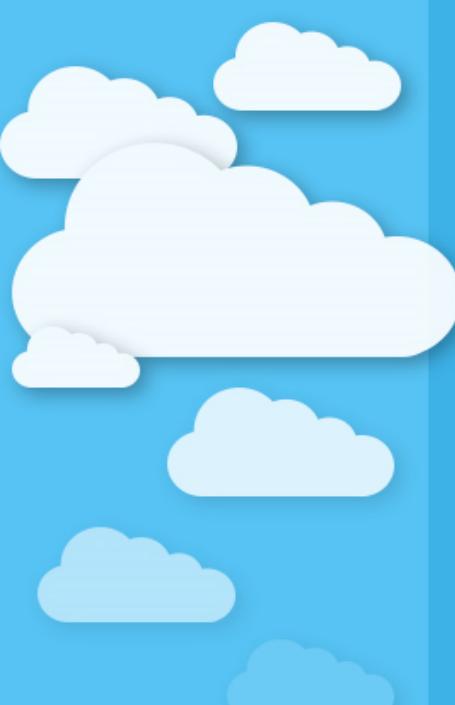


Who done it: Gaining visibility and accountability in the cloud

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 clouformation

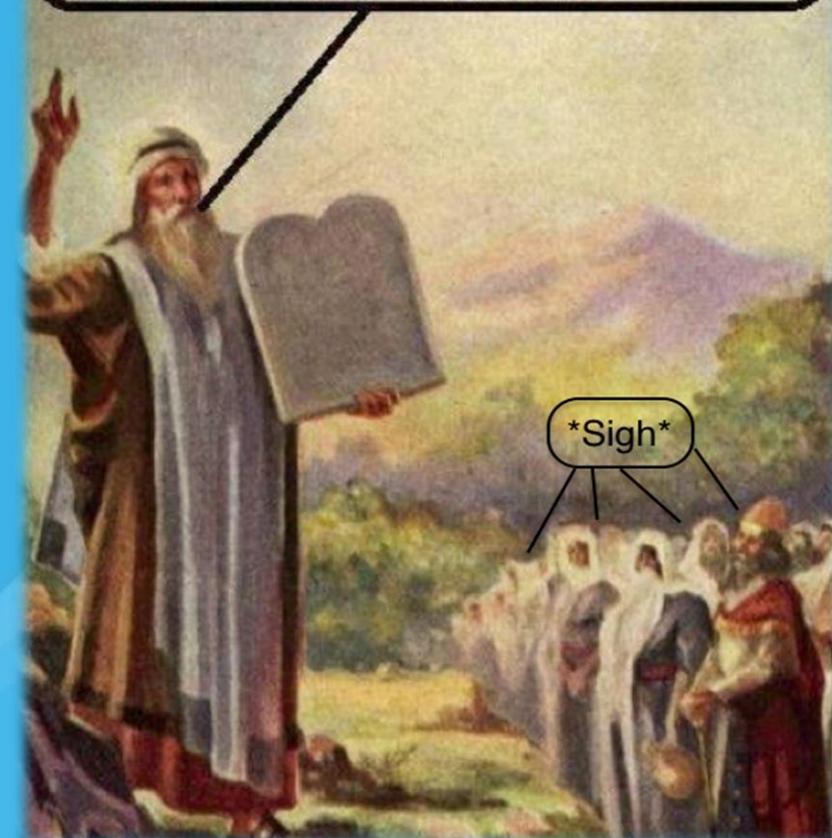
- <https://github.com/sonofagl1tch/AWSDetonationLab>

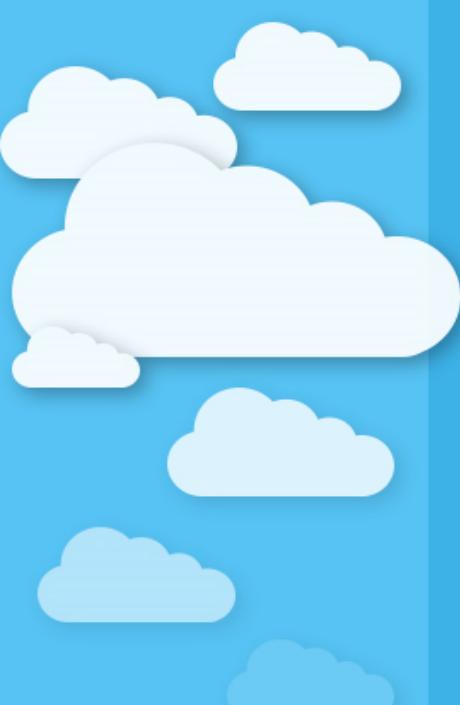


Agenda

- 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

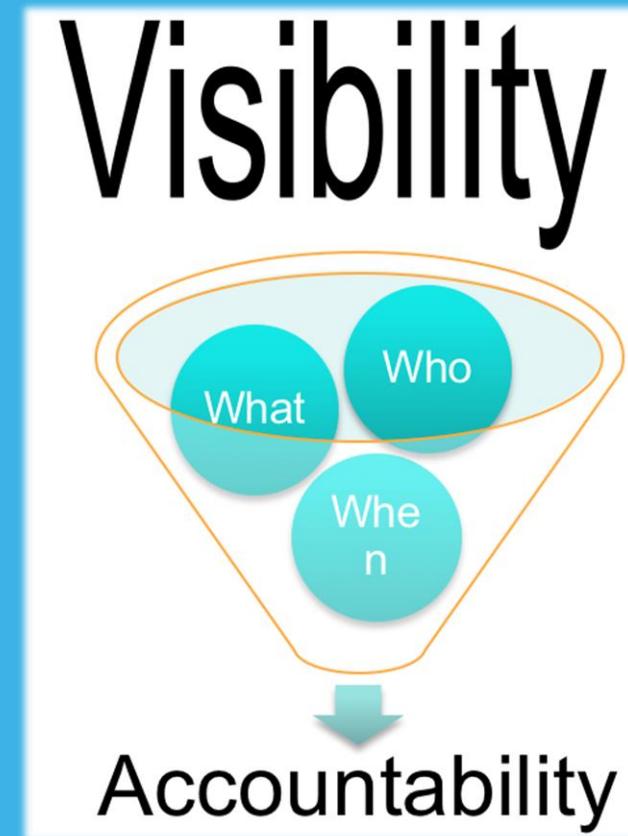
I downloaded these
onto my tablet
from the cloud





Who did what and when

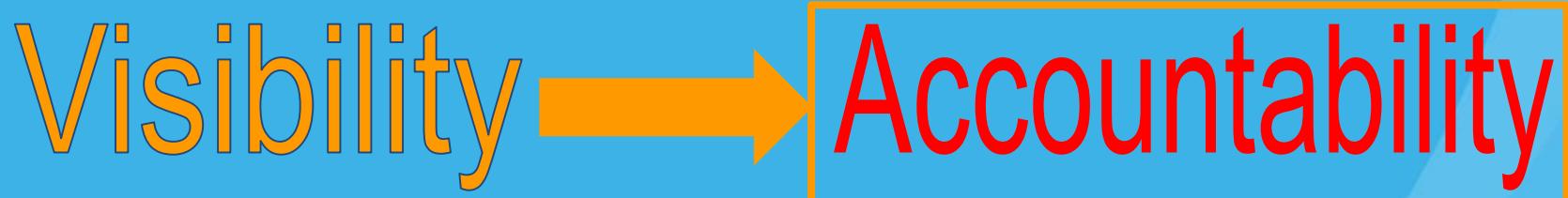
- These are the 3 pillars of each stage of scoping the event
- Will be modified for each iteration
- The analysts should be able to start at any of the stages and complete the cycle



Common Techniques

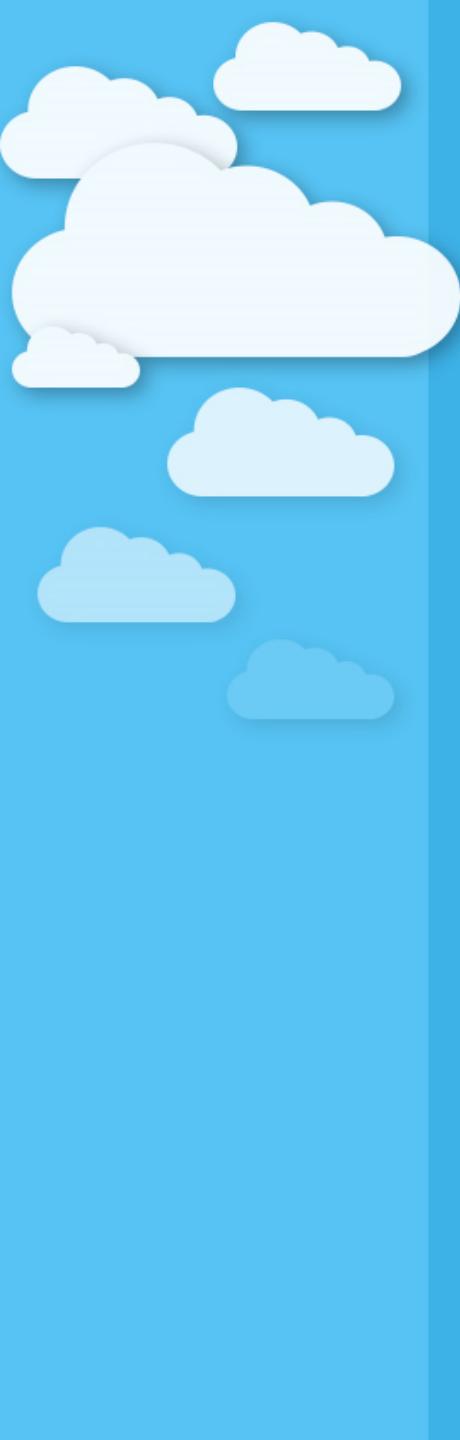
What's Their Goal?

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



Who What When





Common Visibility Tools and Their AWS Equivalent

<u>Traditional Tool</u>	<u>AWS equivalent</u>
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.

