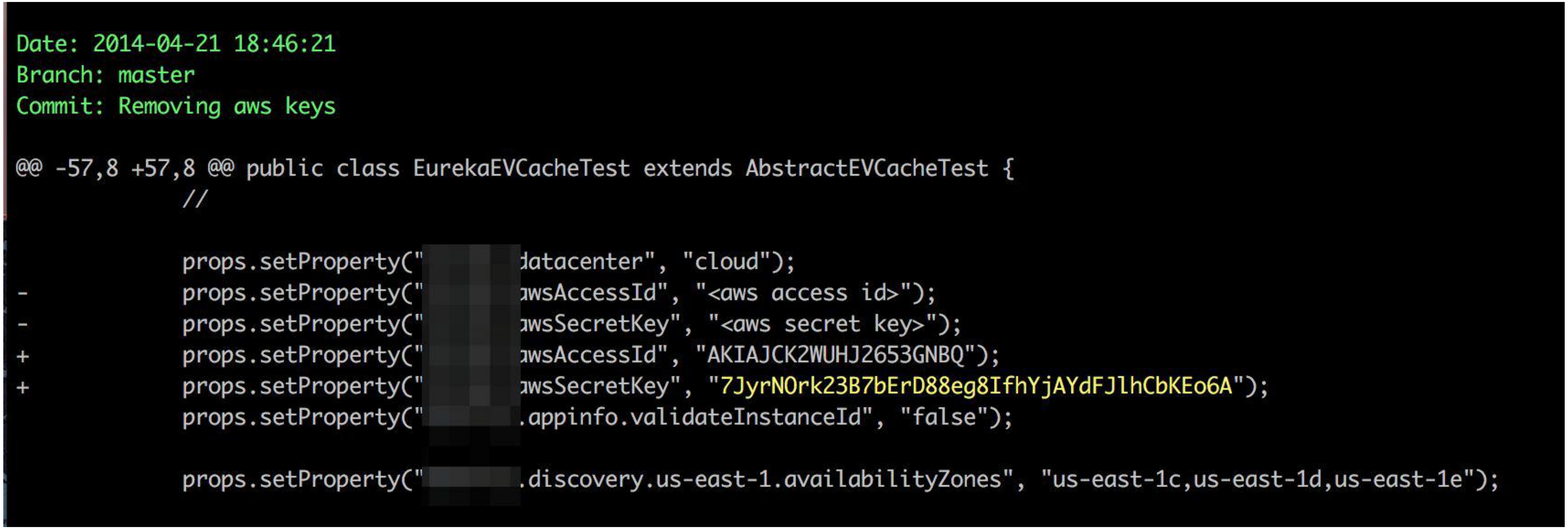
“Let's set a baseline: let's find all the existing secrets in our codebase. We can then rotate, remove and replace to get us to a good start point with no leaked credentials”

Detecting existing secrets - Scripting



```
git grep -i -e
"(api\\|key\\|username\\|user\\|pw\\|password\\|pass\\|email\\
|mail)" -- `git ls-files | grep -v .html` | cat
```

Detecting existing secrets - Trufflehog

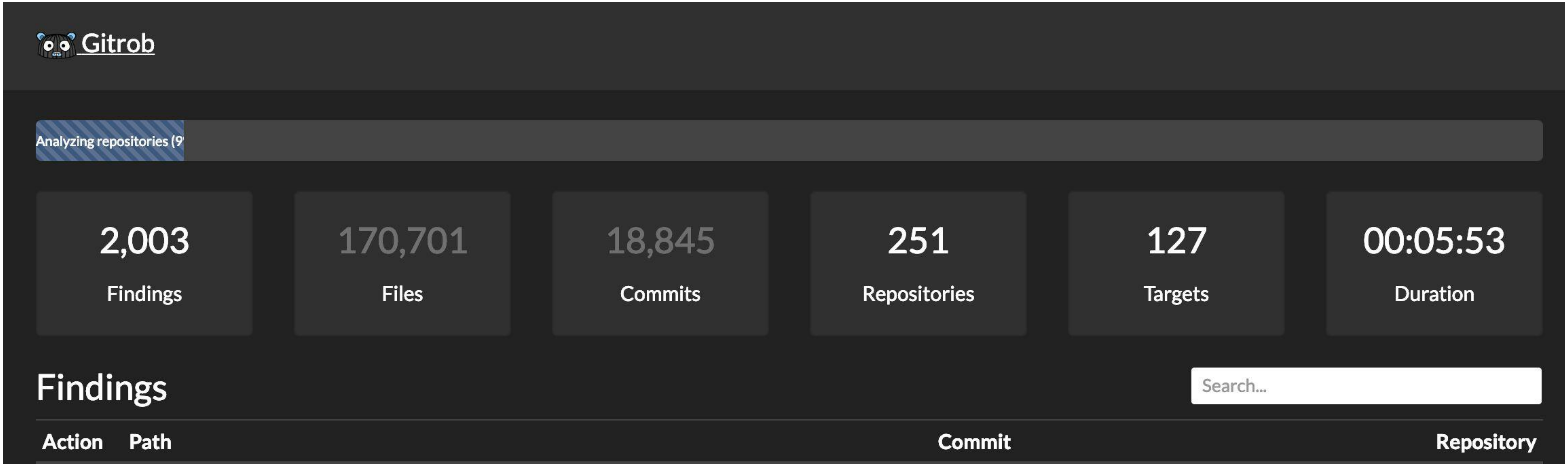


```
Date: 2014-04-21 18:46:21
Branch: master
Commit: Removing aws keys

@@ -57,8 +57,8 @@ public class EurekaEVCacheTest extends AbstractEVCacheTest {
            //

            props.setProperty("[redacted]datacenter", "cloud");
-           props.setProperty("[redacted]awsAccessId", "<aws access id>");
-           props.setProperty("[redacted]awsSecretKey", "<aws secret key>");
+           props.setProperty("[redacted]awsAccessId", "AKIAJCK2WUHJ2653GNBQ");
+           props.setProperty("[redacted]awsSecretKey", "7JyrNOrk23B7bErD88eg8IfhYjAYdFJlhCbKEo6A");
            props.setProperty("[redacted].appinfo.validateInstanceId", "false");

            props.setProperty("[redacted].discovery.us-east-1.availabilityZones", "us-east-1c,us-east-1d,us-east-1e");
```

https://github.com/dxa4481/truffleHog

@petersouter

Detecting existing secrets - Gitrob



Gitrob

Analyzing repositories (9

2,003	170,701	18,845	251	127	00:05:53
Findings	Files	Commits	Repositories	Targets	Duration

