

# **RSA**®Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: ASD-T08

## Enterprise Cloud Security via DevSecOps

### **Shannon Leitz**

---

Sr Mgr, Cloud Security & DevSecOps Leader  
Intuit Information Security  
@devsecops

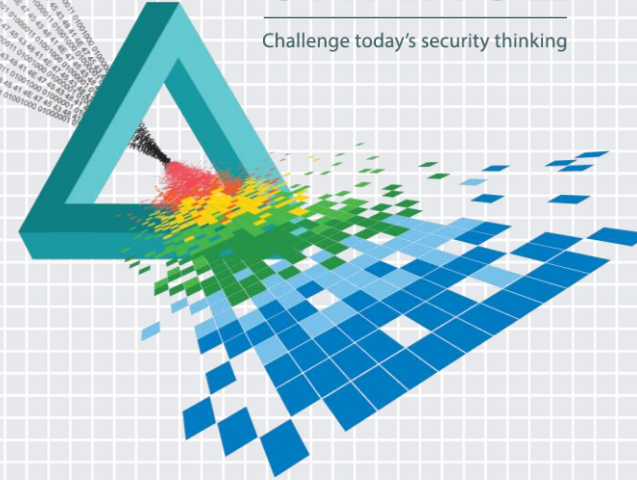
### **Scott C Kennedy**

---

Security Scientist  
Intuit Information Security  
@scknogas

# CHANGE

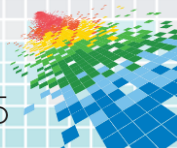
Challenge today's security thinking



# Agenda

- ◆ **Who we are**
  - ◆ Applying DevSecOps for 3+ years to support Enterprise Cloud migrations
  - ◆ 20+ yrs experience with Virtualization, Software Defined Environments and Cloud Security
- ◆ **What we'll cover**
  - ◆ Information about the DevSecOps model and the experiments that helped us discover it
  - ◆ A path for developing your own Enterprise Cloud Security program using DevSecOps practices
- ◆ **Why it's important**
  - ◆ Cloud and DevOps adoption require a different approach to Enterprise Security
  - ◆ Nearly 70% of All Workloads occur in Cloud Data Centers within 2015\*
  - ◆ Public Cloud growth is 50% higher than Private Cloud\*

\* [Cisco Global Cloud Index](#)

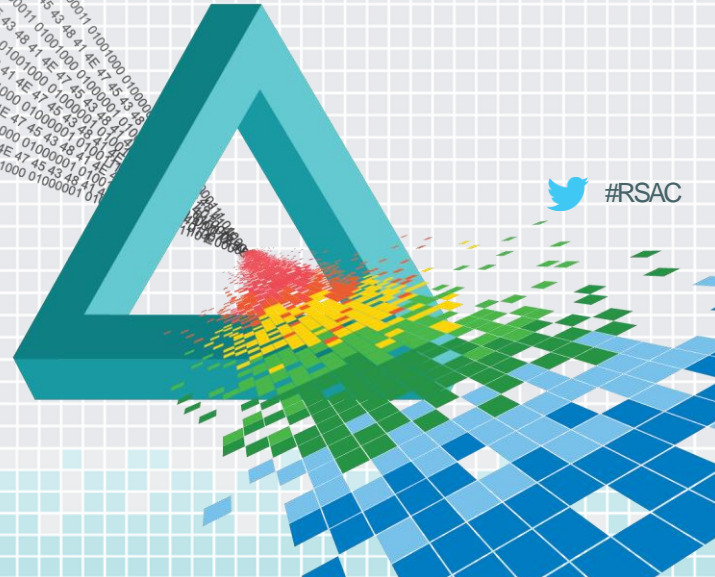


# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

**Spoiler Alert:**

**DevSecOps isn't  
DevOps + Security!**



 #RSAC

# The Challenge

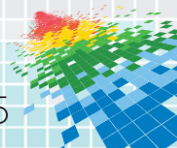
## Securing Enterprise Workloads in the Cloud...

- ◆ Pain
- ◆ Trial & Error
- ◆ Blood, sweat & tears
- ◆ Ouch, my head hurts!



Bang  
Head  
Here

It would have been great to hear this talk a couple years ago....



# The Team

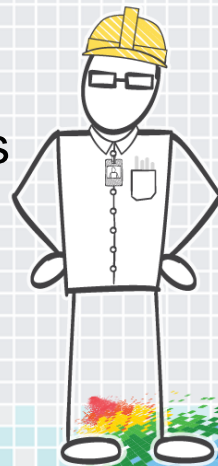
## Intuit Cloud Security

- ◆ Leading Cloud Security at Intuit
- ◆ DevSecOps
- ◆ Lean Start Principles
- ◆ Decision Support
- ◆ Assisting 3000+ Developers

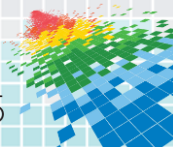
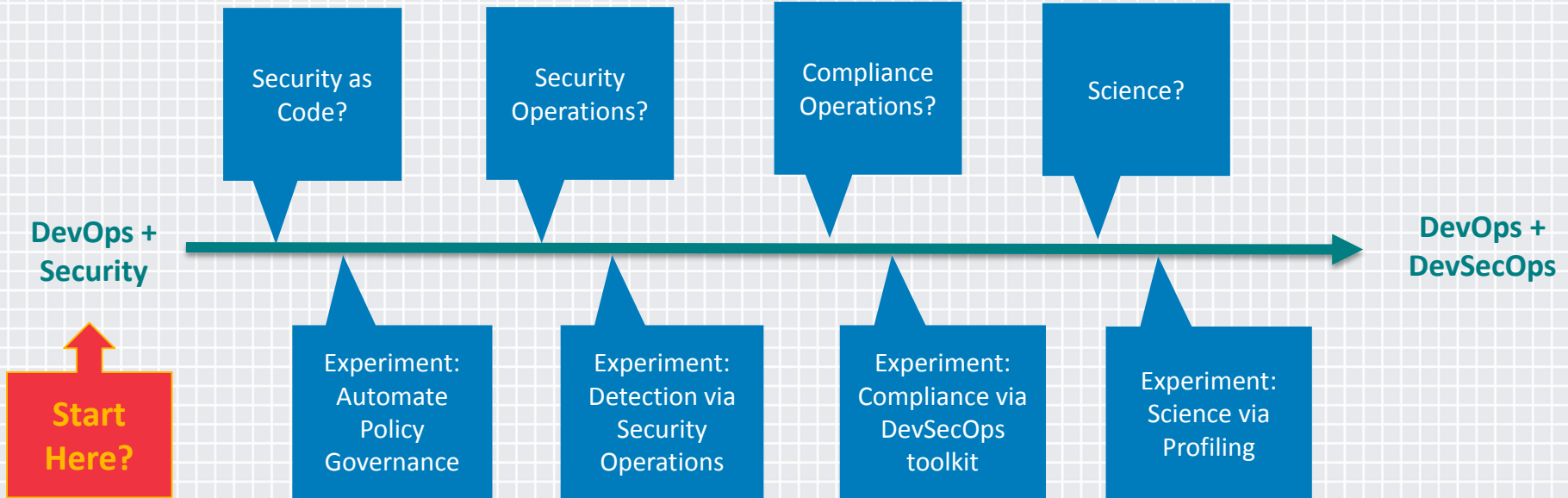


## AWS Professional Services

- ◆ Integrated solutions
- ◆ Delivery assistance
- ◆ Partner coaching
- ◆ Sample code & accelerators
- ◆ Access across AWS teams



# The Timeline

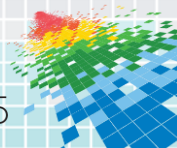




# Drivers for DevSecOps

## Embedding into DevOps Teams was a disaster...

- ◆ There aren't enough Security Professionals to embed into DevOps Teams...
- ◆ Compliance checklists didn't take us very far before we stopped scaling because of manual work...
- ◆ We learned we couldn't keep up with automated deployments without our own automation...
- ◆ Standard Security Operations did not work and continuous change became overwhelming...
- ◆ And we needed far more data than we expected to help the business make decisions...



# The Art of DevSecOps

## DevSecOps

Security  
Engineering

Security  
Operations

Compliance  
Operations

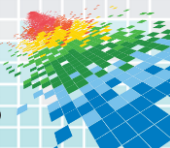
Security  
Science

Experiment,  
Automate, Test

Hunt, Detect,  
Contain

Respond,  
Manage, Train

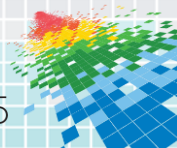
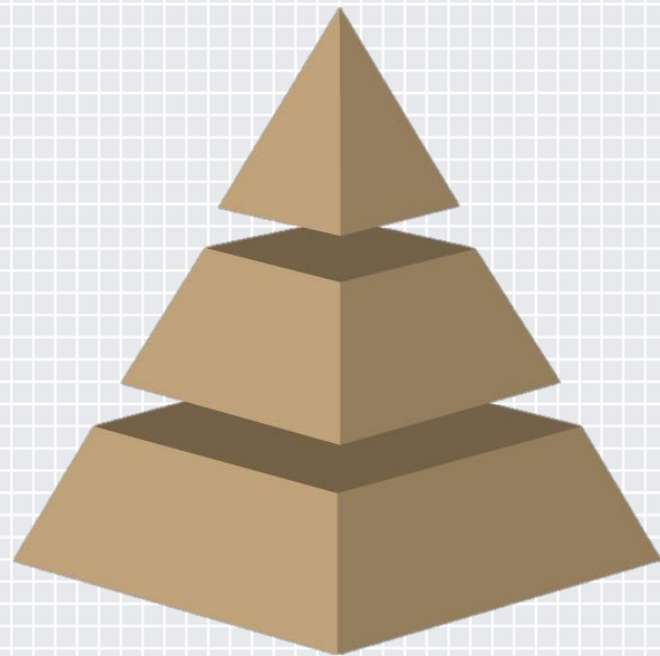
Learn, Measure,  
Forecast

