509.2
Amazon AWS

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

509.2
Amazon AWS

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

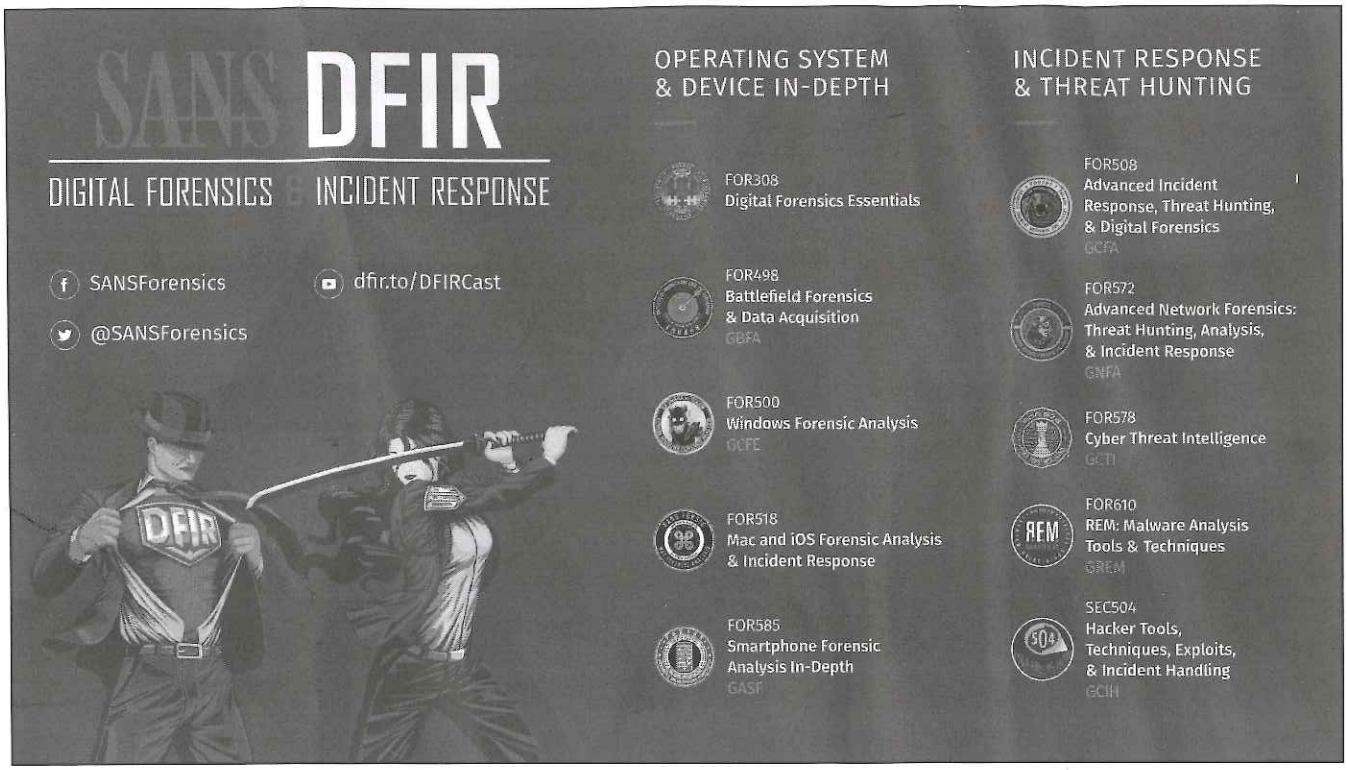
Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

FOR509.2 | Enterprise Cloud Forensics and Incident Response

Amazon AWS

Authors:
David Cowen – dlcowen@gmail.com
https://twitter.com/HECFBlog
https://www.hecfblog.com/

Pierre Lidome – plidome@gmail.com

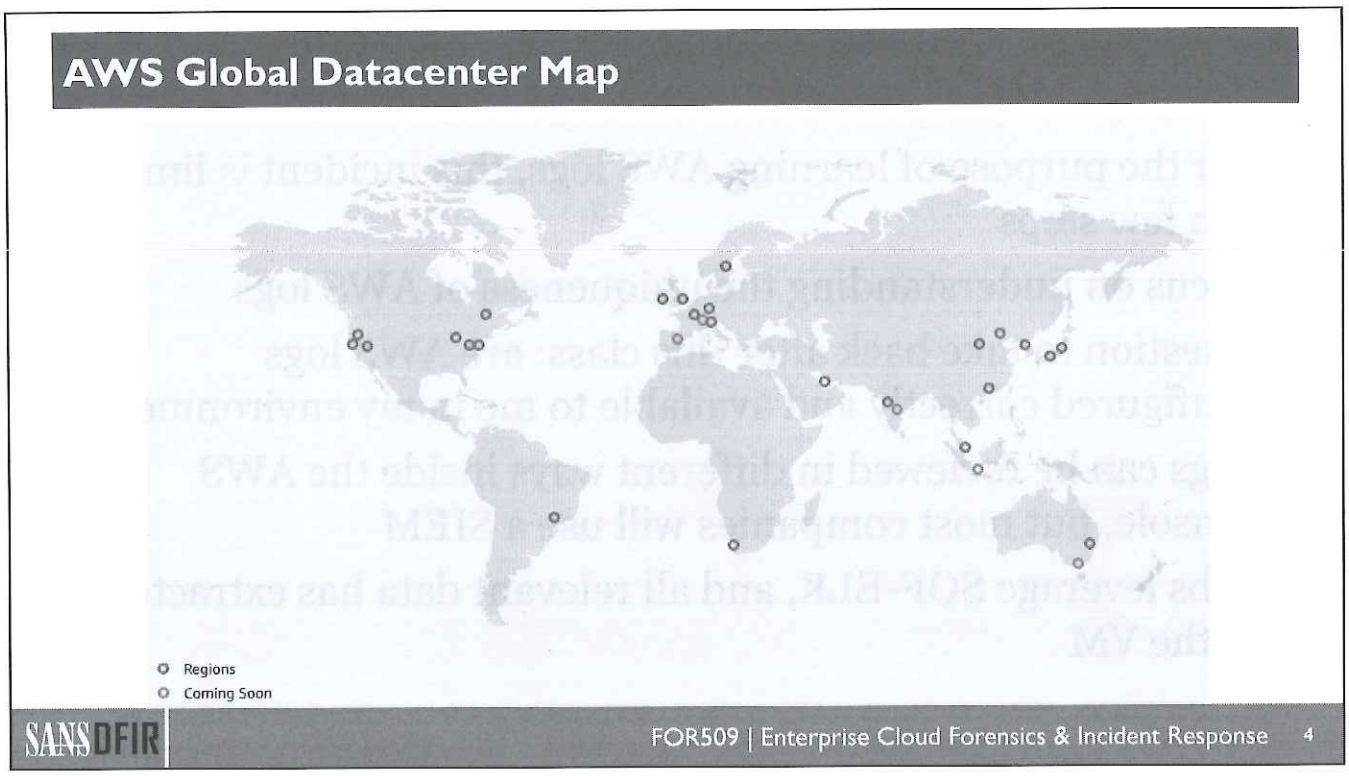


This page intentionally left blank.

Sample Incident: Pymtechlabs

- For the purpose of learning AWS logs, this incident is limited to a few steps
- Focus on understanding the uniqueness of AWS logs
- Question to take back after this class: are AWS logs configured correctly and available to me in my environment?
- Logs can be reviewed in different ways inside the AWS console, but most companies will use a SIEM
- Labs leverage SOF-ELK, and all relevant data has extracted to the VM

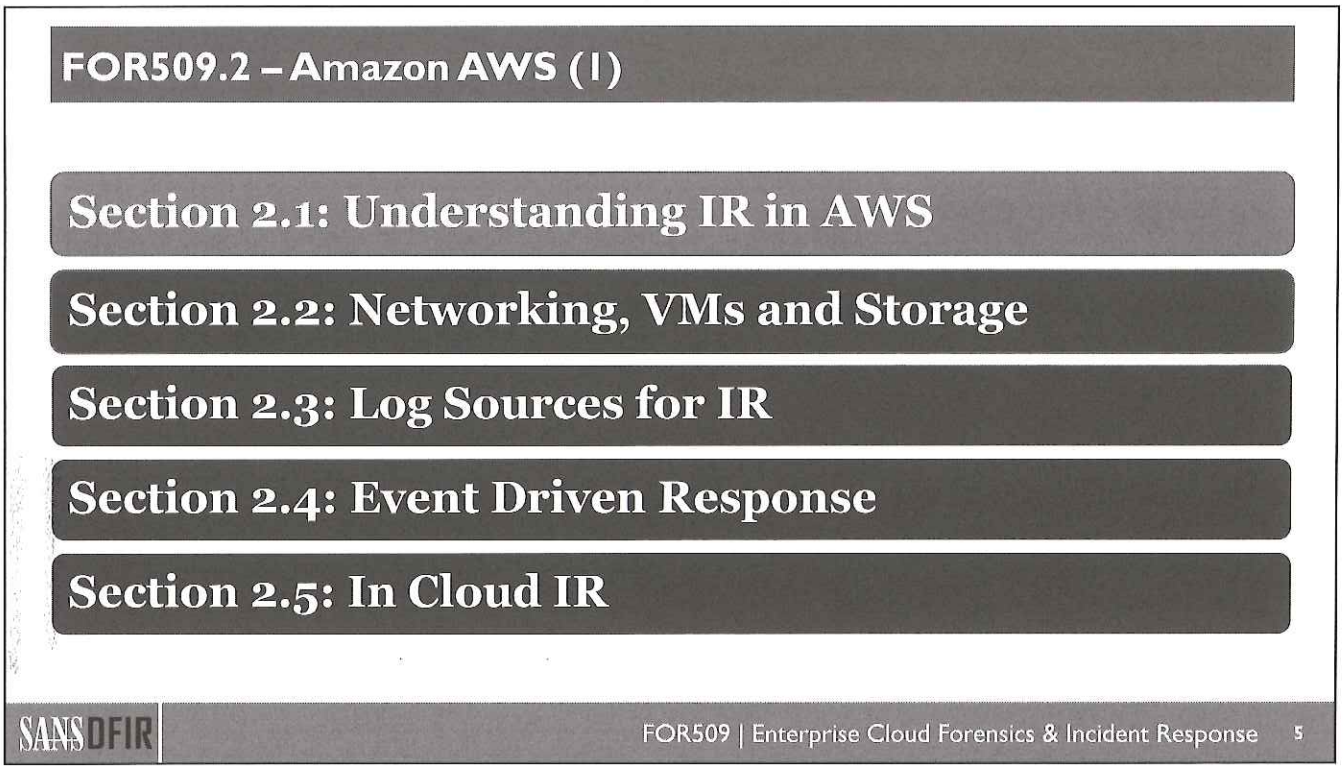
To further the educational experience, we have created a simple scenario that will facilitate learning about the different logs. All the data has been imported into SOF-ELK to facilitate your analysis.



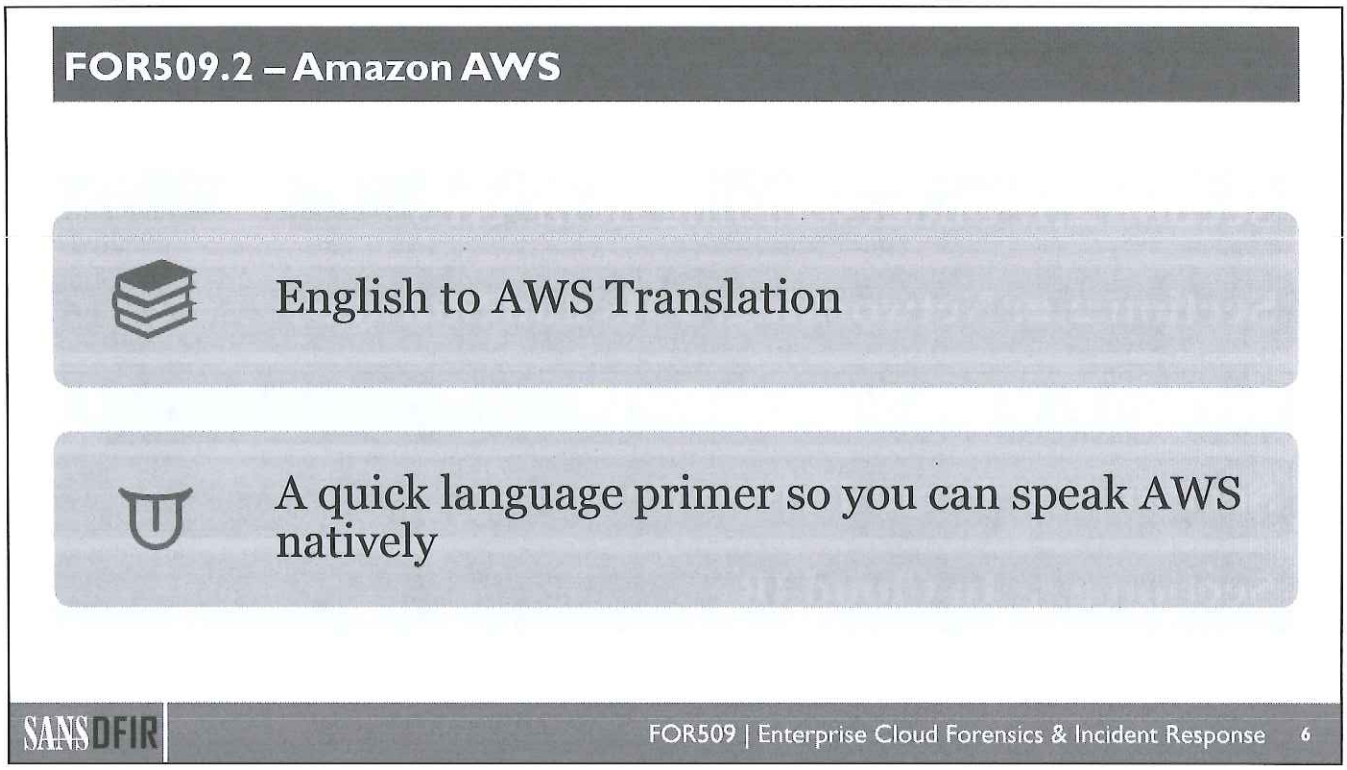
Credit: Amazon AWS

Picture as of 4/17/21

Source: https://aws.amazon.com/about-aws/global-infrastructure/



This page intentionally left blank.