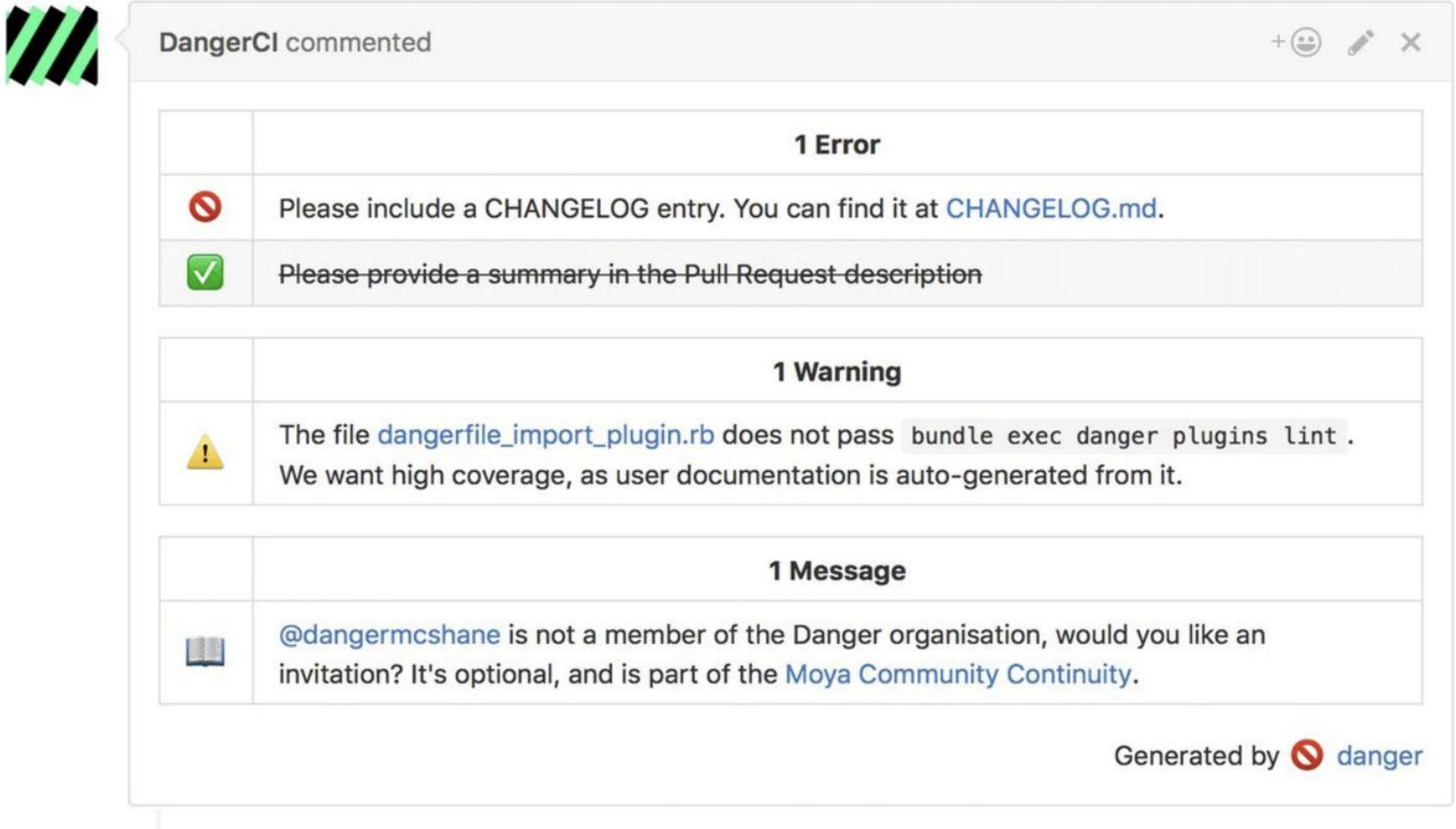
Findings

Action	Path	Commit	Repository

https://github.com/michenriksen/gitrob

@petersouter

Stopping Secrets being reintroduced: https://danger.systems



DangerCI commented

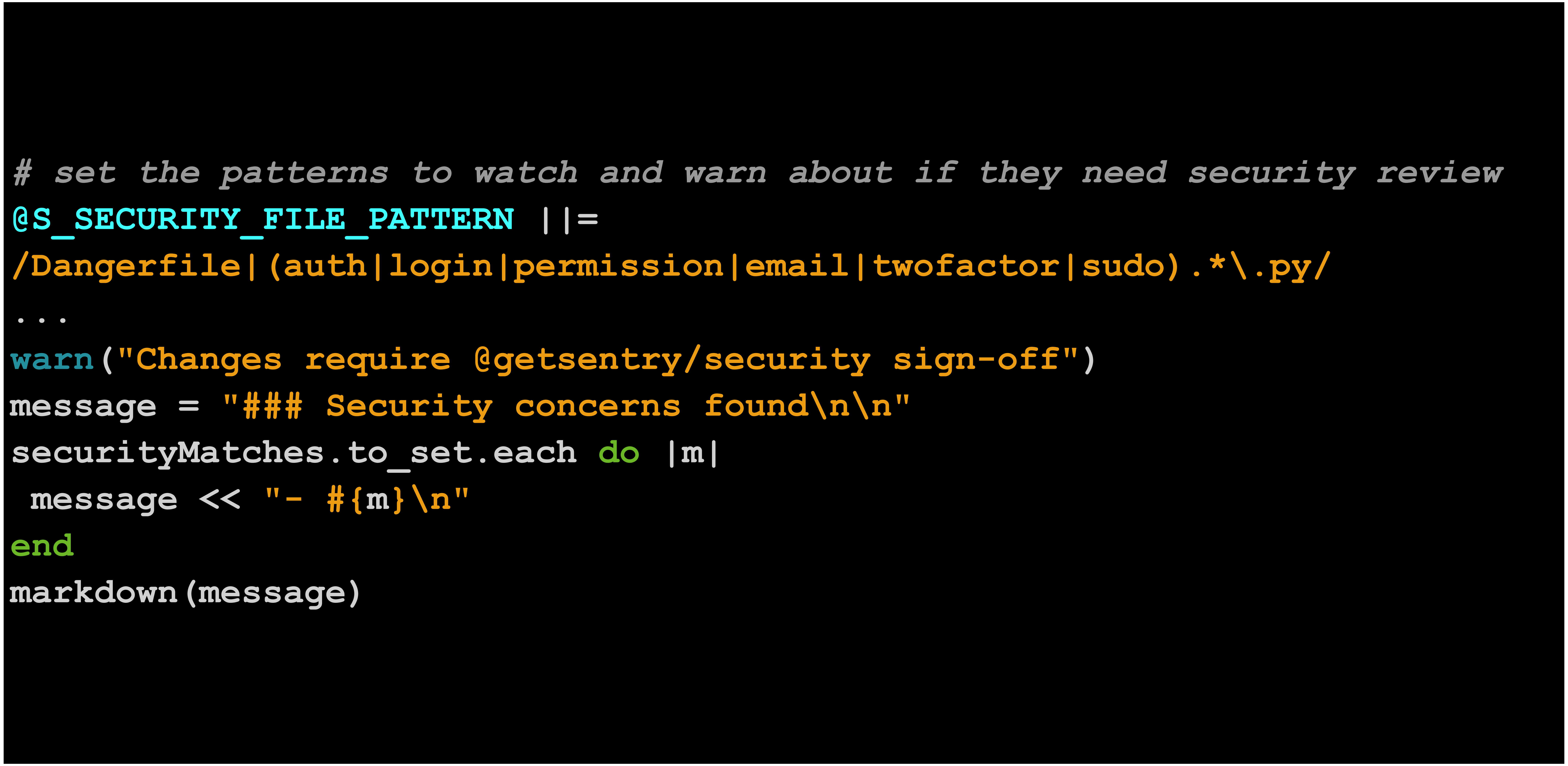
	1 Error
🚫	Please include a CHANGELOG entry. You can find it at CHANGELOG.md.
✅	~~Please provide a summary in the Pull Request description~~

	1 Warning
⚠️	The file dangerfile_import_plugin.rb does not pass `bundle exec danger plugins lint`. We want high coverage, as user documentation is auto-generated from it.

	1 Message
📖	@dangermcshane is not a member of the Danger organisation, would you like an invitation? It's optional, and is part of the Moya Community Continuity.

Generated by 🚫 danger

Sec Focused Code Review: https://danger.systems



```
# set the patterns to watch and warn about if they need security review
@S_SECURITY_FILE_PATTERN ||=
/Dangerfile|(auth|login|permission|email|twofactor|sudo).*\.py/
...
warn("Changes require @getsentry/security sign-off")
message = "### Security concerns found\n\n"
securityMatches.to_set.each do |m|
 message << "- #{m}\n"
end
markdown(message)
```

https://github.com/getsentry/sentry/blob/ac8fe045fb161e67140d5d2959381b74f0738dc8/Dangerfile

Setting a Secrets Baseline: Iteration 2

“Now we have a baseline, lets create a way of storing our secrets in a secure way with good gating processes”

Key Point: Security is not a product!

