Who done it:

Gaining visibility and accountability in the cloud

By Ryan Nolette

Squirrel Edition

$whoami

10+ year veteran of IT, Security Operations, Threat Hunting, Incident Response, Threat Research, and Forensics

GitHub

- https://github.com/sonofagl1tch

Career highlight

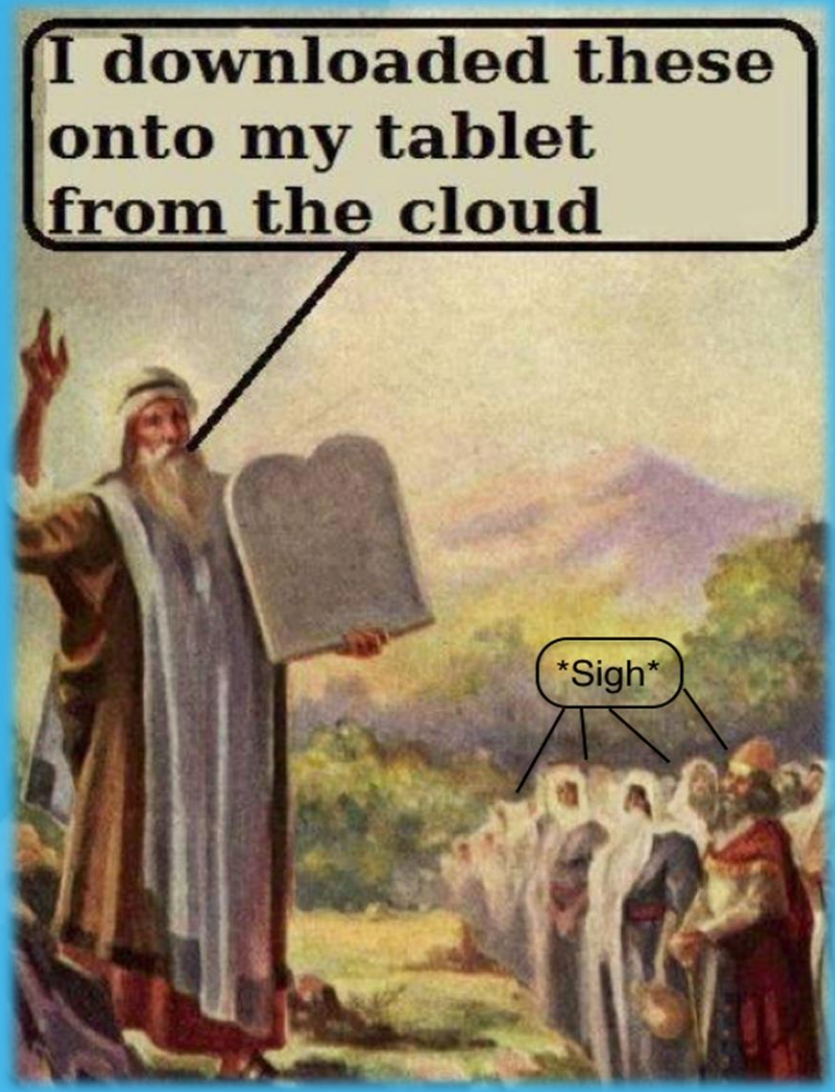
- Time's person of the year 2006

What am I giving away? A full detonation lab built automatically by cloudformation

- https://github.com/sonofagl1tch/AWSDetonationLab

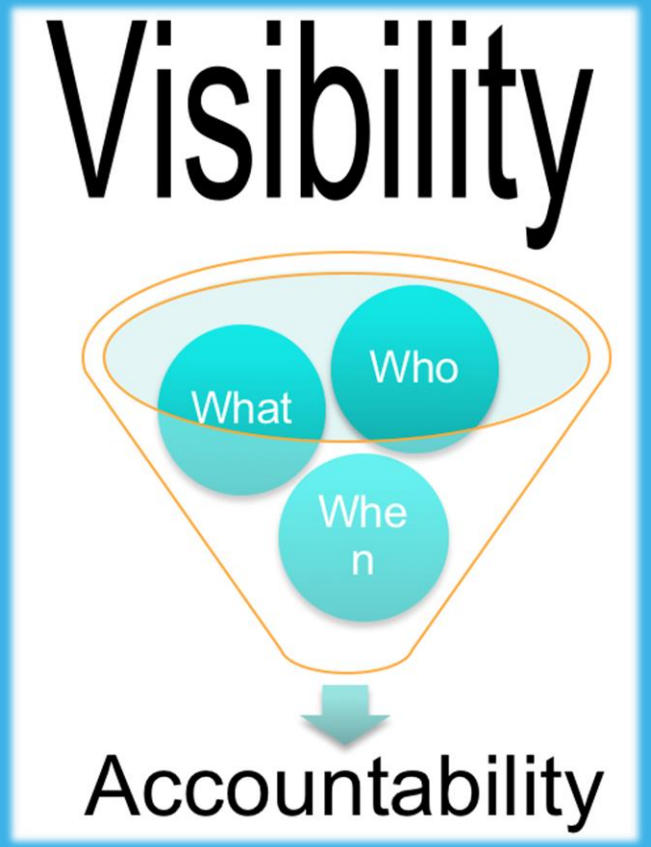
Agenda

- Overview
  - Who did what and when?
  - Common Techniques
  - Common Visibility Tools and Their AWS Equivalent
- Increasing visibility until you have accountability
  - Common Logging
    - Authentication
    - Endpoint
    - Network
    - Vulnerabilities
    - Configuration
- End to end example
  - Detonation Lab
  - Logging Pipelines and Services
- Finding What Matters



Who did what and when

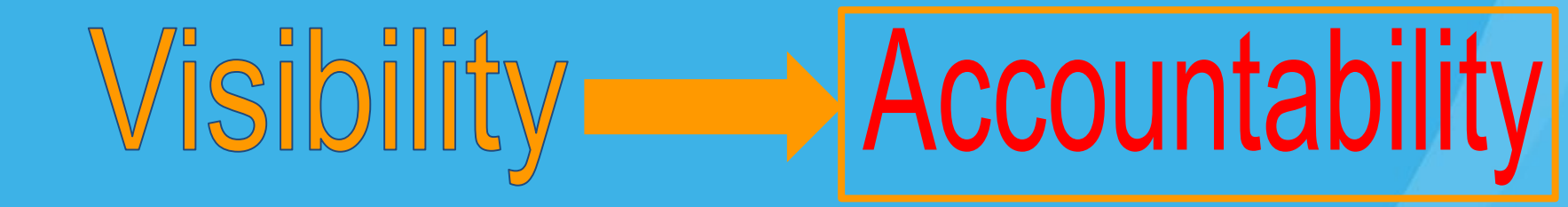
- These are the 3 pillars of each stage of scoping the event
- Will be modified for each iteration
- The analysts should be able to start at any of the stages and complete the cycle



Common Techniques

What's Their Goal?

- OS hardening
- Config management
- Identity Management
- Process monitoring



Who What When

Common Visibility Tools and Their AWS Equivalent

Traditional Tool	AWS equivalent
IDS/IPS	guardDuty
DLP	Macie
EDR	Cloudwatch + osquery, GRR
Netflow	Cloudwatch + VPCFlow
DNS	Cloudwatch + Route53
Access and authentication auditing	CloudTrail
Active Directory	Directory Service
Identity Management	IAM
Single Sign On	AWS SSO
Vulnerability scanner	Inspector
Configuration Management	AWS config
Logging	Cloudwatch + Firehose + Lambda

Increasing visibility until you have accountability

The process of asking who did what and when and increasing logging and controls until you can answer those questions for every scenario you can think of.

OS hardening

- CIS guidelines audit and hardening scripts.
- Additional logging and hardening scripts created by experience over time.

Logging

- Common logging like auth logs and process creation etc

Authentication

- /var/log/secure
- IAM logs
- IAM roles
- IAM policies

Endpoint

- EDR
- HIDS
- Cloudwatch
- GuardDuty

Network

- IDS
- Netstat
- Tcpdump
- Vpc flow logs
- Dns route 53 logs

Vulnerabilities/ Configuration

- Generic vuln scanner
- Inspector
- NVD/CVE usage
- Aws config
- OS hardening
- Applications config

End to end example

Always Squirrel away your logs

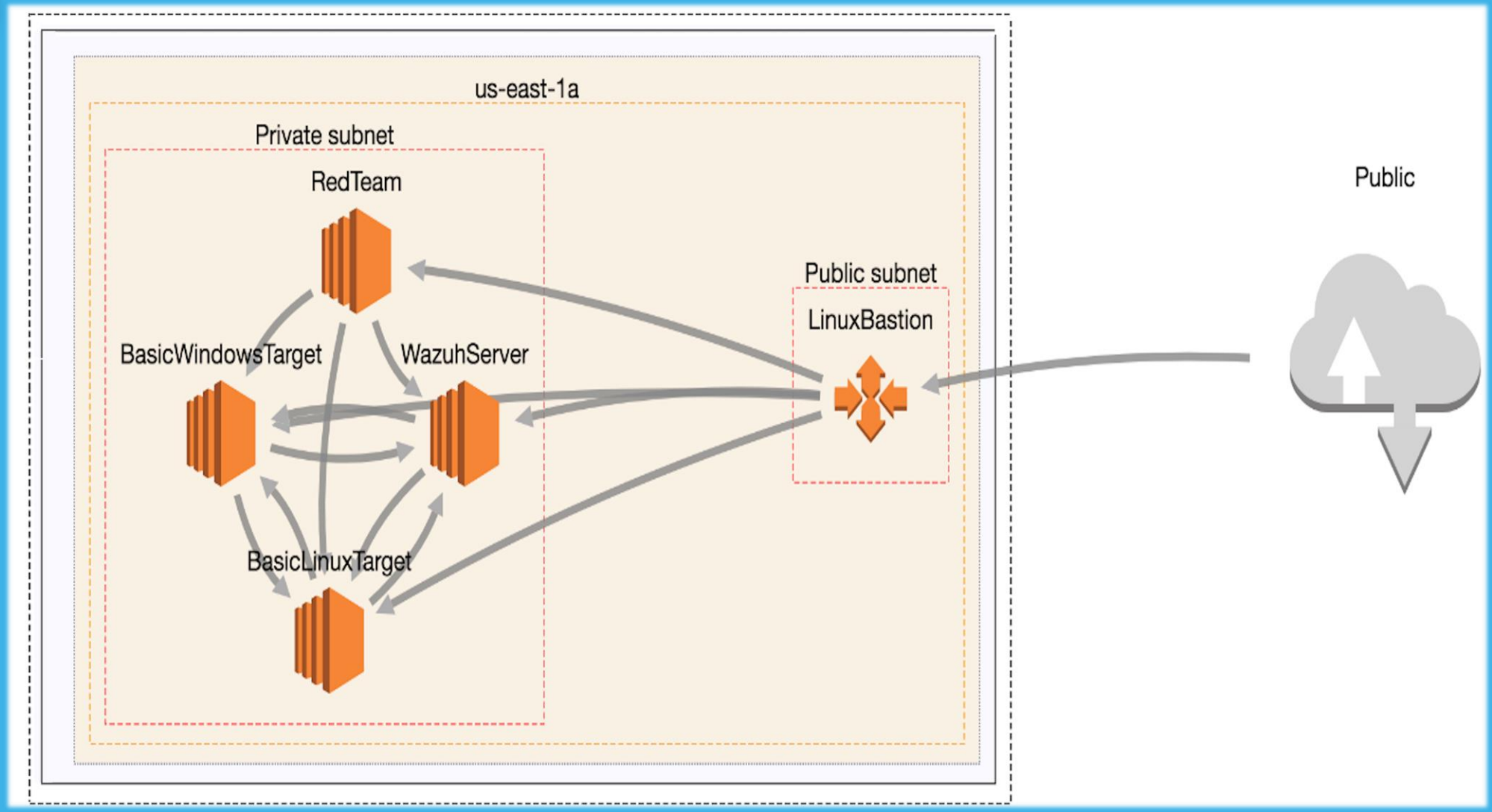
DevOps Installs new tool that is backdoored with a CryptoMiner