This section will introduce you to the language of AWS. The major services that are involved with most environments as well as the forensic data we can expect to receive from them. This course is not meant to teach how to configure, maintain or deploy AWS services but how to investigate and respond to breaches within them.

When talking to AWS professionals having the ability to speak their language will go a long way in their ability to assist you in your investigation.

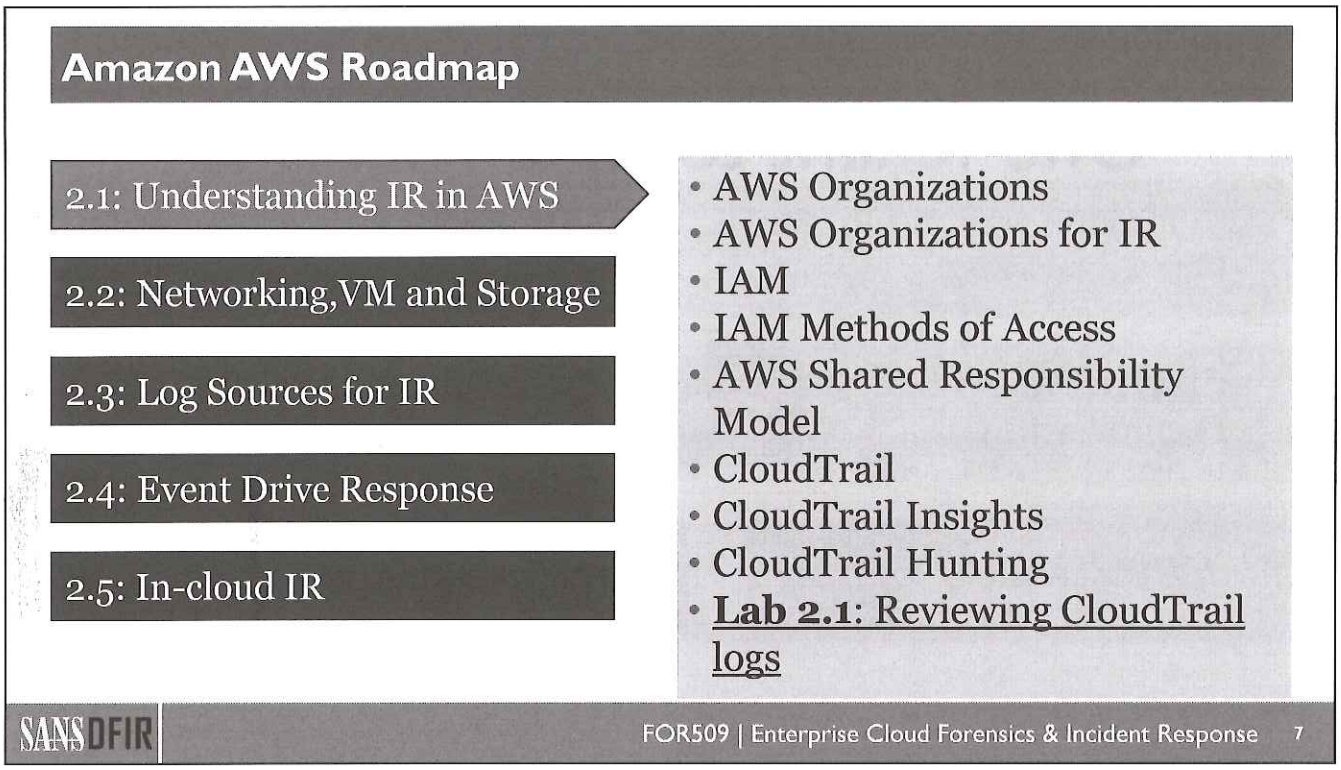
For instance here are several questions that result in good forensic data:

"Where do you store CloudTrail logs?

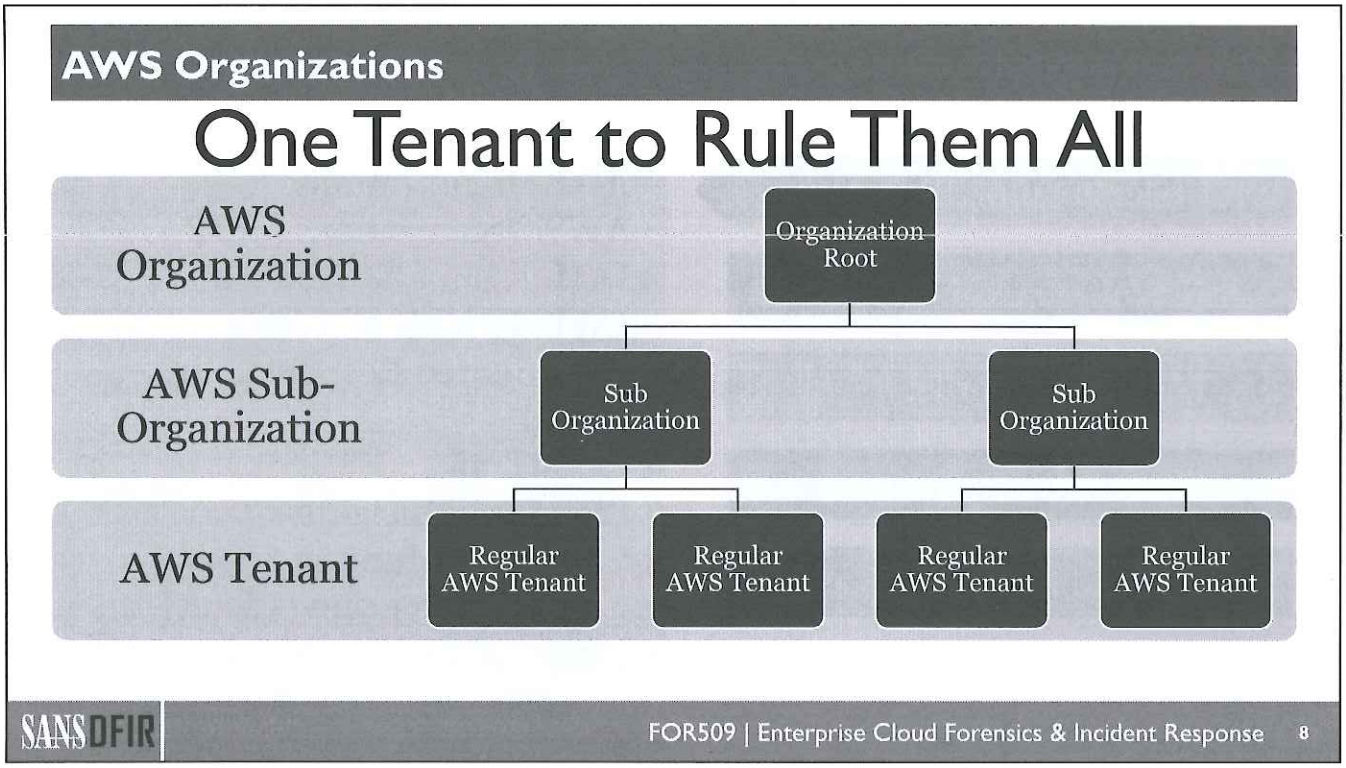
"Do you have flow logs for this VPC?"

"Can this AKS cluster reach the metadata service?"

Don't understand what all these things mean? No problem that's what this section will help you understand while making sure those in the AWS world can understand you!



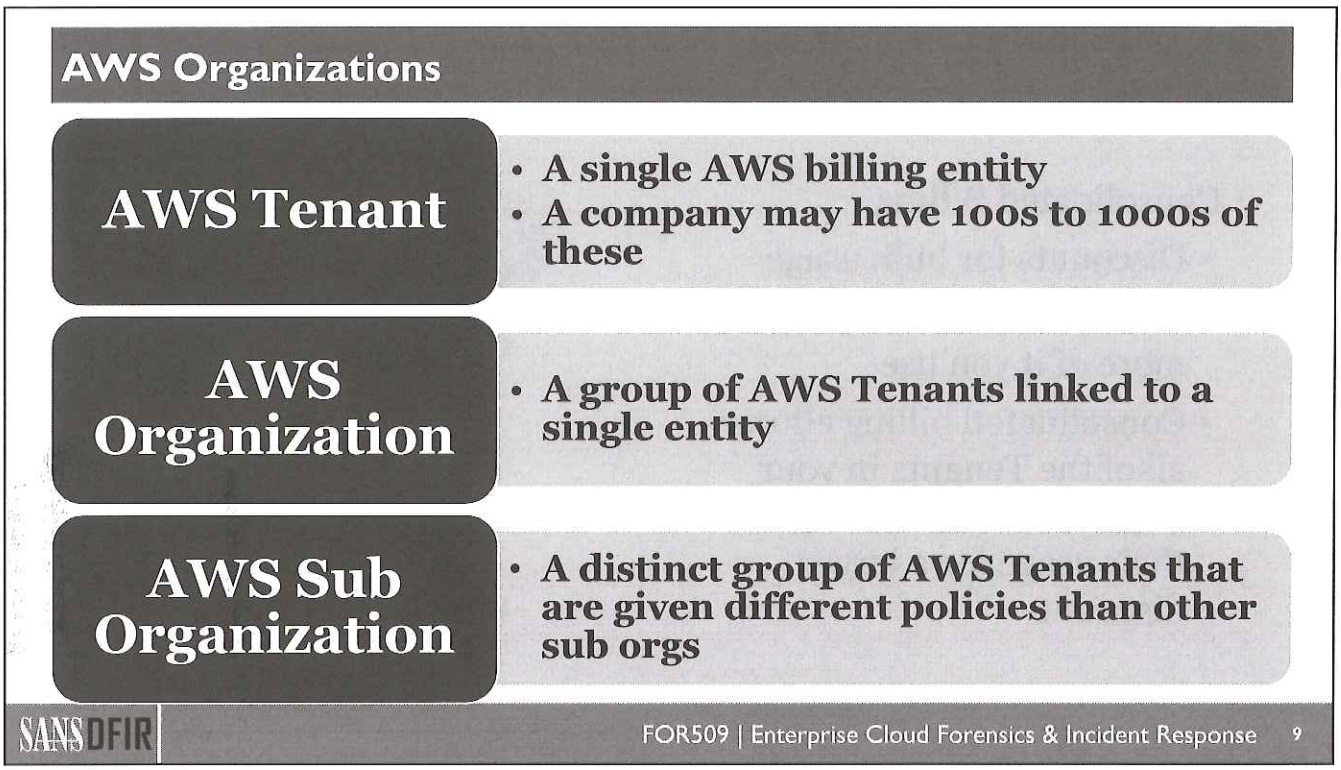
This page intentionally left blank.



AWS Organizations are a way to group all your companies AWS Tenants into one tree so that you can:

- Manage access between AWS Tenants
- Establish single sign on across your AWS Tenants
- Recognize cost savings by allowing you usage to be accumulated across all Tenants for volume discounts

You can learn more about them here: https://aws.amazon.com/organizations/



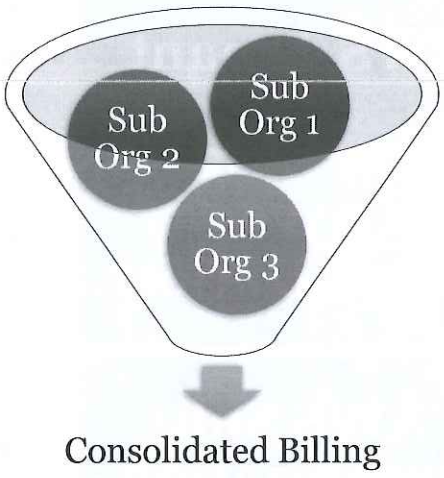
AWS Tenant – A single AWS tenant that you've created with Amazon Web services. If you've just started with AWS, then you likely have one of these. In large organizations each department could have an AWS Tenant per project, per group or per department. It's not unusual as cloud adoption grows to find over 100 AWS tenants operating for one company.