We'll be talking about an area I've worked in a lot

and a product from my company that can help

But remember: **Security is not something that you can be sold!**

It's monitoring and metrics, gating and reviews

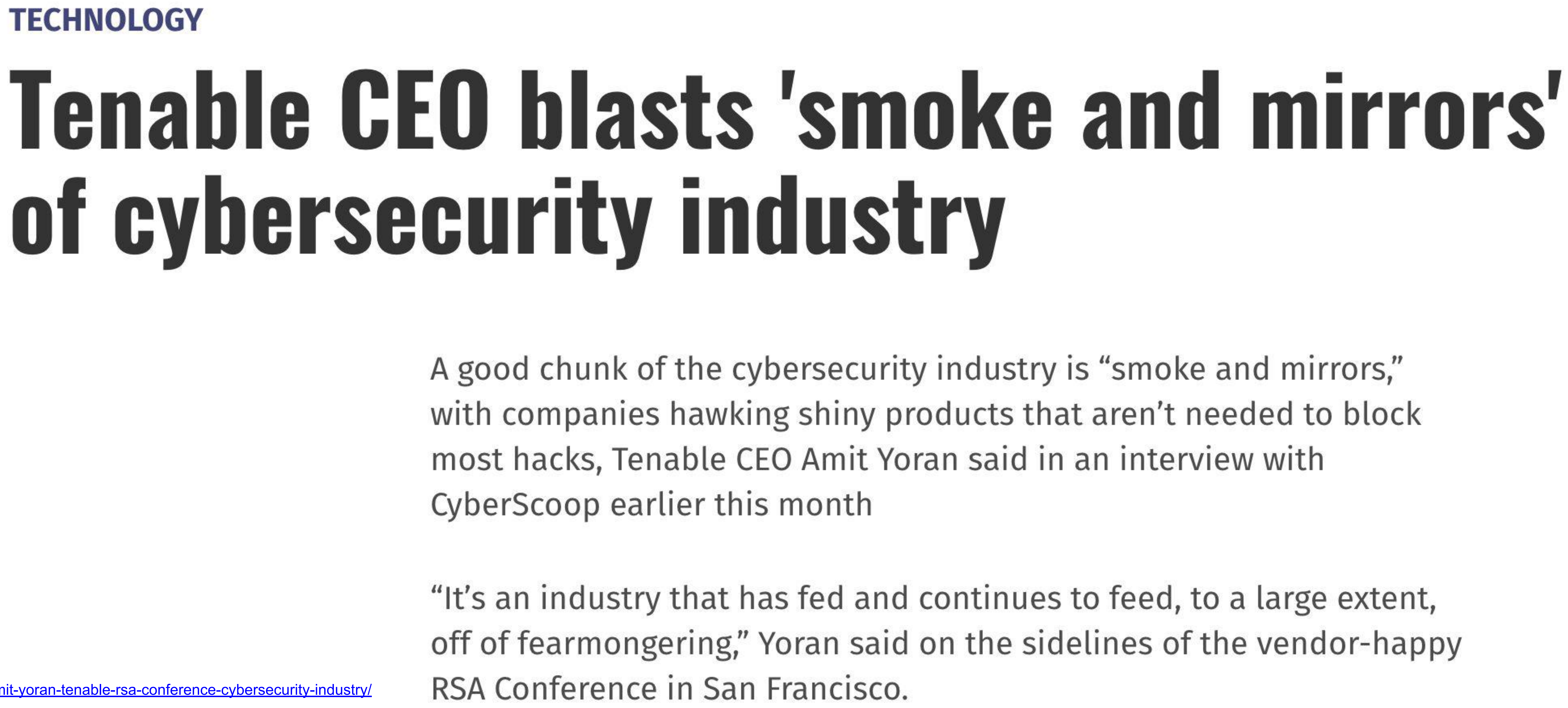
It's People and Processes

Software can be part of those processes, but **it is not the silver bullet!**

Just like you can't buy DevOps in a box…

You can't buy DevSecOps in a box!

Don’t just take my word for it…



TECHNOLOGY

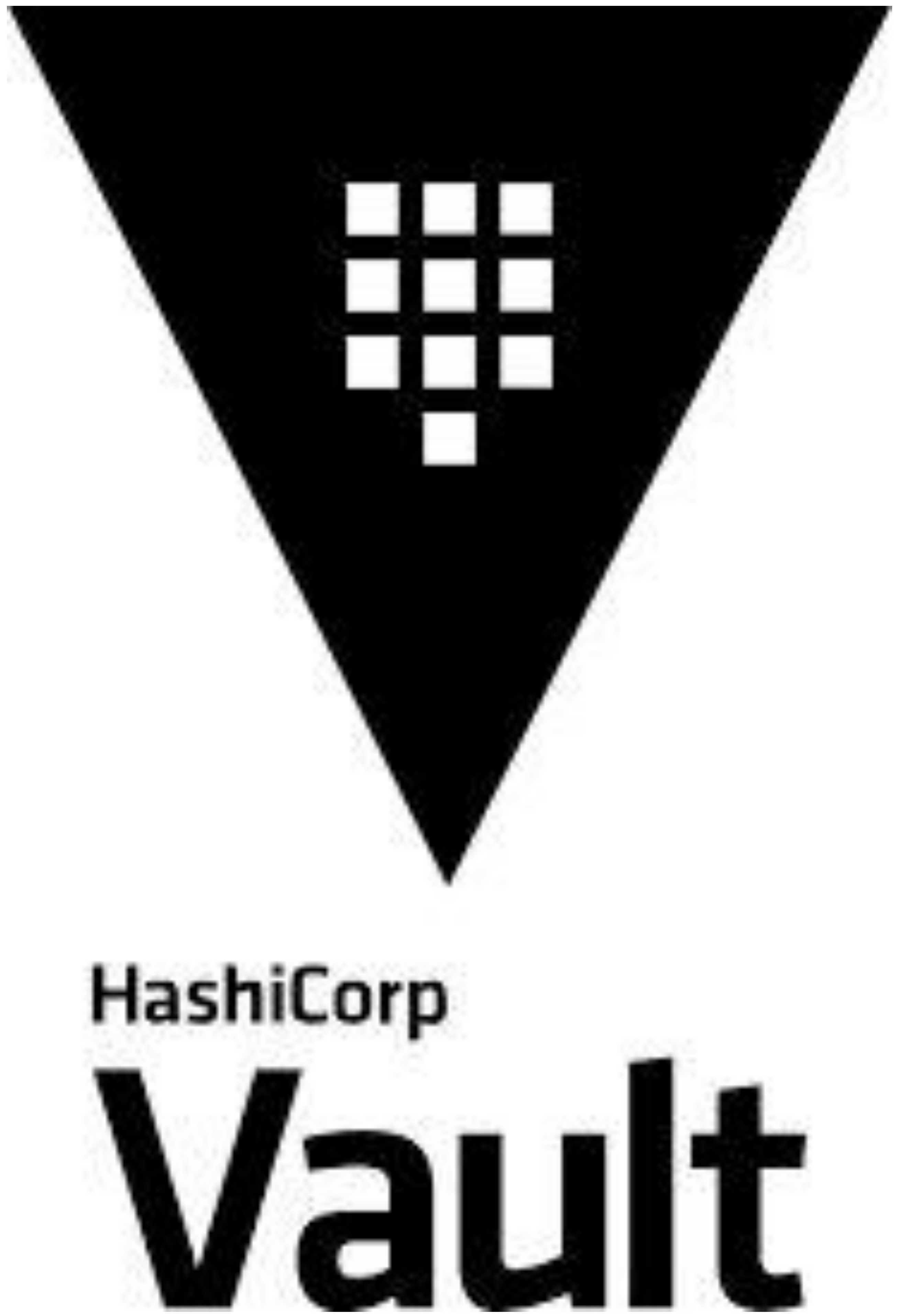
Tenable CEO blasts 'smoke and mirrors' of cybersecurity industry

A good chunk of the cybersecurity industry is “smoke and mirrors,” with companies hawking shiny products that aren’t needed to block most hacks, Tenable CEO Amit Yoran said in an interview with CyberScoop earlier this month