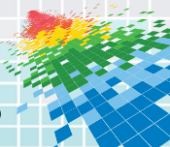
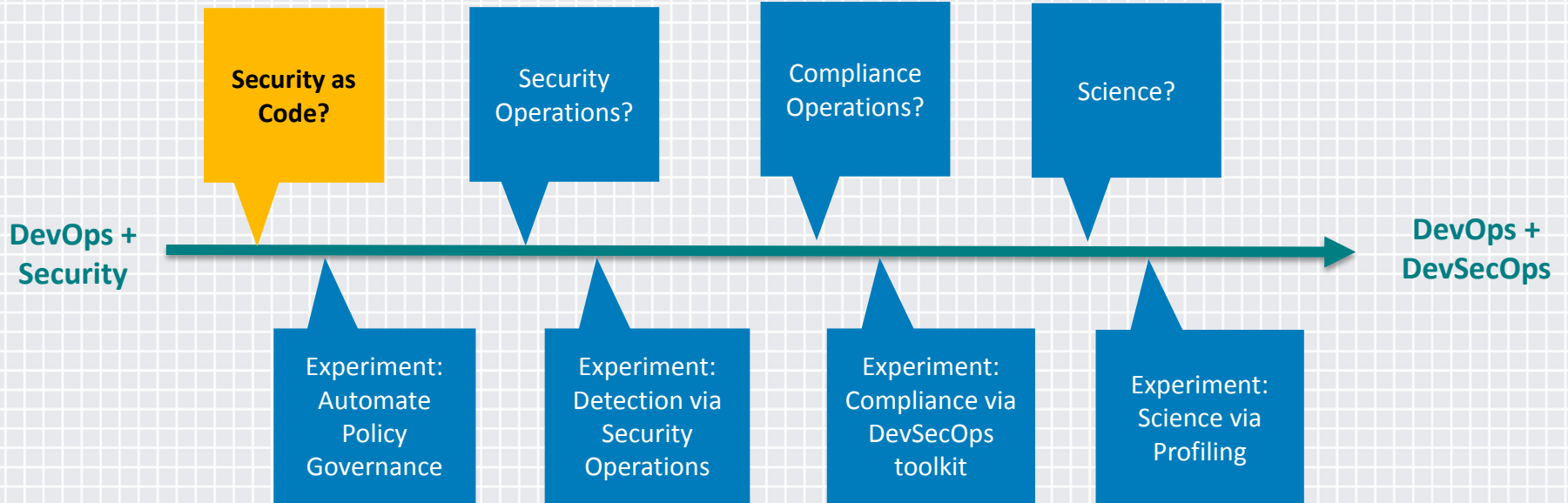




# Step Zero: Establishing Principles

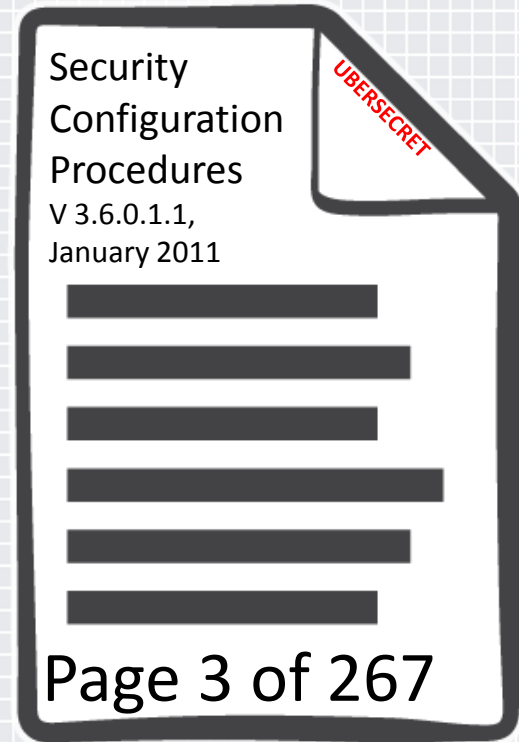
1. Customer focused mindset
2. Scale, scale, scale
3. Objective criteria
4. Proactive hunting
5. Continuous detection & response



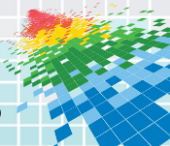


# Security as Word Doc

- ◆ Double-click installer
- ◆ Click "Next"
- ◆ Click "Next"
- ◆ Click "Next"
- ◆ Click "Next"
- ◆ Click "Next"
- ◆ Click "Next"
- ◆ Click "Next"
- ◆ Click "Next"
- ◆ Click "Next"
- ◆ Click "Next"
- ◆ Click "Next"



Frozen in Time



# Security as Code is Easy with AWS

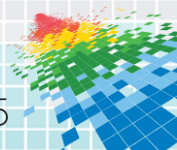
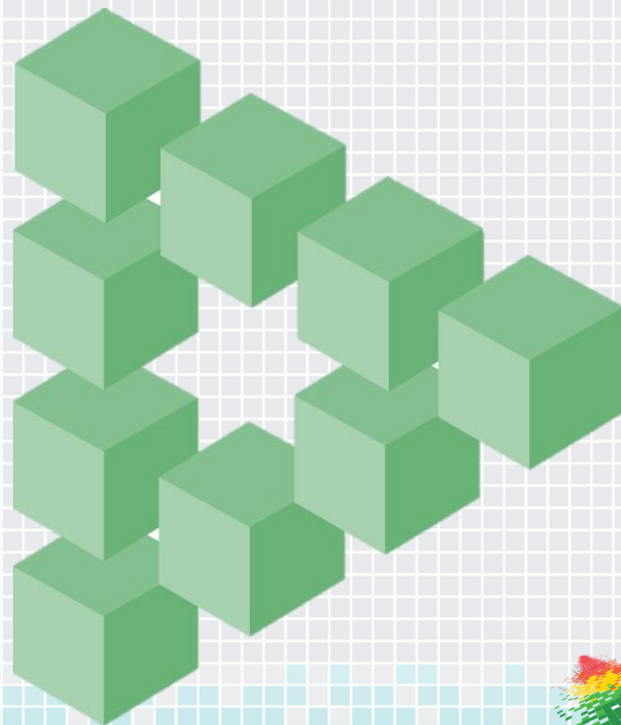
AWS provides a programmable infrastructure

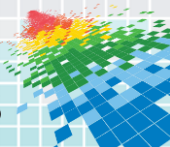
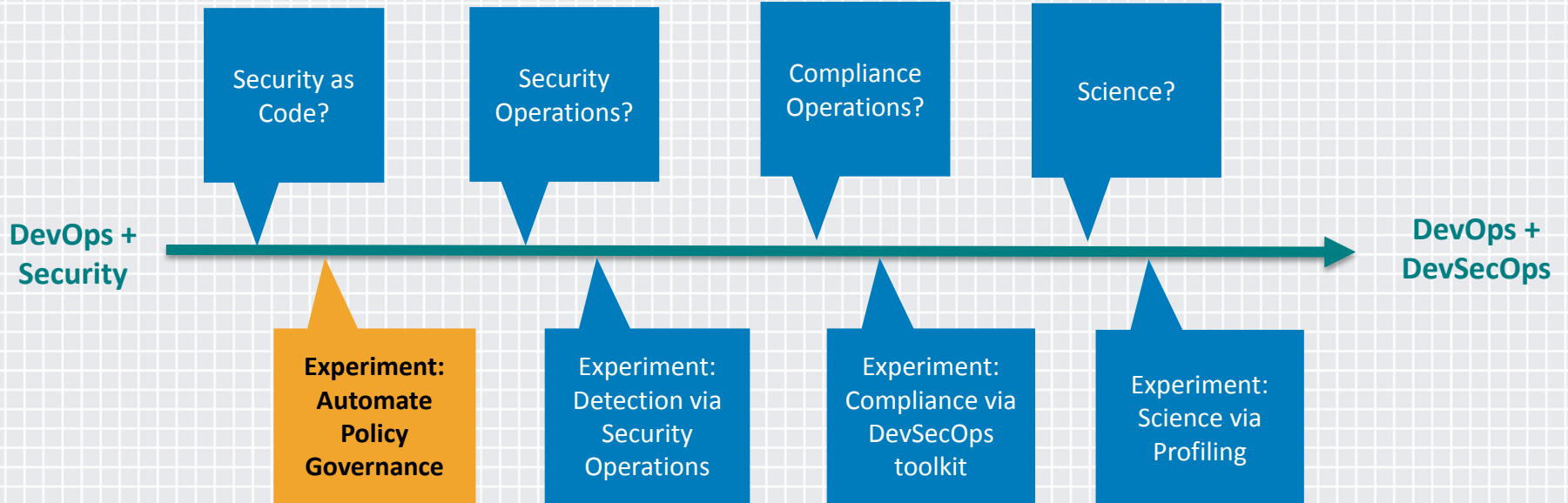
## ◆ Benefits

- ◆ Easily automated
- ◆ Repeatable
- ◆ Auditable
- ◆ Easy to iterate

## ◆ Forms of Code

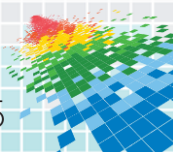
- ◆ Access Policy documents
- ◆ CloudFormation templates
- ◆ Ruby scripts
- ◆ Custom APIs