AWS Organization – A group of AWS Tenants with one tenant serving as the master.

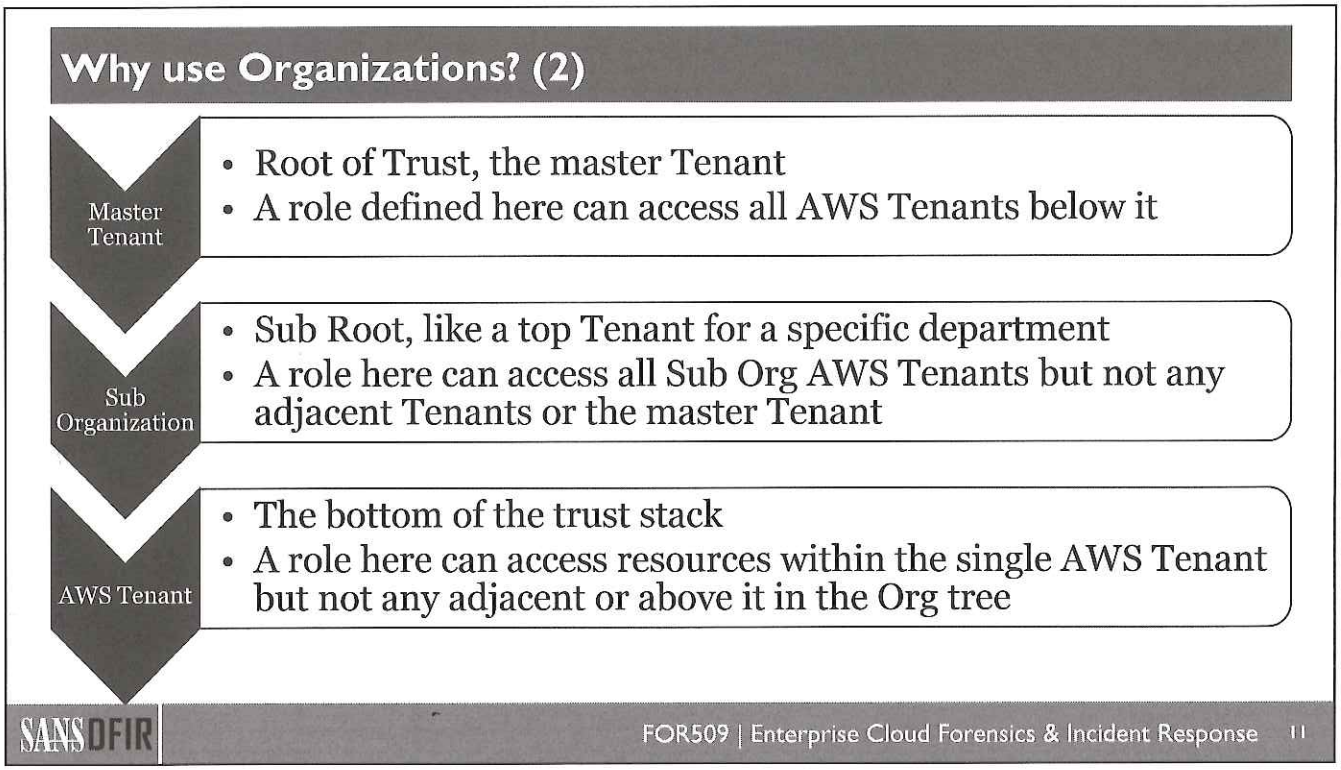
AWS Sub Organization -

Why use Organizations? (1)

- Consolidated Billing
  - Discounts for bulk usage
  - AWS Provides discounts the more of it you use
  - Consolidated billing allows all of the Tenants in your Organization to add up all their usage for a larger discount



This page intentionally left blank.



This page intentionally left blank.

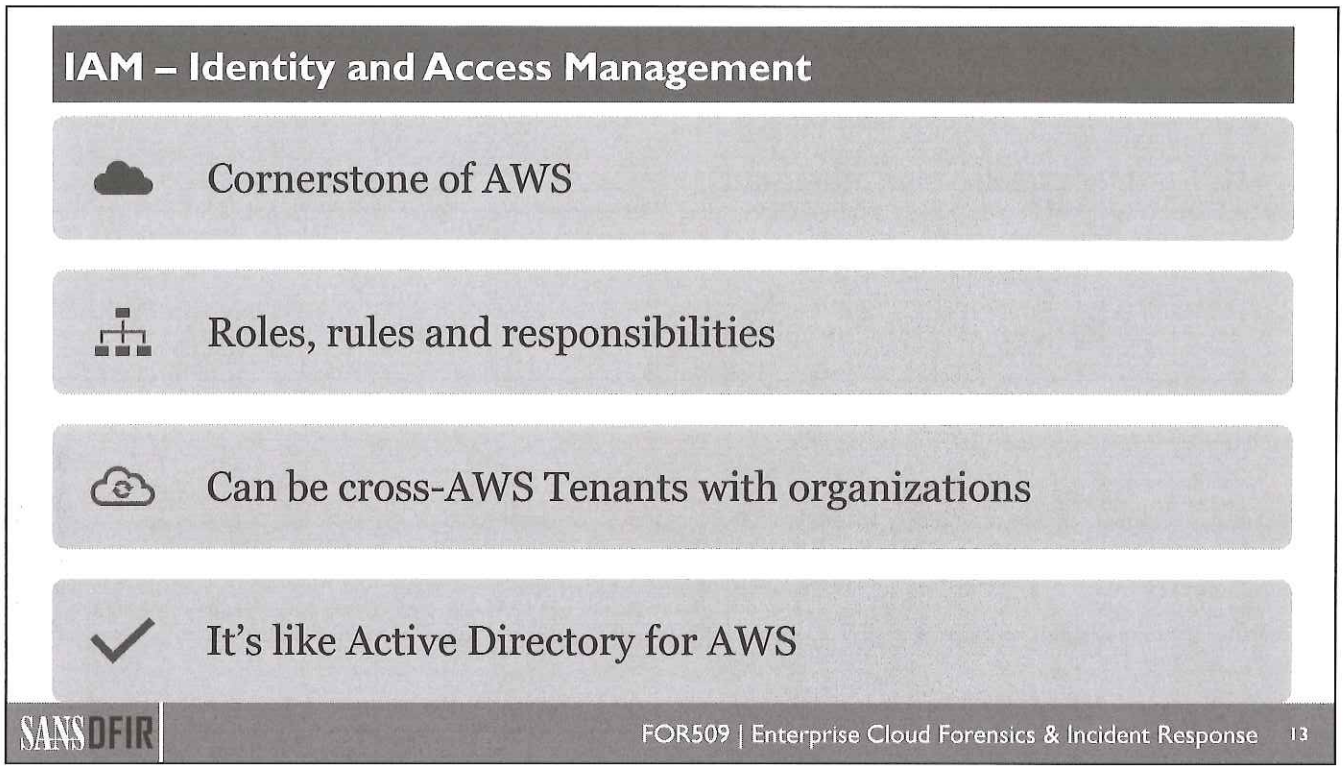
IR Roles in Organizations

Automatic Write Blocking!

You can define read only global access too:

S3 Buckets
EC2 Virtual Machines
EBS Data Stores
Databases
Containers
And More!

This page intentionally left blank.



This page intentionally left blank.