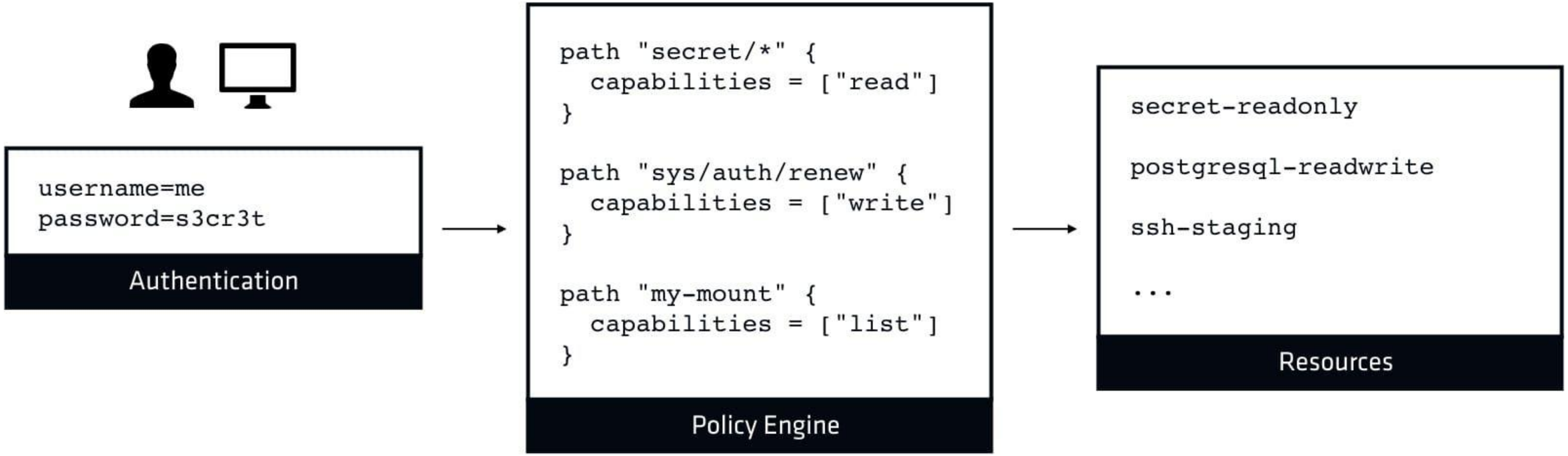
“It’s an industry that has fed and continues to feed, to a large extent, off of fearmongering,” Yoran said on the sidelines of the vendor-happy RSA Conference in San Francisco.

https://www.cyberscoop.com/amit-yoran-tenable-rsa-conference-cybersecurity-industry/

That being said… let's talk about Vault!



Vault Authentication -> Authorization Flow

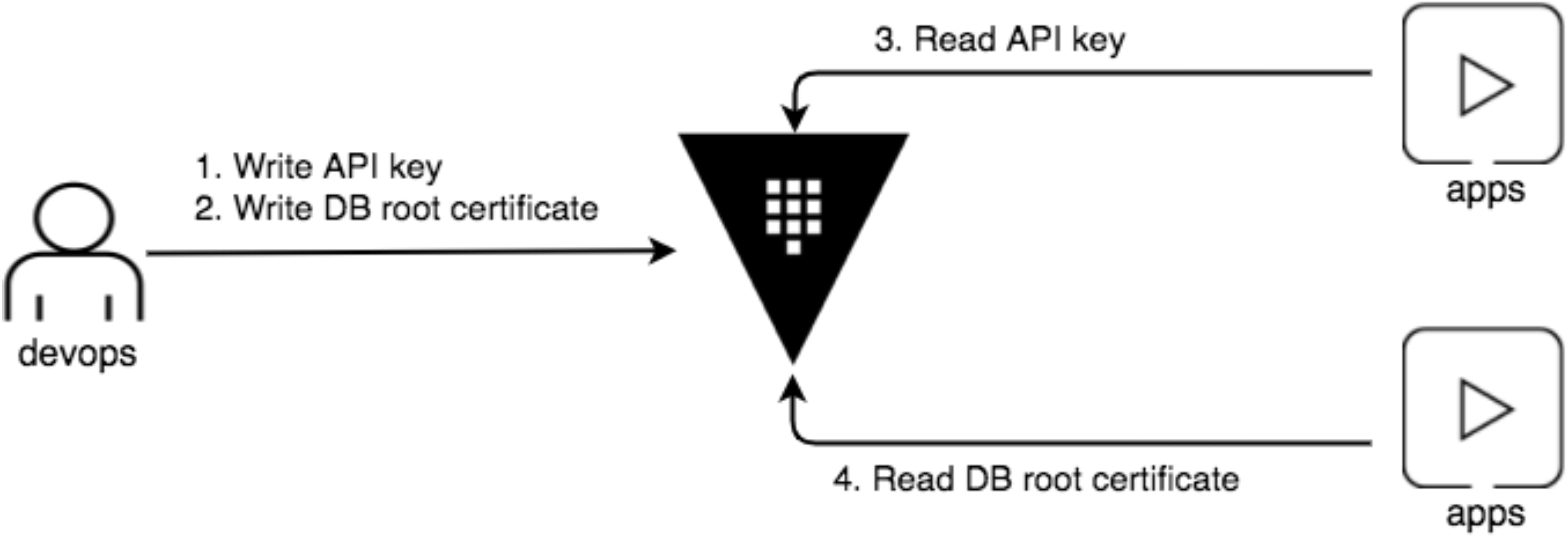


```
username=me
password=s3cr3t
```

```
path "secret/*" {
  capabilities = ["read"]
}

path "sys/auth/renew" {
  capabilities = ["write"]
}

path "my-mount" {
  capabilities = ["list"]
}
```

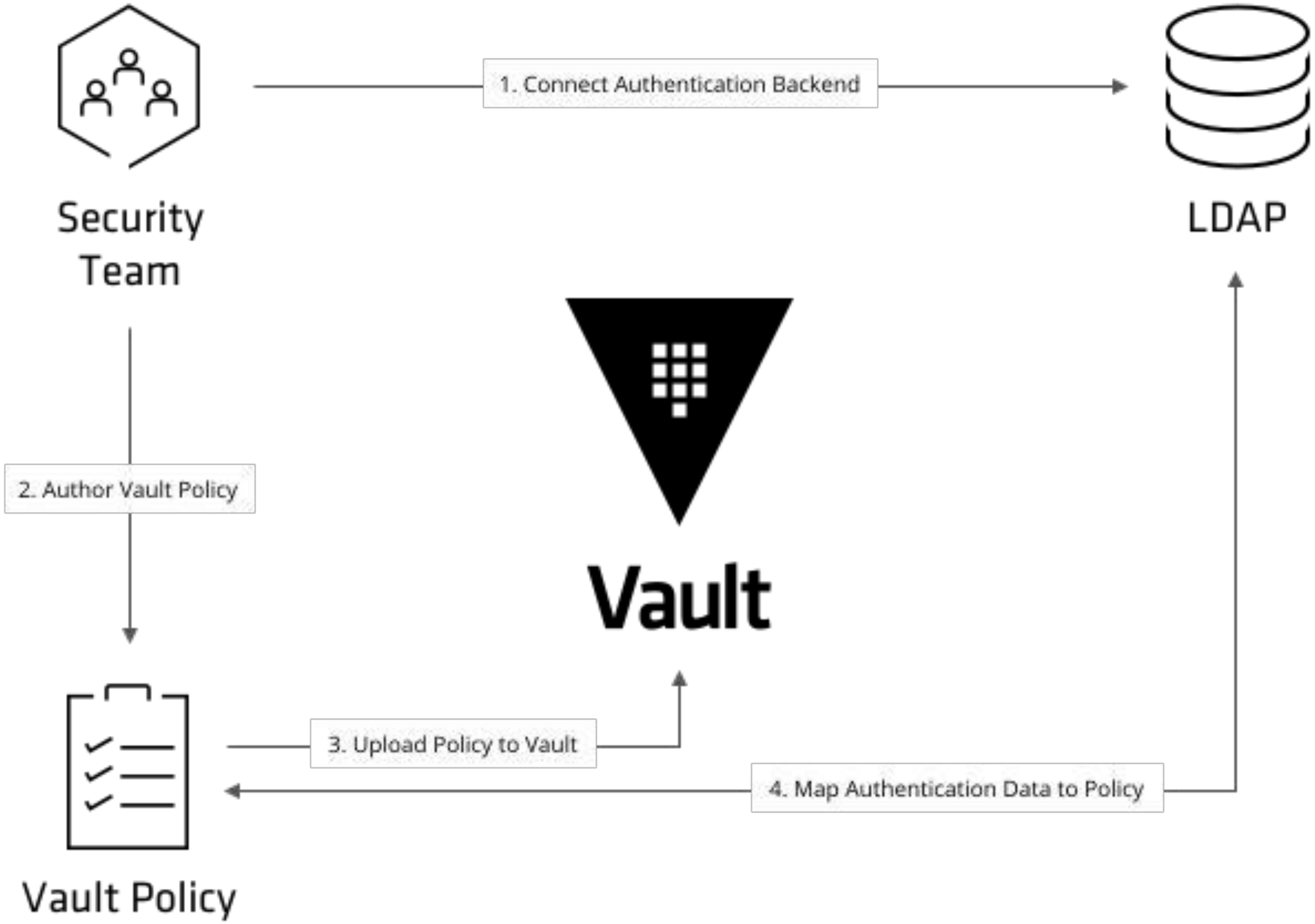
```
secret-readonly

postgresql-readwrite

ssh-staging

...
```