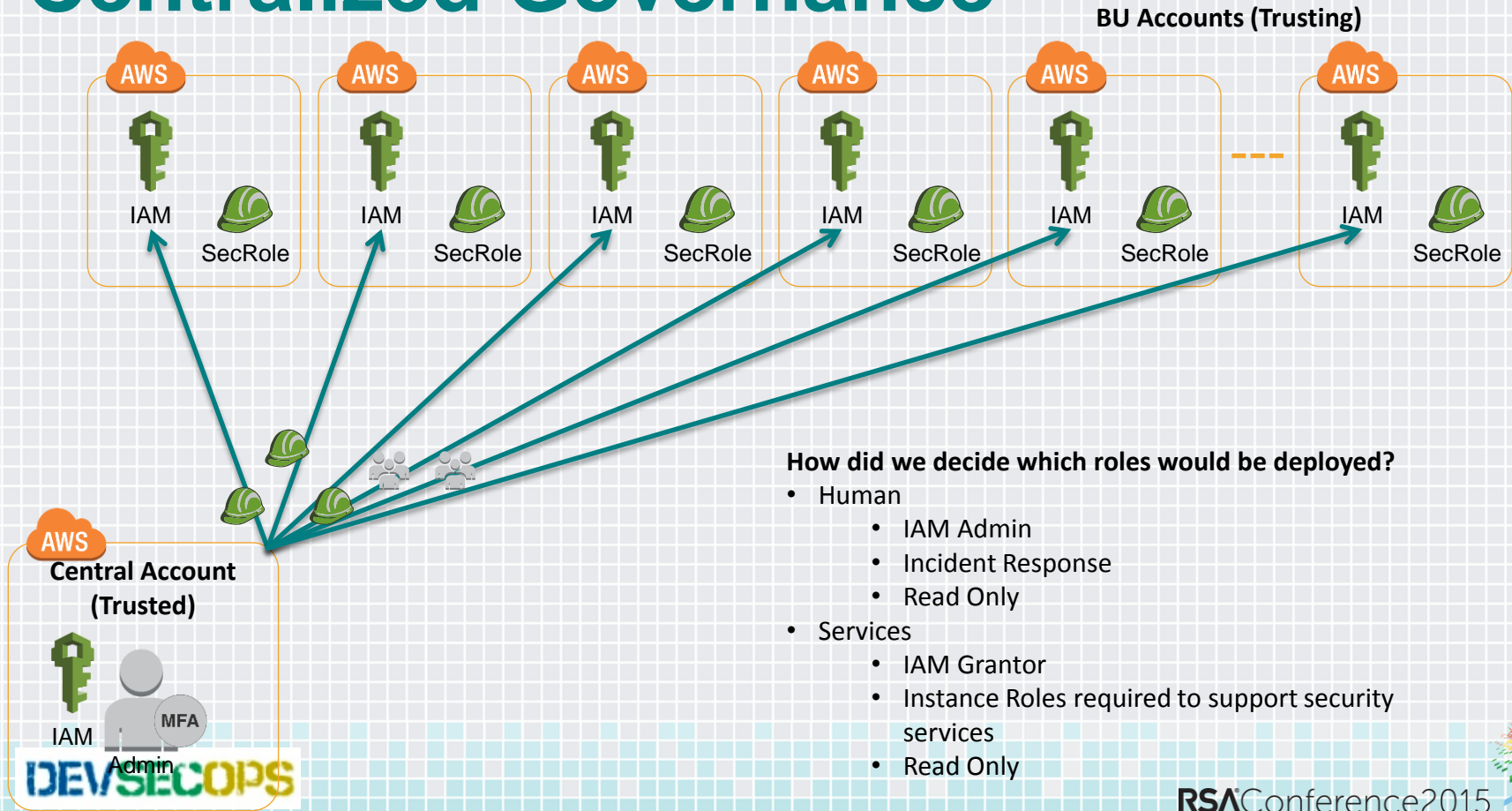
# Experiment with Centralized & Transparent Governance

- ◆ Manage hundreds of AWS accounts
  - ◆ Push baseline IAM Roles and IAM Groups
  - ◆ Push associated trust policies and access policies
- ◆ Design to support an authoritative code source
  - ◆ Include git support
- ◆ Add behavior modifications
  - ◆ Discover only (--dry-run)
  - ◆ Detect drift and show differences (--diff)
  - ◆ Replace with approved baseline (no --dry-run)
  - ◆ Tune verbosity (--debug)



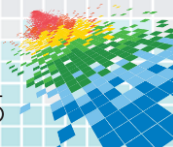


# Centralized Governance

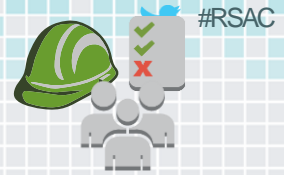


### How did we decide which roles would be deployed?

- Human
  - IAM Admin
  - Incident Response
  - Read Only
- Services
  - IAM Grantor
  - Instance Roles required to support security services
  - Read Only



# Baseline IAM Role Catalog

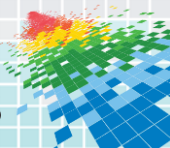
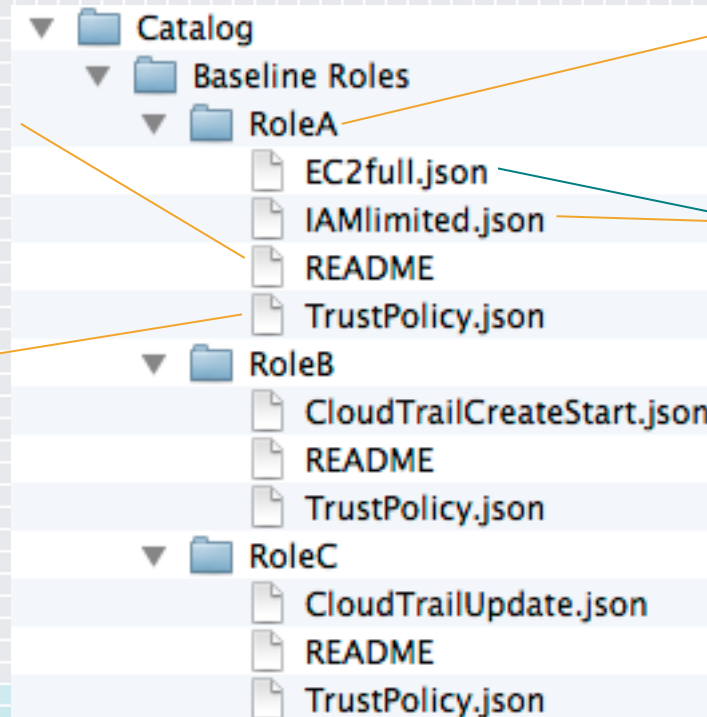


Role Name

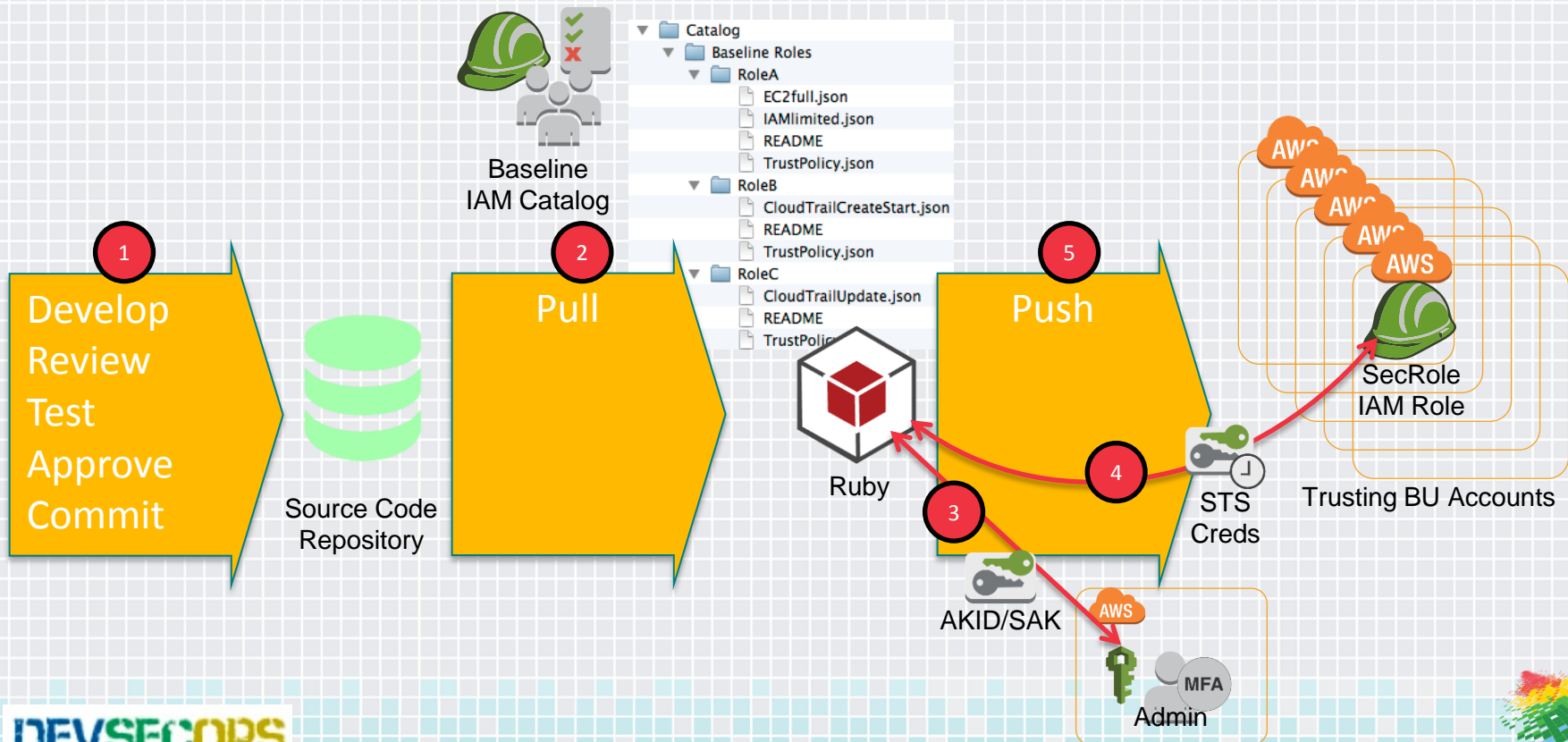
Access Policies

Short Description

Trust Policy



# Centralized Governance Workflow



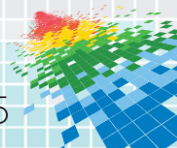
# Acting on Drift Detection

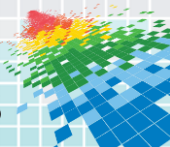
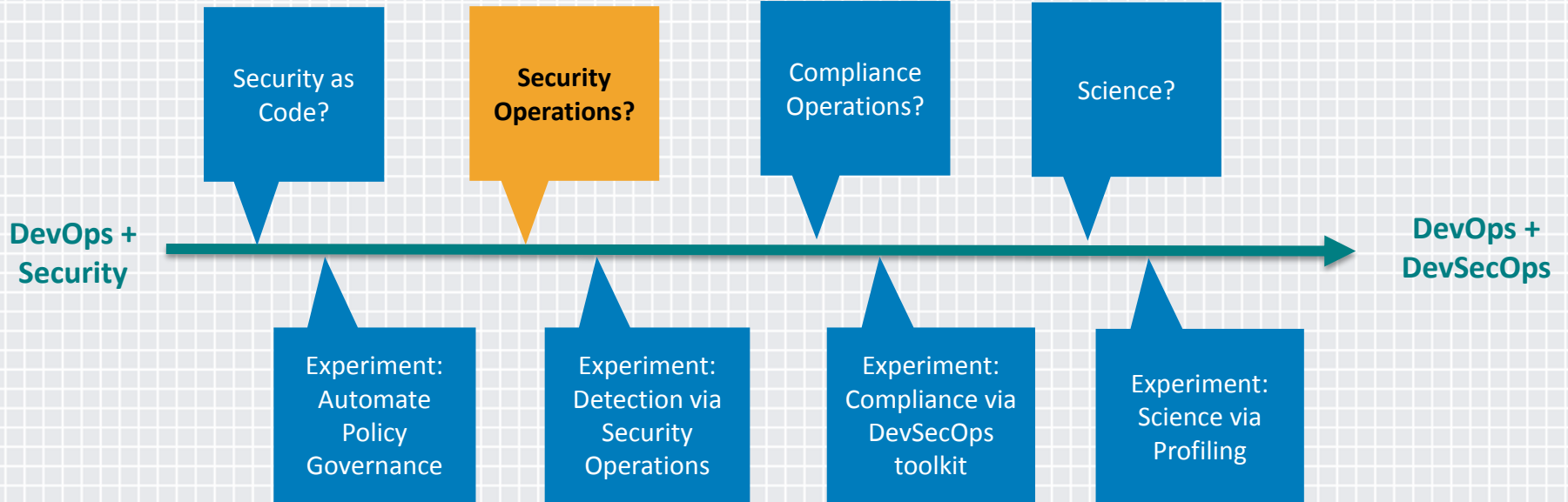
```
begin
  (iam.client.list_role_policies(:role_name => role)[:policy_names]\
    - roledb.list_policies(role)).each do |policy|
    log.warn("Deleting Policy \"#{policy}\", which is not part of the approved baseline.")
    if policydiff("{}\"",
      URI.decode(iam.client.get_role_policy(\
        :role_name => role,
        :policy_name => policy
     )[:policy_document]),
      {:argv => ARGV, :diff => options.diff})
    end
    options.dryrun ? nil : \
      iam.client.delete_role_policy(
        :role_name => role,
        :policy_name => policy
      )
    end
end
```