<u>OS hardening</u>	<u>Logging</u>	<u>Authentication</u>	<u>Endpoint</u>	<u>Network</u>	<u>Vulnerabilities/Configuration</u>
<ul style="list-style-type: none">CIS guidelines audit and hardening scripts.Additional logging and hardening scripts created by experience over time.	<ul style="list-style-type: none">Common logging like auth logs and process creation etc	<ul style="list-style-type: none">/var/log/secureIAM logsIAM rolesIAM policies	<ul style="list-style-type: none">EDRHIDSCloudwatchGuardDuty	<ul style="list-style-type: none">IDSNetstatTcpdumpVpc flow logsDns route 53 logs	<ul style="list-style-type: none">Generic vuln scannerInspectorNVD/CVE usageAws configOS hardeningApplications 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



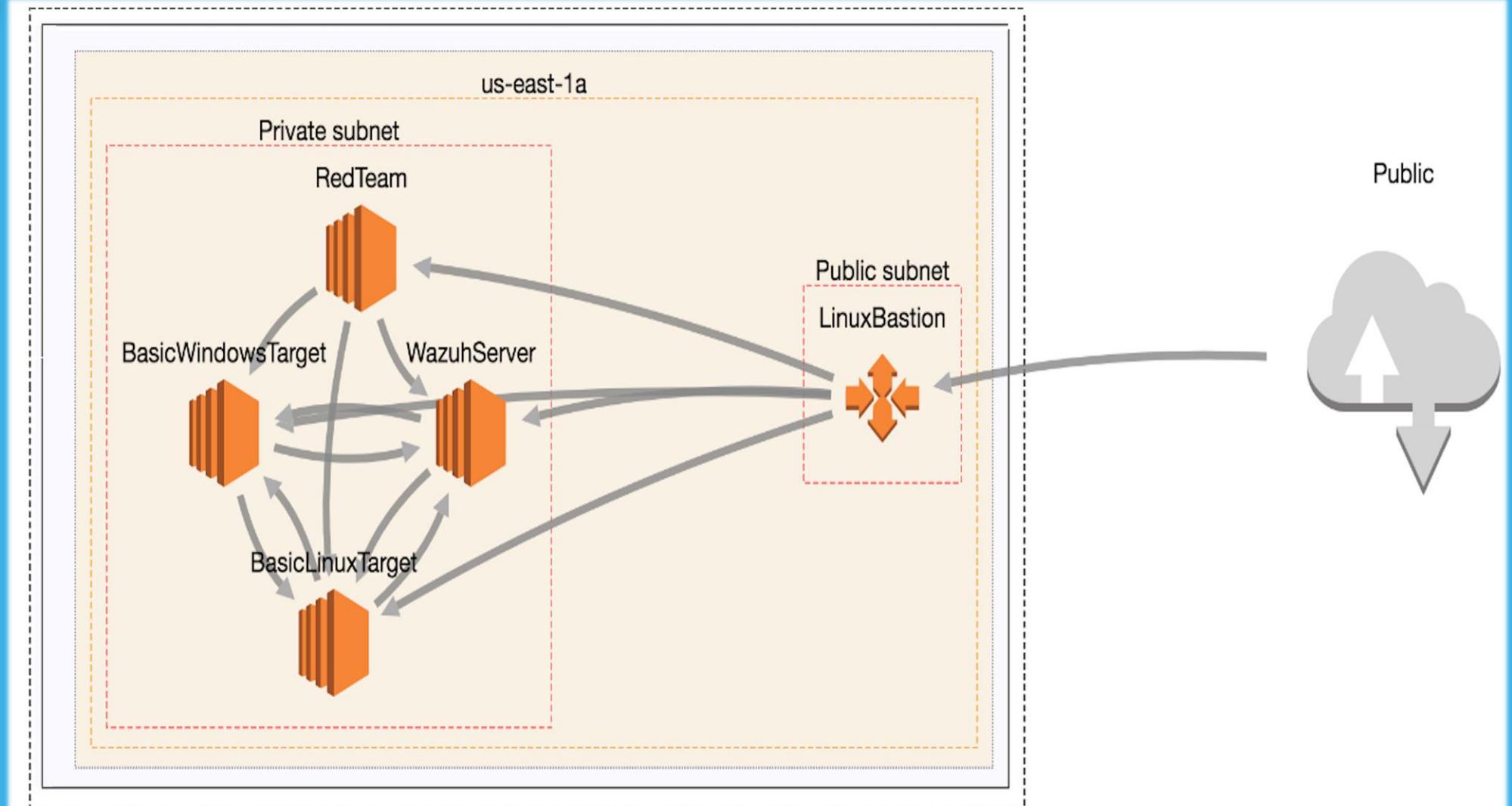
SecOps remains
vigilant



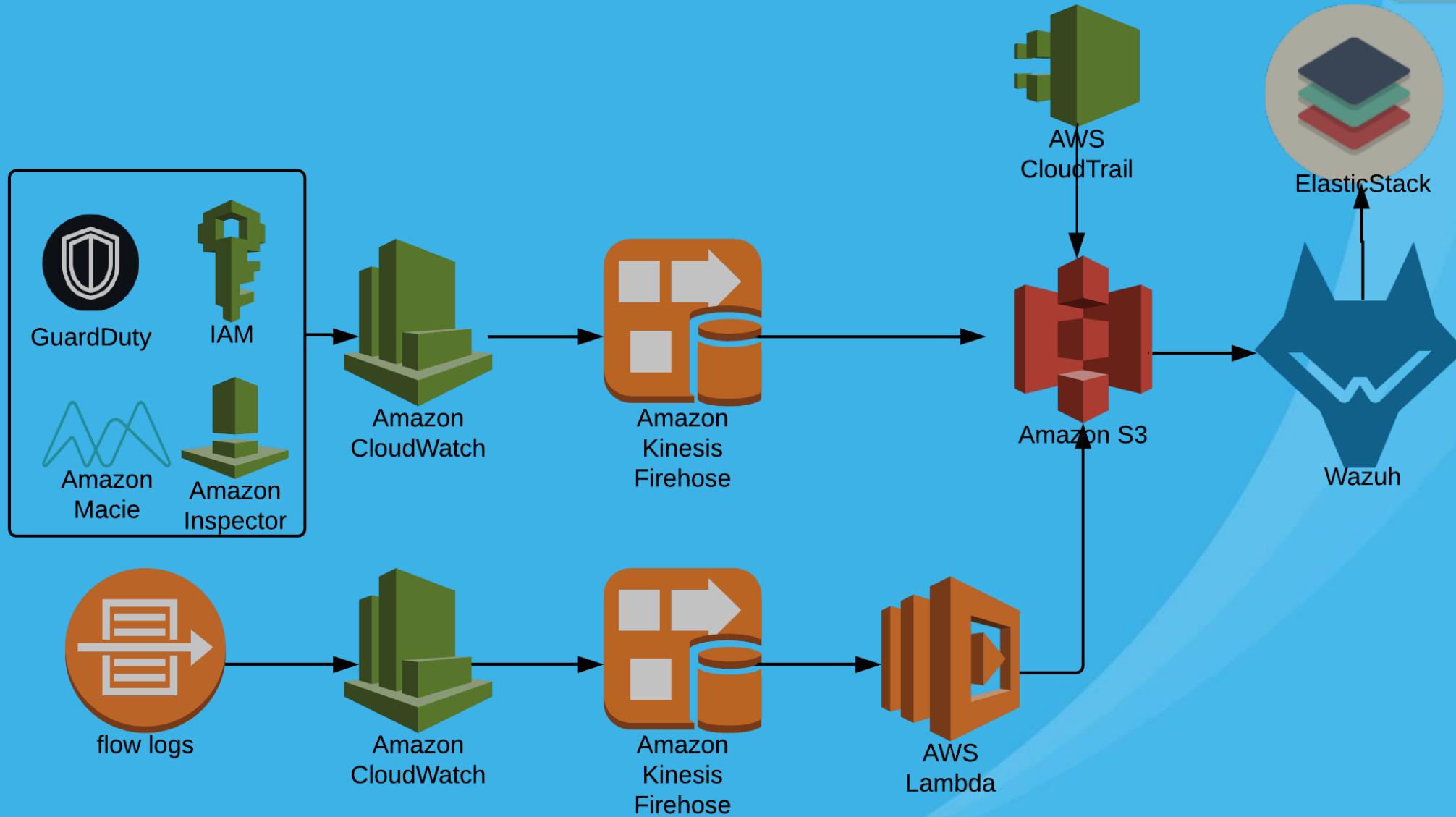
SecOps Defends



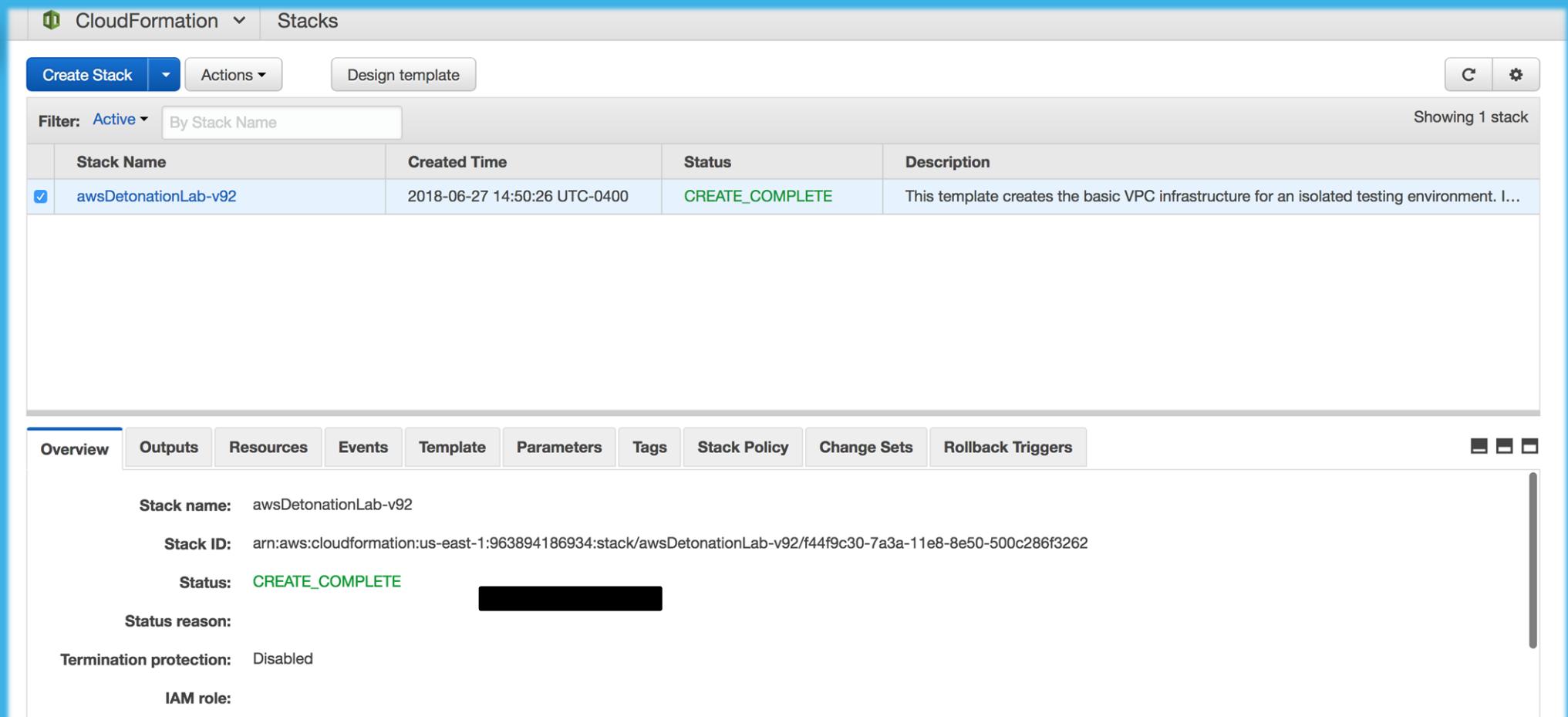
Detonation Lab Topology



Pipelines



CloudFormation



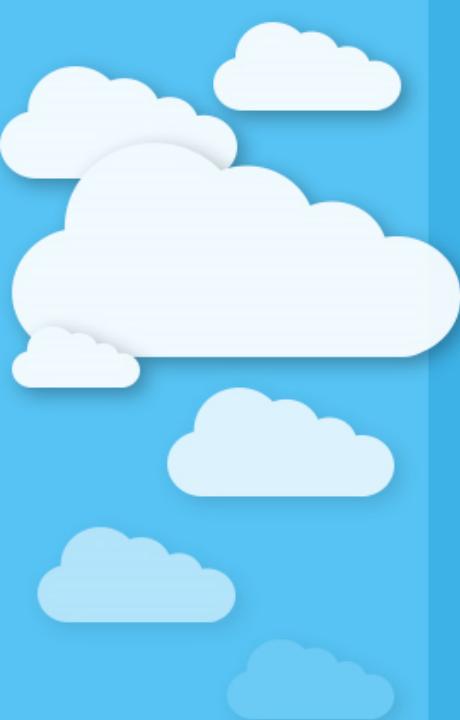
The screenshot shows the AWS CloudFormation console interface. At the top, there's a navigation bar with 'CloudFormation' and 'Stacks'. Below it is a toolbar with 'Create Stack', 'Actions', and 'Design template' buttons. A filter dropdown set to 'Active' and a search bar for 'By Stack Name' are also present. On the right, a gear icon and a settings gear icon are visible.

The main area displays a table titled 'Showing 1 stack'. The table has columns for 'Stack Name', 'Created Time', 'Status', and 'Description'. One row is shown, corresponding to the stack 'awsDetonationLab-v92' created on '2018-06-27 14:50:26 UTC-0400' with a 'CREATE_COMPLETE' status. The description indicates it creates basic VPC infrastructure for a testing environment.

Below the table, a navigation bar includes tabs for 'Overview' (which is selected), 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', 'Stack Policy', 'Change Sets', and 'Rollback Triggers'. The 'Overview' tab displays detailed information about the stack:

- Stack name: awsDetonationLab-v92
- Stack ID: arn:aws:cloudformation:us-east-1:963894186934:stack/awsDetonationLab-v92/f44f9c30-7a3a-11e8-8e50-500c286f3262
- Status: CREATE_COMPLETE
- Status reason: [REDACTED]
- Termination protection: Disabled
- IAM role: [REDACTED]

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.

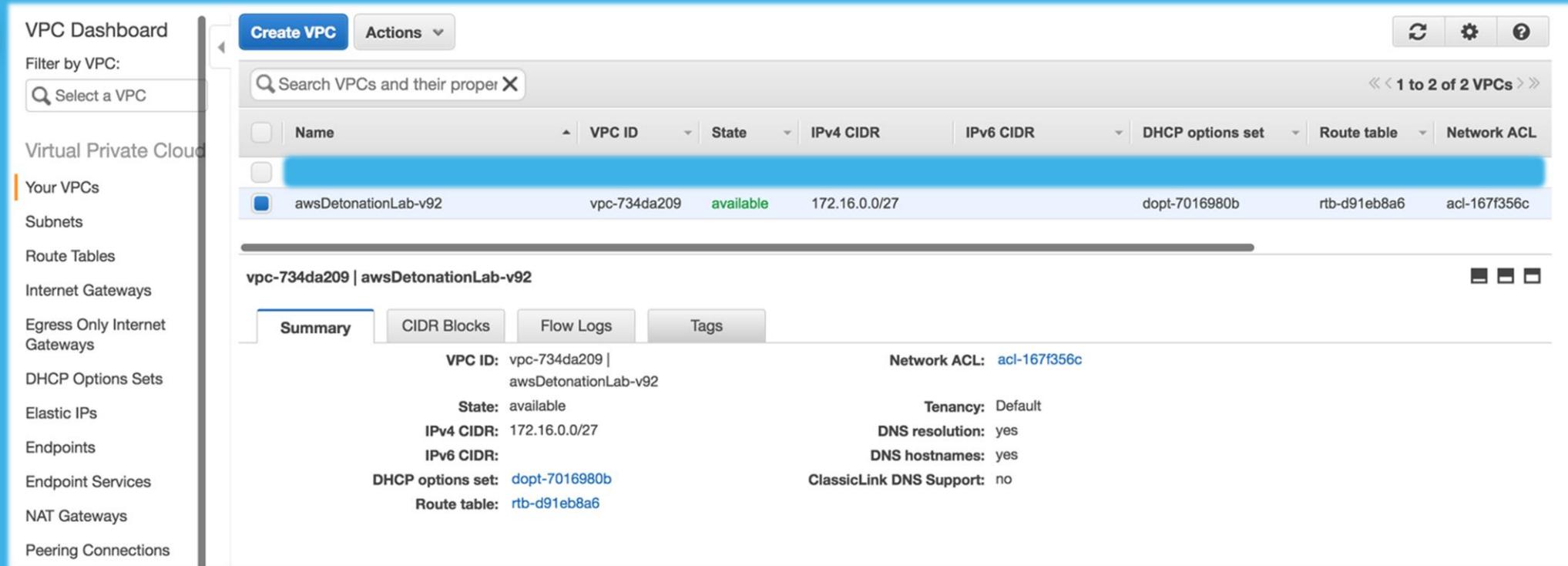


S3

Search for buckets			
	+ Create bucket	Delete bucket	Empty bucket
 awsdetonationlab-v92-s3bucketcloudtrail-v9d4yqs8ytsh	Not public *	US East (N. Virginia)	Jun 27, 2018 2:50:33 PM GMT-0400
 awsdetonationlab-v92-s3bucketguardduty-jkremr5l7ijb	Not public *	US East (N. Virginia)	Jun 27, 2018 2:50:33 PM GMT-0400
 awsdetonationlab-v92-s3bucketiam-1y00gbul8vi82	Not public *	US East (N. Virginia)	Jun 27, 2018 2:50:32 PM GMT-0400
 awsdetonationlab-v92-s3bucketinspector-1xz05by24ypuk	Not public *	US East (N. Virginia)	Jun 27, 2018 2:50:32 PM GMT-0400
 <u>awsdetonationlab-v92-s3bucketmacie-1tv3blodhx6fl</u>	Not public *	US East (N. Virginia)	Jun 27, 2018 2:50:33 PM GMT-0400
 awsdetonationlab-v92-s3bucketvpcflow-167orji11dqu1	Not public *	US East (N. Virginia)	Jun 27, 2018 2:50:32 PM GMT-0400