Static Credentials Retrieved Safely: Iteration 2



@petersouter

Static Credentials Retrieved Safely: Iteration 2



1. Connect Authentication Backend

2. Author Vault Policy

3. Upload Policy to Vault

4. Map Authentication Data to Policy

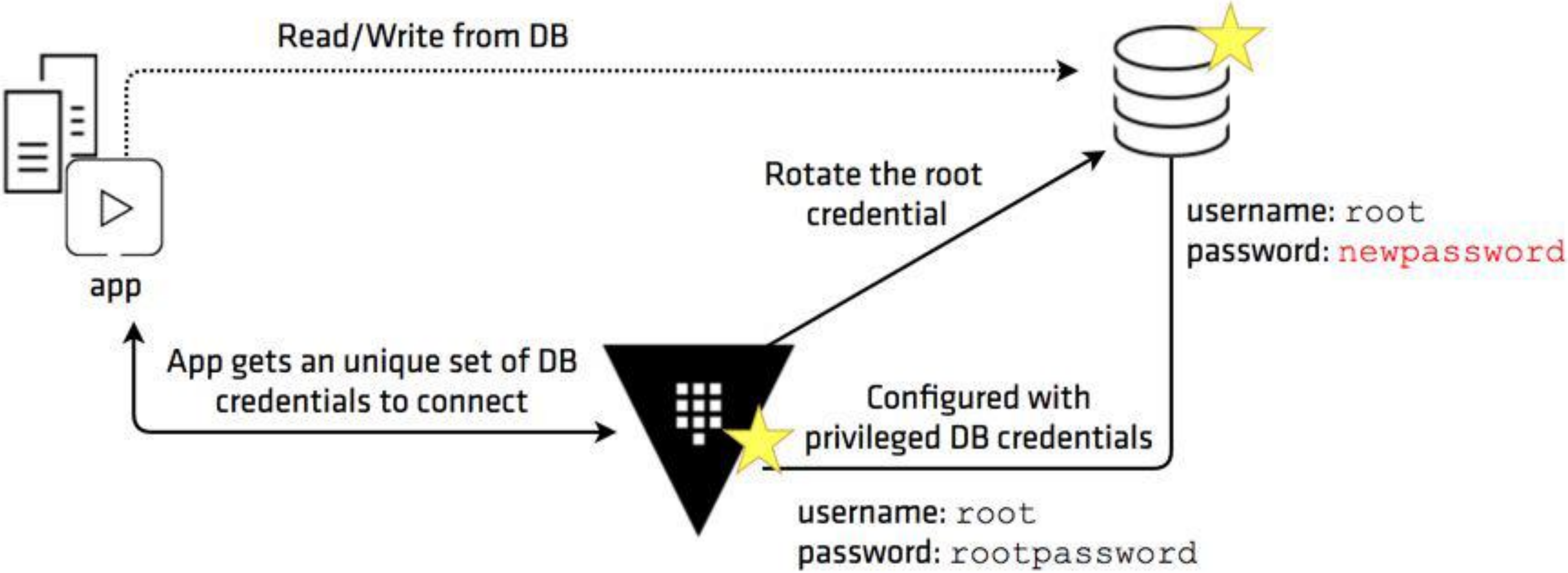
@petersouter

Dynamic leased secrets: Iteration 3

"Now we have our workflows setup correctly, I want to make sure that we are reducing the blast area: credentials that are dynamically created and then removed within a limited time window"

@petersouter

Dynamic Database Credentials


Read/Write from DB
app
Rotate the root credential
username: root
password: newpassword
App gets an unique set of DB credentials to connect
Configured with privileged DB credentials
username: root
password: rootpassword

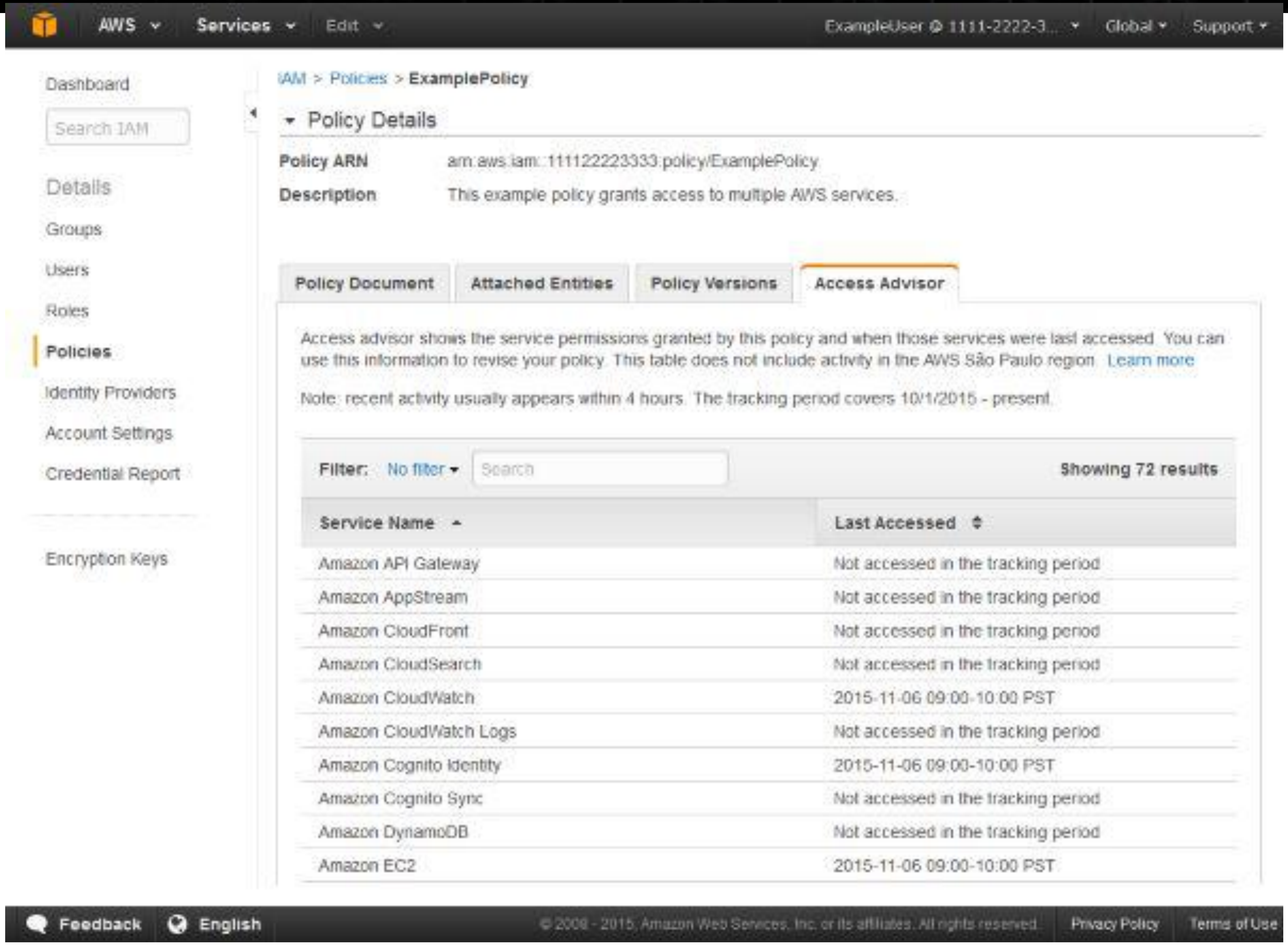
https://learn.hashicorp.com/vault/secrets-management/db-root-rotation