**Account Grade:**

C

Heal Account?

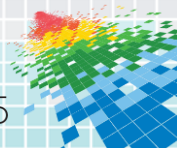
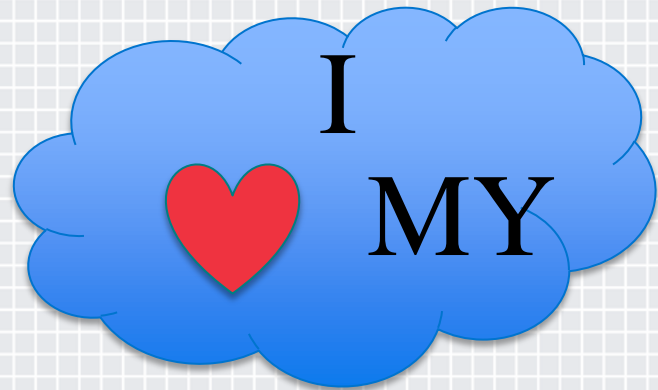




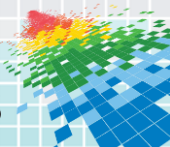
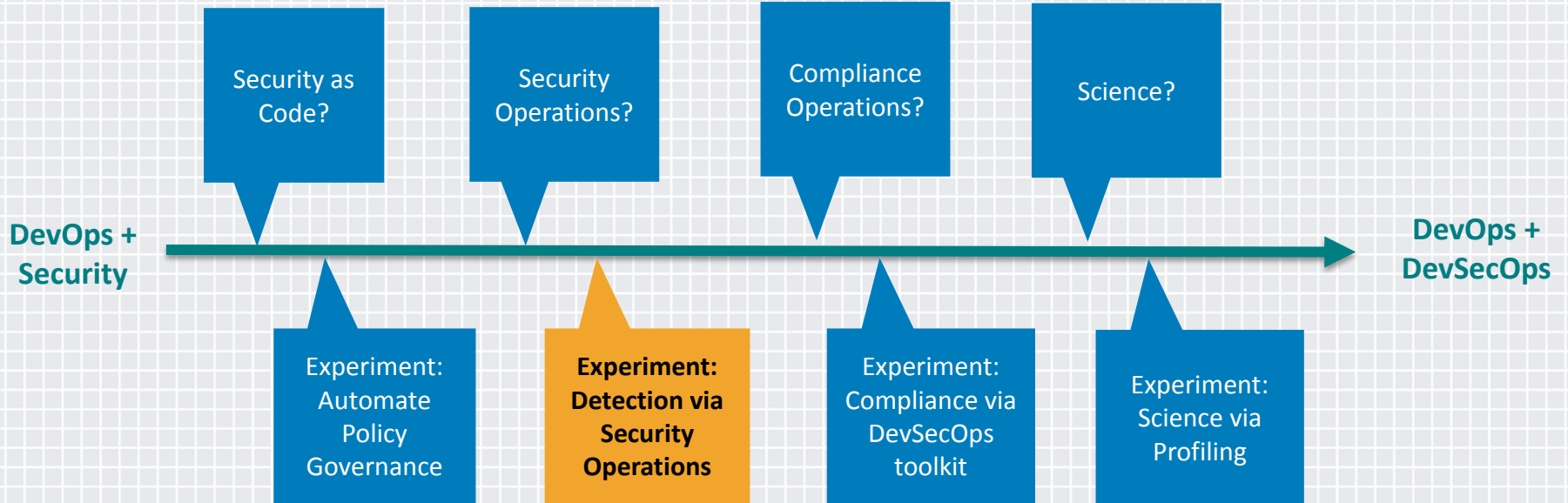
# Sec Ops Reloaded for the Cloud

applying these principles...

- ◆ Dynamic Attack Trees created and maintained by SecOps
- ◆ Data collection is tied to Threat Modeling
- ◆ Rules & Alerting support Hunting
- ◆ Inline Forensics...



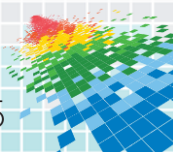




# Threat Analytics Platform – Data Sources

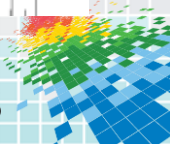
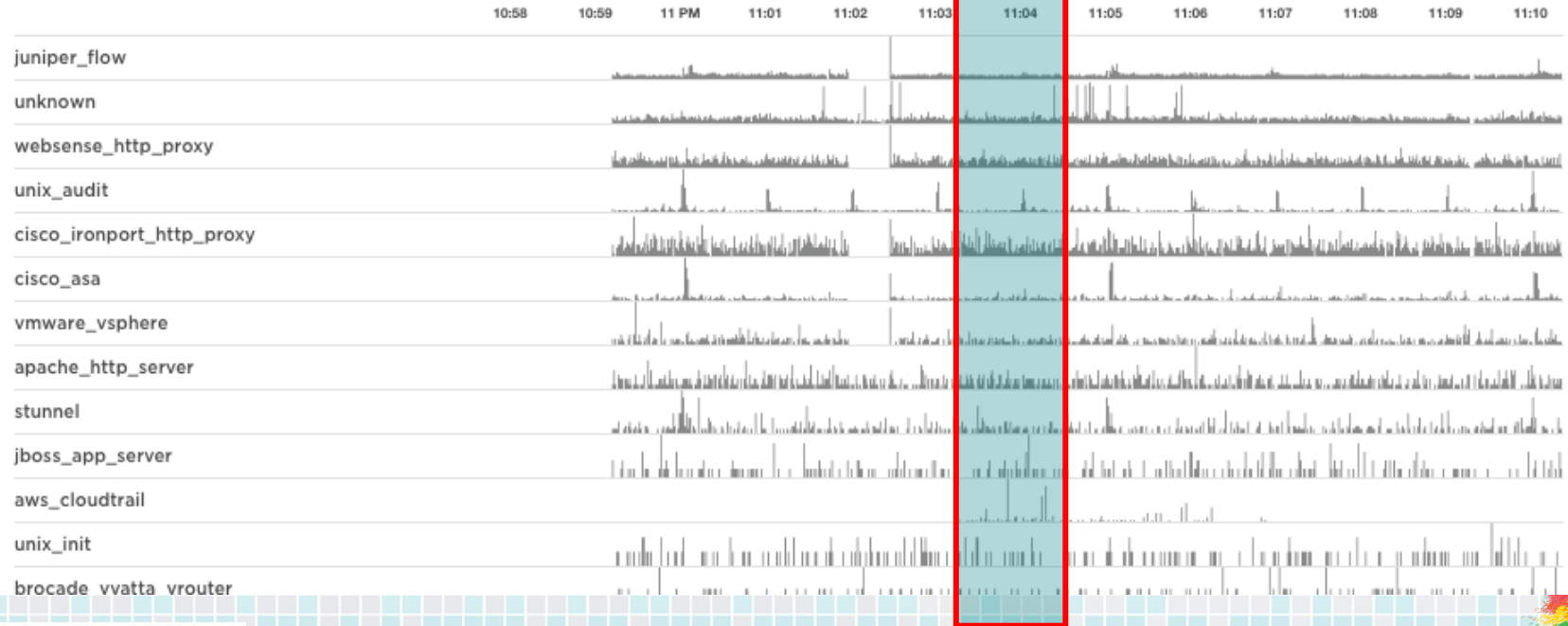
## PAST 24 HOURS:

APACHE_HTTP_SERVER	15.1M	AWS_CLOUDTRAIL	4.1M	BROCADE_VYATTA_VROUTER	1.8M	CISCO_ACS	8.6K
CISCO_ASA	37.0M	CISCO_ASA_THREAT_DETEC...	4.5K	CISCO_FIREWALL	1.9M	CISCO_FWSM	34.1K
CISCO_IOS	71	CISCO_IRONPORT_HTTP_PR...	36.1M	CISCO_NEXUS	1	CISCO_PIX	28
CISCO_VPN	5.6K	DHCLIENT_DHCP	75.9K	F5	137.0K	F5_BIGIP_APM	241.4K
FIREEYE	11	JBOSS_APP_SERVER	5.0M	<b>JUNIPER_FLOW</b>	<b>325.7M</b>	JUNIPER_VPN	585.8K
MS_WINDOWS_EVENT	1.5M	NGINX	416.5K	NTPD	33	PUPPET	6.2K
RSYSLOG	1.6K	SOURCEFIRE	4.7K	SPLUNK	128.3K	STUNNEL	5.6M
SYMANTEC_ENDPOINT_PRO...	1.1K	UNIX	379	UNIX_AUDIT	42.0M	UNIX_CRON	8.1K
UNIX_INIT	3.2M	UNIX_KERNEL	2	UNIX_PAM	272	UNIX_SSH	34.4K
UNIX_XNTPD	541	UNKNOWN	97.0M	VMWARE_VSPHERE	14.8M	WEBSense_HTTP_PROXY	26.0M