Static defense controls do not stop miner installation

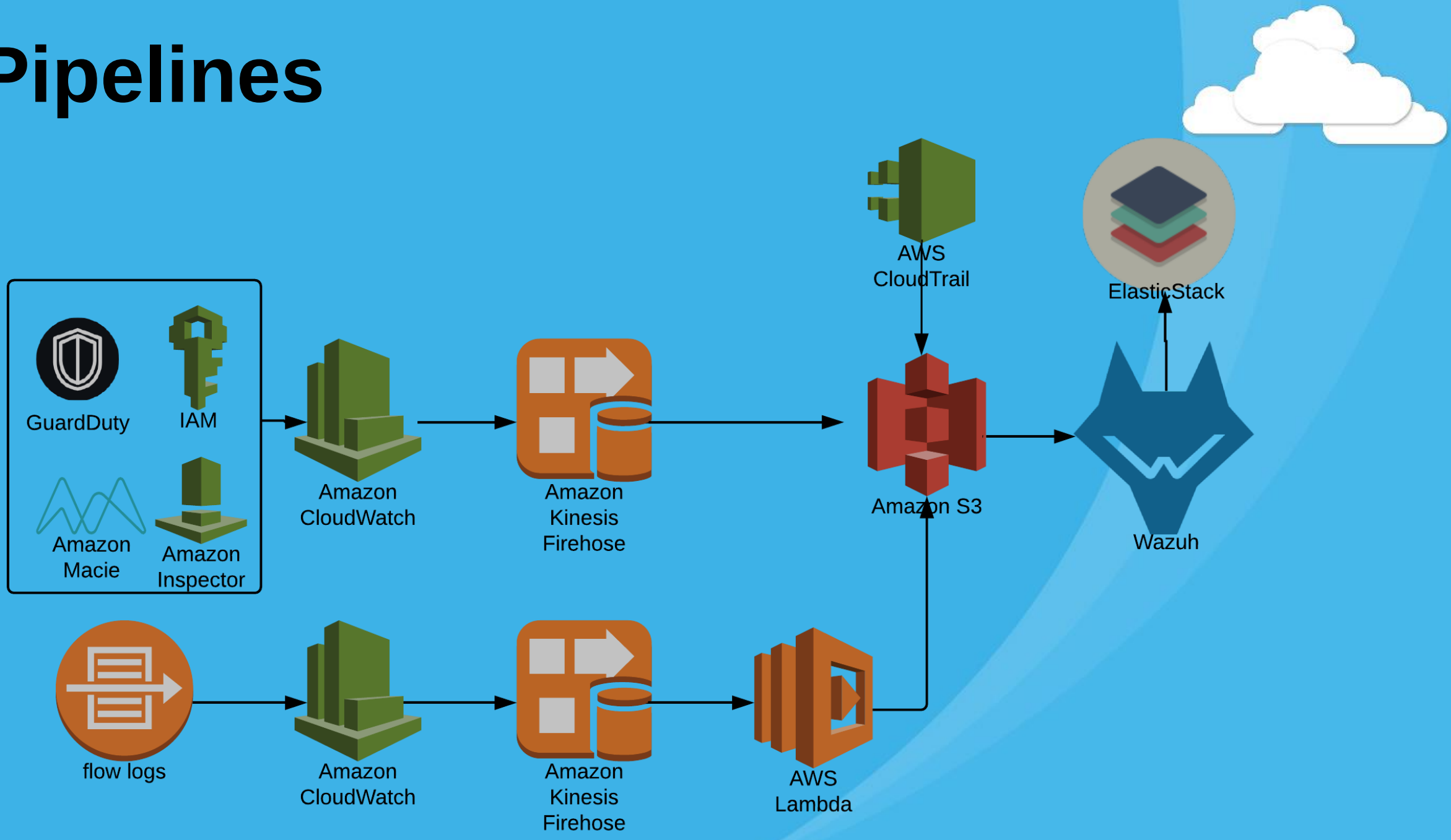
SecOps remains vigilant

SecOps Defends

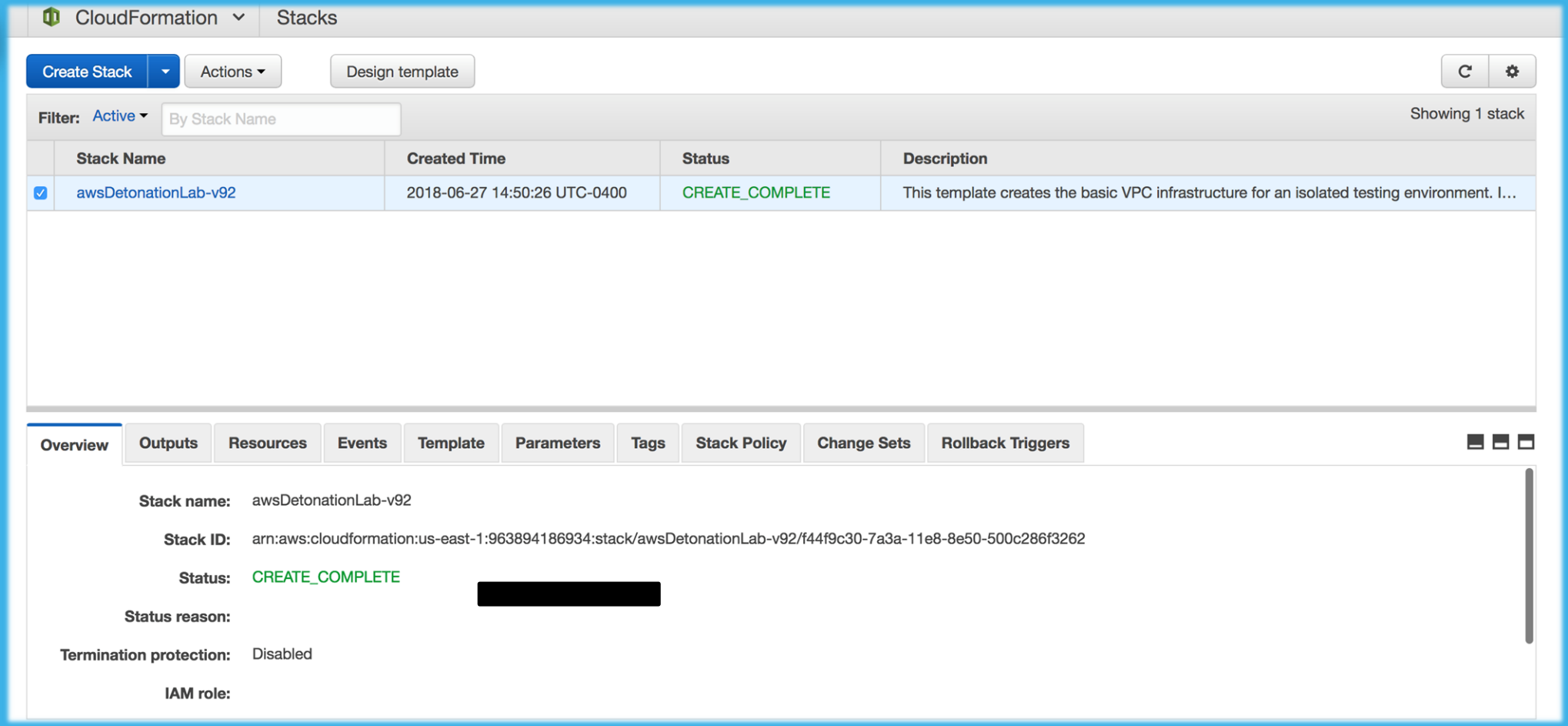
Detonation Lab Topology



Pipelines

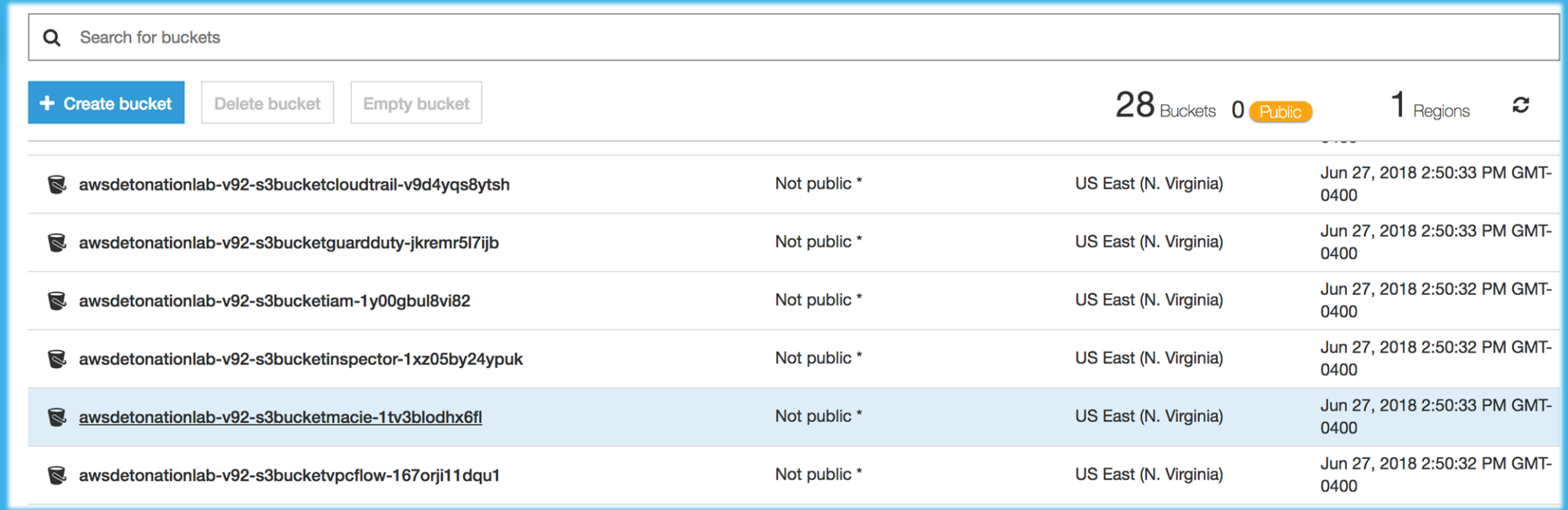

GuardDuty
IAM
Amazon Macie
Amazon Inspector
Amazon CloudWatch
Amazon Kinesis Firehose
AWS CloudTrail
Amazon S3
ElasticStack
Wazuh
flow logs
Amazon CloudWatch
Amazon Kinesis Firehose
AWS Lambda