Dynamic Database Credentials

```
$ curl --header "X-Vault-Token:
1c97b03a-6098-31cf-9d8b-b404e52dcb4a" \

https://vault.example.com:8200/v1/database/creds/readonly |
jq
{
   "request_id": "527970fd-f5e8-4de5-d4ed-1b7970eaef0b",
   "lease_id":
"database/creds/readonly/ac79265e-668c-242f-4f67-1dae33da09
4c",
   "renewable": true,
   "lease_duration": 3600,
   "data": {
     "password": "A1a-0tr8u15y0us2u08v",
     "username":
"v-root-readonly-x7v65y1xuprzxv9vpt80-1525378873"
   },
   "wrap_info": null,
   "warnings": null,
   "auth": null
}
```

```
$ psql -h postgres.host.address -p 5432 \
       -U v-root-readonly-x6q809467q98yp4yx4z4-1525378026e
postgres
Password for user
v-root-readonly-x6q809467q98yp4yx4z4-1525378026:

postgres=> \du
Role name                                        |
Attributes                      | Member of
------------------------------------------------+-------------------------------
-----------------------------+----------
postgres                                         | Superuser, Create role, Create
DB, Replication, Bypass RLS | {}
v-root-readonly-x6q809467q98yp4yx4z4-1525378026 | Password valid until
2018-05-03 21:07:11+00                    | {}
v-root-readonly-x7v65y1xuprzxv9vpt80-1525378873 | Password valid until
2018-05-03 21:21:18+00                    | {}

 postgres=> \q
```

Minimising blast radius: Iteration 4



Policy Details

Policy ARN arn:aws:iam::111122223333:policy/ExamplePolicy

Description This example policy grants access to multiple AWS services.

Access advisor shows the service permissions granted by this policy and when those services were last accessed. You can use this information to revise your policy. This table does not include activity in the AWS São Paulo region. Learn more

Note: recent activity usually appears within 4 hours. The tracking period covers 10/1/2015 - present.

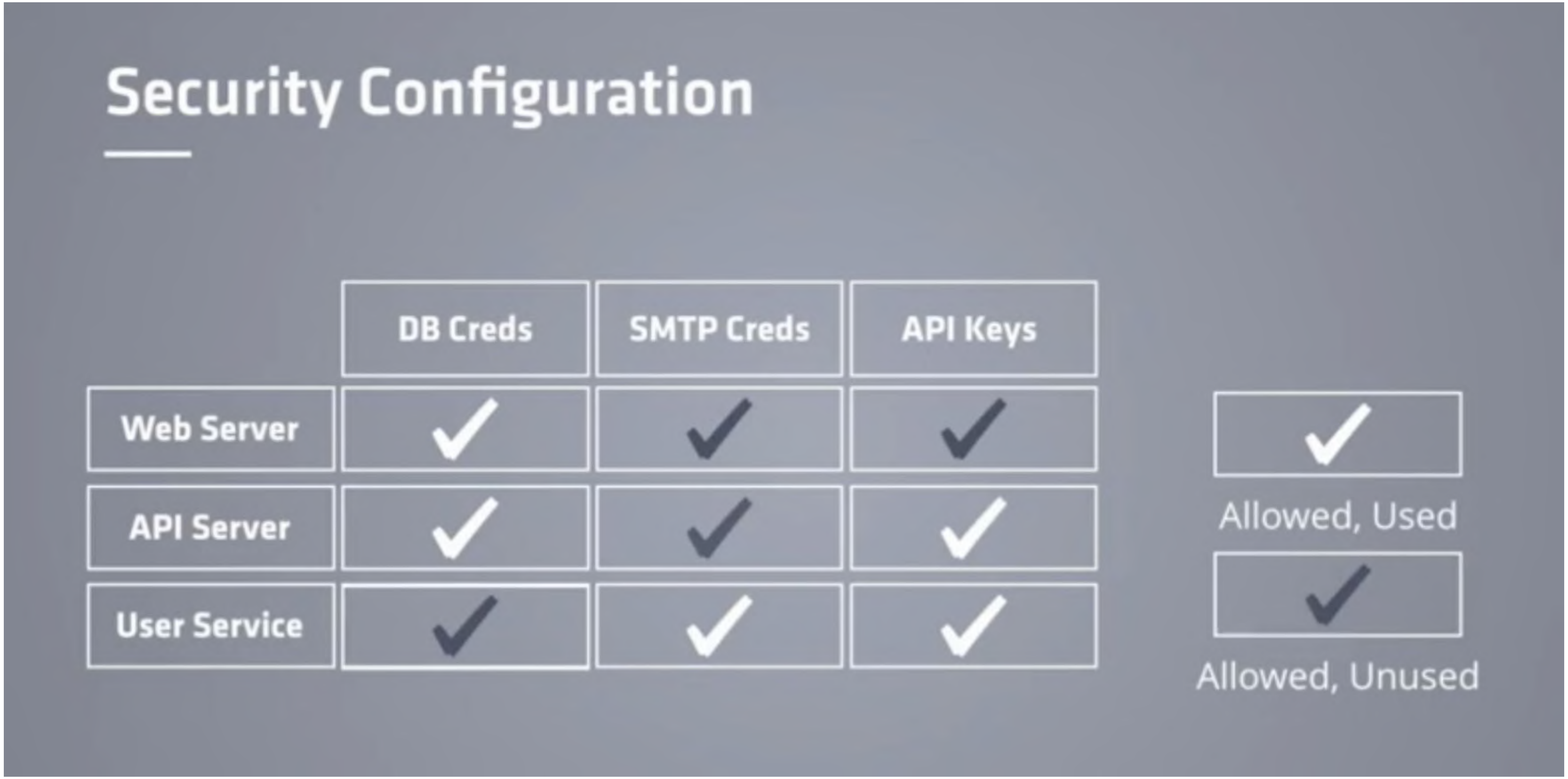
Filter: No filter Search Showing 72 results

Service Name	Last Accessed
Amazon API Gateway	Not accessed in the tracking period
Amazon AppStream	Not accessed in the tracking period
Amazon CloudFront	Not accessed in the tracking period
Amazon CloudSearch	Not accessed in the tracking period
Amazon CloudWatch	2015-11-06 09:00-10:00 PST
Amazon CloudWatch Logs	Not accessed in the tracking period
Amazon Cognito Identity	2015-11-06 09:00-10:00 PST
Amazon Cognito Sync	Not accessed in the tracking period
Amazon DynamoDB	Not accessed in the tracking period
Amazon EC2	2015-11-06 09:00-10:00 PST

© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.

https://aws.amazon.com/blogs/security/remove-unnecessary-permissions-in-your-iam-policies-by-using-service-last-accessed-data/

Minimising blast radius: Iteration 4



Security Configuration

	DB Creds	SMTP Creds	API Keys
Web Server	✓	✔	✔
API Server	✓	✔	✓
User Service	✔	✓	✓