Ways of Accessing AWS

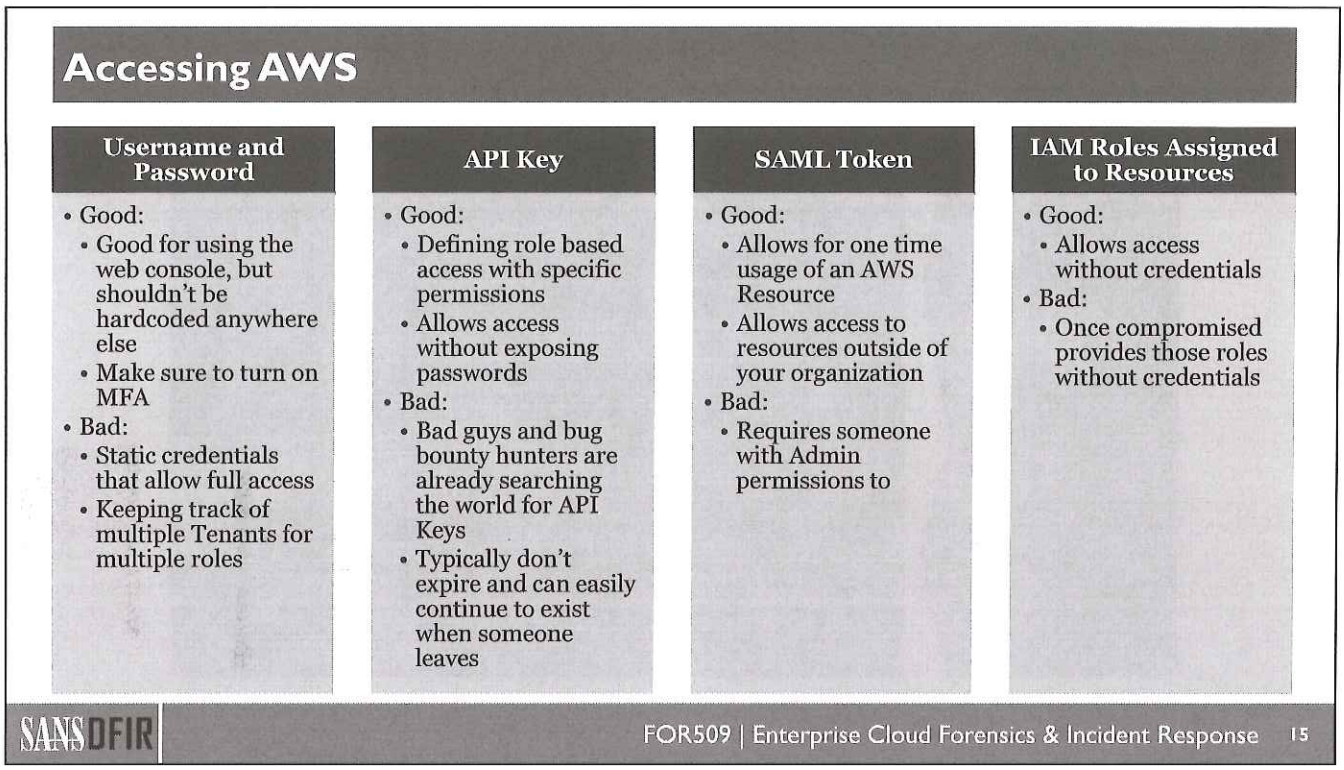
Username and password = Tired

API Key = The New Normal

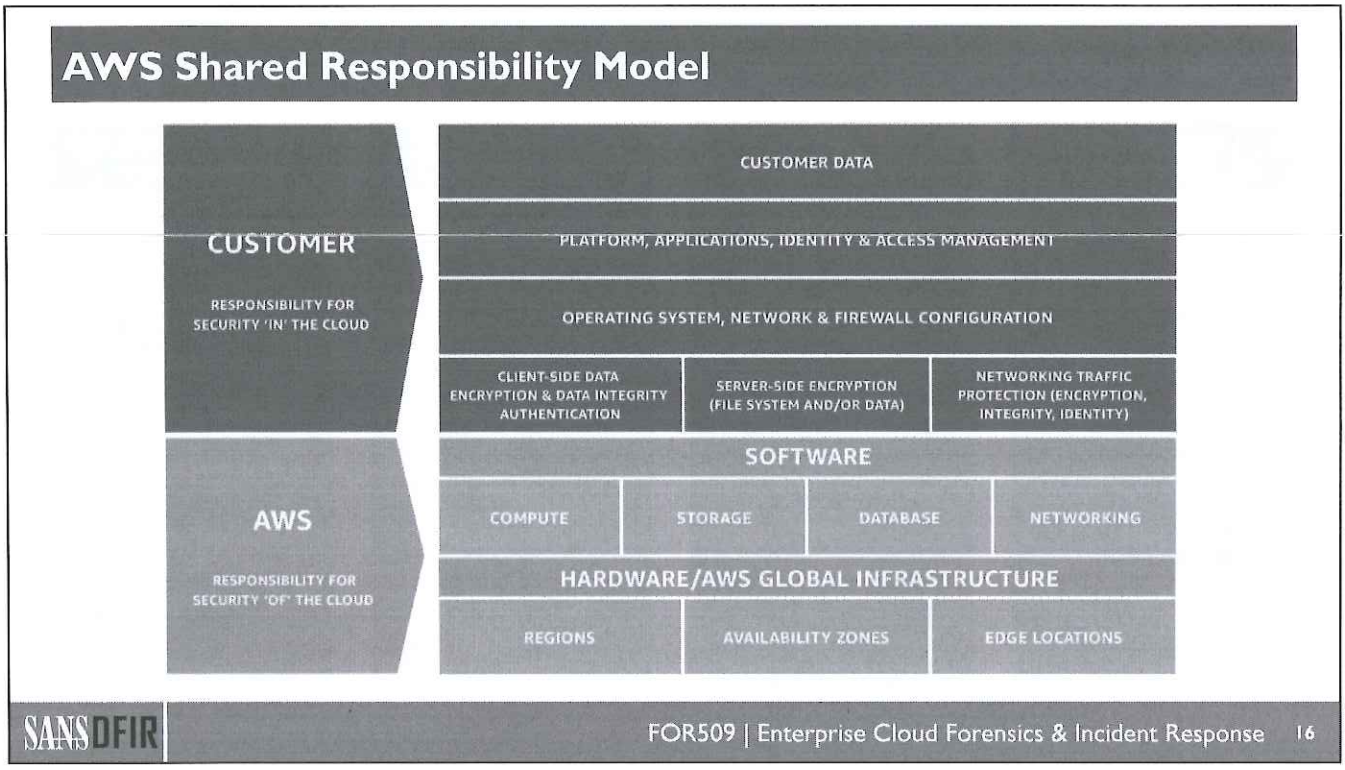
SAML Token = Cool Kids Club

IAM Roles Assigned = Robot Uprising

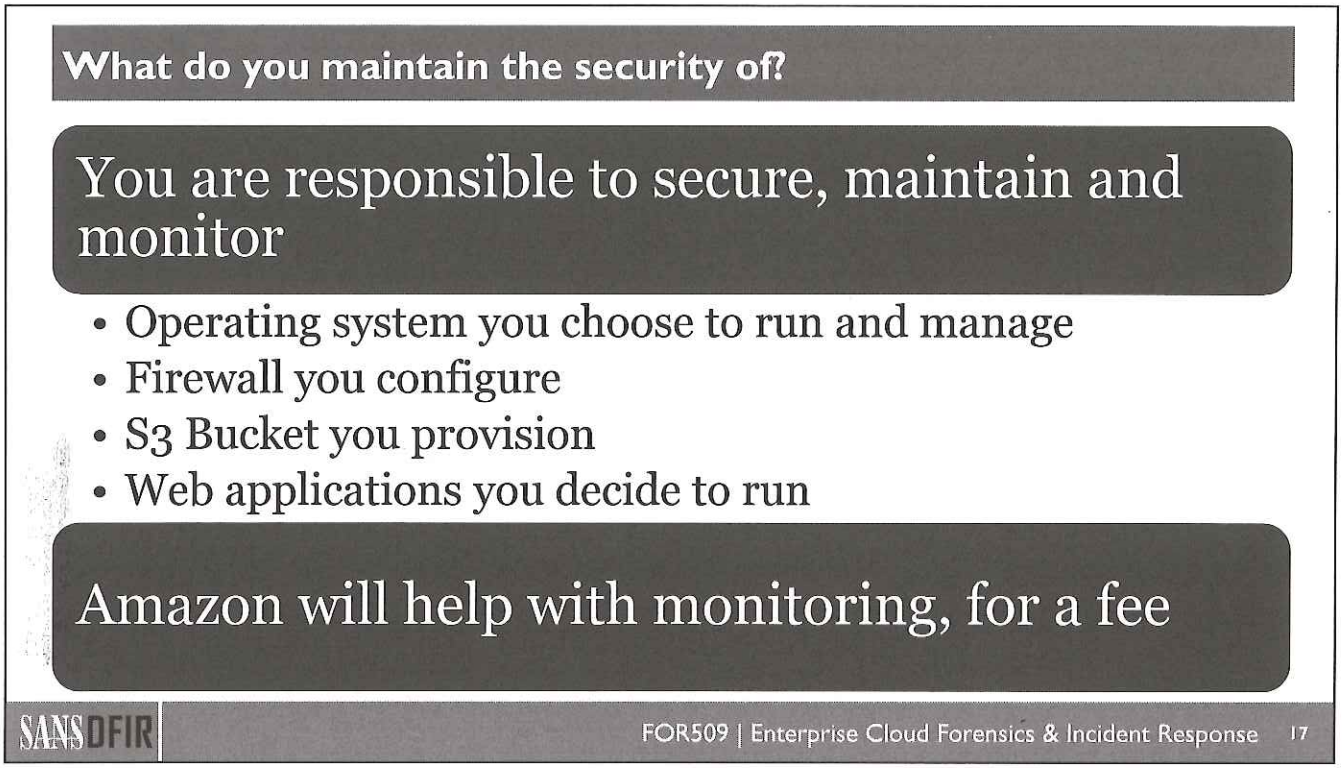
This page intentionally left blank.



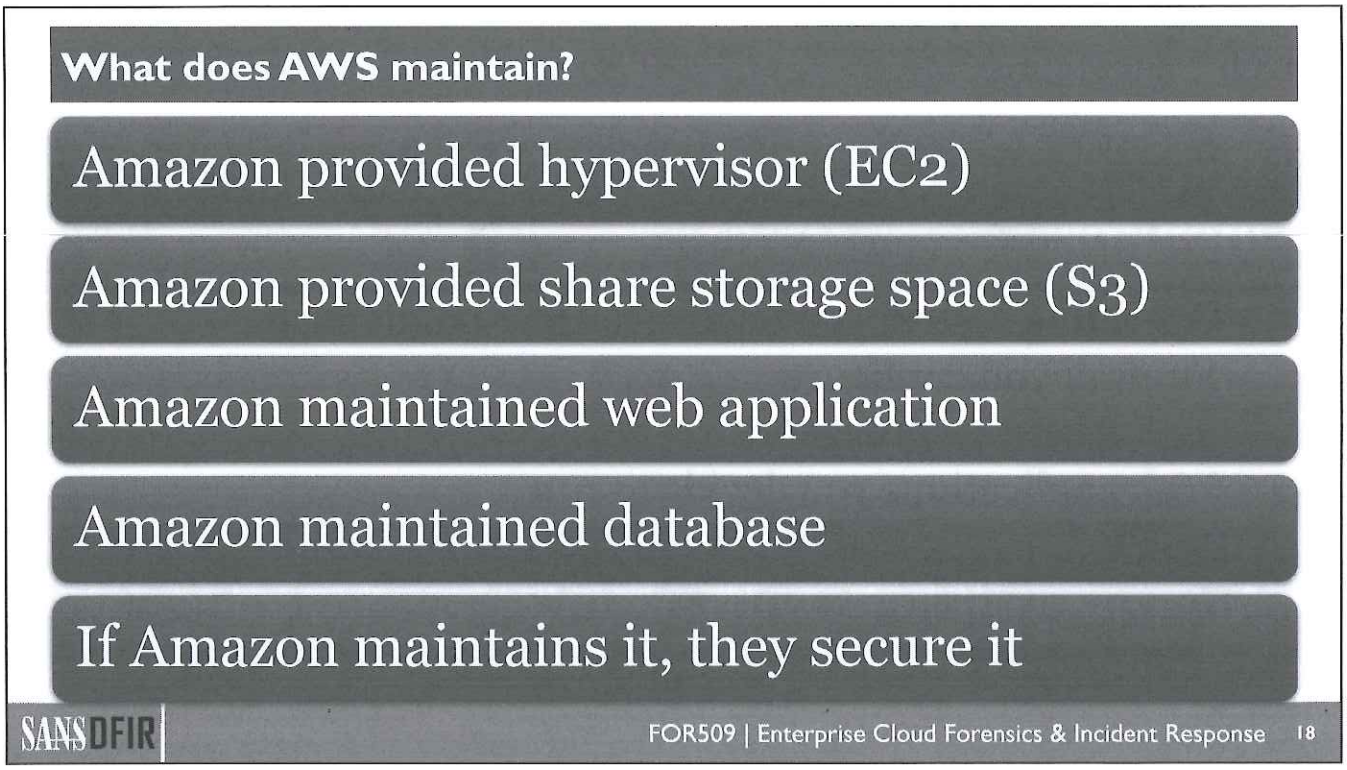
This page intentionally left blank.



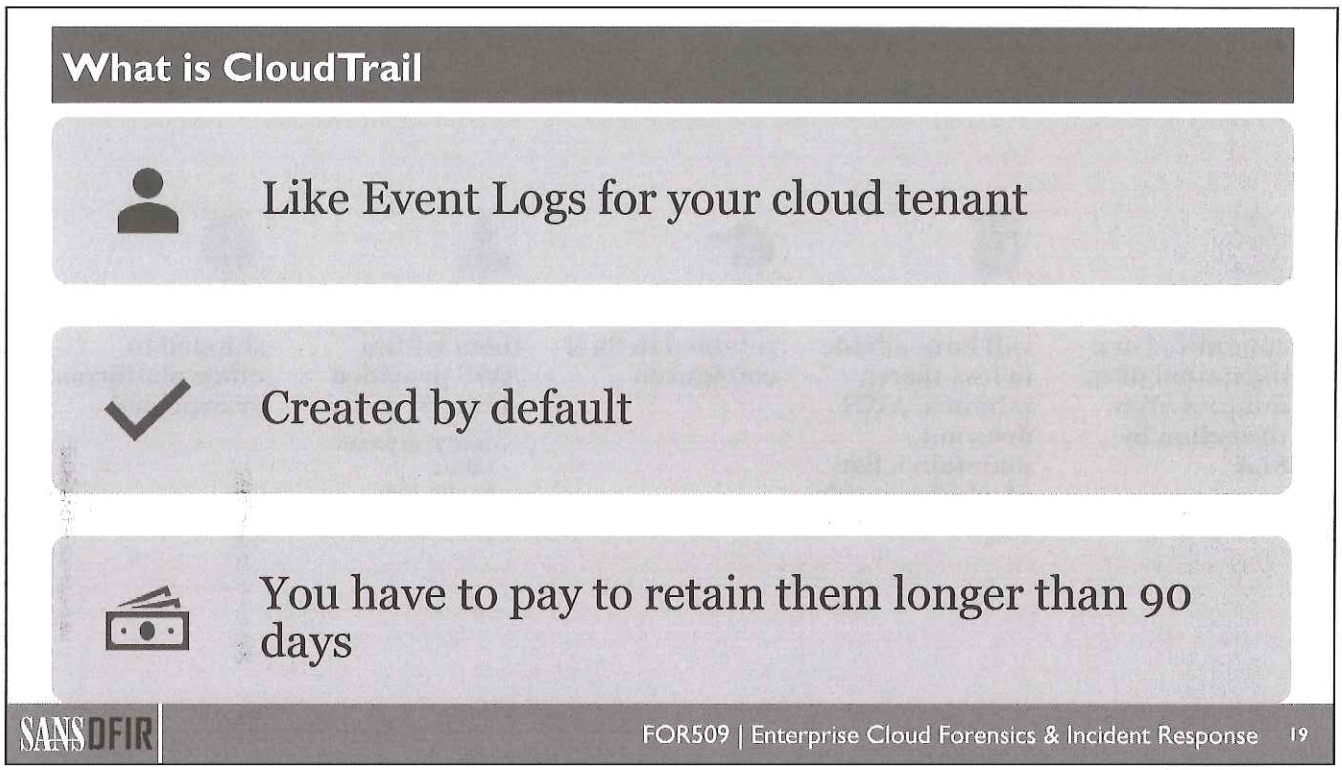
This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.