# Threat Analytics Platform - Trends

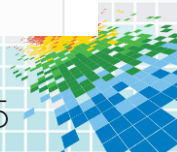
## TIMELINE



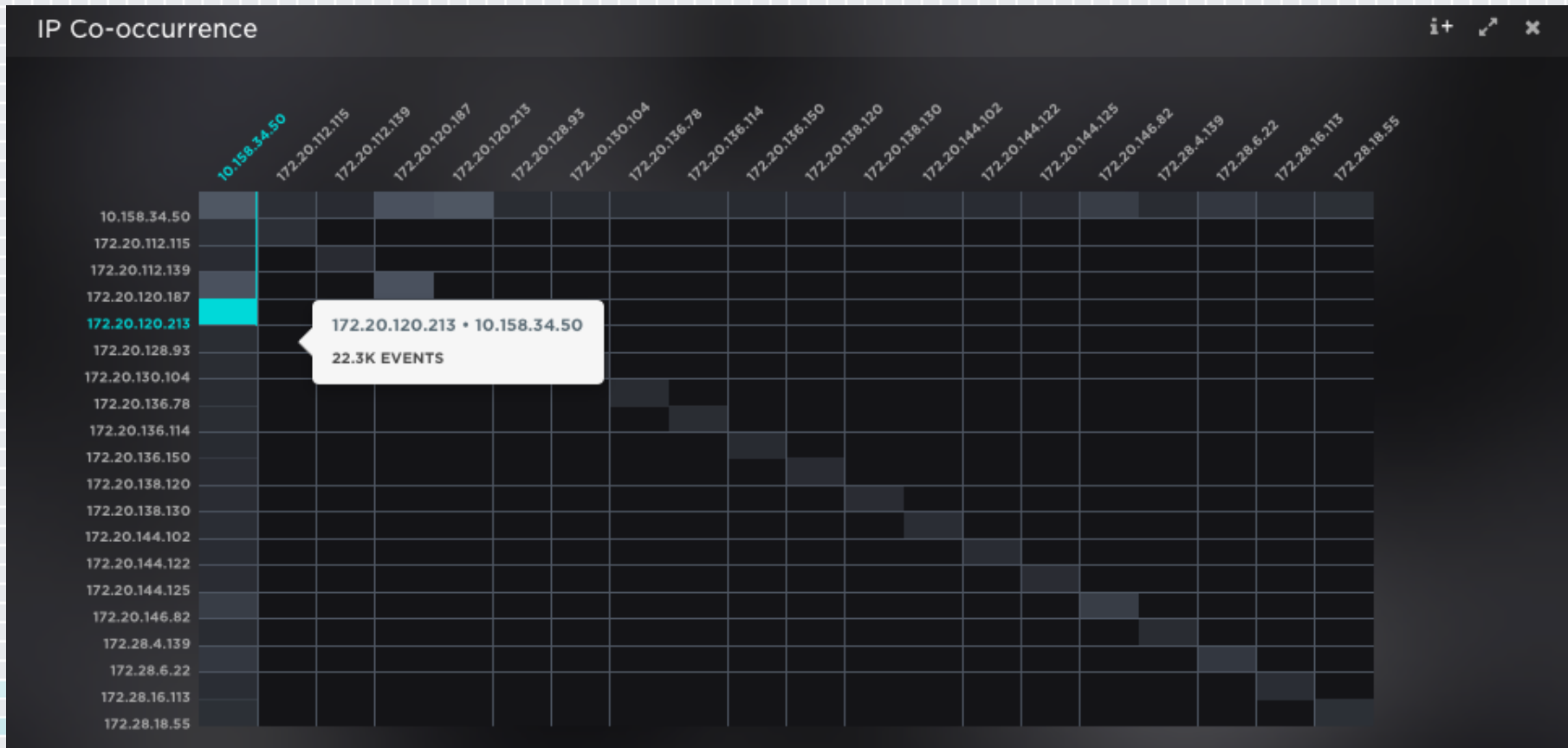
# Threat Analytics Platform – Shared Rules

FIREEYE RULES
CUSTOMER RULES
RISK: ALL ▾
STATUS: ALL ▾
RULE PACK: VENDOR - AWS CLOUDTR... ▾
*Search Rules*

ID	Name	Rule Pack	Risk	Distinguisher	Status	
1.1.613	AWS EC2 [Console Output Requested Via API]	Vendor - AWS CloudTrail	Low	username	Disabled	
1.1.612	AWS EC2 [Instance Monitoring Turned Off]	Vendor - AWS CloudTrail	Low	username	Enabled	
1.1.611	AWS EC2 [Encrypted Windows Password Retrieved]	Vendor - AWS CloudTrail	Low	username	Enabled	
1.1.610	AWS EC2 [AMI Shared]	Vendor - AWS CloudTrail	Low	username	Disabled	
1.1.609	AWS EC2 [AMI Made Public]	Vendor - AWS CloudTrail	Low	username	Disabled	
1.1.608	AWS EC2 [EBS Volume Snapshot Shared]	Vendor - AWS CloudTrail	Low	username	Enabled	
1.1.607	AWS IAM [Manual Action Without MFA]	Vendor - AWS CloudTrail	Low	username	Disabled	
1.1.606	AWS IAM [New Signing Certificate Uploaded]	Vendor - AWS CloudTrail	Low	username	Disabled	
1.1.605	AWS IAM [New Server Certificate Uploaded]	Vendor - AWS CloudTrail	Low	username	Disabled	
1.1.604	AWS IAM [Policy Change to Cloudtrail]	Vendor - AWS CloudTrail	Low	username	Disabled	 ▾
1.1.603	AWS EC2 [Several Instances Manually Created/Started]	Vendor - AWS CloudTrail	Low	username	Enabled	
1.1.602	AWS EC2 [EBS Volume Snapshot Made Public]	Vendor - AWS CloudTrail	Low	username	Disabled	
1.1.601	AWS [Non-service Root Account Usage]	Vendor - AWS CloudTrail	Low	username	Disabled	



# Threat Analytics Platform - Visualization



# Threat Analytics Platform - Alerts



**ALERT: [P1] - AWS IAM [Policy Change to Cloudtrail]**  
*2 days ago*

RISK:  
● MEDIUM

ORIGIN:  
CUSTOMER RULE

TRIGGER:  
9999.0.44 [P1] - AWS IAM [...]

EVENTS:  
9 HITS

INVESTIGATE

## Details

**CREATED:**  
2014-12-12 23:11:18 UTC

**LAST UPDATED:**  
2014-12-12 23:11:23 UTC

**STATE:**  
OPEN

**DISTINGUISHERS:**  
username - dsa-qdog-learning-aws-sandbox

### DESCRIPTION:

This behavioral rule looks for AWS IAM policy changes specific to Cloudtrail. Allowing unauthorized users access to Cloudtrail could represent a policy violation, or an attacker giving a user account access to create, delete, or stop logging infrastructure.

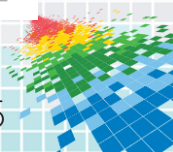
### QUERY:

```
class=aws_cloudtrail srczone=iam.amazonaws.com action=[putgrouppolicy,putrolepolicy,putuserpolicy] NOT username=[iss.casv1.awsuser, accessMgmt] rawmsg=/Action.*cloudtrail:(createtrail|deletetrail|updatetrail|startlogging|stoplogging)/ NOT rawmsg="/roleName": "kaos\-cloudtrail\-admin"/
```

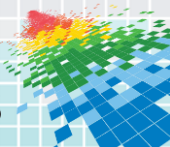
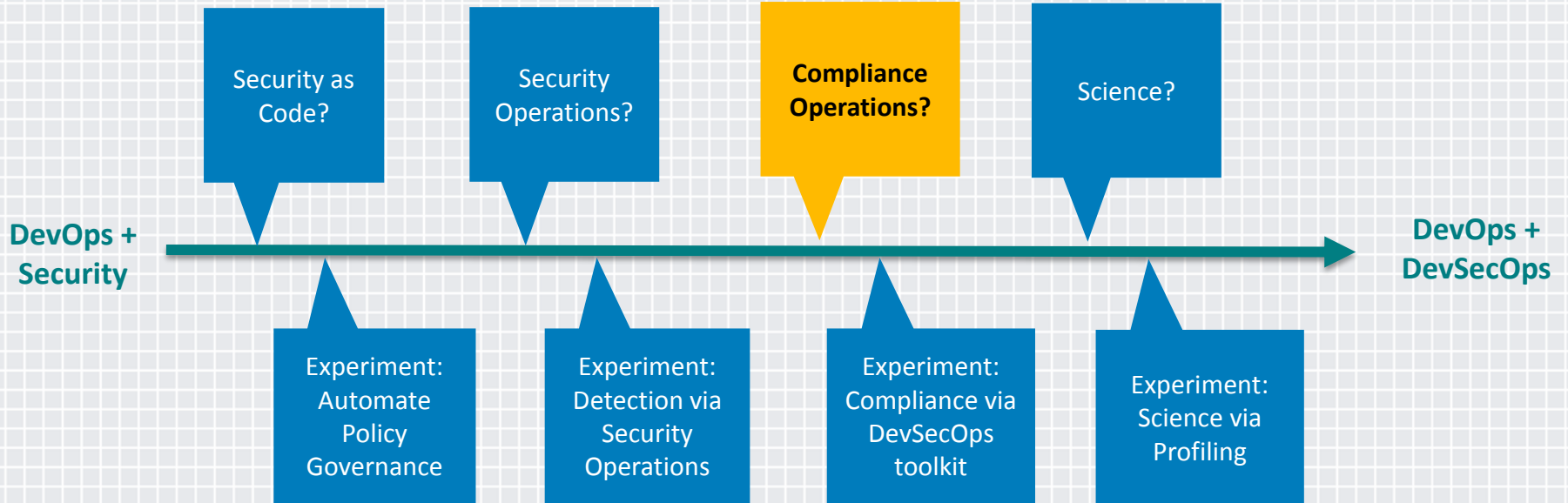
Events (9)

Revisions (1)

Notes (0)