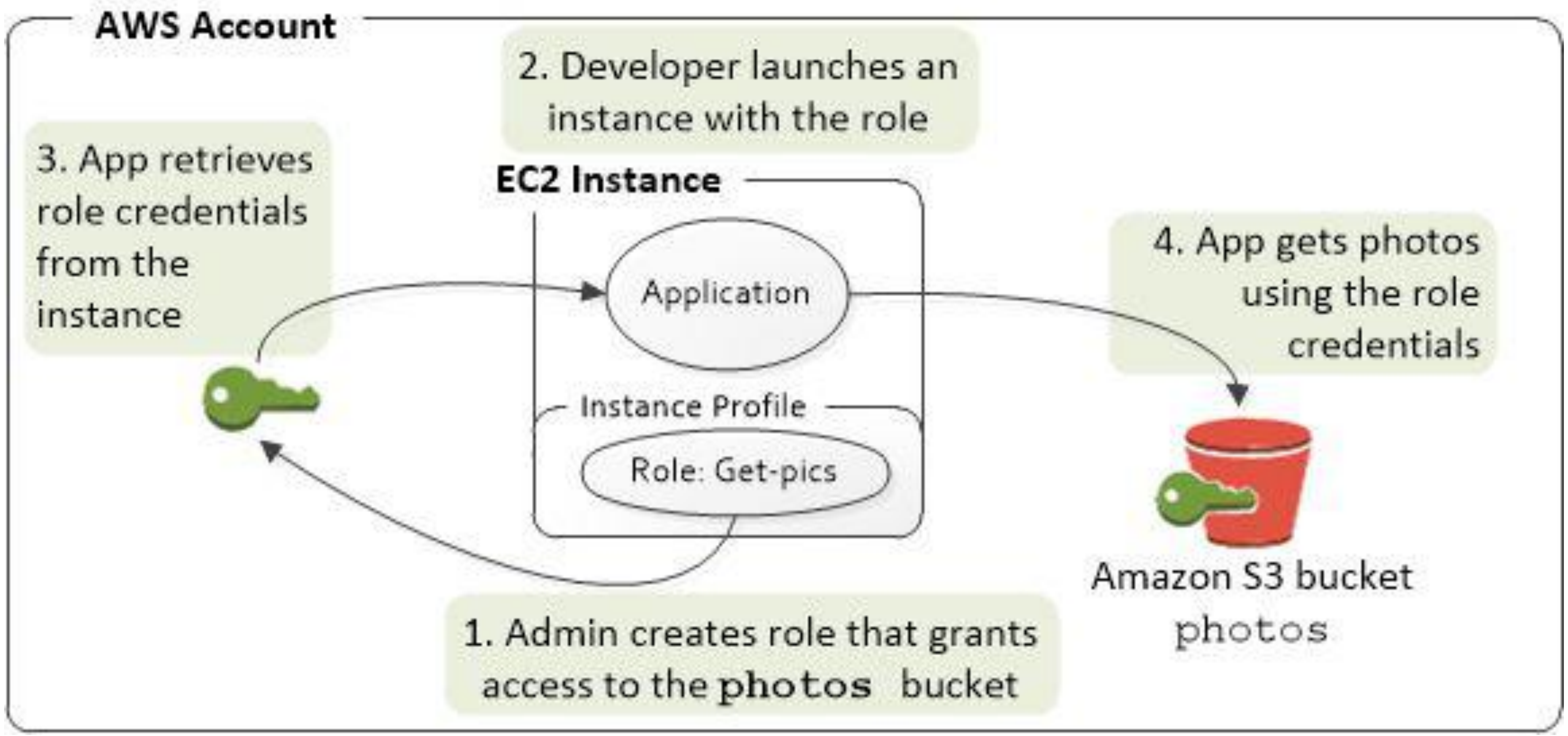
✓ Allowed, Used

✔ Allowed, Unused

https://www.hashicorp.com/resources/keynote-vault-advisor

@petersouter

Remove need for Secrets where possible: Iteration 4



1. Admin creates role that grants access to the photos bucket

2. Developer launches an instance with the role

3. App retrieves role credentials from the instance

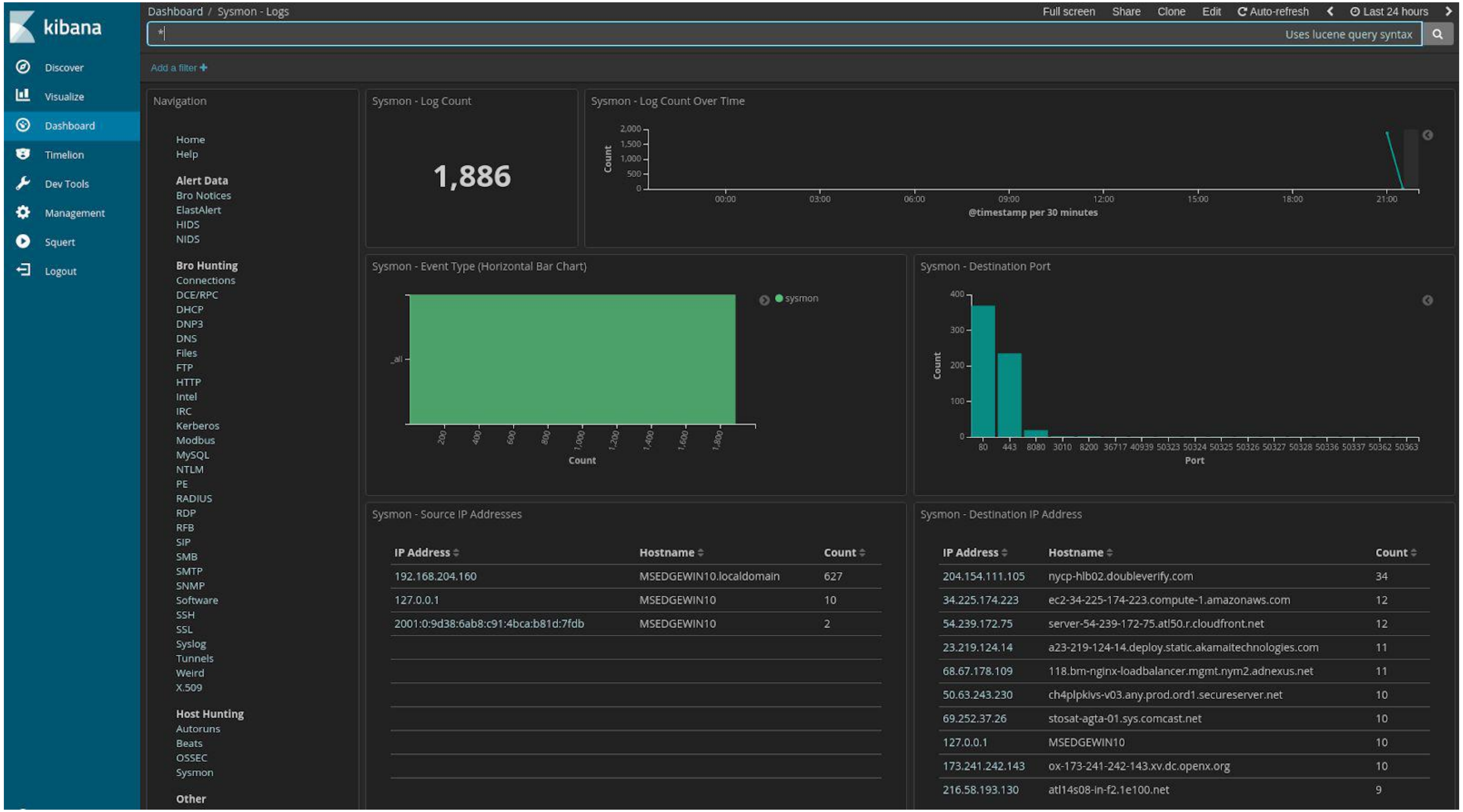
4. App gets photos using the role credentials

https://aws.amazon.com/blogs/aws/iam-roles-for-ec2-instances-simplified-secure-access-to-aws-service-apis-from-ec2/