CloudTrail

Records are committed at a maximum of 15 minutes after the action by SLA

Some records will be available in less than 5 minutes, AWS does not maintain a list of which get this SLA

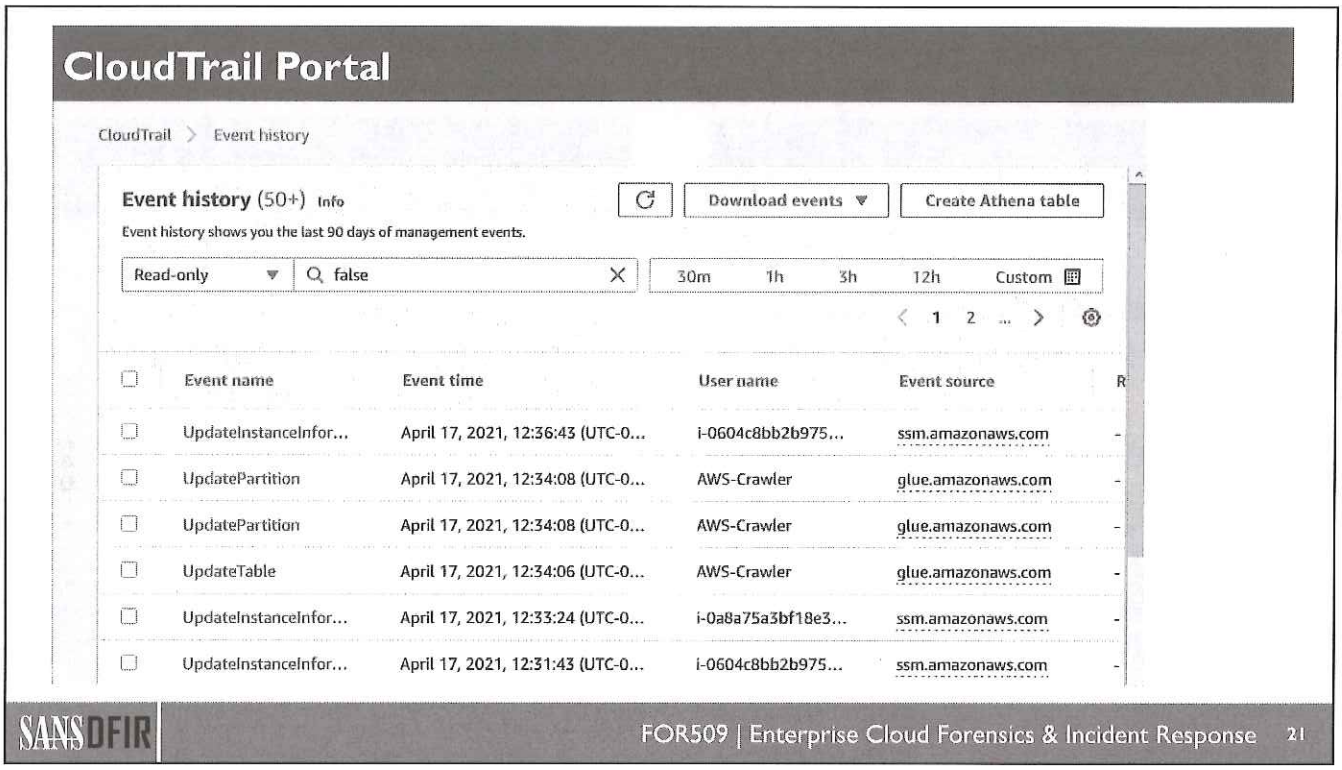
Logs can be retained in S3 if configured

You can search them within AWS provided services

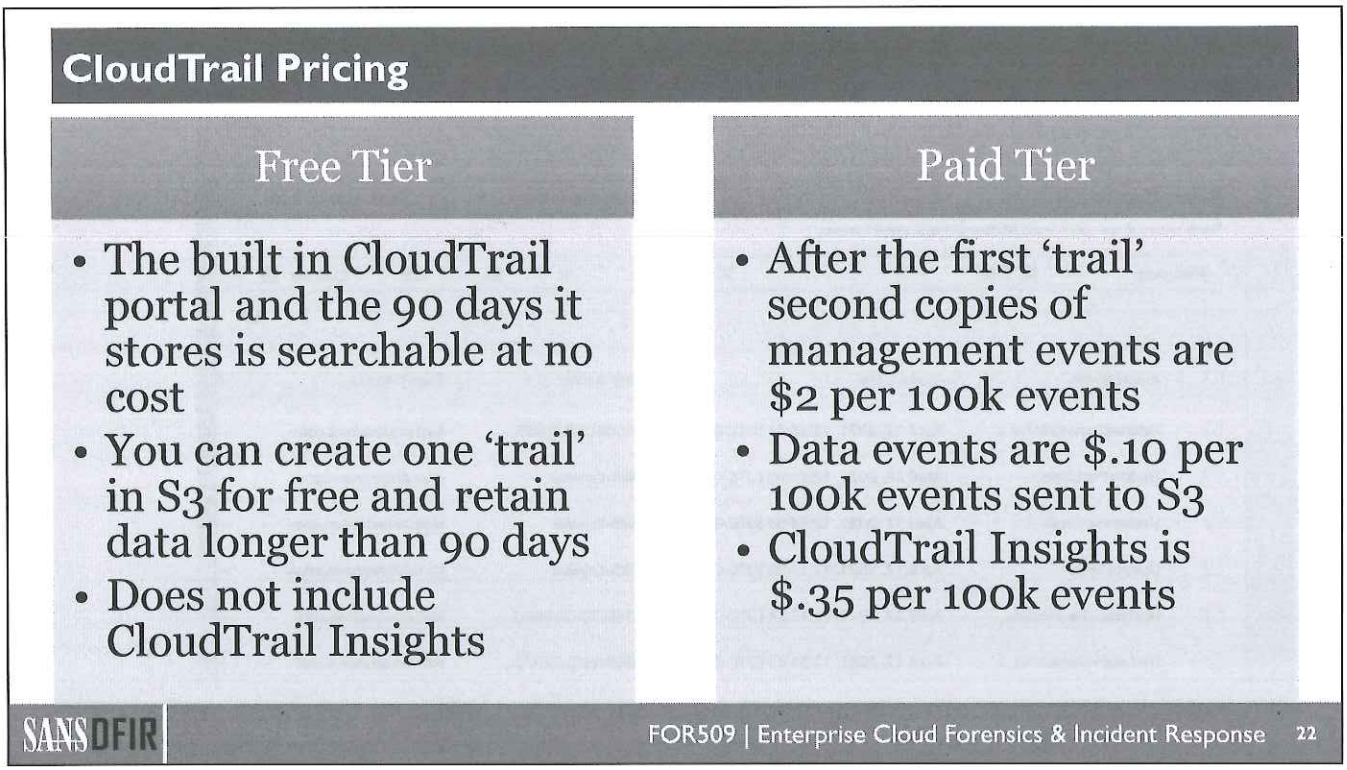
- CloudTrail portal
- Athena
- Security Hub

Can also be shipped to other platforms or exported

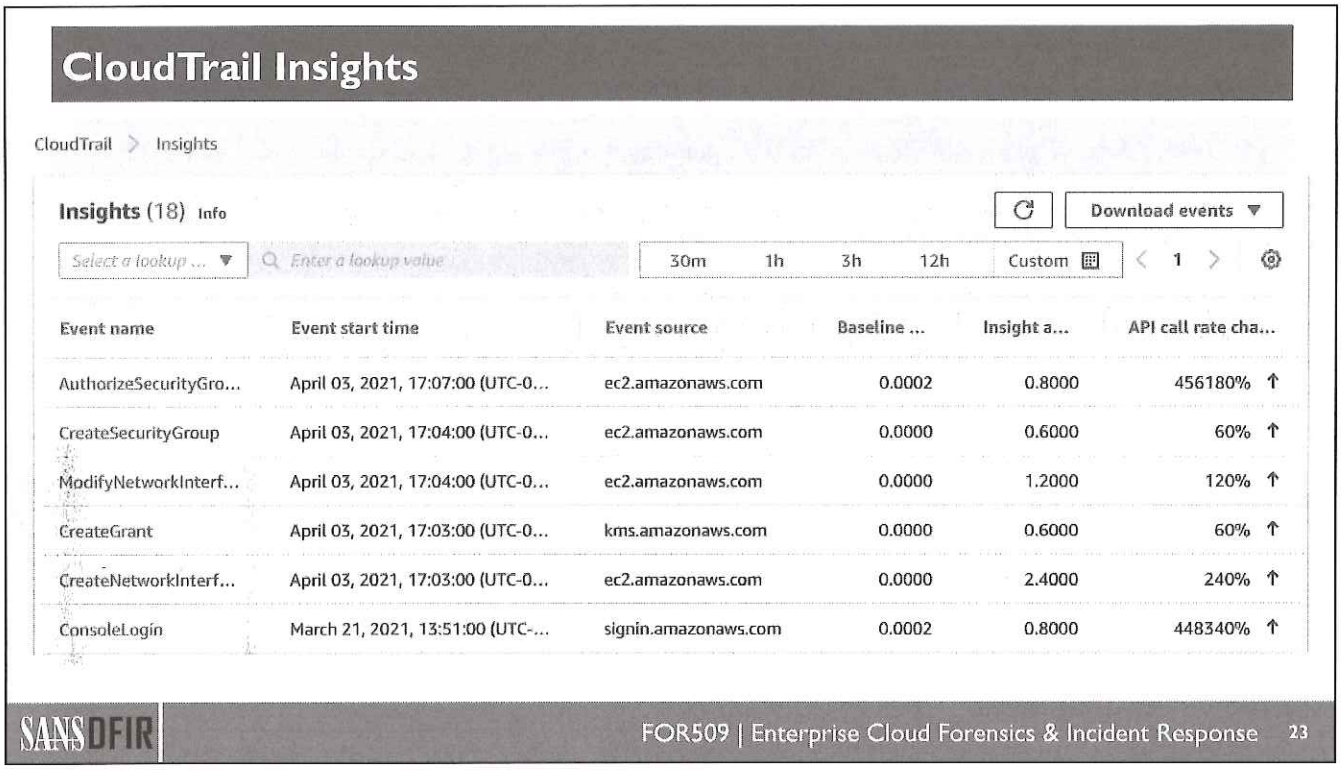
This page intentionally left blank.



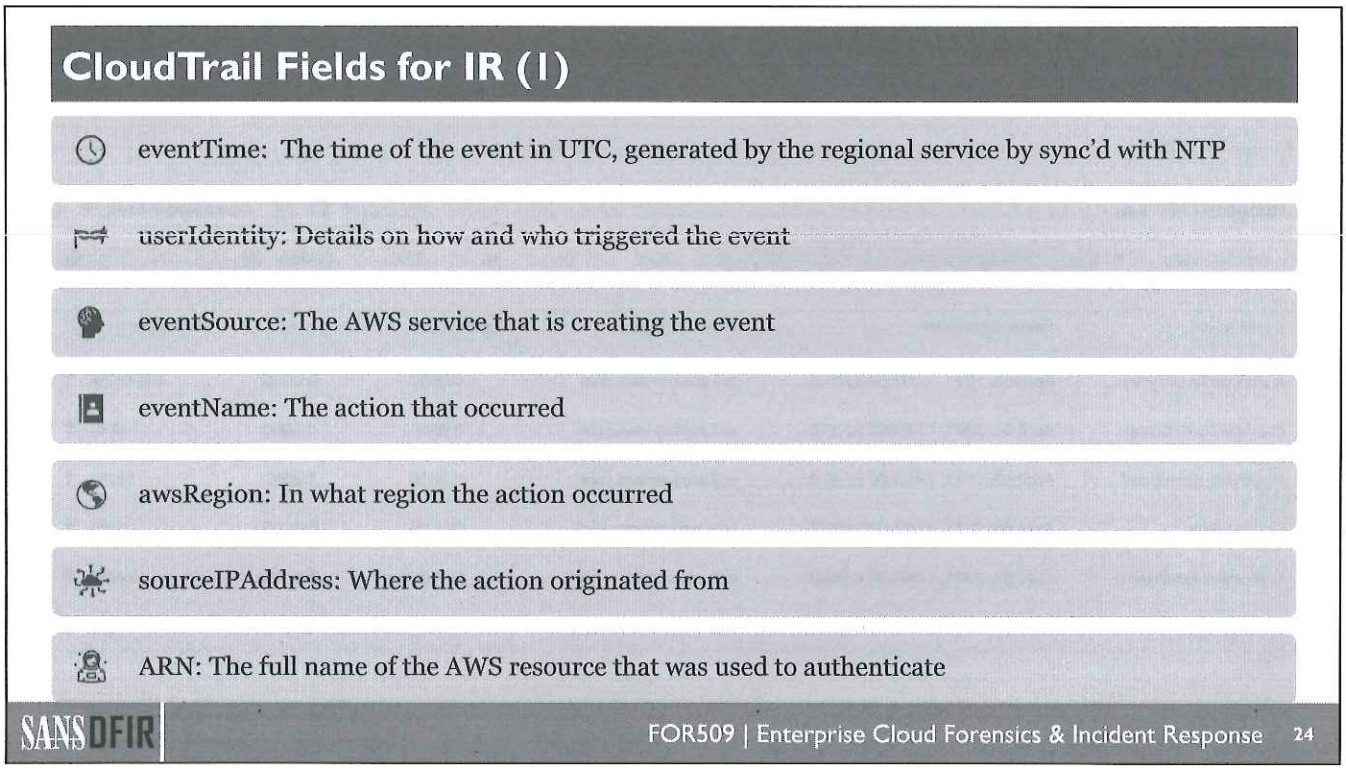
This page intentionally left blank.