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

VPC

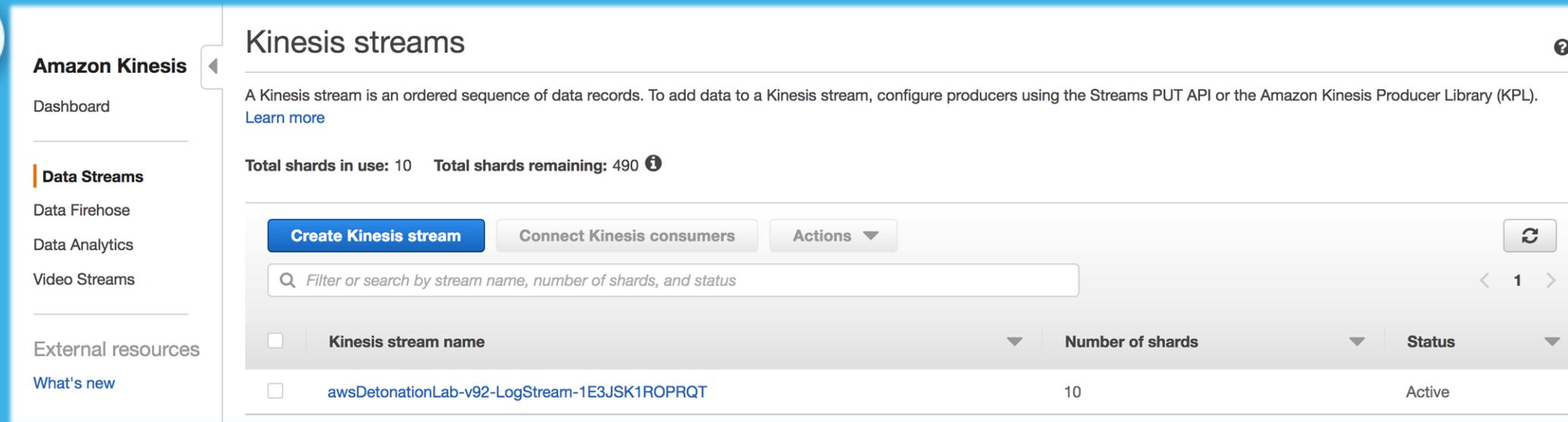


The screenshot shows the AWS VPC Dashboard. On the left, there's a sidebar with navigation links: VPC Dashboard, Filter by VPC (with a 'Select a VPC' dropdown), Virtual Private Cloud, Your VPCs (which is selected and highlighted in orange), Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, and Peering Connections. At the top right, there are buttons for 'Create VPC', 'Actions', and icons for refresh, settings, and help. Below the sidebar is a search bar labeled 'Search VPCs and their properties'. The main content area displays a table of VPCs. The first row of the table has a blue header with columns: Name, VPC ID, State, IPv4 CIDR, IPv6 CIDR, DHCP options set, Route table, and Network ACL. The second row shows a single VPC entry: 'awsDetonationLab-v92' (VPC ID: 'vpc-734da209', State: 'available', IPv4 CIDR: '172.16.0.0/27', DHCP options set: 'dopt-7016980b', Route table: 'rtb-d91eb8a6', Network ACL: 'acl-167f356c'). Below this table is a summary card for 'vpc-734da209 | awsDetonationLab-v92'. It contains tabs for 'Summary' (which is selected), 'CIDR Blocks', 'Flow Logs', and 'Tags'. The 'Summary' tab displays various configuration details:

Setting	Value
VPC ID	vpc-734da209 awsDetonationLab-v92
State	available
IPv4 CIDR	172.16.0.0/27
IPv6 CIDR	
DHCP options set	dopt-7016980b
Route table	rtb-d91eb8a6
Network ACL	acl-167f356c
Tenancy	Default
DNS resolution	yes
DNS hostnames	yes
ClassicLink DNS Support	no

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

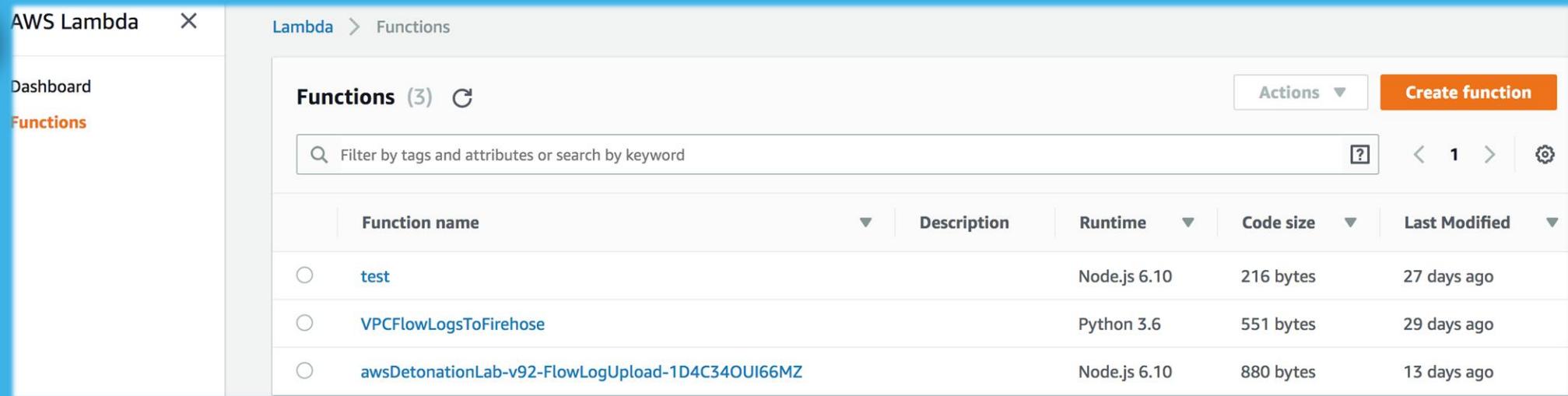


The screenshot shows the Amazon Kinesis Data Streams interface. On the left, a sidebar menu includes 'Dashboard', 'Data Streams' (which is selected and highlighted in orange), 'Data Firehose', 'Data Analytics', and 'Video Streams'. Below that is 'External resources' and 'What's new'. The main content area is titled 'Kinesis streams' and contains a brief description: 'A Kinesis stream is an ordered sequence of data records. To add data to a Kinesis stream, configure producers using the Streams PUT API or the Amazon Kinesis Producer Library (KPL). [Learn more](#)'. It displays statistics: 'Total shards in use: 10' and 'Total shards remaining: 490'. Below this are three buttons: 'Create Kinesis stream', 'Connect Kinesis consumers', and 'Actions'. A search bar allows filtering by 'stream name, number of shards, and status'. A table lists existing streams. The first stream listed is 'awsDetonationLab-v92-LogStream-1E3JSK1ROPRQT', which has 10 shards and is in an 'Active' status.

Kinesis stream name	Number of shards	Status
awsDetonationLab-v92-LogStream-1E3JSK1ROPRQT	10	Active

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

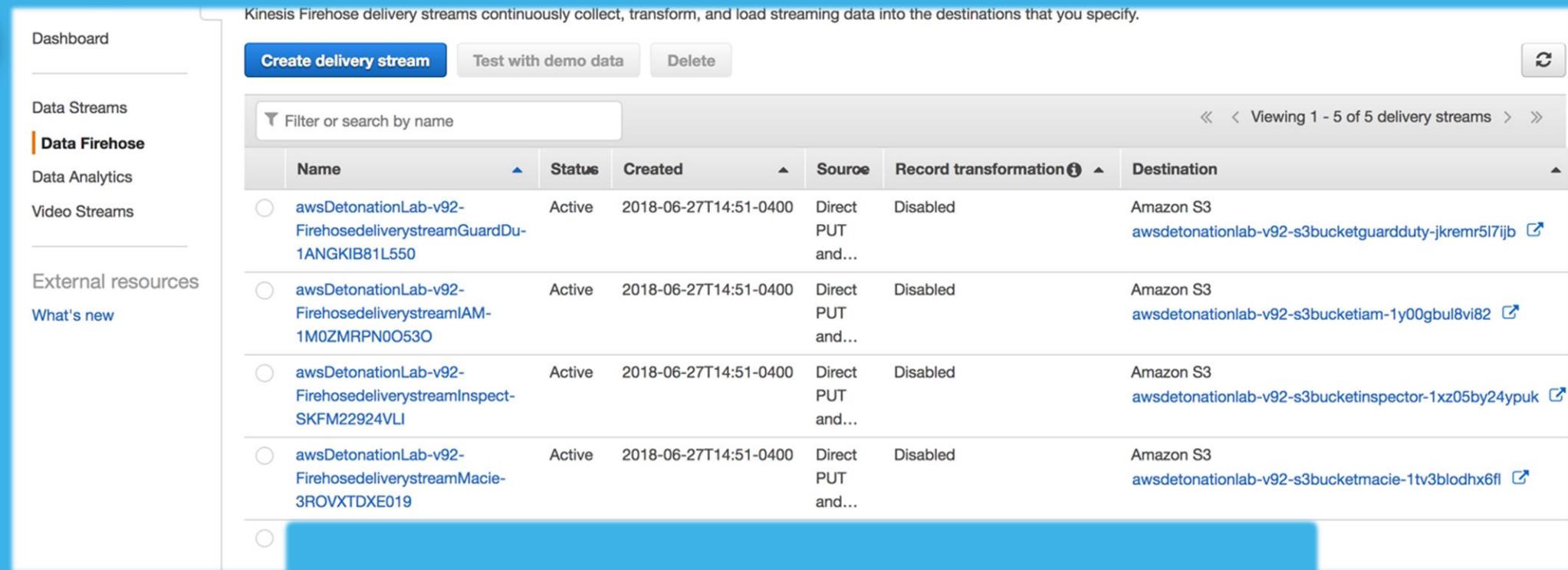


The screenshot shows the AWS Lambda Functions page. The left sidebar has 'Dashboard' and 'Functions' selected. The main area shows a table with three rows:

Function name	Description	Runtime	Code size	Last Modified
test		Node.js 6.10	216 bytes	27 days ago
VPCFlowLogsToFirehose		Python 3.6	551 bytes	29 days ago
awsDetonationLab-v92-FlowLogUpload-1D4C34OUI66MZ		Node.js 6.10	880 bytes	13 days ago