Observe and detect outliers: Iteration 5

splunk>
DATADOG
honeycomb

Observe and detect outliers: Iteration 5



Sysmon - Log Count

1,886

Sysmon - Source IP Addresses

IP Address	Hostname	Count
192.168.204.160	MSEDGEWIN10.localdomain	627
127.0.0.1	MSEDGEWIN10	10
2001:0:9d38:6ab8:c91:4bca:b81d:7fdb	MSEDGEWIN10	2

Sysmon - Destination IP Address

IP Address	Hostname	Count
204.154.111.105	nycp-hlb02.doubleverify.com	34
34.225.174.223	ec2-34-225-174-223.compute-1.amazonaws.com	12
54.239.172.75	server-54-239-172-75.atl50.r.cloudfront.net	12
23.219.124.14	a23-219-124-14.deploy.static.akamaitechnologies.com	11
68.67.178.109	118.bm-nginx-loadbalancer.mgmt.nym2.adnexus.net	11
50.63.243.230	ch4plpkivs-v03.any.prod.ord1.secureserver.net	10
69.252.37.26	stosat-agta-01.sys.comcast.net	10
127.0.0.1	MSEDGEWIN10	10
173.241.242.143	ox-173-241-242-143.xv.dc.openx.org	10
216.58.193.130	atl14s08-in-f2.1e100.net	9

https://securityonion.net/

@petersouter

Red Teams and Attackers: Iteration 6

Secrets: Areas now hit for processes

Plan	**Develop**	**Test**	**Deploy**	**Operate**
‘Evil user’ stories	Hardened Software Frameworks	🟩 Static Analysis	System Hardening	🟩 Observability
🟩 Security Requirements	🟩 Sec Focused Code Review	Pentesting	Patching	🟩 Anomaly and Threat detection
		🟩 Game Days - Red Teams		

DevSecOps: Different requirements for Secrets are met!

I can use the database I want in my app without jumping through hoops and get credentials using my existing auth methods!

Dev

I can operationally run the apps without worrying about managing secrets

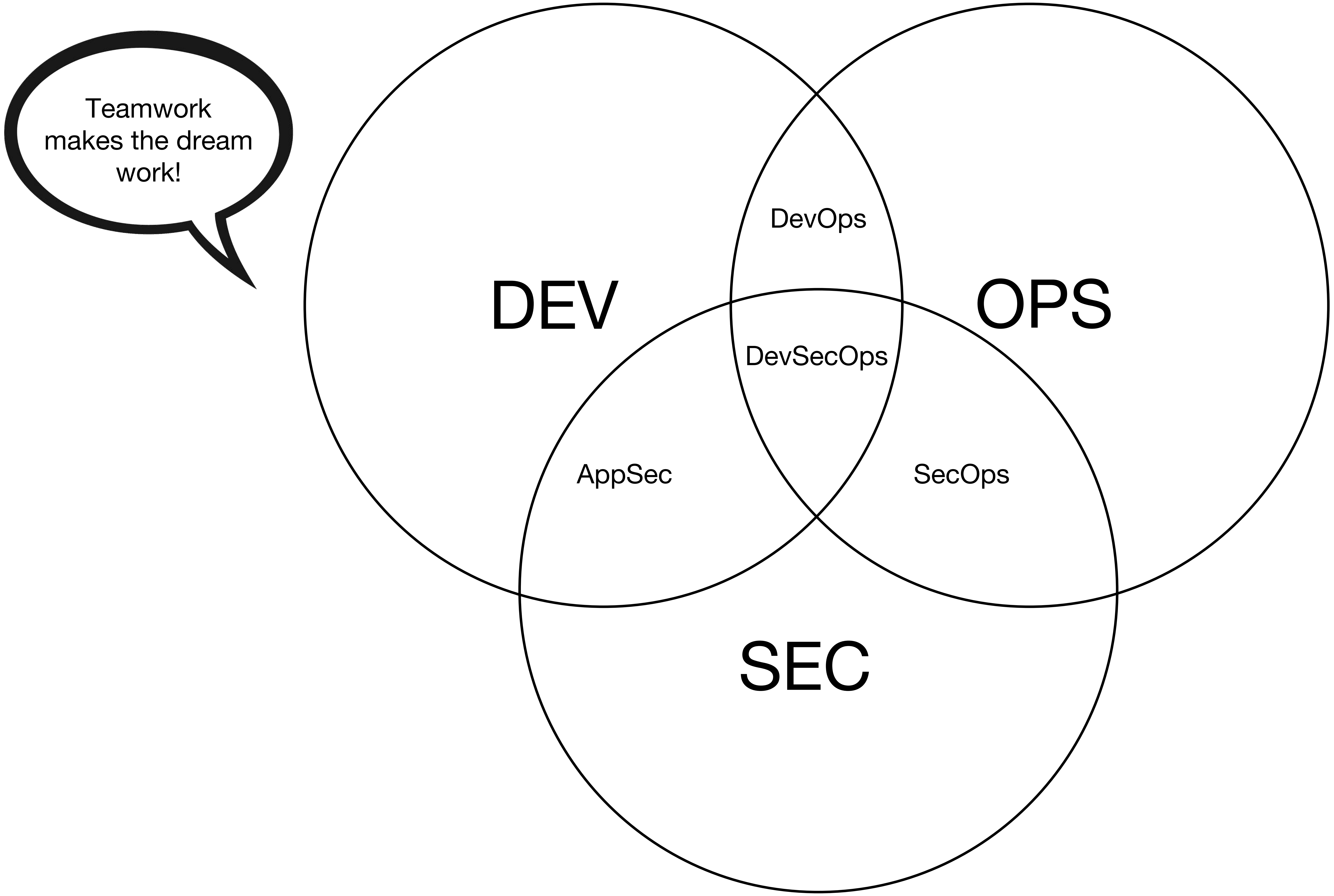
Ops

Credentials are provided automatically following our policies and are short lived and rotatable

Sec

@petersouter

Secrets have been DevSecOps-ified!



@petersouter

Other good areas to pick

App Sec - OWASP,
Dependency Management - Greenkeeper, Snyk,
System Hardening - CIS, Audit
Authentication - Duo, 2FA, Authy, Oath
CI/CD Security - Inspec, DangerCI

Keep it up and you'll end up with this!

https://twitter.com/signalsciences/status/647533893617238016?lang=en

Summary: What have we learnt?

Security can become the new silo
Break down those walls and work together
Security is everyone's responsibility!

Summary: What have we learnt?

Move security left

Make it a part of your process, rather than an afterthought

Summary: What have we learnt?

Pick an area to improve

Don’t do a big-bang change all at once

Summary: What have we learnt?

Secrets are a good test-bed
Most teams have a secrets problem, and
it’s a good testing ground for processes

Summary: What have we learnt?

Iterate on that area

Incrementally improve that area, taking input from all teams on the requirements

Summary: What have we learnt?

Security is not a product

There's no magic bullet product to fix your problems

Summary: What have we learnt?

But...

Vault is still cool, try it out ☻

Would you like to know more?

- **DevSecOps, An Organizational Primer** - Tim Anderson, AWS Security https://www.youtube.com/watch?v=Q7TymregonI
- **DevSecOps Whitepaper** - Francois Raynaud, DevSecCon Founder. https://www.devseccon.com/devsecops-whitepaper/
- **DevSecOps State of the Union** - Clint Gibler, Senior Sec Consultant, NCC Group https://programanalys.is/bsidessf-devsecops-state-of-the-union
- **How to Integrate Security Into a DevOps World** - Franklin Mosley, Senior AppSec Engineer, PagerDuty https://www.threatstack.com/blog/how-to-integrate-security-into-a-devops-world
- **Release your inner DevSecOp** - James Wickett - Research Head, Signal Sciences https://www.rsaconference.com/events/us19/rsac-ondemand/videos/525/release-your-inner-devsecop

Thank you.

HashiCorp

www.hashicorp.com hello@hashicorp.com