CloudFormation



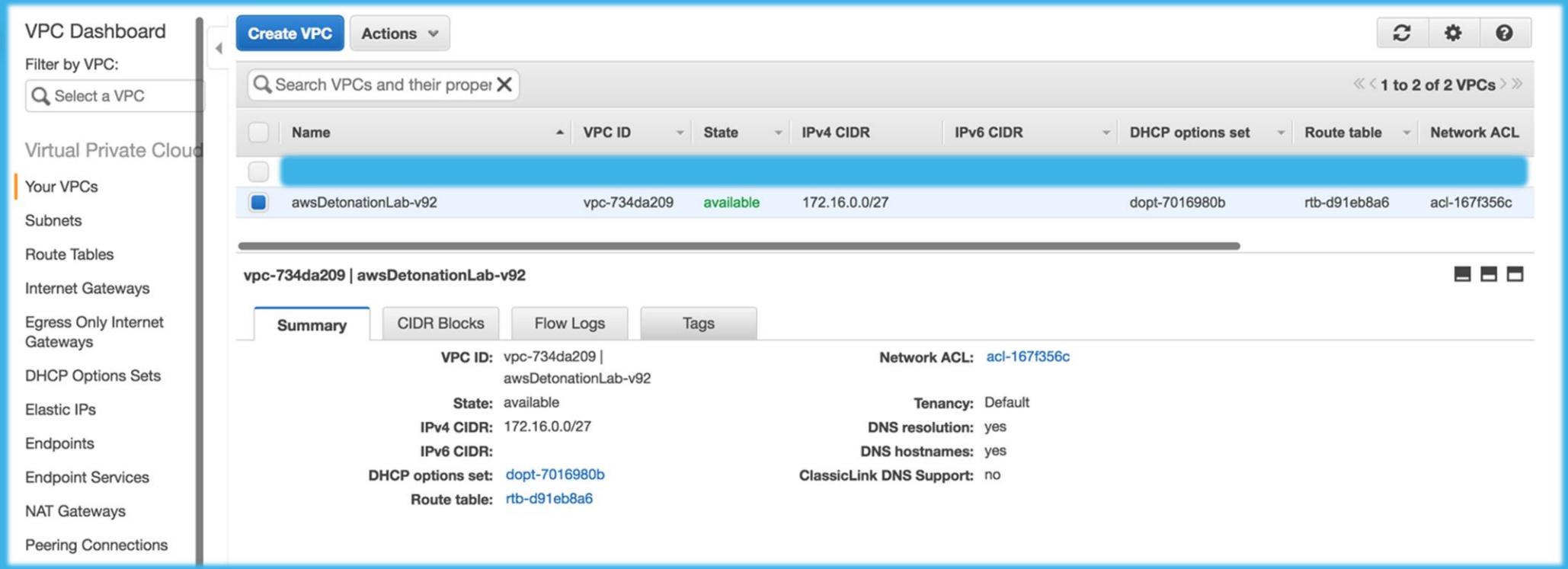
CloudFormation allows you to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts.

S3



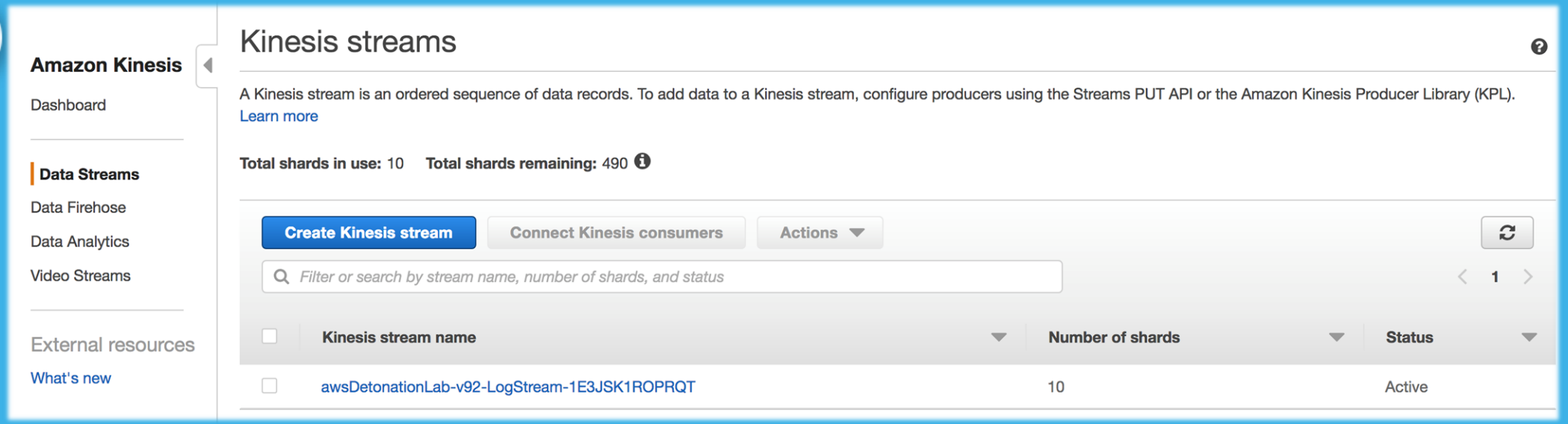
Amazon S3 is object storage built to store and retrieve any amount of data from anywhere

VPC



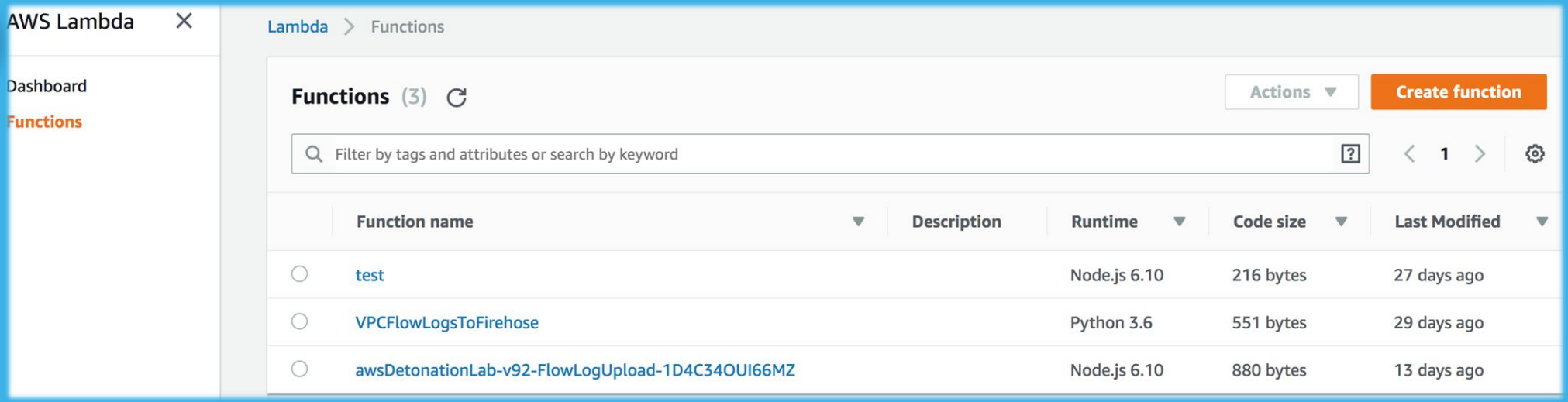
Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define.

VPC Flow - Kinesis Stream



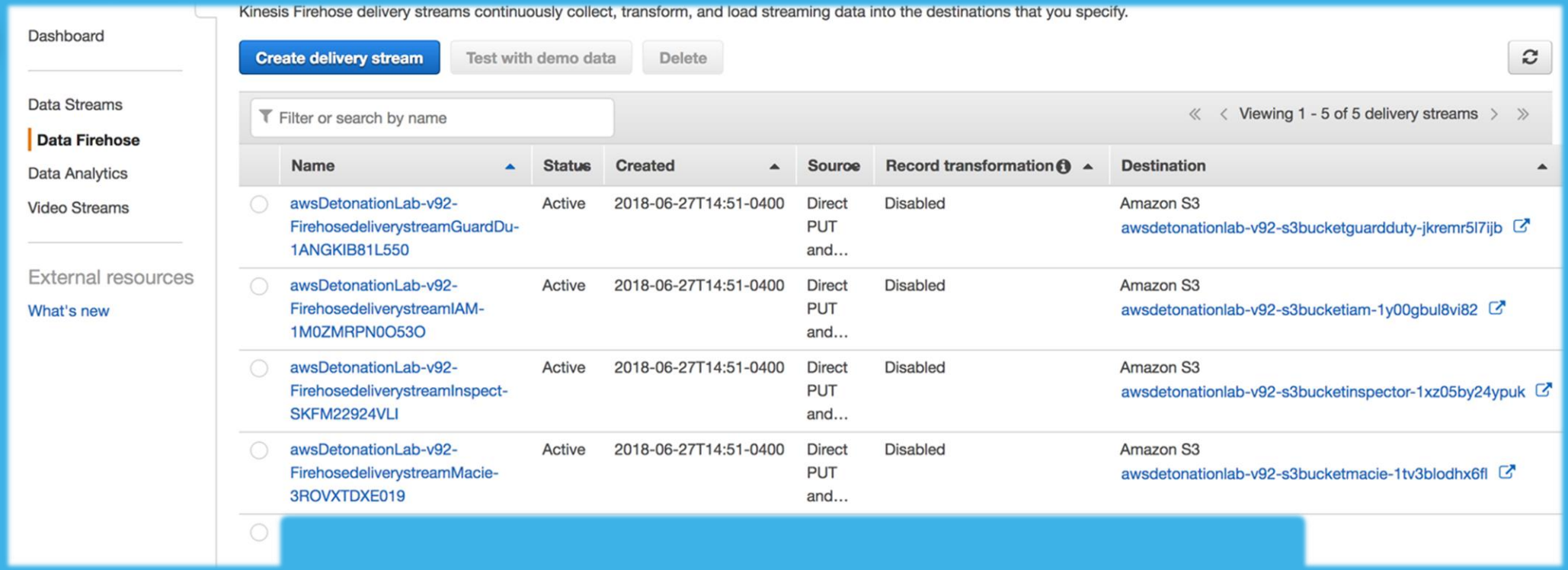
Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events.