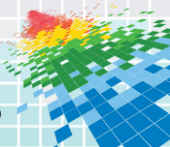
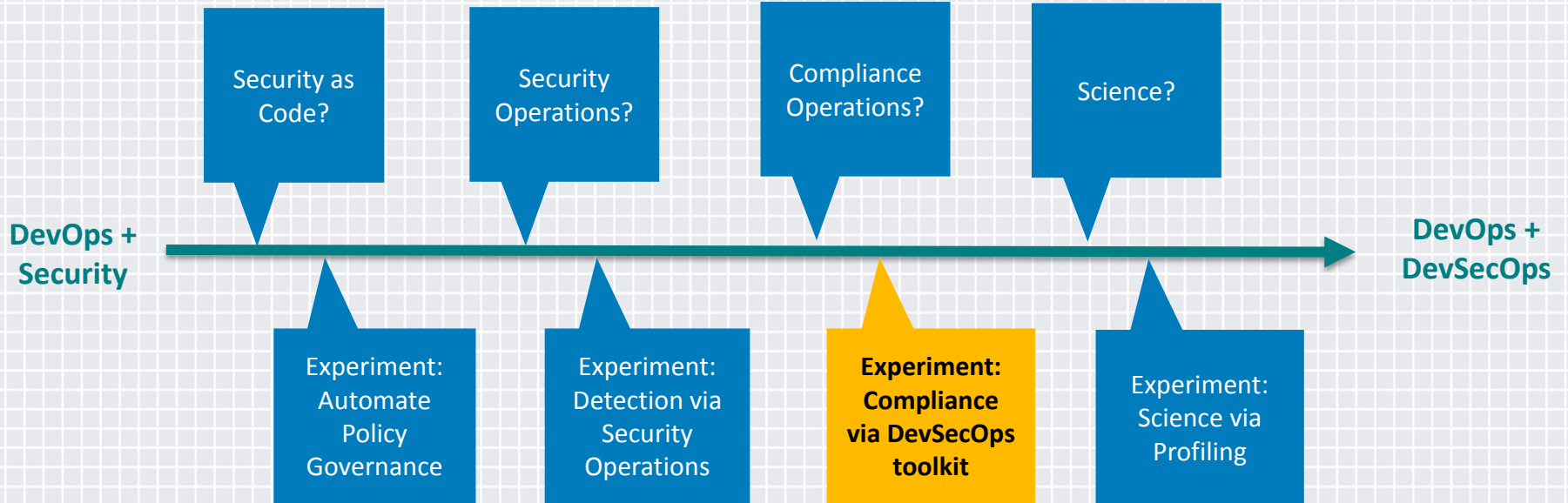


# Compliance Operations for Actionable Inline Feedback

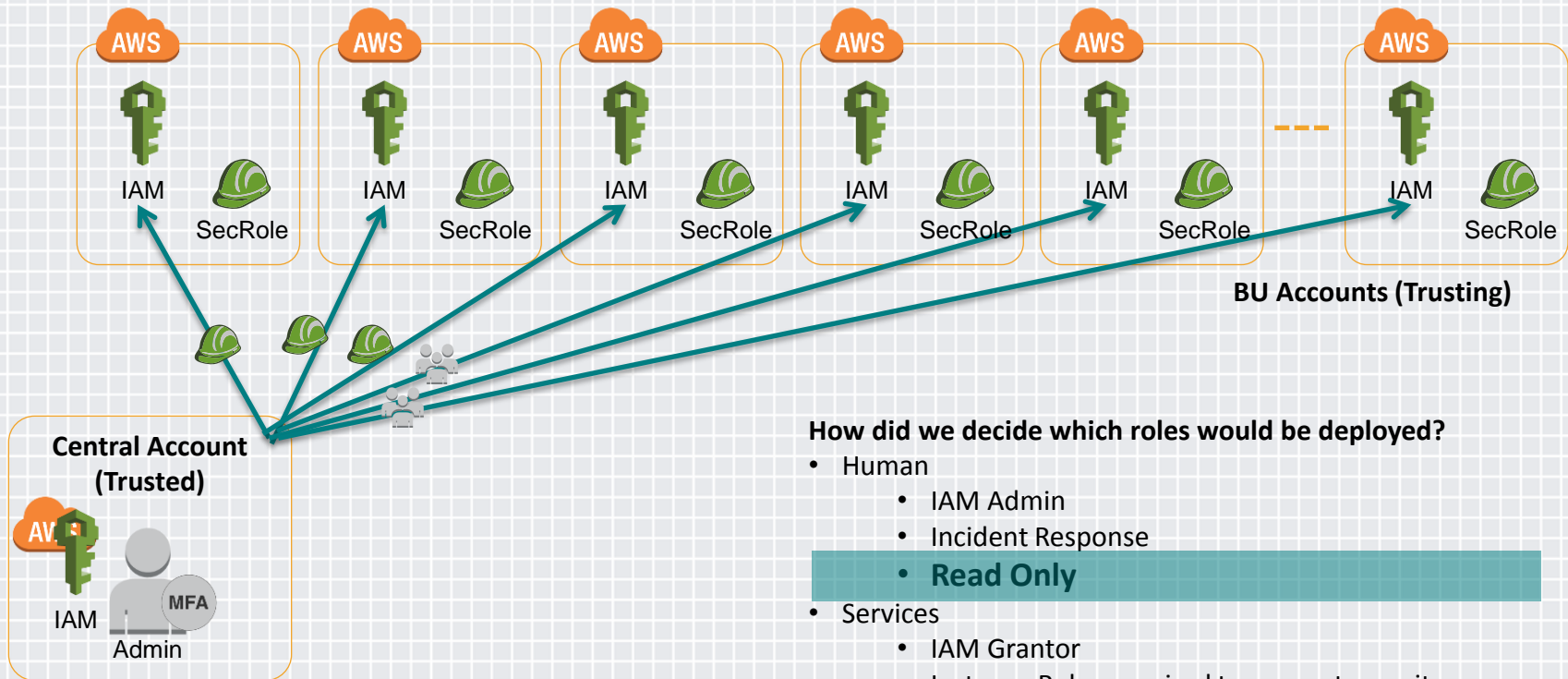
experimenting with these principles...

- ◆ Dynamic automated evaluations
- ◆ Compliance alerts are provided in real-time
- ◆ Self-Service Security Education
- ◆ Education on-demand



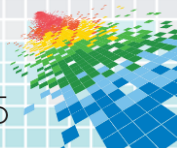


# DevSecOps Toolkit – Cross-Account Roles



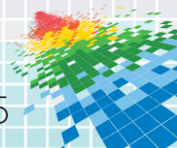
## How did we decide which roles would be deployed?

- Human
  - IAM Admin
  - Incident Response
  - **Read Only**
- Services
  - IAM Grantor
  - Instance Roles required to support security services
  - Read Only



# DevSecOps Toolkit – MFA via Google Authenticator

- ◆ Human Admins are dangerous and require AWS integrated MFA with Google Authenticator to protect your account.
- ◆ Important for AWS to validate a human being vs. using external MFA to support authentication that could be hijacked.
- ◆ MFA placed on the Assumed Role which is trusted by the child account role.



# DevSecOps Toolkit – Help & Interactive Mode

```
lionsess-9:toolkit shannon$ bundle exec bin/tk help config
```

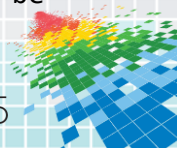
Usage:

```
tk config
```

Options:

<code>-i, [--interactive], [--no-interactive]</code>	<code># interactive mode for q&amp;a to set up config</code>
<code>-p, [--profile-name=PROFILE_NAME]</code>	<code># profile name in .aws config file</code>
<code>-r, [--master-region=MASTER_REGION]</code>	<code># region for master account</code>
	<code># Default: us-west-2</code>
<code>-a, [--master-account=MASTER_ACCOUNT]</code>	<code># 12 digit AWS account number without dashes</code>
<code>-n, [--master-role-name=MASTER_ROLE_NAME]</code>	<code># name of master role to assume cross-account roles</code>
	<code># Default: master-auditor</code>
<code>-t, [--target-account-list=TARGET_ACCOUNT_LIST]</code>	<code># location for csv file containing accounts list to audit</code>
	<code># Default: config/accounts.csv</code>
<code>-d, [--output-dir=OUTPUT_DIR]</code>	<code># directory for storing results</code>
	<code># Default: home</code>
<code>-f, [--output-type=OUTPUT_TYPE]</code>	<code># supports csv</code>
	<code># Default: csv</code>

Description: Using the devsecops toolkit requires a master configuration file to establish the credentials, role, MFA, etc. used to support cross-account usage. This command provides you with an interactive and advanced interface for creating a configuration file to support your usage. The configuration file can be found in your home directory under `.tk/config` and you can also hand edit this file using `yaml`.

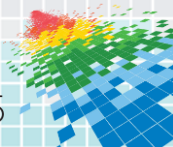
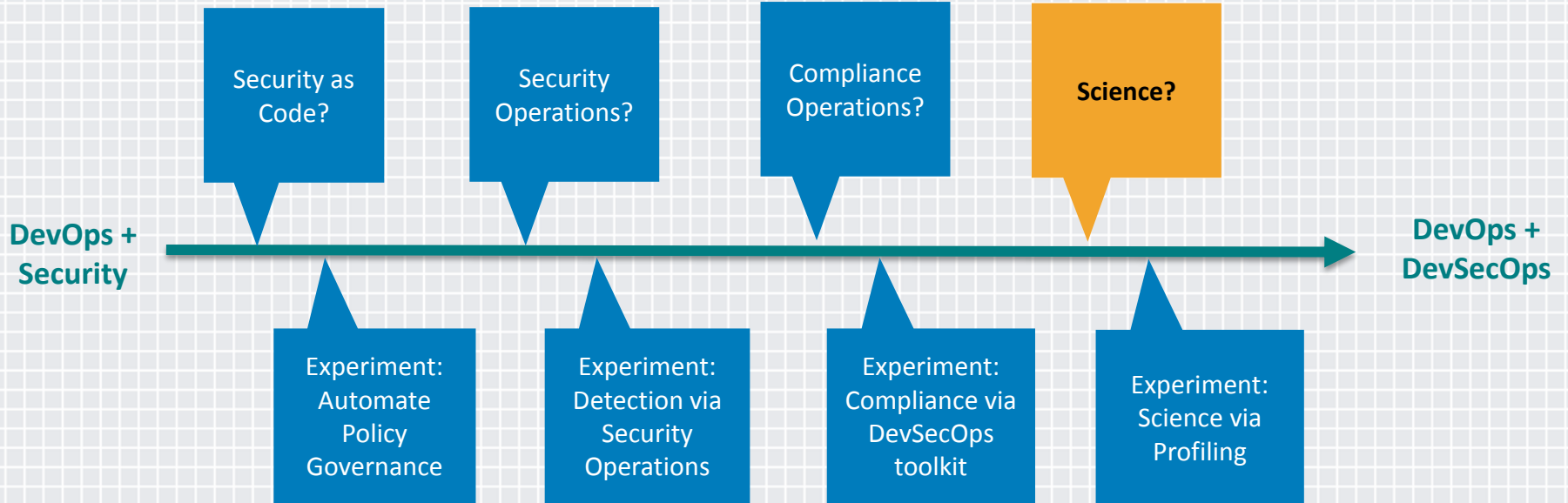