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

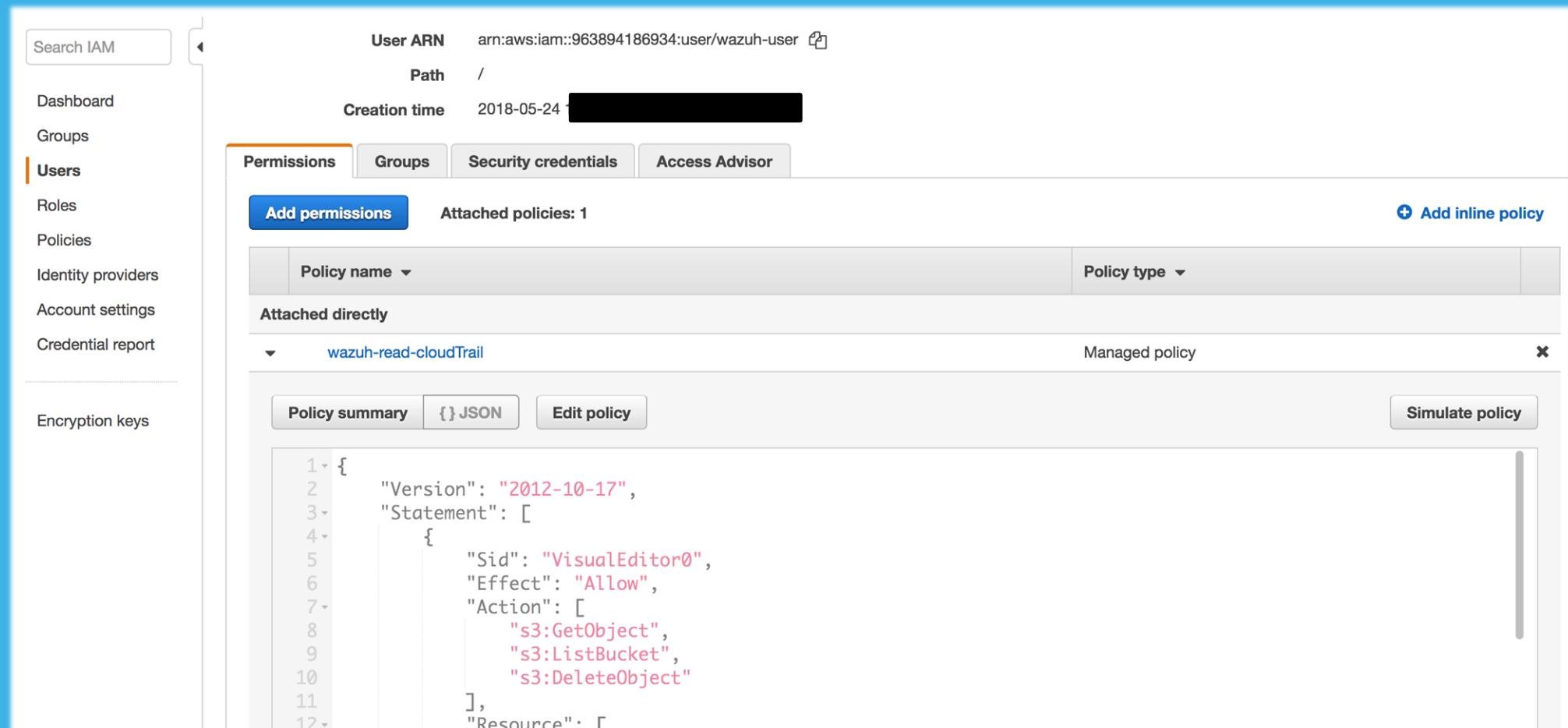


The screenshot shows the Amazon Kinesis Data Firehose console. On the left, a sidebar menu includes 'Dashboard', 'Data Streams' (selected), 'Data Analytics', 'Video Streams', 'External resources', and 'What's new'. The main area displays a table of delivery streams. At the top of the table are buttons for 'Create delivery stream', 'Test with demo data', and 'Delete'. A search bar labeled 'Filter or search by name' is present. The table has columns for Name, Status, Created, Source, Record transformation, and Destination. Five delivery streams are listed:

Name	Status	Created	Source	Record transformation	Destination
awsDetonationLab-v92-FirehosedeliverystreamGuardDuty-1ANGKIB81L550	Active	2018-06-27T14:51-0400	Direct PUT and...	Disabled	Amazon S3 awsdetonationlab-v92-s3bucketguardduty-jkremr5l7ijb
awsDetonationLab-v92-FirehosedeliverystreamIAM-1M0ZMRPN0O53O	Active	2018-06-27T14:51-0400	Direct PUT and...	Disabled	Amazon S3 awsdetonationlab-v92-s3bucketiam-1y00gbul8vi82
awsDetonationLab-v92-FirehosedeliverystreamInspect-SKFM22924VLI	Active	2018-06-27T14:51-0400	Direct PUT and...	Disabled	Amazon S3 awsdetonationlab-v92-s3bucketinspector-1xz05by24ypuk
awsDetonationLab-v92-FirehosedeliverystreamMacie-3ROVXTDXE019	Active	2018-06-27T14:51-0400	Direct PUT and...	Disabled	Amazon S3 awsdetonationlab-v92-s3bucketmacie-1tv3blodhx6fl

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

IAM



The screenshot shows the AWS IAM User Management interface. On the left, a sidebar lists navigation options: Search IAM, Dashboard, Groups, **Users** (selected), Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area displays user details for 'wazuh-user': User ARN (arn:aws:iam::963894186934:user/wazuh-user), Path (/), and Creation time (2018-05-24). Below these are tabs for Permissions, Groups, Security credentials, and Access Advisor, with 'Permissions' selected. A 'Add permissions' button is available. Under 'Attached policies: 1', the policy 'wazuh-read-cloudTrail' is listed as a Managed policy. The 'Policy summary' tab shows the JSON code:

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Sid": "VisualEditor0",  
6             "Effect": "Allow",  
7             "Action": [  
8                 "s3:GetObject",  
9                 "s3>ListBucket",  
10                "s3>DeleteObject"  
11            ],  
12            "Resource": [  
13                "  
14            ]  
15        }  
16    ]  
17}
```

A 'Simulate policy' button is located at the bottom right of the policy summary panel.

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

CloudTrail

Dashboard

Event history

Trails

Trails > Configuration

Logging ON

awsDetonationLab-v92-detonationLabCloudTrail-12AFVKOV05S6T

Trail settings

When a trail applies to all regions, the trail exists in all regions and delivers log files for all regions to one Amazon S3 bucket and an optional CloudWatch Logs log group. To see all of your trails, click [Trails](#).

Apply trail to all regions No

Management events

Management events provide insights into the management operations that are performed on resources in your AWS account. [Learn more](#)

Read/Write events All

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

The screenshot displays the Amazon Macie user interface. On the left, a sidebar lists navigation options: DASHBOARD, ALERTS (selected), USERS, RESEARCH, SETTINGS, and INTEGRATIONS. The main content area shows a summary: Active (12), Archived (0), All (12). A message states: "Amazon Macie is monitoring 0 new S3 objects since the last alert generated 12 days ago. [Learn more](#)". Below this, three alerts are listed:

- INFO** User or role Access Denied while attempting to List S3 buckets from non-AWS IP. Type: SUSPICIOUS ACCESS, BASIC ALERT. Occurred 12 days ago by user 963894186934:us... in us-east-1. 1 Results, 0 Views.
- LOW** Large quantity of S3 buckets deleted. Type: INFORMATION LOSS, BASIC ALERT. Occurred 14 days ago by user 963894186934:us... in us-east-1. 94 Results, 0 Views.
- LOW** Change to Cloudtrail logging policy. Type: CONFIG COMPLIANCE, BASIC ALERT. Occurred 14 days ago. 1580 Results, 0 Views.

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

Inspector

Dashboard
Assessment targets
Assessment templates
Assessment runs
Findings

Amazon Inspector - Assessment Runs

An assessment run is the process of discovering potential security issues through the analysis of your assessment target's behavior against selected rules packages. [Learn more.](#)

Last updated on July 10, 2018 2:00:25 PM (0m ago)

Viewing 1-3 of 3

	Start time	Status	Template name	Findings	Findings by sev...	Exclusions
<input type="checkbox"/>	06/21/2018 (GMT-4)	Analysis complete	wazuhTest	18	High Medium L...	0

Assessment - Run - wazuhTest - 2018-06-21T23:45:45.732Z

ARN arn:aws:inspector:us-east-1:963894186934:target/0-QAirwNjD/template/0-yUo1qHUi/run/0-p6r6VEI9

Start 06/21/2018 (GMT-4) (19 days ago) [REDACTED]

End 06/21/2018 (GMT-4) (19 days ago)

Target name [wazuhTest](#)

Template name [wazuhTest](#)

Rules packages [Common Vulnerabilities and Exposures-1.1](#)
[Security Best Practices-1.0](#)

Duration 1 Hour (Recommended)

Status Analysis complete

Findings 18

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

The image shows the Amazon CloudWatch interface with two main sections: 'Rules' and 'Log Groups'.

Rules Section:

- Left Sidebar:** Shows navigation links: CloudWatch, Dashboards, Alarms, ALARM (0), INSUFFICIENT (0), OK (0), Billing, Events, **Rules**, Event Buses, Logs, Metrics, Favorites, and Add a dashboard.
- Header:** 'Rules' and a sub-header: 'Rules route events from your AWS resources for processing by selected targets. You can create, edit, and delete rules.'
- Buttons:** 'Create rule' and 'Actions'.
- Table:** A list of rules with columns: Status, Name, and Description.
 - GuardDuty-Alerts: record guardDuty alerts and send to firehose
 - IAM-Alerts: send IAM alerts to firehose
 - Macie-Alerts: this is to collect all Macie Alerts
 - inspector-Alerts: this will send inspector alerts to firehose
- Pagination:** 'Viewing 1 to 5 of 5 Rules'.

Log Groups Section:

- Left Sidebar:** Same as the Rules sidebar.
- Header:** 'CloudWatch > Log Groups'
- Buttons:** 'Create Metric Filter' and 'Actions'.
- Table:** A list of log groups with columns: Log Groups, Expire Events After, Metric Filters, and Subscriptions.
 - /aws/kinesisfirehose/GuardDuty-Alerts: Never Expire, 0 filters, None
 - /aws/kinesisfirehose/IAM-Alerts: Never Expire, 0 filters, None
 - /aws/kinesisfirehose/Macie-Alerts: Never Expire, 0 filters, None
 - /aws/kinesisfirehose/Inspector-Alerts: Never Expire, 0 filters, None
 - /aws/lambda/awsDetonationLab-v72-FlowLogUpload-196Z7ILBGZZFC: Never Expire, 0 filters, None
 - /aws/lambda/awsDetonationLab-v92-FlowLogUpload-1D4C34OUI66MZ: Never Expire, 0 filters, None
 - /aws/lambda/awsDetonationLab-v92-FlowLogUpload-UHW68F0ORQKJ: Never Expire, 0 filters, None
 - awsDetonationLab-v92-BastionMainLogGroup-SWHTFNE7ZQ1L: Never Expire, 1 filter, None
 - awsDetonationLab-v92-FlowLogs-6QZWD4W93YAV: 1 day, 0 filters, Kinesis (awsDetonationLab-v92-LogStream-1E3JSK1ROPRQT)