Lambda



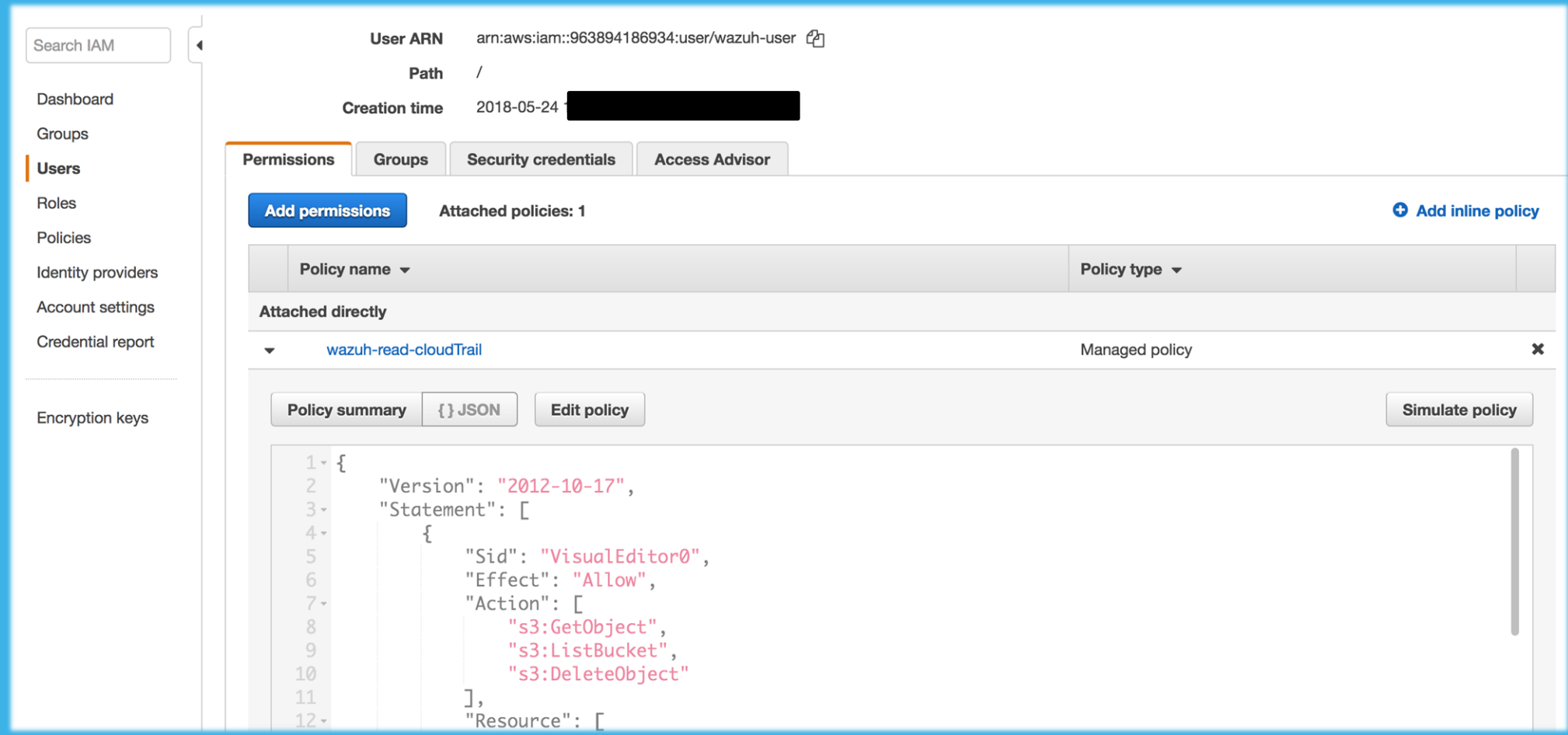
AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume - there is no charge when your code is not running.

Firehose



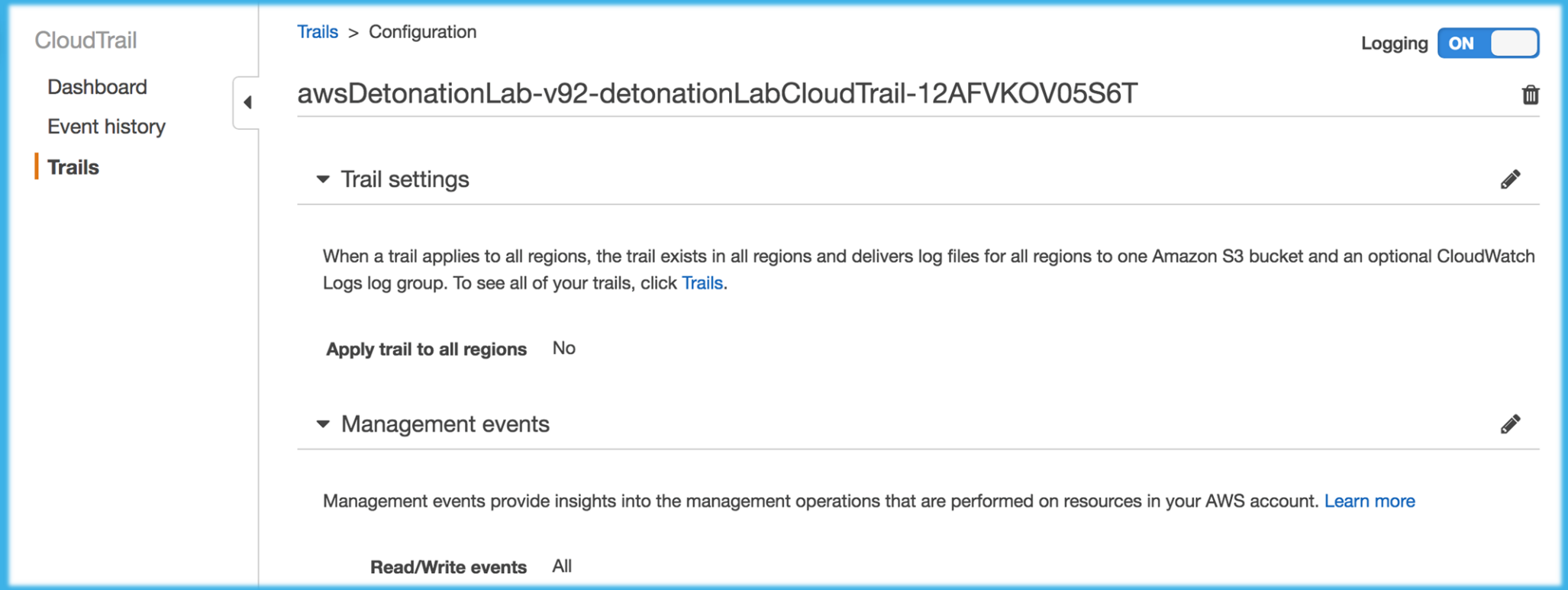
Amazon Kinesis Data Firehose is the easiest way to reliably load streaming data into data stores and analytics tools.

IAM



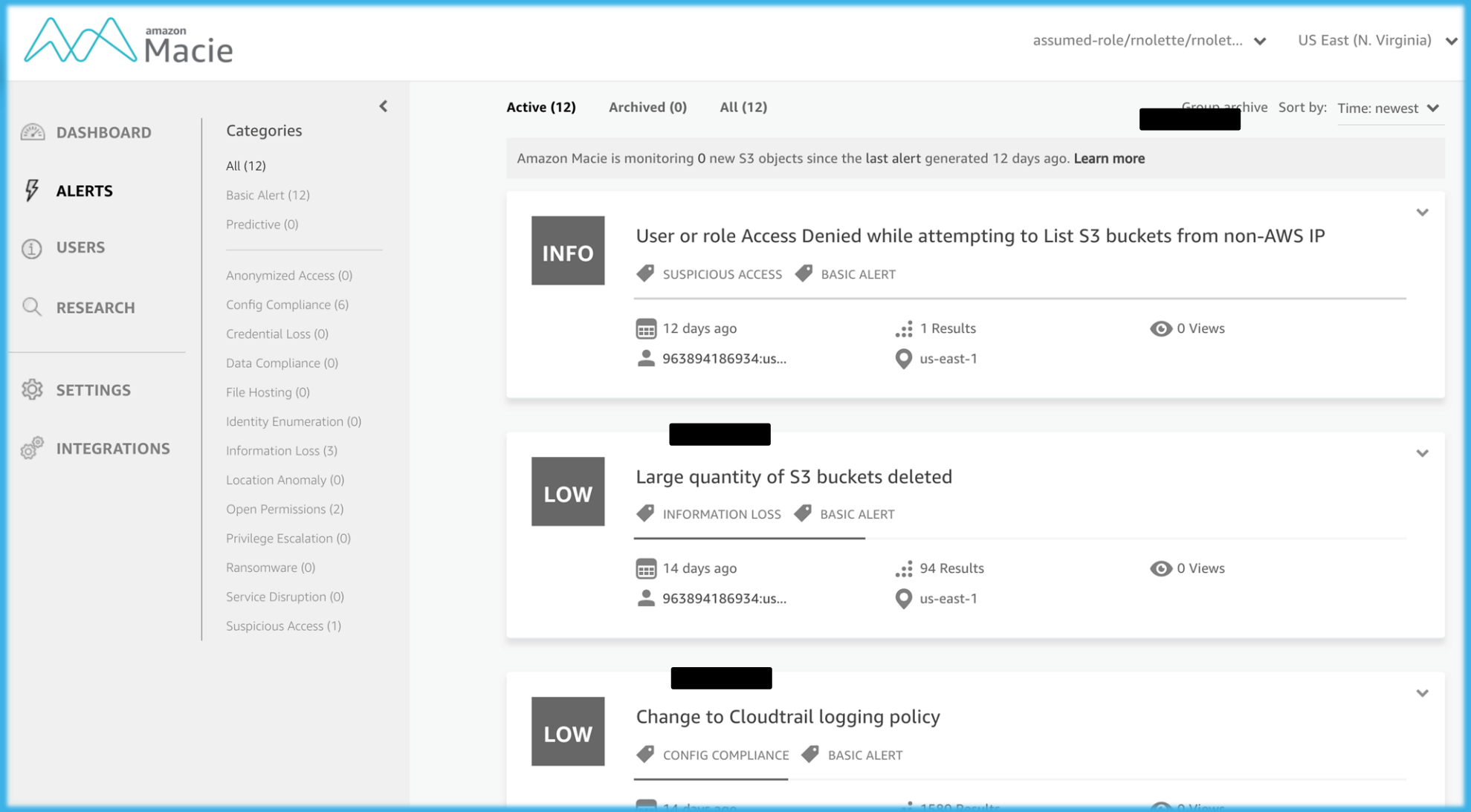
AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