# DevSecOps Toolkit – Output to CSV

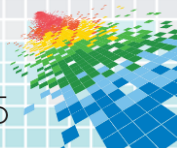
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	account_alias	account_nur	check_date	iam_instance	image_id	instance_id	instance_typ	launch_time	owner_id	placement_a	placement_t	platform	private_dns	private_ip_a pr
2	cto-dev-tramalfad	8.8507E+11	2014-11-13 22:48:43 UTC	ami-c9d89bf	i-f1e8e0fc	m3.medium	2014-10-02 22:00	8.8507E+11	us-west-2a	dedicated				10.81.3.171
3	cto-dev-tramalfad	8.8507E+11	2014-11-13 22:48:44 UTC	ami-9fa2efaf	i-4ddb2c47	c3.large	2014-10-10 23:00	8.8507E+11	us-west-2a	dedicated				10.81.3.25
4	cto-dev-tramalfad	8.8507E+11	2014-11-13 22:48:44 UTC	ami-9fa2efaf	i-c3839cce	c3.large	2014-10-10 22:59	8.8507E+11	us-west-2a	dedicated				10.81.3.6
5	tramalfadore-pre-f	7.7804E+11	2014-11-13 22:49:12 UTC	ami-b600bdc	i-0c1845e2	c3.large	2014-10-13 23:59	7.7804E+11	us-east-1b	dedicated			ip-10-80-200	10.80.200.14 ex
6	tramalfadore-pre-f	7.7804E+11	2014-11-13 22:49:12 UTC	ami-b600bdc	i-89ede862	c3.large	2014-10-13 23:59	7.7804E+11	us-east-1c	dedicated			ip-10-80-200	10.80.200.53 ex
7	tramalfadore-pre-f	7.7804E+11	2014-11-13 22:49:12 UTC	arn:aws:iam::	ami-c8cb41a	i-29ad33c3	m3.medium	2014-11-11 00:00	7.7804E+11	us-east-1c	dedicated		ip-10-80-204	10.80.204.154
8	tramalfadore-pre-f	7.7804E+11	2014-11-13 22:49:16 UTC	ami-9fa2efaf	i-7f699b75	c3.large	2014-10-13 23:59	7.7804E+11	us-west-2b	dedicated				10.80.192.65
9	tramalfadore-pre-f	7.7804E+11	2014-11-13 22:49:16 UTC	arn:aws:iam::	ami-2f9bd01	i-4774d84d	m3.medium	2014-11-11 00:00	7.7804E+11	us-west-2b	dedicated			10.80.195.75
10	tramalfadore-pre-f	7.7804E+11	2014-11-13 22:49:16 UTC	arn:aws:iam::	ami-2f9bd01	i-6474d86e	m3.medium	2014-11-11 00:00	7.7804E+11	us-west-2b	dedicated			10.80.195.146
11	tramalfadore-pre-f	7.7804E+11	2014-11-13 22:49:17 UTC	ami-9fa2efaf	i-7375167c	c3.large	2014-10-13 23:59	7.7804E+11	us-west-2c	dedicated				10.80.192.145

Count of subnet_id	Column Labels	54.187.208.45	54.187.35.1	54.201.138.81	54.201.142.175	54.85.174.190	54.85.42.13	(blank)	Grand Total
subnet-009e6877								1	1
subnet-056d7371								1	1
subnet-1a9e686d			1						1
subnet-24aaa046				1					1
subnet-29aaa04b							2		2
subnet-57cbd523							1		1
subnet-9a88dfdc					1				1
subnet-9b7aabfe		1							1
subnet-a36f348b						1			1
(blank)									
<b>Grand Total</b>		<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>4</b>	<b>10</b>



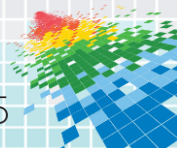
# The Principles of Security Science

- ◆ Death to F.U.D. (No proof, no problem)
- ◆ Rely on data
- ◆ Prove your assumptions
- ◆ Model the solutions
- ◆ Provide tools to support decisions



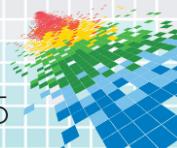
# Goals of Security Science

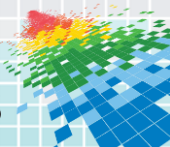
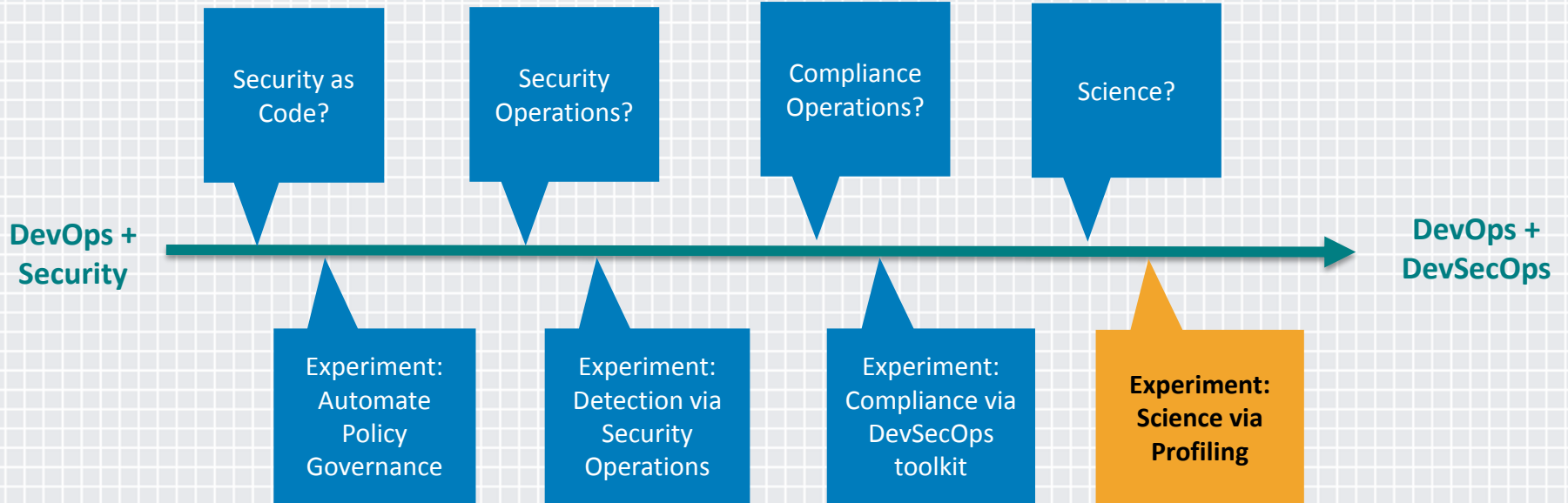
- ◆ Empower teams to make sane security decisions
- ◆ Prevent security breaches by guiding process
- ◆ Uncover new threats and vulnerabilities through data analysis
- ◆ Seek out new life and new civilizations, to boldly go where no Security Team has gone before



# Examples of Security Science

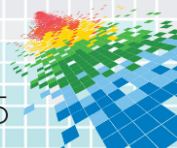
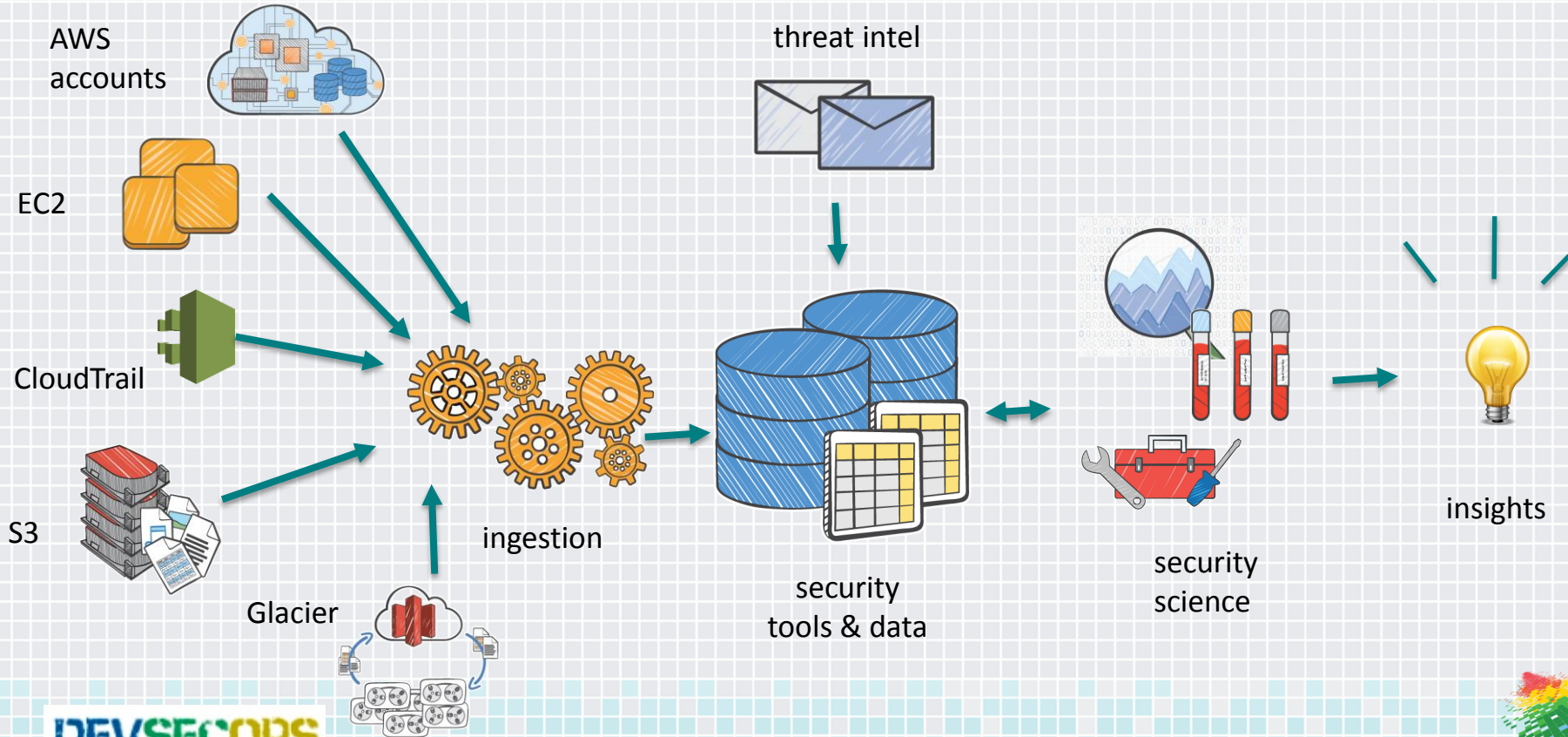
- ◆ 90 day password length vs. \$10k attacker offline cracker speed
  - ◆ MD-5 = 19 characters
  - ◆ SHA-512 = 11 characters
  - ◆ BCrypt = 8 characters
- ◆ With RHEL6 and goal of CVSS < 4, how often to restack?
  - ◆ Amazon RHEL 6 Server = 5.3 days
  - ◆ Our base AMI = 10.5 days