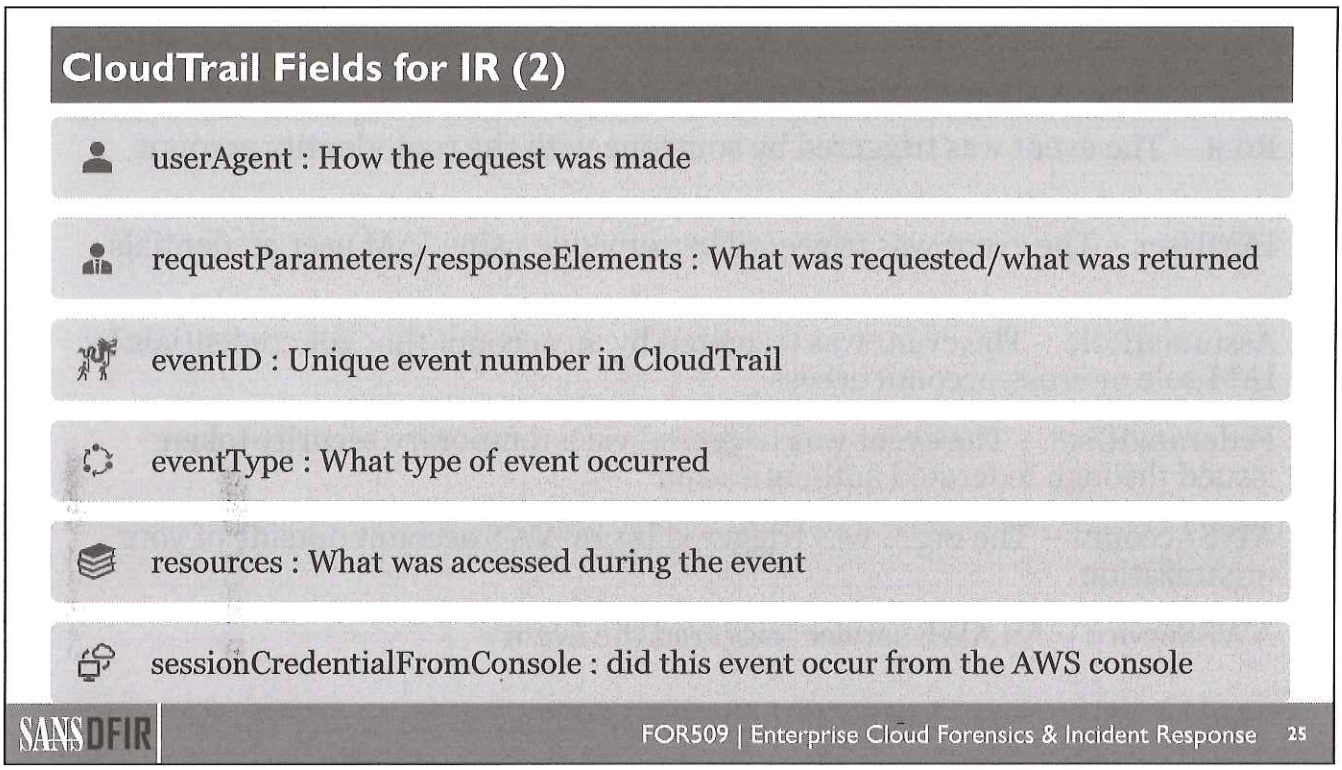
This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.

CloudTrail userIdentity Types

Root – The event was triggered by someone with the root identity account

IAMUser – The event was triggered by someone using IAM user credentials

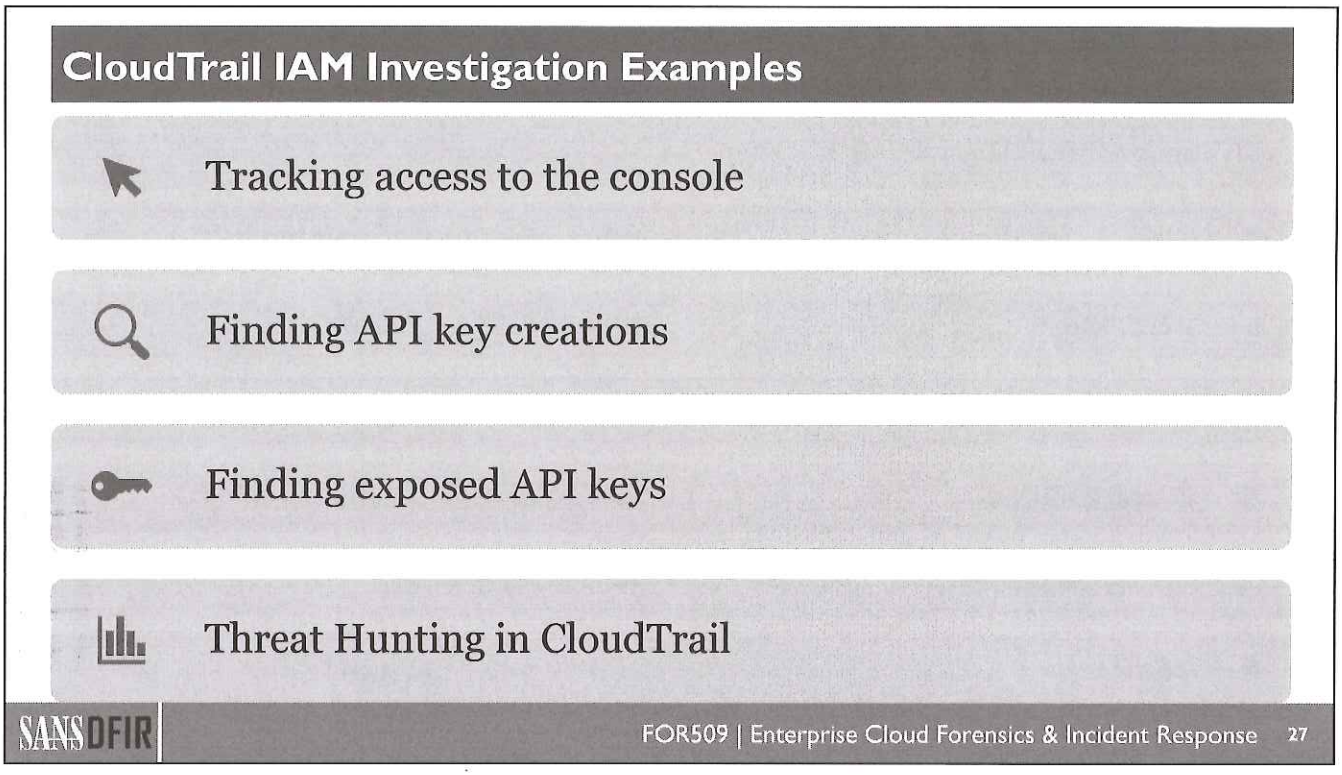
AssumedRole - The event was triggered by an account that got credentials by IAM role or cross-account access

FederatedUser – The event was triggered via a temporary security token issued through federated authentication

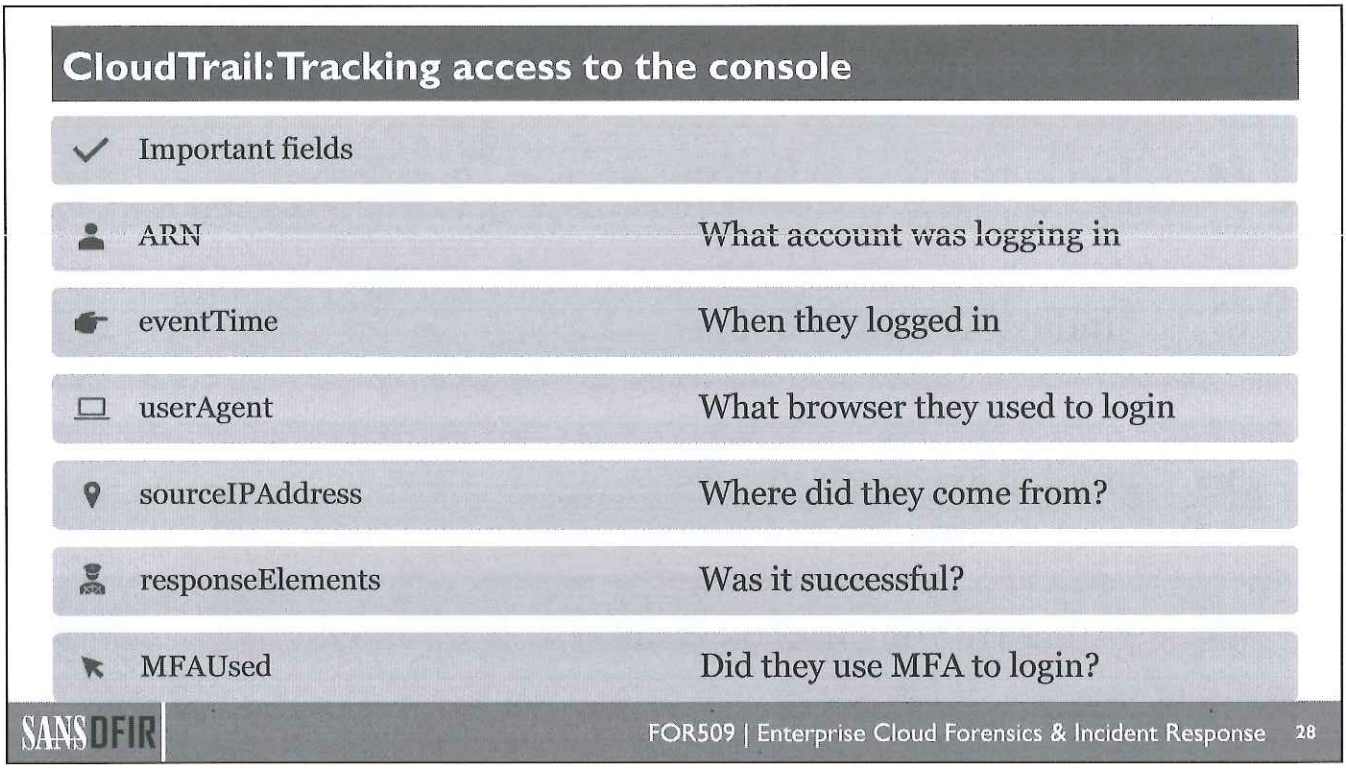
AWSAccount – The event was triggered by an AWS account outside of your organization

AWSService – An AWS service triggered the event

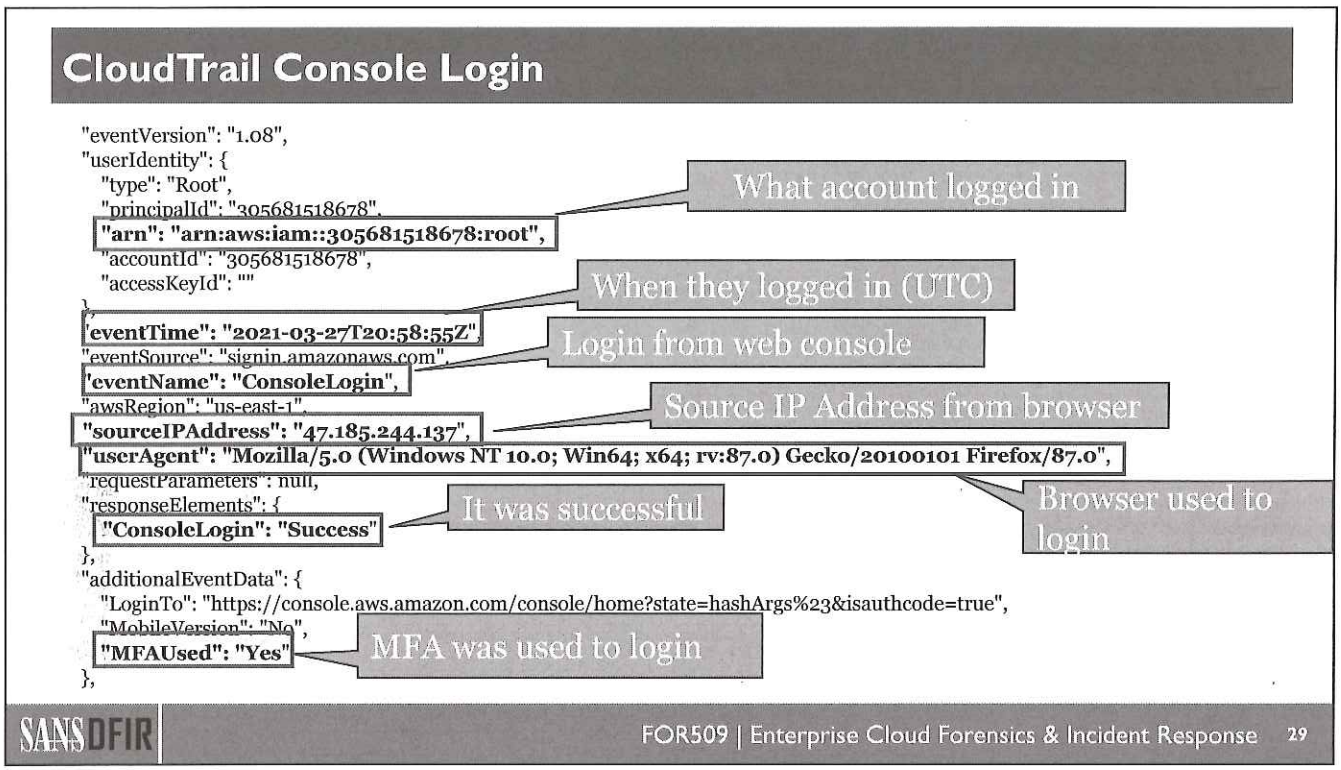
This page intentionally left blank.