 - detonationLab-linux: Never Expire, 0 filters, None
 - detonationLab-windows: Never Expire, 0 filters, None
- Pagination:** 'Log Groups 1-11'.

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

GuardDuty

GuardDuty

Findings

Showing 181 of 181 101 44 36

Actions

Saved filters / Auto-archive
No saved filters

Add filter criteria

	Finding type	Resource	Last Seen	Count
<input type="checkbox"/>	Recon:EC2/PortProb...	Instance: i-05aa12a	31 days ago	62
<input type="checkbox"/>	UnauthorizedAccess:...	Instance: i-05aa12a	8 hours ago	1
<input type="checkbox"/>	Recon:EC2/PortProb...	Instance: i-04dc3dc	14 days ago	987
<input type="checkbox"/>	UnauthorizedAccess:...	Instance: i-08215d7	21 days ago	1
<input type="checkbox"/>	CryptoCurrency:EC2...	Instance: i-0648216	21 days ago	5
<input type="checkbox"/>	Backdoor:EC2/C&C...	Instance: i-0648216	21 days ago	2
<input type="checkbox"/>	UnauthorizedAccess:...	Instance: i-0648216	21 days ago	2
<input type="checkbox"/>	UnauthorizedAccess:...	Instance: i-0648216	21 days ago	1
<input type="checkbox"/>	Recon:EC2/Portscan	Instance: i-0648216	21 days ago	1
<input type="checkbox"/>	UnauthorizedAccess:...	Instance: i-04671c8	21 days ago	1
<input type="checkbox"/>	UnauthorizedAccess:...	Instance: i-04dc3dc	3 days ago	2
<input type="checkbox"/>	UnauthorizedAccess:...	Instance: i-04dc3dc	3 days ago	31
<input type="checkbox"/>	UnauthorizedAccess:...	Instance: i-04dc3dc	5 days ago	2

Useful?

CryptoCurrency:EC2/BitcoinTool.B!DNS

Finding ID: [26b242d38f22f514179531eb5b4383dd](#)

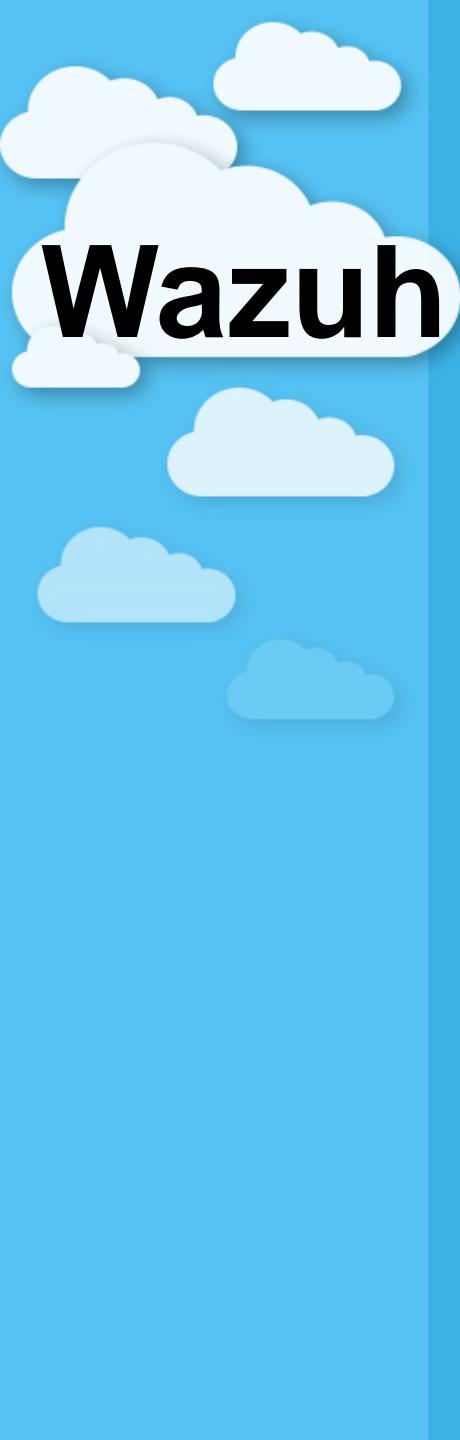
EC2 instance i-06482168eb9976da1 is querying a domain name that is associated with Bitcoin-related activity.

Severity	Region	Count
Medium	us-east-1	5
Account ID	Resource ID	Threat list name
[REDACTED]	i-06482168eb9976da1	ProofPoint
Created at	Updated at	
07-10-2018 15:24:39 (20 hours ago)	07-10-2018 15:40:08 (19 hours ago)	

Resource affected

Resource role	Resource type
TARGET	Instance
Instance ID	Instance type
i-06482168eb9976da1	m4.large
Instance state	Availability zone
running	us-east-1a
Image ID	Image description
ami-428aa838	Amazon Linux 2 LTS Candidate AMI 2017.12.0.2...
Launch time	
06-27-2018 14:54:17	
Instance profile	
Arn: arn:aws:iam::[REDACTED]:instance-profile/cloudwatch-writeLogs	
ID: AIPA17Q44ZZE64MHB3AS2	
Tags	

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

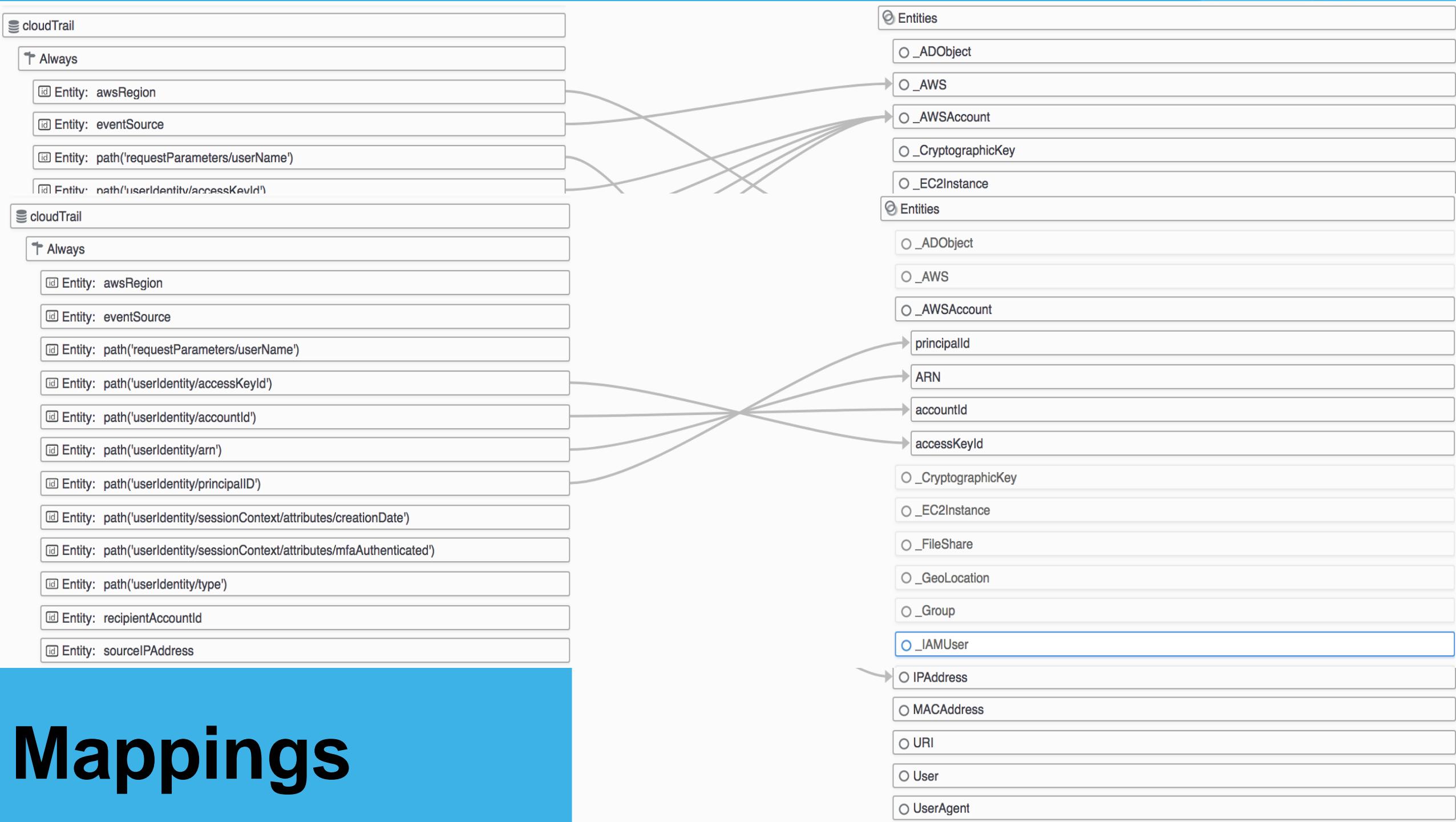


The screenshot shows the Wazuh web interface. At the top, there's a navigation bar with links for Overview, Manager, Agents, Discover, and Dashboards. Below the navigation is a search bar and a timestamp filter for "Last 24 hours".

The main dashboard area is divided into several sections:

- General Metrics:** Displays four key statistics: 299,066 Alerts, 140,564 Level 10 or above alerts, 166,221 Authentication failure, and 65 Authentication success.
- Events:** A bar chart showing event counts over time (every 30 minutes) from 19:00 to 16:00. The count generally fluctuates between 5,000 and 10,000 events per period.
- Agents:** Two charts. On the left, a stacked area chart shows agent counts by type (vpc-agent-centos..., vpc-agent-ubuntu..., vpc-agent-windows, vpc-agent-debian8, vpc-ossec-manager, vpc-agent-debian, vpc-agent-centos, vpc-agent-ubuntu, ip-10-0-0-76) over time. On the right, a line chart tracks the unique count of agents by status (Disconnected, Never connected, Active) over time.
- Top Metrics:** Four summary boxes: root (Top source user), 58.218.204.181 (Top source ip), syslog (Top group), and 10.2.5 (Top PCI DSS requirement).
- Groups:** A stacked area chart showing the count of various groups over time, including syslog, authentication_failed, authentication_failures, attacks, pam, sshd, access_control, and windows.
- Alert level evolution:** A line chart showing the count of alerts at different levels (5, 10, 3, 7, 6, 9, 15, 8, 12) over time.
- Alerts summary:** A table listing alert details such as Rule ID, Description, Level, Groups, PCI DSS requirement, and Count.

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



Mappings

Simple Dashboards

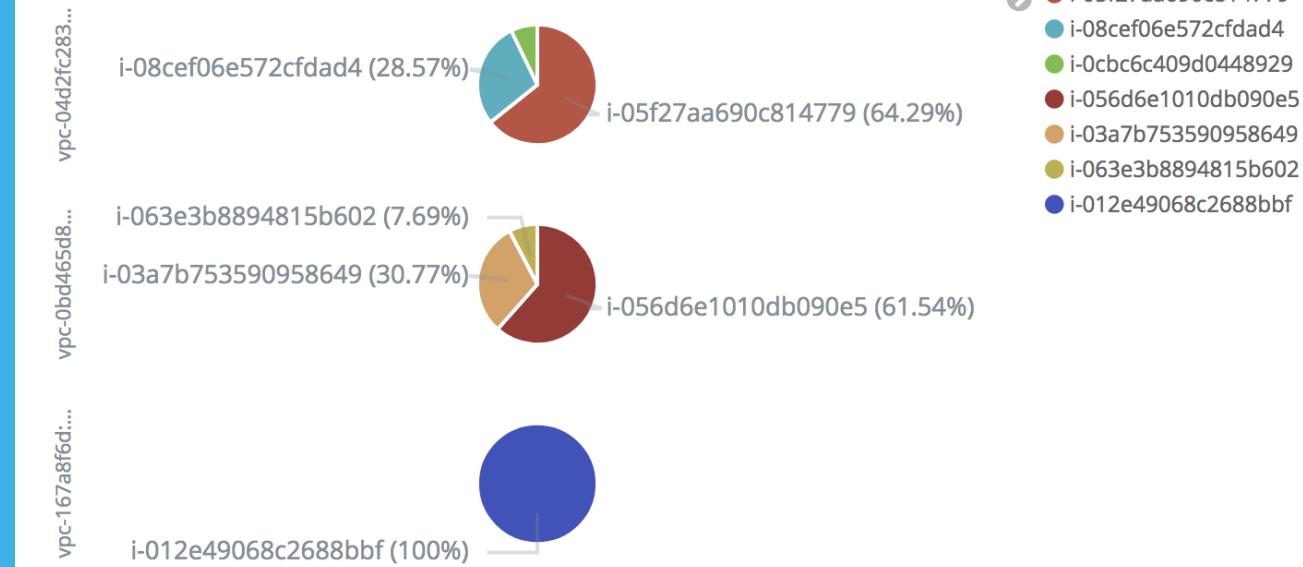
VPCFlow-Top10ExternalDestinationIP-Table

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

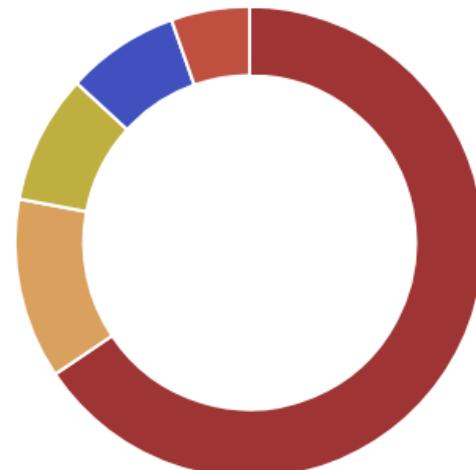
GuardDuty-MostCommonAccountId-Table

Account ID	Count
963894186934	40

GuardDuty-BreakdownOfAlertsPerInstancePerVPC-Pie



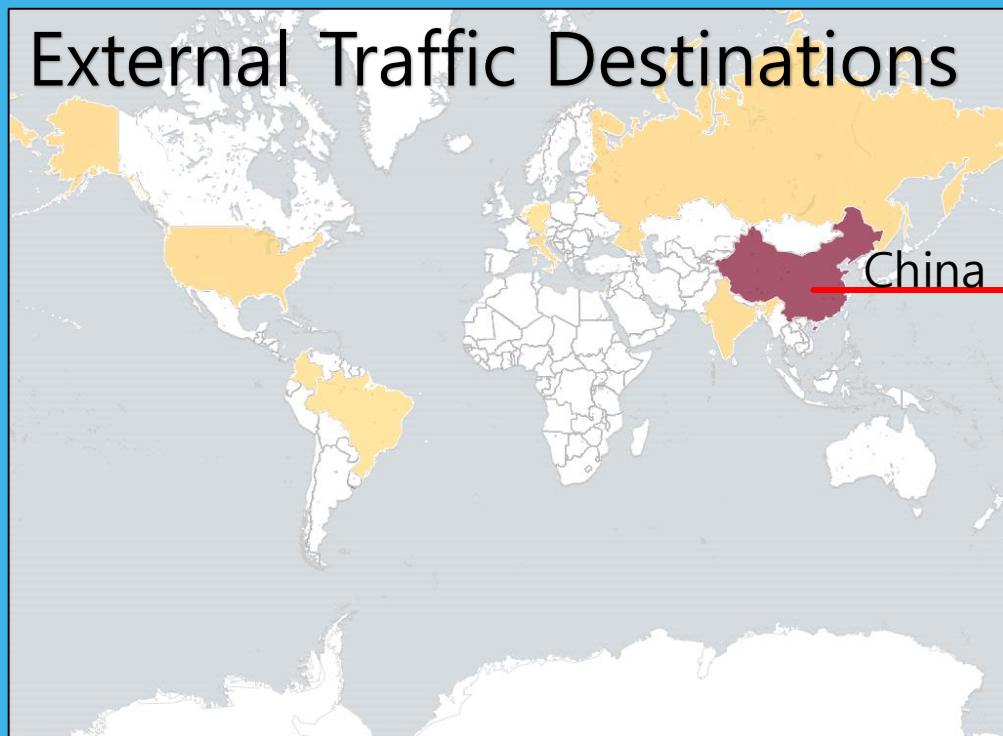
CloudTrail-EventNames-pie



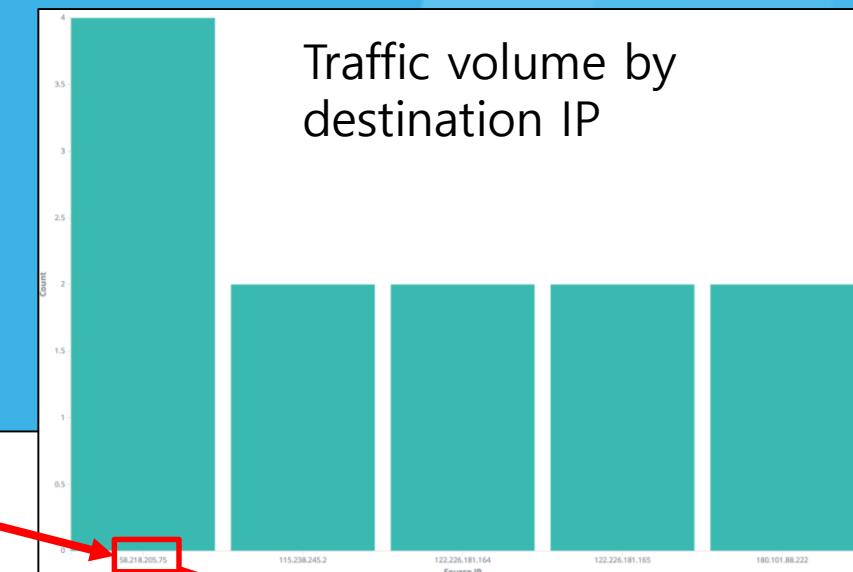
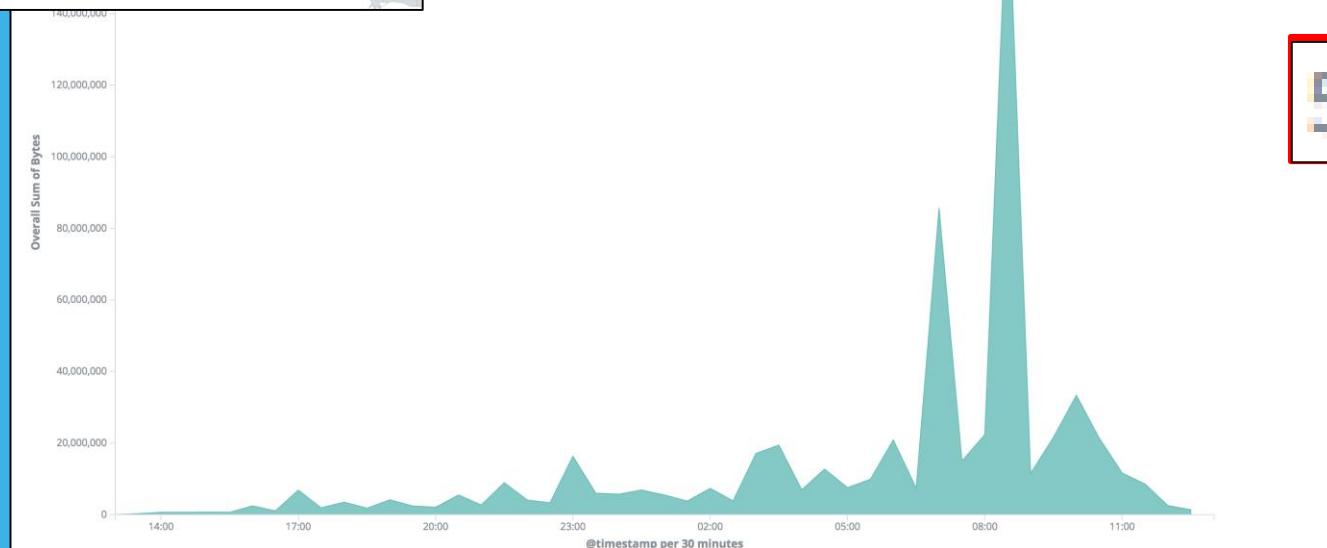
- Legend:
- ListAliases
 - ListUsers
 - AssociateAddress
 - ListGroups
 - AuthorizeSecurityGro...

Finding what matters

External Traffic Destinations



Massive spike in traffic to china



58.218.205.75

Most common destination

Finding what matters

58.218.205.75

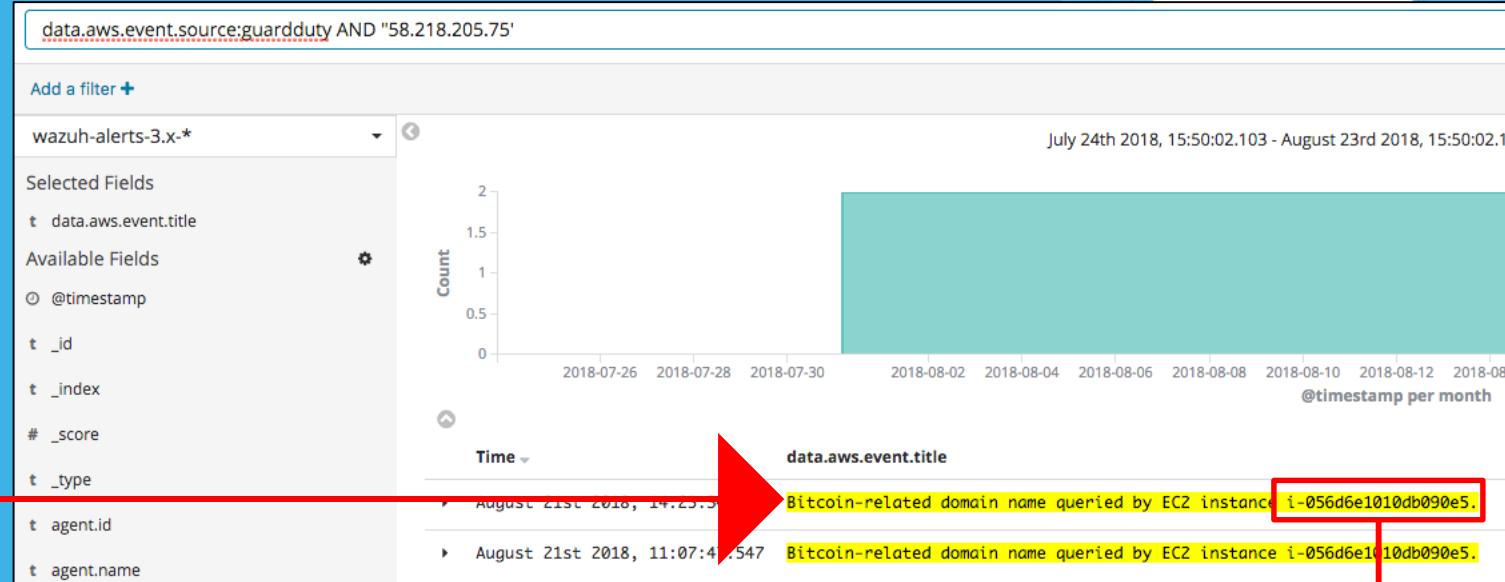
Most common destination

loggingSourcesFor-58.218.205.75

AWS Logging Sources

vpc
guardduty

Logs with Destination



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

Ec2 Instance involved

Hostname of findings

All Guardduty Findings for instance

Finding what matters