CloudTrail



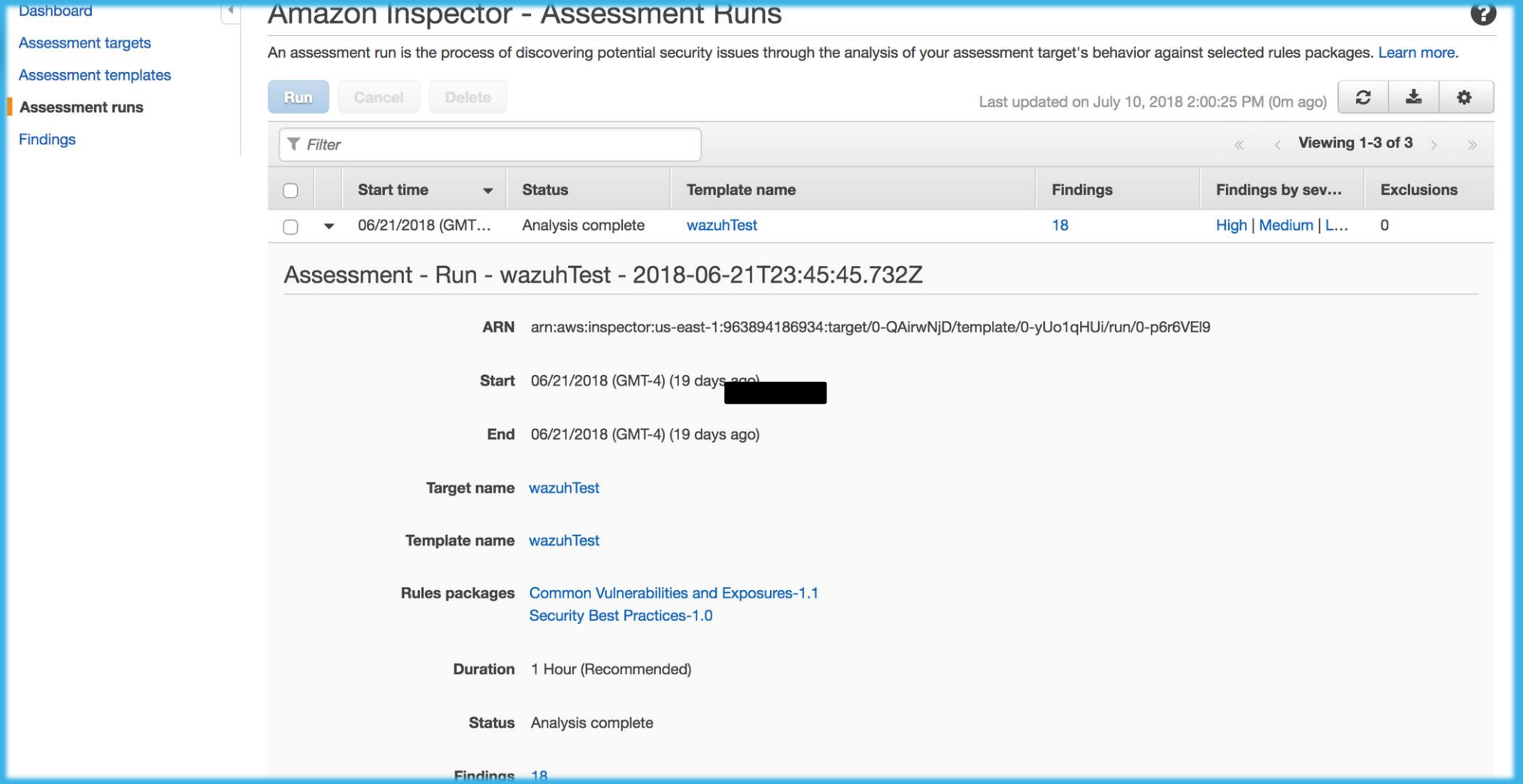
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.

Macie



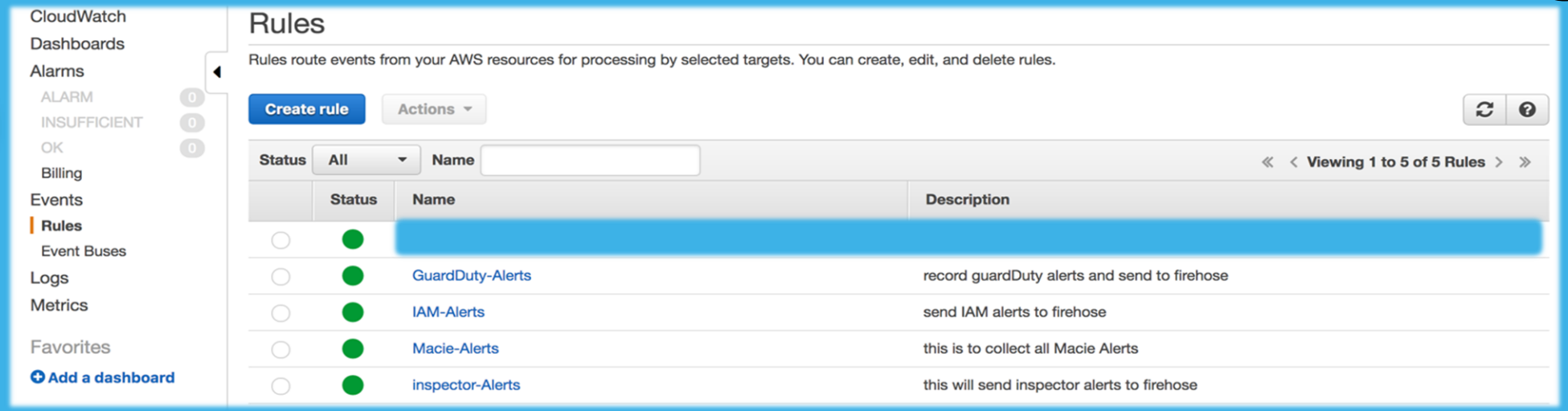
Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS.