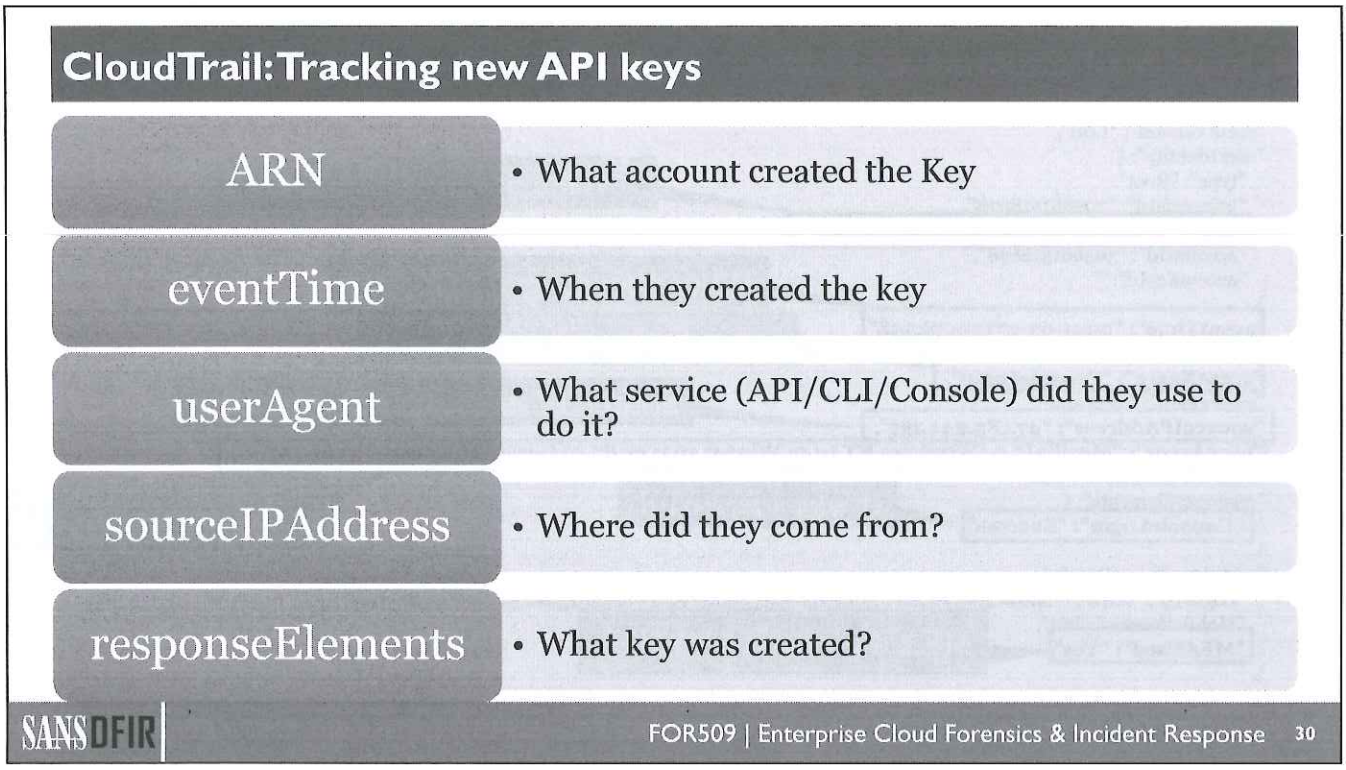
This page intentionally left blank.



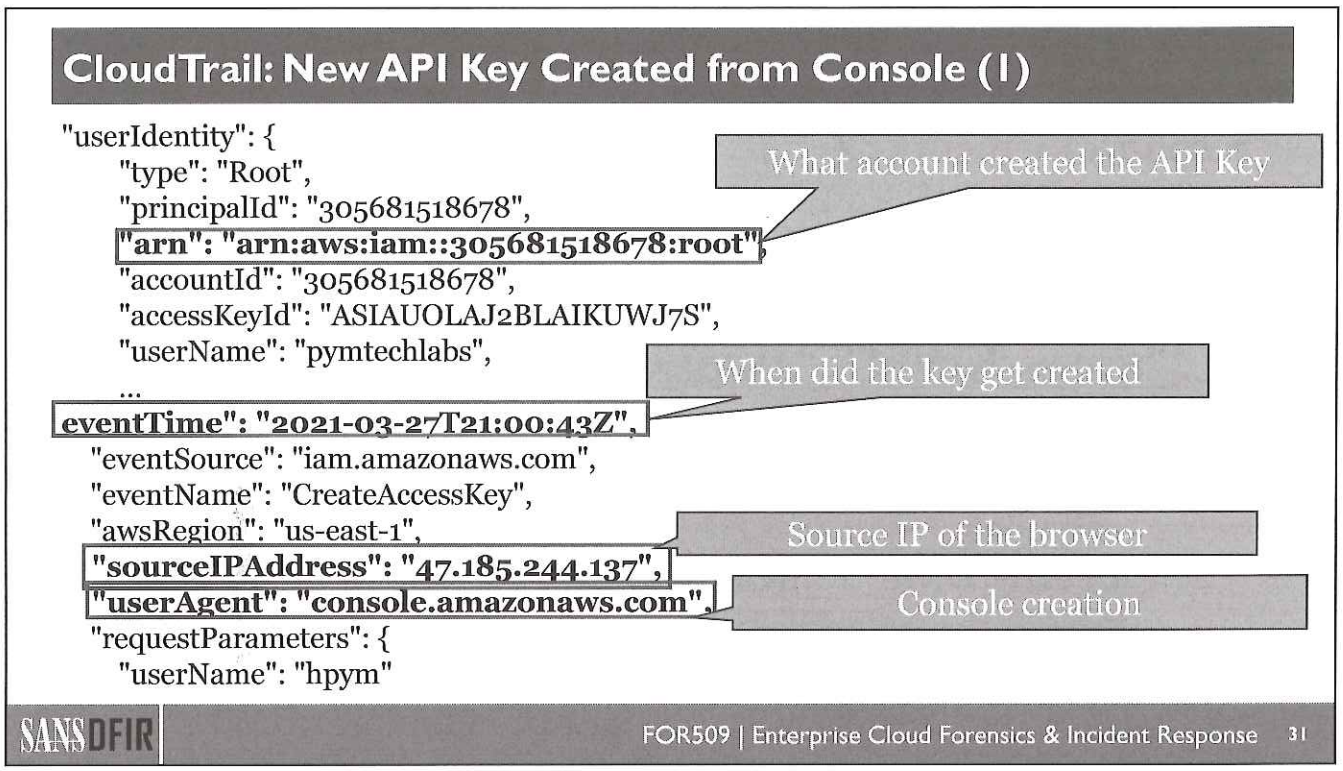
This page intentionally left blank.



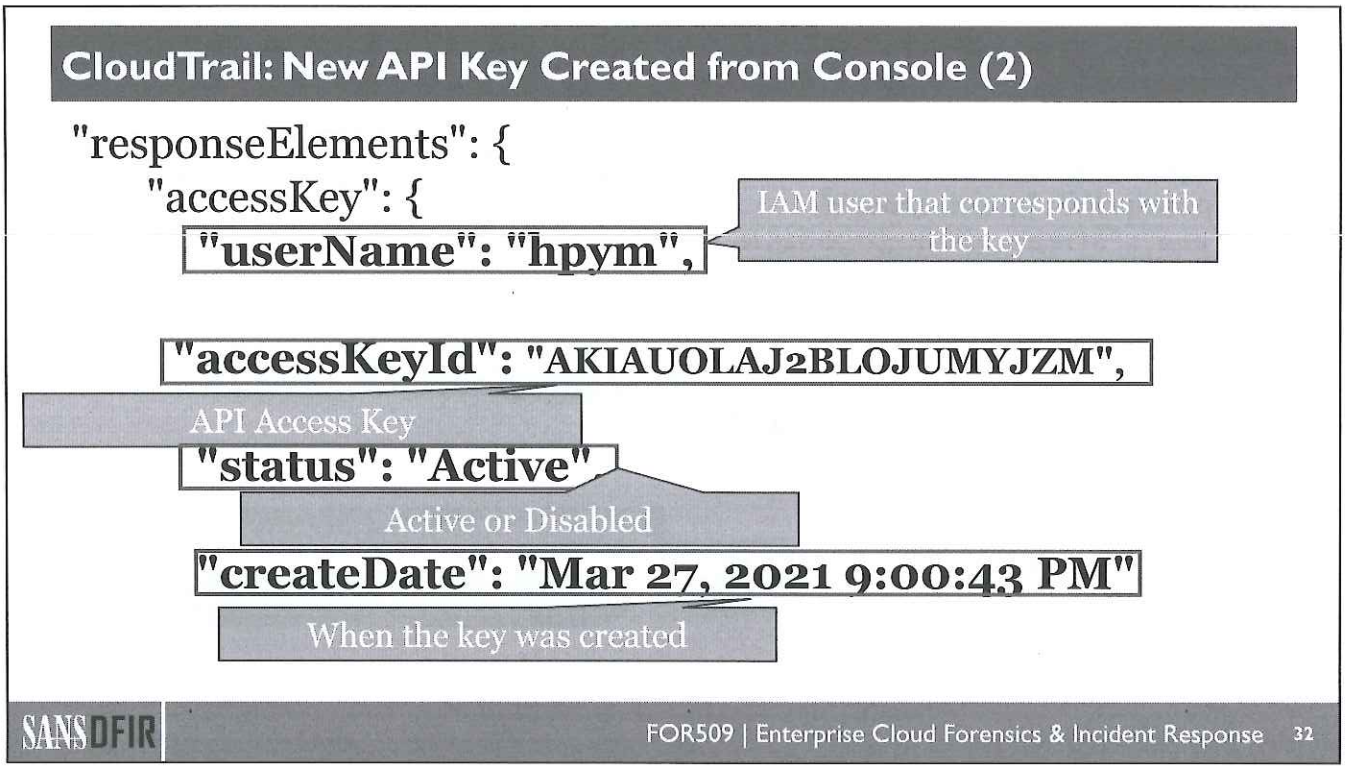
This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.

This page intentionally left blank.