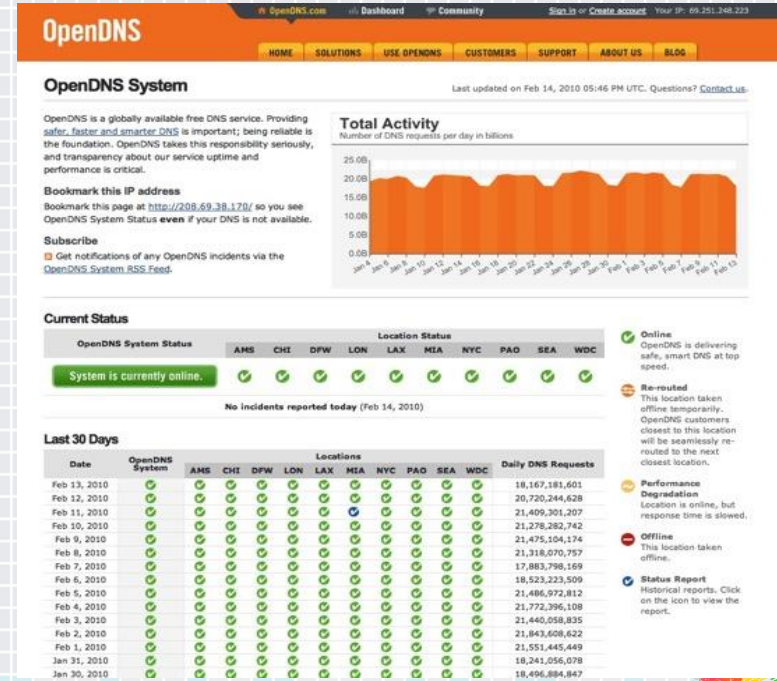
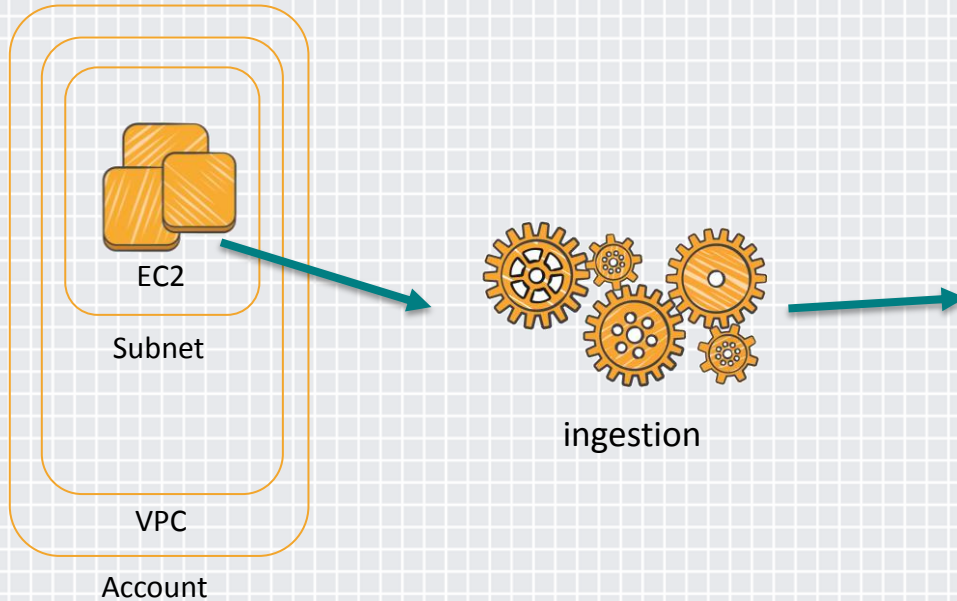


# ...profiling drift on accounts, services and instances...





# ...egress monitoring + threat intel to detect Suspicious Exfiltration...



**OpenDNS System** Last updated on Feb 14, 2010 05:46 PM UTC. Questions? [Contact Us](#).

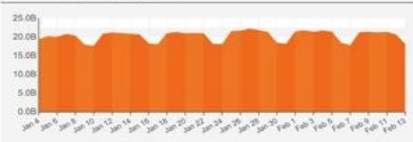
OpenDNS is a globally available free DNS service. Providing **safer, faster and smarter DNS** is important; being reliable is the foundation. OpenDNS takes this responsibility seriously, and transparency about our service uptime and performance is critical.

**Bookmark this IP address**  
Bookmark this page at <http://208.69.38.170/> so you see OpenDNS System Status **even** if your DNS is not available.

**Subscribe**  
 Get notifications of any OpenDNS incidents via the [OpenDNS System RSS Feed](#).

### Total Activity

Number of DNS requests per day in billions



**Current Status**

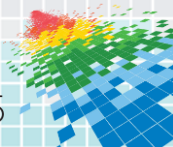
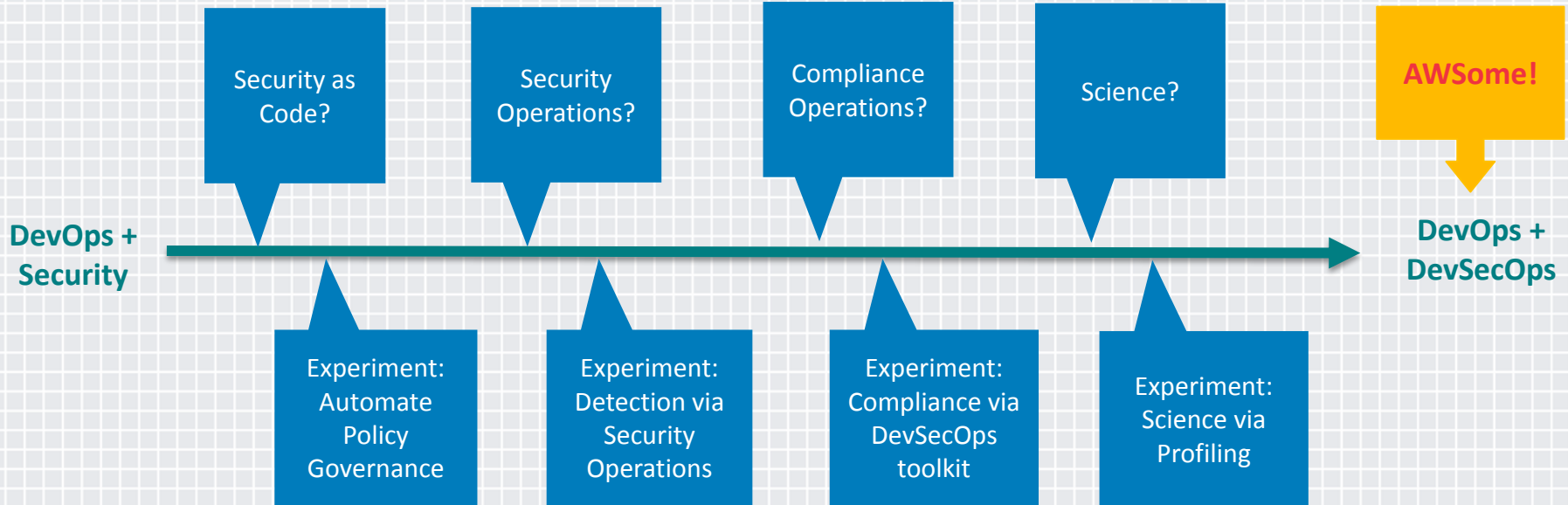
OpenDNS System Status	Location Status									
	AMS	CHI	DFW	LON	LAX	MEA	NYC	PAO	SEA	WDC
<b>System is currently online.</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

No incidents reported today (Feb 14, 2010)

### Last 30 Days

Date	OpenDNS System	Locations										Daily DNS Requests
		AMS	CHI	DFW	LON	LAX	MEA	NYC	PAO	SEA	WDC	
Feb 13, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	18,167,181,601	
Feb 12, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	20,720,244,628	
Feb 11, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	21,409,301,207	
Feb 10, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	21,278,282,742	
Feb 9, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	21,475,104,174	
Feb 8, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	21,318,070,757	
Feb 7, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	17,883,798,159	
Feb 6, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	18,523,223,509	
Feb 5, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	21,486,972,812	
Feb 4, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	21,772,396,108	
Feb 3, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	21,440,058,835	
Feb 2, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	21,843,608,422	
Feb 1, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	21,551,445,449	
Jan 31, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	18,241,056,078	
Jan 30, 2010	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	18,494,884,847	

- Online**  
OpenDNS is delivering safe, smart DNS at top speed.
- Re-routed**  
This location taken offline temporarily. OpenDNS customers closest to this location will be seamlessly re-routed to the next closest location.
- Performance Degradation**  
Location is online, but response time is slowed.
- Offline**  
This location taken offline.
- Status Report**  
Historical reports. Click on the icon to view the report.



# Apply What You Have Learned Today



- ◆ Next week you should:
  - ◆ Join the DevSecOps Community via the LinkedIn Group and Twitter
  - ◆ Determine which coding language makes sense for your team
  - ◆ Start with assessing your org's cloud adoption strategy, security requirements and work backwards
- ◆ In the first three months following this presentation you should:
  - ◆ Develop a whitelisting roadmap
  - ◆ Identify policies that need to be converted to code
  - ◆ Start with Access as a foundation and develop standard naming conventions
- ◆ Within six months you should:
  - ◆ Have a platform that supports basic decisions
  - ◆ Have a wealth of data to gain insights
  - ◆ Begin to provide real-time insights for teams to remediate their issues based on scores/grades