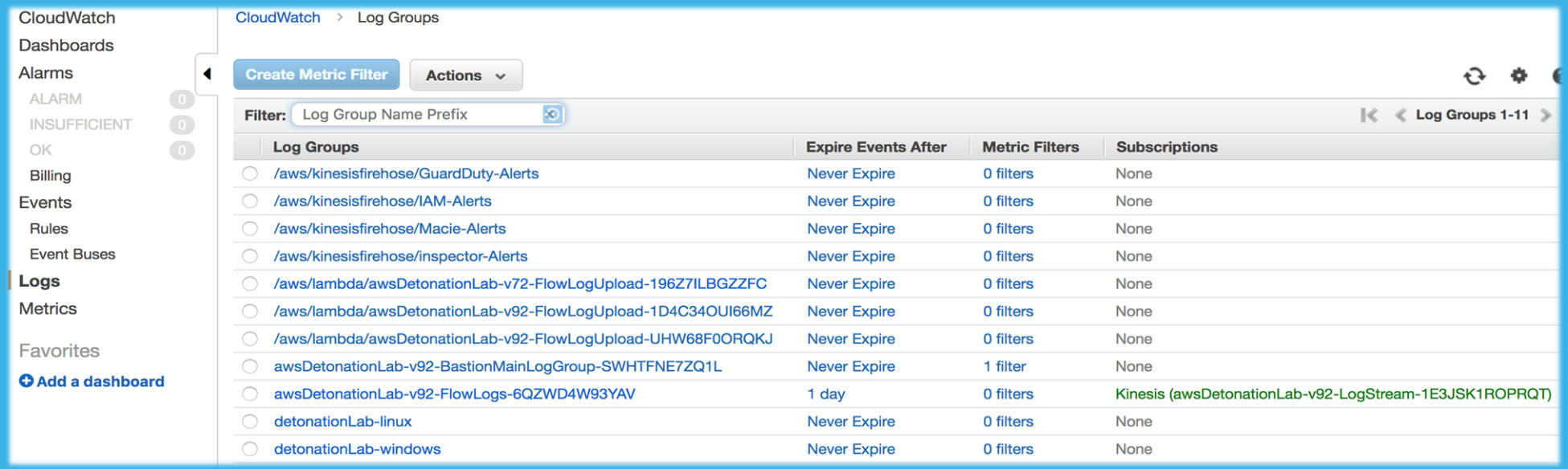
Inspector



Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

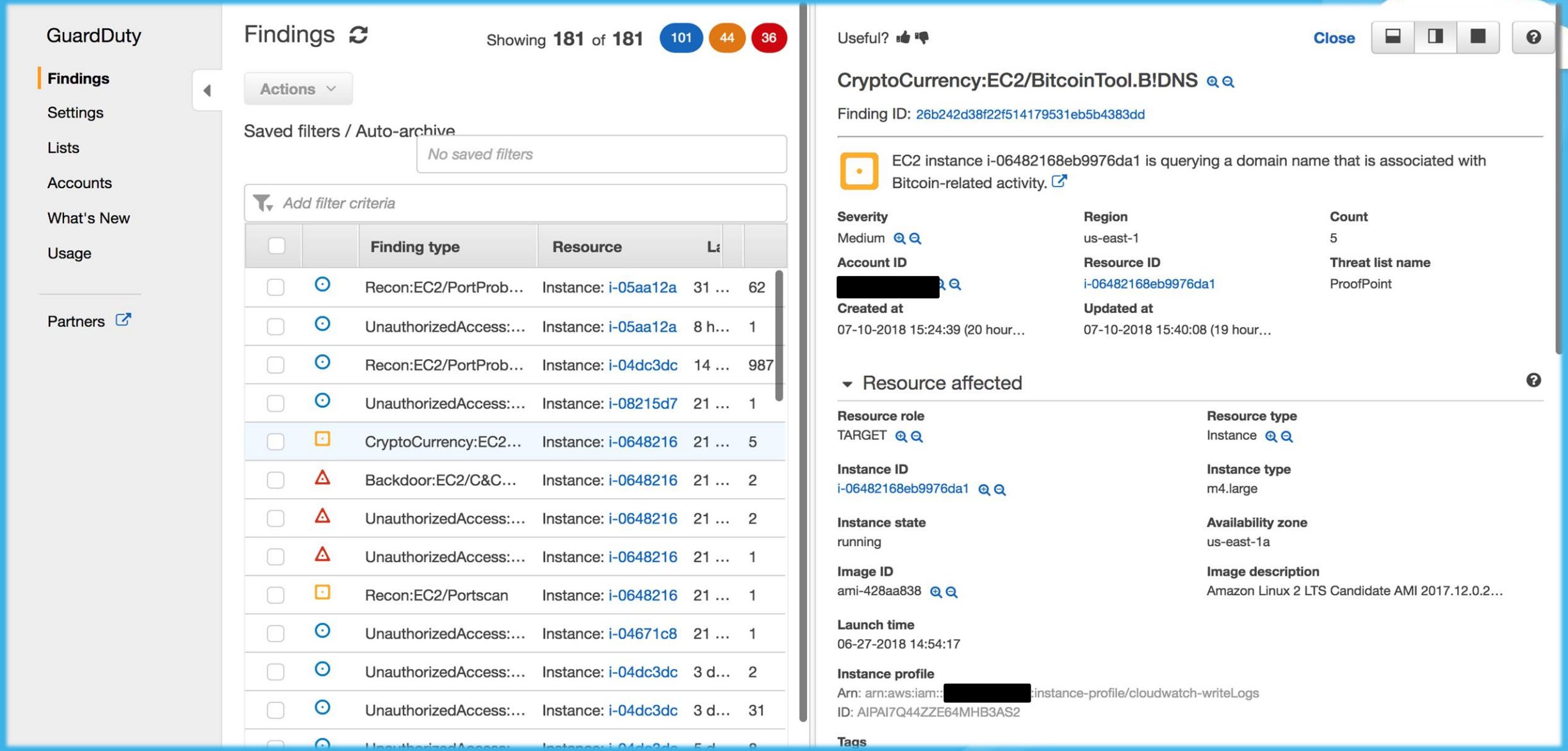
CloudWatch Event Rules and Logs





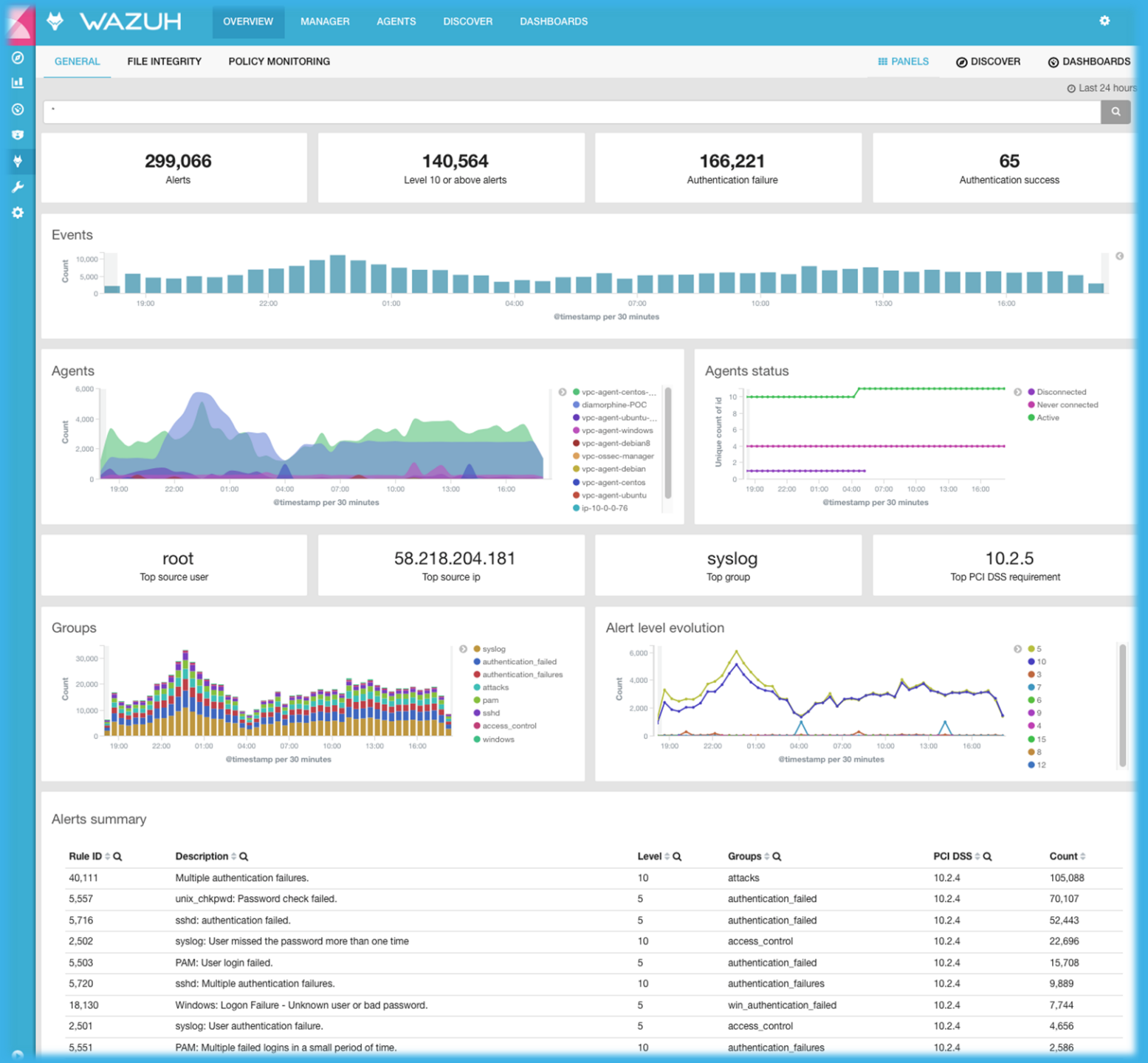
Amazon CloudWatch is a monitoring and management service built for developers, system operators, site reliability engineers (SRE), and IT managers.

GuardDuty

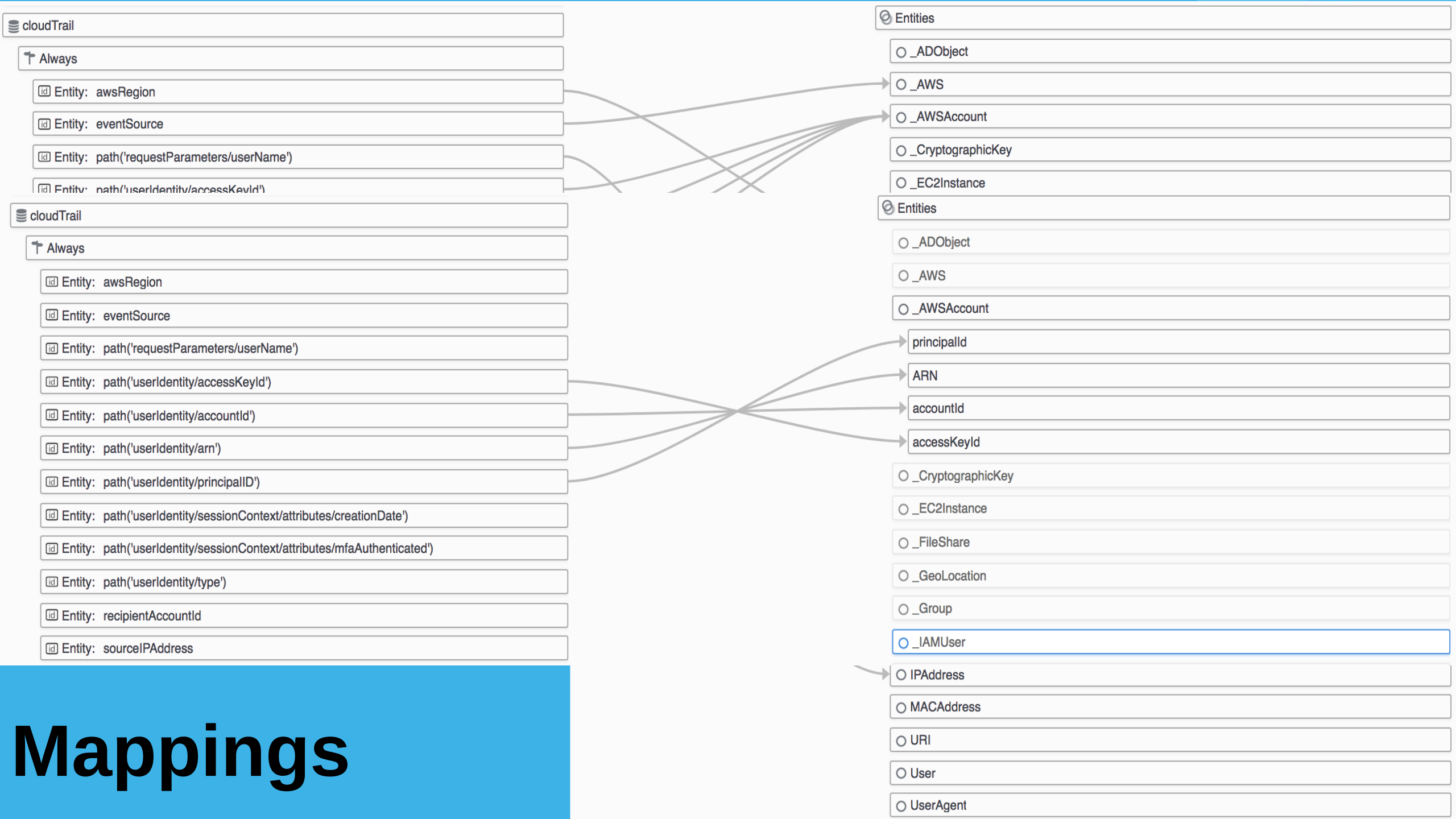


Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads.

Wazuh



Wazuh is a free, open-source host-based intrusion detection system (HIDS).


cloudTrail
Always
Entity: awsRegion
Entity: eventSource
Entity: path('requestParameters/userName')
Entity: path('userIdentity/accessKeyId')
cloudTrail
Always
Entity: awsRegion
Entity: eventSource
Entity: path('requestParameters/userName')
Entity: path('userIdentity/accessKeyId')
Entity: path('userIdentity/accountId')
Entity: path('userIdentity/arn')
Entity: path('userIdentity/principalID')
Entity: path('userIdentity/sessionContext/attributes/creationDate')
Entity: path('userIdentity/sessionContext/attributes/mfaAuthenticated')
Entity: path('userIdentity/type')
Entity: recipientAccountId
Entity: sourceIPAddress
Entities
_ADObject
_AWS
_AWSAccount
_CryptographicKey
_EC2Instance
Entities
_ADObject
_AWS
_AWSAccount
principalId
ARN
accountId
accessKeyId
_CryptographicKey
_EC2Instance
_FileShare
_GeoLocation
_Group
_IAMUser
IPAddress
MACAddress
URI
User
UserAgent

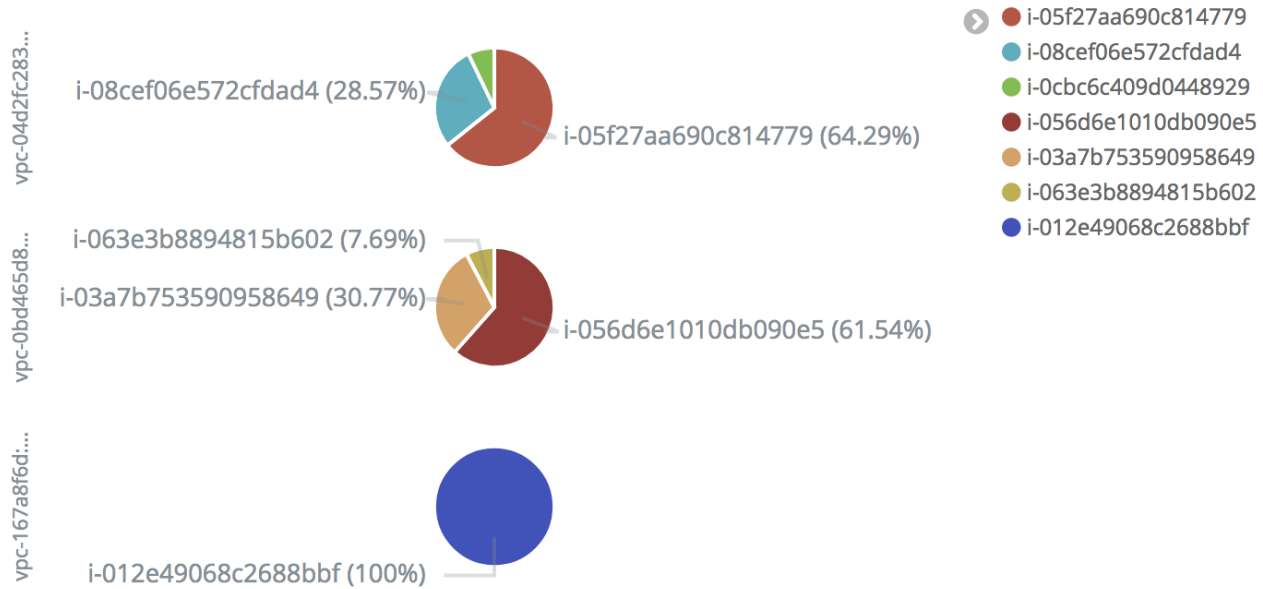
Mappings

Simple Dashboards

VPCFlow-Top10ExternalDestinationIP-Table

Top 10 External Destination IP	Count
54.239.31.225	4,406
54.239.25.71	4,282
54.239.25.60	4,150
54.239.30.177	2,478
54.239.30.195	2,465
45.127.112.2	1,709
54.239.29.61	1,469
66.241.101.63	477
209.141.60.238	291