```
@timestamp     Q Q D * August 24th 2018, 16:16:44.349
t _id          Q Q D * tZelUbWUB-pbw9wu1_DB9
t _index        Q Q D * wazuh-alerts-3.x-2018.08.24
# _score        Q Q D *
t _type         Q Q D * wazuh
t agent.id      Q Q D * 002
agent.ip       Q Q D * 172.16.0.21
t agent.name    Q Q D * linuxVictim2
t decoder.name  Q Q D * ossec
t full_log      Q Q D * 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
t id          Q Q D * 1535141804.148908
t location     Q Q D * netstat outbound connections
t manager.name Q Q D * ip-172-16-0-21.ec2.internal
t path         Q Q D * /var/ossec/logs/alerts/alerts.json
t previous_log Q Q D * 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
t previous_output Q Q D * 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
t rule.description Q Q D * Listened ports status (netstat nputw) changed (new port opened or closed).
# rule.firetimes Q Q D * 9
t rule.gdpr     Q Q D * IV_35.7.d
t rule.gpg13    Q Q D * 10.1
t rule.groups   Q Q D * local, syslog, sshd
t rule.id       Q Q D * 100002
# rule.level    Q Q D * 7
@ rule.mail     Q Q D * false
t rule.pci_dss  Q Q D * 10.2.7, 10.6.1
```

Most common destination

58.218.205.75

File added to the system.