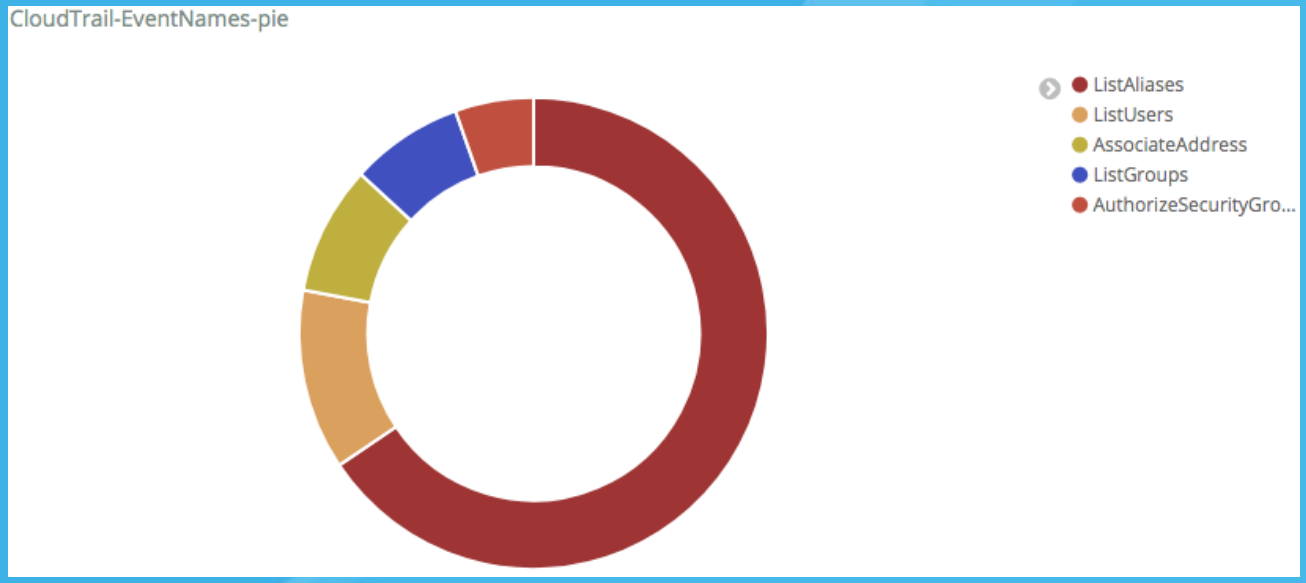
GuardDuty-BreakdownOfAlertsPerInstancePerVPC-Pie