```
@timestamp     Q Q D * August 20th 2018, 16:06:59.483
t _id          Q Q D * cDvyWGUBy4A8_JfJnR4Z
t _index        Q Q D * wazuh-alerts-3.x-2018.08.20
# _score        Q Q D *
t _type         Q Q D * wazuh
t agent.id      Q Q D * 000
t agent.name    Q Q D * ip-172-16-0-21.ec2.internal
t decoder.name  Q Q D * syscheck_integrity_changed
t full_log      Q Q D * 
t id          Q Q D * 1534795619.119545
t location     Q Q D * syscheck
t manager.name Q Q D * ip-172-16-0-21.ec2.internal
t path         Q Q D * /var/ossec/logs/alerts/alerts.json
t predecoder.hostname Q Q D * 172-16-0-21
New file '/bin/pip3.7' added to the file system.
```

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

```
# rule.firetimes Q Q D * 11
t rule.gdpr     Q Q D * II_5.1.f
t rule.gpg13    Q Q D * 4.11
t rule.groups   Q Q D * ossec, syscheck
t rule.id       Q Q D * 554
# rule.level    Q Q D * 5
@ rule.mail     Q Q D * false
t rule.pci_dss  Q Q D * 11.5
t syscheck.event Q Q D * added
t syscheck.gid_after Q Q D * 0
t syscheck.gname_after Q Q D * root
t syscheck.inode_after Q Q D * 13311903
t syscheck.md5_after Q Q D * fb7791757901a24800f67f0f950b281d
@ syscheck.mtime_after Q Q D * May 2nd 2018, 13:40:47.000
t syscheck.path  Q Q D * /bin/pip3.7
t syscheck.perm_after Q Q D * 100755
t syscheck.sha1_after Q Q D * 4f7c79d247490ce12b159b1cef9832e60a9513b9
t syscheck.sha256_after Q Q D * 1e2f03917015b52c71432ffd382e0ee970d551eebf9457b2498b1434ce8ab466
# syscheck.size_after Q Q D * 206
t syscheck.uid_after Q Q D * 0
t syscheck.uname_after Q Q D * root
```

VT Results

	53 engines detected this file
SHA-256	1e2f03917015b52c71432ffd382e0ee970d551eebf9457b2498b1434ce8ab466
File name	fb7791757901a24800f67f0f950b281d.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
<input type="checkbox"/>	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-IT0JiioL/template/0-S7AjlH5cj/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

Visibility

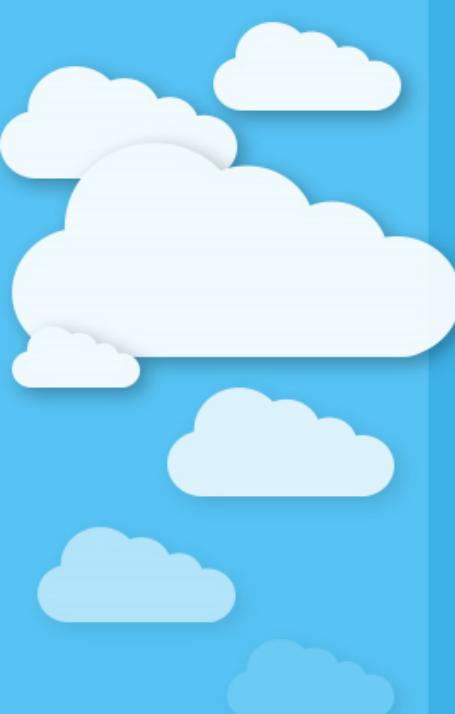


<u>Traditional Tool</u>	<u>AWS equivalent</u>
IDS/IPS	guardDuty
DLP	Macie
EDR	Cloudwatch + osquery, GRR
Netflow	Cloudwatch + VPCFlow
DNS	Cloudwatch + Route53
Access and authentication auditing	CloudTrail
Active Directory	Directory Service
Identity Management	IAM
Single Sign On	AWS SSO
Vulnerability scanner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



Personal
**Attacker Life
cycle**





Flag it, Tag it, and Bag it.



whorsee58