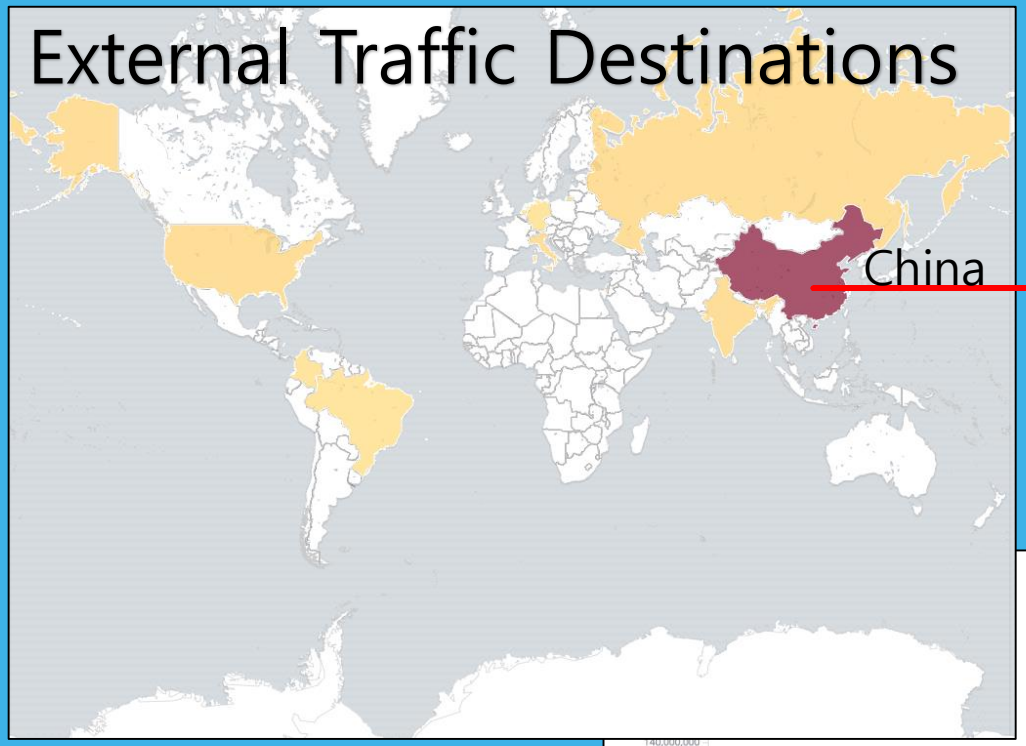
GuardDuty-MostCommonAccountID-Table

Account ID	Count
963894186934	40

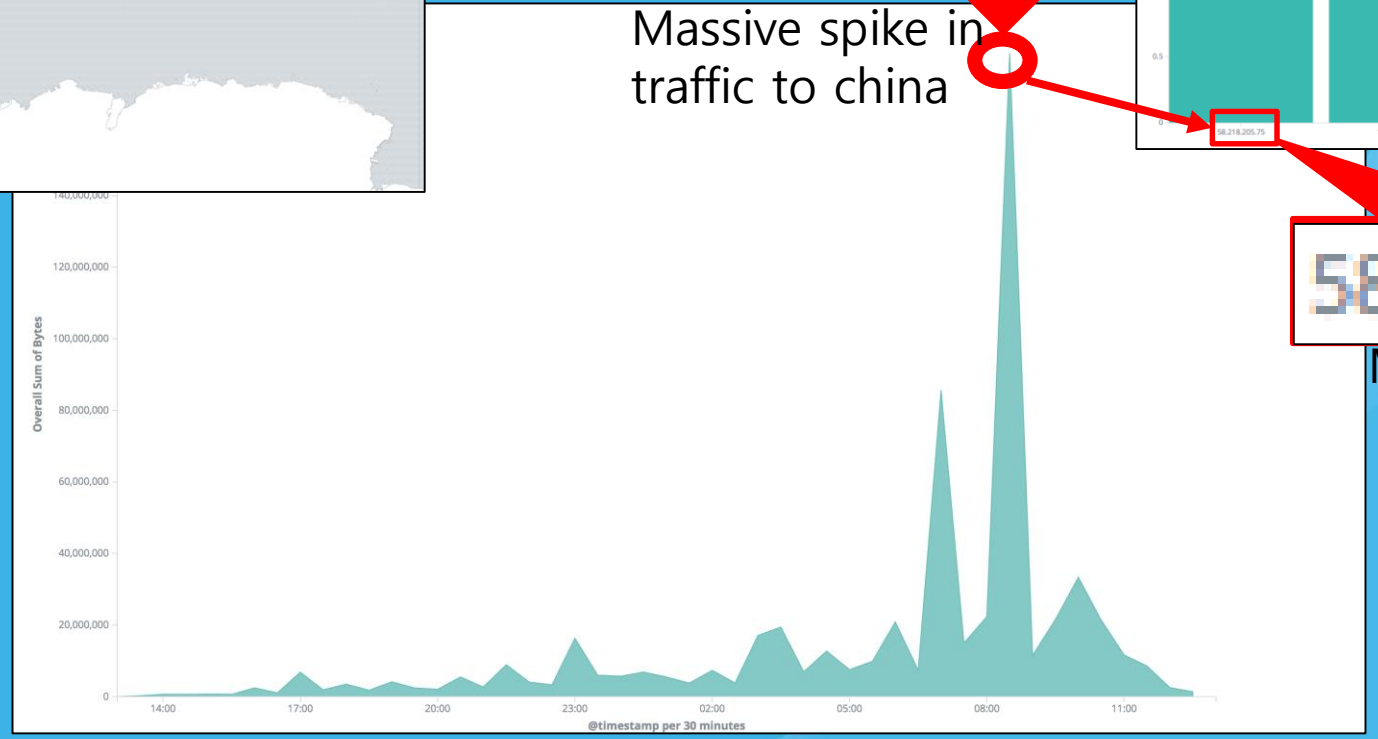
CloudTrail-EventNames-pie

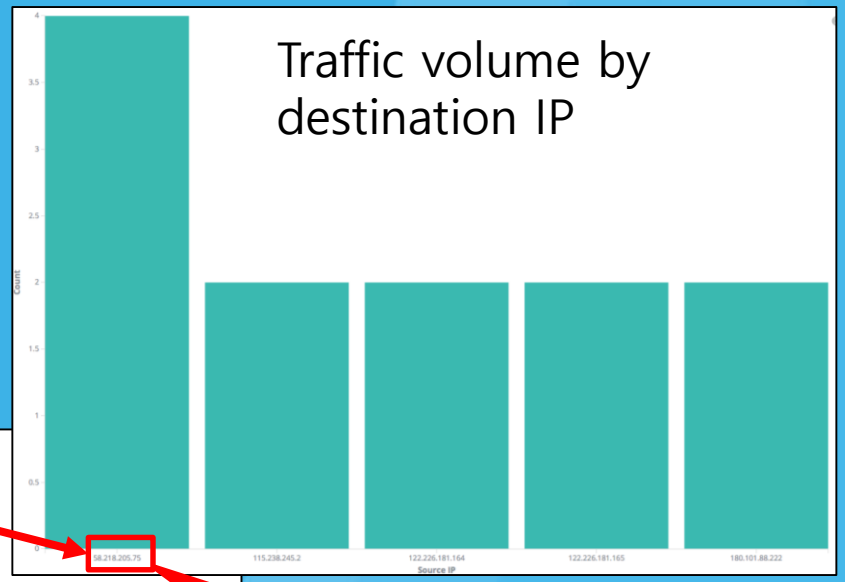


Finding what matters



Massive spike in traffic to china





58.218.205.75

Most common destination

Finding what matters

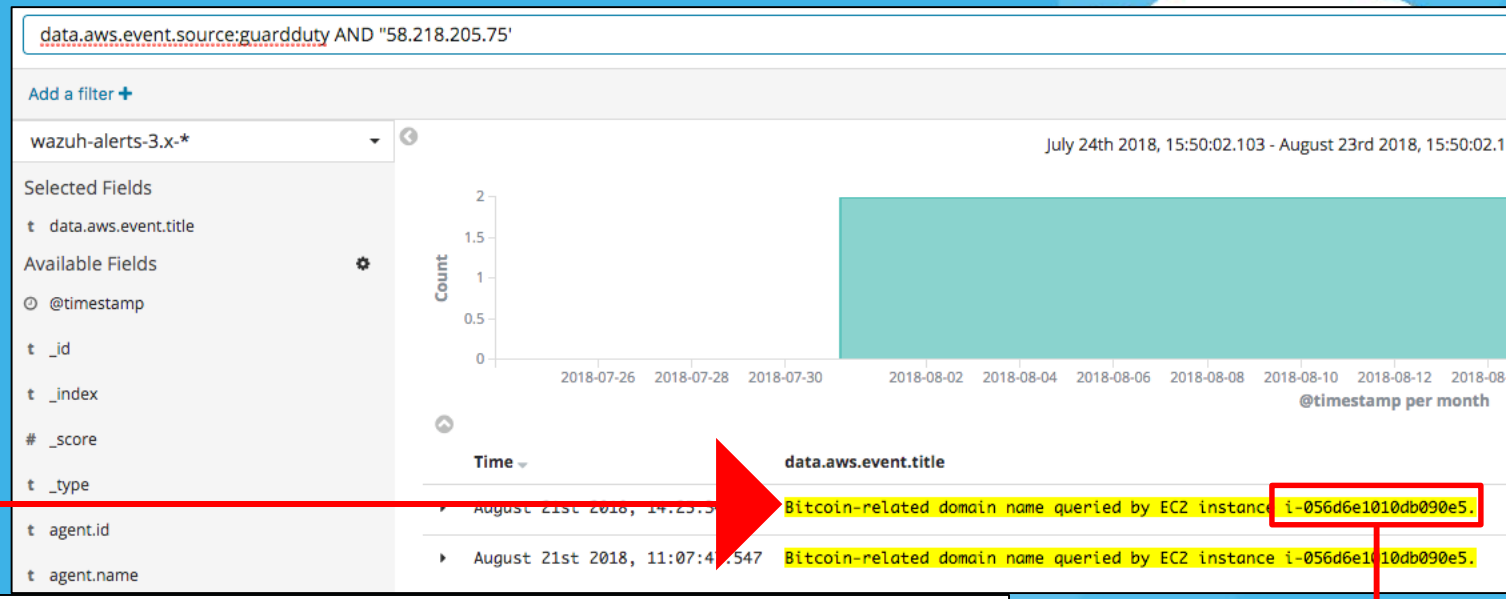
58.218.205.75

Most common destination

loggingSourcesFor-58.218.205.75

AWS Logging Sources
vpc
guardduty

Logs with Destination



Ec2 Instance involved

Time	data.aws.event.title	rule.groups	rule.description	predecoder.hostname
August 21st 2018, 14:25:34	i-056d6e1010db090e5 is performing RDP brute force attacks against 172.16.0.23.	amazon	Guard Duty Finding with a high level: i-056d6e1010db090e5 is performing RDP brute force attacks against 172.16.0.23. Brute force attacks are used to gain unauthorized access to your instance by guessing the RDP password.	ip-172-16-0-21
August 21st 2018, 14:25:34.589	Bitcoin-related domain name queried by EC2 instance i-056d6e1010db090e5.	amazon	Guard Duty Finding with a medium level: EC2 instance i-056d6e1010db090e5 is querying a domain name that is associated with Bitcoin-related activity.	ip-172-16-0-21
August 21st 2018, 14:25:34.589	Command and Control server domain name queried by EC2 instance i-056d6e1010db090e5.	amazon	Guard Duty Finding with a high level: EC2 instance i-056d6e1010db090e5 is querying a domain name associated with a known Command & Control server.	ip-172-16-0-21
August 21st 2018, 11:07:47.547	Bitcoin-related domain name queried by EC2 instance i-056d6e1010db090e5.	amazon	Guard Duty Finding with a medium level: EC2 instance i-056d6e1010db090e5 is querying a domain name that is associated with Bitcoin-related activity.	ip-172-16-0-21
August 21st 2018, 10:57:48.155	Command and Control server domain name queried by EC2 instance i-056d6e1010db090e5.	amazon	Guard Duty Finding with a high level: EC2 instance i-056d6e1010db090e5 is querying a domain name associated with a known Command & Control server.	ip-172-16-0-21
August 21st 2018, 09:27:43.800	i-056d6e1010db090e5 is performing RDP brute force attacks against 172.16.0.23.	amazon	Guard Duty Finding with a high level: i-056d6e1010db090e5 is performing RDP brute force attacks against 172.16.0.23. Brute force attacks are used to gain unauthorized access to your instance by guessing the RDP password.	ip-172-16-0-21
August 21st 2018, 09:27:43.800	Outbound portscan from EC2 instance i-056d6e1010db090e5.	amazon	Guard Duty Finding with a medium level: EC2 instance i-056d6e1010db090e5 is performing outbound port scans against remote host 172.16.0.22.	ip-172-16-0-21
August 21st 2018, 09:27:43.790	i-056d6e1010db090e5 is performing SSH brute force attacks against 172.16.0.22.	amazon	Guard Duty Finding with a high level: i-056d6e1010db090e5 is performing SSH brute force attacks against 172.16.0.22. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.	ip-172-16-0-21

Hostname of findings

All Guardduty Findings for instance

Finding what matters

@timestamp		August 24th 2018, 16:16:44.349
_id		tZeUbWUB-pbw9wu1_DB9
_index		wazuh-alerts-3.x-2018.08.24
_score		-
_type		wazuh
agent.id		002
agent.ip		172.16.0.21
agent.name		linuxVictim2
decoder.name		ossec
full_log		ossec: output: 'netstat outbound connections': Active Internet connections (w/o servers) Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name tcp 0 1 172.16.0.21:38272 58.218.205.75:80 SYN_SENT 6621/pip3.7 tcp 54 0 172.16.0.21:44062 54.239.30.177:443 CLOSE_WAIT 3492/awsagent tcp 0 0 172.16.0.21:22 172.16.0.5:50146 ESTABLISHED 3545/sshd: ec2-user udp 0 0 172.16.0.21:50387 172.16.0.21:1514 ESTABLISHED 6597/ossec-agentd
id		1535141804.148908
location		netstat outbound connections
manager.name		ip-172-16-0-21.ec2.internal
path		/var/ossec/logs/alerts/alerts.json
previous_log		ossec: output: 'netstat outbound connections': Active Internet connections (w/o servers) Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name tcp 0 1 172.16.0.21:38272 58.218.205.75:80 SYN_SENT 6621/pip3.7 tcp 53 0 172.16.0.21:52698 54.239.30.195:443 ESTABLISHED 3492/awsagent tcp 0 0 172.16.0.21:22 172.16.0.5:50146 ESTABLISHED 3545/sshd: ec2-user udp 0 0 172.16.0.21:50387 172.16.0.21:1514 ESTABLISHED 6597/ossec-agentd
previous_output		ossec: output: 'netstat outbound connections': Active Internet connections (w/o servers) Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name tcp 0 1 172.16.0.21:38272 58.218.205.75:80 SYN_SENT 6621/pip3.7 tcp 53 0 172.16.0.21:52698 54.239.30.195:443 ESTABLISHED 3492/awsagent tcp 0 0 172.16.0.21:22 172.16.0.5:50146 ESTABLISHED 3545/sshd: ec2-user udp 0 0 172.16.0.21:50387 172.16.0.21:1514 ESTABLISHED 6597/ossec-agentd
rule.description		Listened ports status (netstat nputw) changed (new port opened or closed).
rule.firedtimes		9
rule.gdpr		IV_35.7.d
rule.gpg13		10.1
rule.groups		local, syslog, sshd
rule.id		100002
rule.level		7
rule.mail		false
rule.pci_dss		10.2.7, 10.6.1

Most common destination

58.218.205.75

File added to the system.

August 20th 2018, 16:06:59.483 - ossec, syscheck — File added to the system.

@timestamp		August 20th 2018, 16:06:59.483
_id		cDvyWGUBy4A8_JfJnR4Z
_index		wazuh-alerts-3.x-2018.08.20
_score		-
_type		wazuh
agent.id		000
agent.name		ip-172-16-0-21.ec2.internal
decoder.name		syscheck_integrity_changed
full_log		New file '/bin/pip3.7' added to the file system.
id		1534795619.119545
location		syscheck
manager.name		ip-172-16-0-21.ec2.internal
path		/var/ossec/logs/alerts/alerts.json
predecoder.hostname		ip-172-16-0-21
rule.gdpr		II_5.1.f
rule.gpg13		4.11
rule.groups		ossec, syscheck
rule.id		554
rule.level		5
rule.mail		false
rule.pci_dss		11.5
syscheck.event		added
syscheck.gid_after		0
syscheck.gname_after		root
syscheck.inode_after		13311903
syscheck.md5_after		fb7791757901a24800f67f0f950b281d
syscheck.mtime_after		May 2nd 2018, 13:40:47.000
syscheck.path		/bin/pip3.7
syscheck.perm_after		100755
syscheck.sha1_after		4f7c79d247490ce12b159b1cef9832e6[illegible]9513b9
syscheck.sha256_after		1e2f03917015b52c71432ffd382e0ee970d551eebf9457b2498b1434ce8ab466
syscheck.size_after		206
syscheck.uid_after		0
syscheck.uname_after		root

New file '/bin/pip3.7' added to the file system.

File responsible for outbound connection

VT Results

EXE

53 / 68

53 engines detected this file

SHA-256	1e2f03917015b52c71432ffd382e0ee970d551eebf9457b2498b1434ce8ab466
File name	fb7791757901a24800f67f0f950b[illegible]d.virus
File size	1.57 MB
Last analysis	2018-06-18 23:34:18 UTC
Community score	-57

How did they get in?

Severity	Date	Finding	Target	Template	Rules Package
High	Yesterday at…	Instance i-063e3b8894815b602 is vulnerable to C…	everything	everything	Common Vulnerabilities and Exposures-1.1

Finding for assessment target 'everything' and template 'everything'

ARN arn:aws:inspector:us-east-1:963894186934:target/0-ITOJiioL/template/0-S7AjH5cj/run/0-JGN1eNRF/finding/0-jkRXhbLT

Run name 5f44c7fb-3421-133f-1833-5ef4328e05a6_885e45c5-3f8a-9b6d-d70f-194994c58260

Target name everything

Template name everything

Start Yesterday at 10:55 PM (GMT-4) (12 hours ago)

End Yesterday at 11:56 PM (GMT-4) (11 hours ago)

Status Analysis complete

Rules package Common Vulnerabilities and Exposures-1.1

AWS agent ID i-063e3b8894815b602

Finding Instance i-063e3b8894815b602 is vulnerable to CVE-2018-10897

Severity High

Description A directory traversal issue was found in reposync, a part of yum-utils, where reposync fails to sanitize paths in remote repository configuration files. If an attacker controls a repository, they may be able to copy files outside of the destination directory on the targeted system via path traversal. If reposync is running with heightened privileges on a targeted system, this flaw could potentially result in system compromise via the overwriting of critical system files. Version 1.1.31 and older are believed to be affected.

Recommendation Use your Operating System's update feature to update package yum-plugin-priorities-0:1.1.31-45.amzn2.0.1, yum-utils-0:1.1.31-45.amzn2.0.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10897

Show Details

Recap

Traditional Tool	AWS equivalent
IDS/IPS	guardDuty
DLP	Macie
EDR	Cloudwatch + osquery, GRR
Netflow	Cloudwatch + VPCFlow
DNS	Cloudwatch + Route53
Access and authentication a uditing	CloudTrail
Active Directory	Directory Service
Identity Management	IAM
Single Sign On	AWS SSO
Vulnerability scanner	Inspector
Configuration Management	AWS config
Logging	Cloudwatch + Firehose + La mbda

Personal

Attacker Life cycle

Flag it, Tag it, and Bag it.