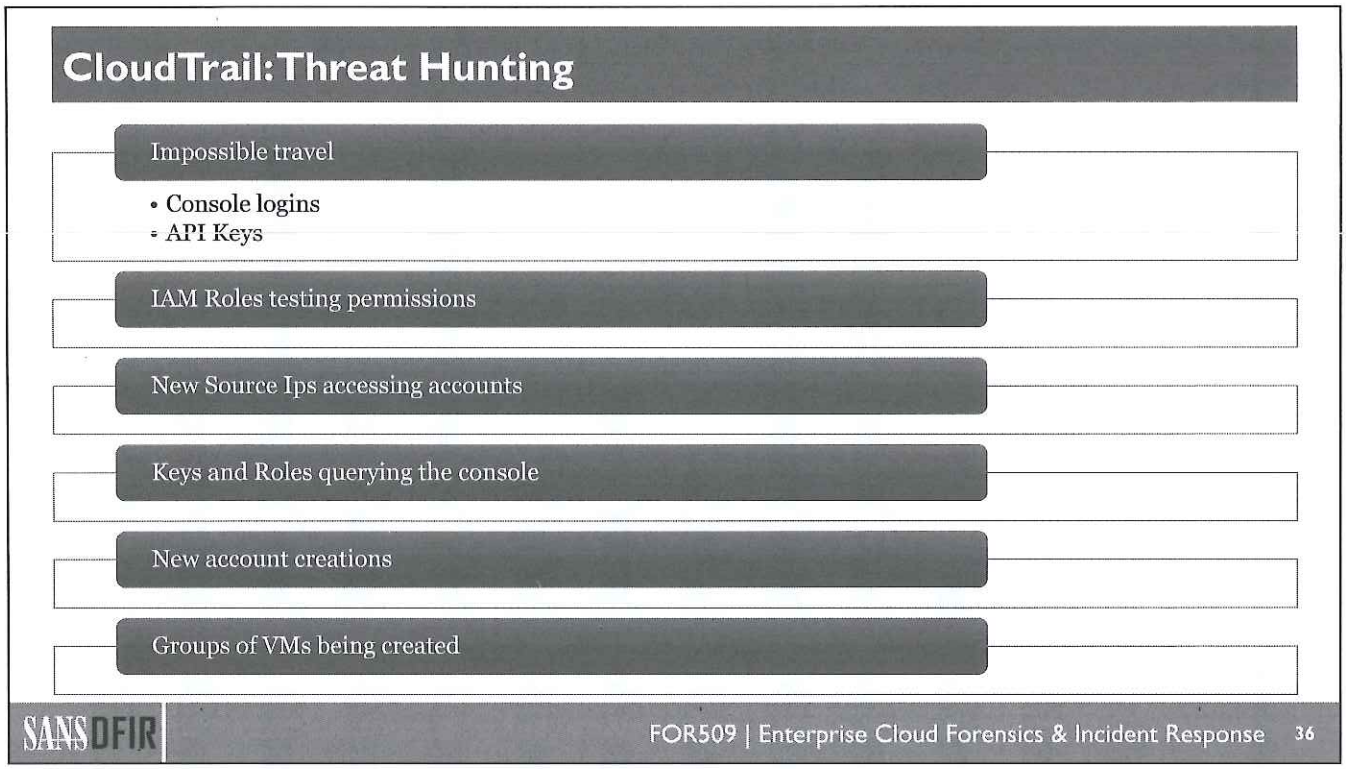
CloudTrail: Finding Exposed API Keys

Role Enumeration

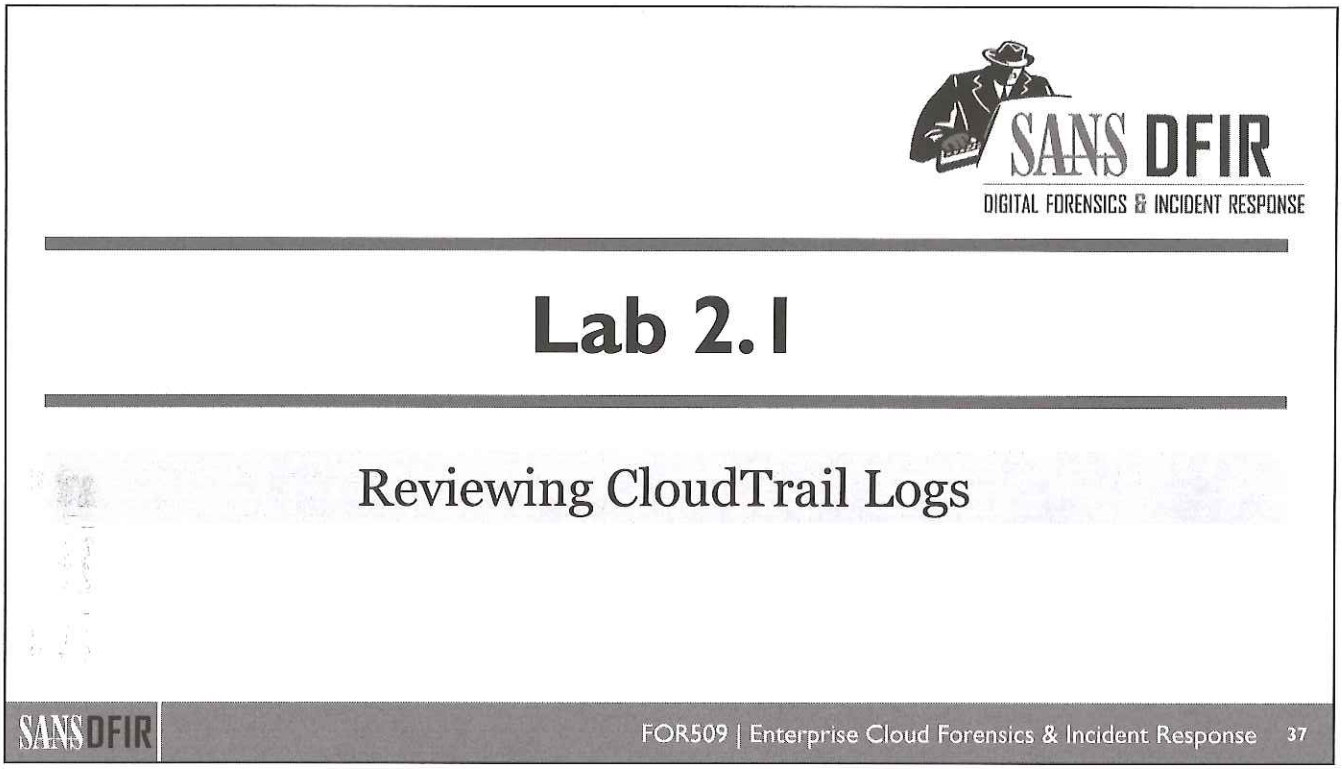
eventtime	eventsource	eventname	sourceipaddress	useragent	requestparameters	eventtype
2021-04-03T18:36:36Z	iam.amazonaws.com	ListRoles	47.185.244.137	aws-cli/2.1.32 Python/3.8.8 Windows/10 exe/AMD64 prompt/off	null	AwsApiCall
2021-04-03T18:43:36Z	iam.amazonaws.com	ListGroupsForUser	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"userName":"hpym"}	AwsApiCall
2021-04-03T18:43:36Z	iam.amazonaws.com	GetUser	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	null	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	GetPolicy	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"policyArn":"arn:aws:iam::aws:policy/AdministratorAccess"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	GetPolicyVersion	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"policyArn":"arn:aws:iam::aws:policy/IAMUserChangePassword","versionId":"v2"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	ListUserPolicies	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"userName":"hpym"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	ListAttachedGroupPolicies	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"groupName":"admin-access"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	ListAttachedUserPolicies	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"userName":"hpym"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	GetPolicyVersion	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"policyArn":"arn:aws:iam::aws:policy/AdministratorAccess","versionId":"v1"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	ListGroupPolicies	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"groupName":"admin-access"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	GetPolicy	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"policyArn":"arn:aws:iam::aws:policy/IAMUserChangePassword"}	AwsApiCall
2021-04-03T18:44:25Z	iam.amazonaws.com	ListAttachedGroupPolicies	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"groupName":"admin-access"}	AwsApiCall
2021-04-03T18:44:25Z	iam.amazonaws.com	ListGroupsForUser	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"userName":"hpym"}	AwsApiCall

This page intentionally left blank.

eventtime	eventsource	eventname	sourceipaddress	useragent	requestparameters	eventtype
2021-04-03T18:36:36Z	iam.amazonaws.com	ListRoles	47.185.244.137	aws-cli/2.1.32 Python/3.8.8 Windows/10 exe/AMD64 prompt/off cmd/null		AwsApiCall
2021-04-03T18:43:36Z	iam.amazonaws.com	ListGroupsForUser	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"userName":"hpym"}	AwsApiCall
2021-04-03T18:43:36Z	iam.amazonaws.com	GetUser	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	null	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	GetPolicy	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"policyArn":"arn:aws:iam::aws:policy/AdministratorAccess"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	GetPolicyVersion	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"policyArn":"arn:aws:iam::aws:policy/IAMUserChangePassword","versionId":"v2"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	ListUserPolicies	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"userName":"hpym"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	ListAttachedGroupPolicies	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"groupName":"admin-access"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	ListAttachedUserPolicies	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"userName":"hpym"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	GetPolicyVersion	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"policyArn":"arn:aws:iam::aws:policy/AdministratorAccess","versionId":"v1"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	ListGroupPolicies	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"groupName":"admin-access"}	AwsApiCall
2021-04-03T18:43:37Z	iam.amazonaws.com	GetPolicy	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"policyArn":"arn:aws:iam::aws:policy/IAMUserChangePassword"}	AwsApiCall
2021-04-03T18:44:25Z	iam.amazonaws.com	ListAttachedGroupPolicies	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"groupName":"admin-access"}	AwsApiCall
2021-04-03T18:44:25Z	iam.amazonaws.com	ListGroupsForUser	47.185.244.137	Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44	{"userName":"hpym"}	AwsApiCall



This page intentionally left blank.



This page intentionally left blank.

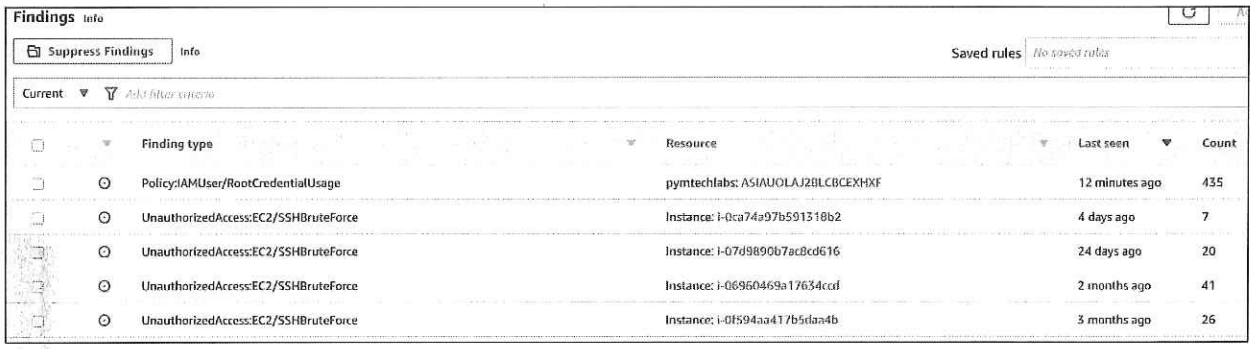
Guard Duty (1)

Now that you've learned how to manually review CloudTrail logs, don't you wish there was an easier way to find that likely threat?

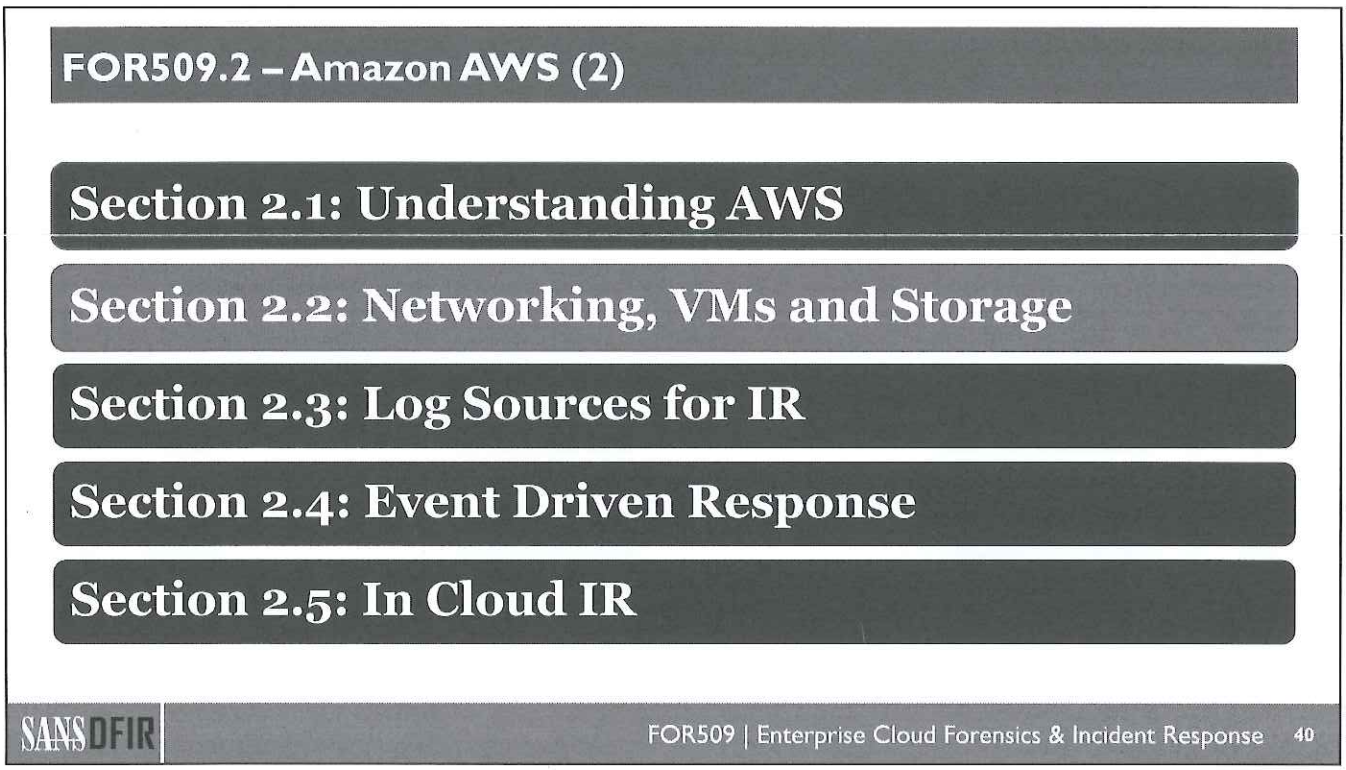
Enter Guard Duty!

This page intentionally left blank.

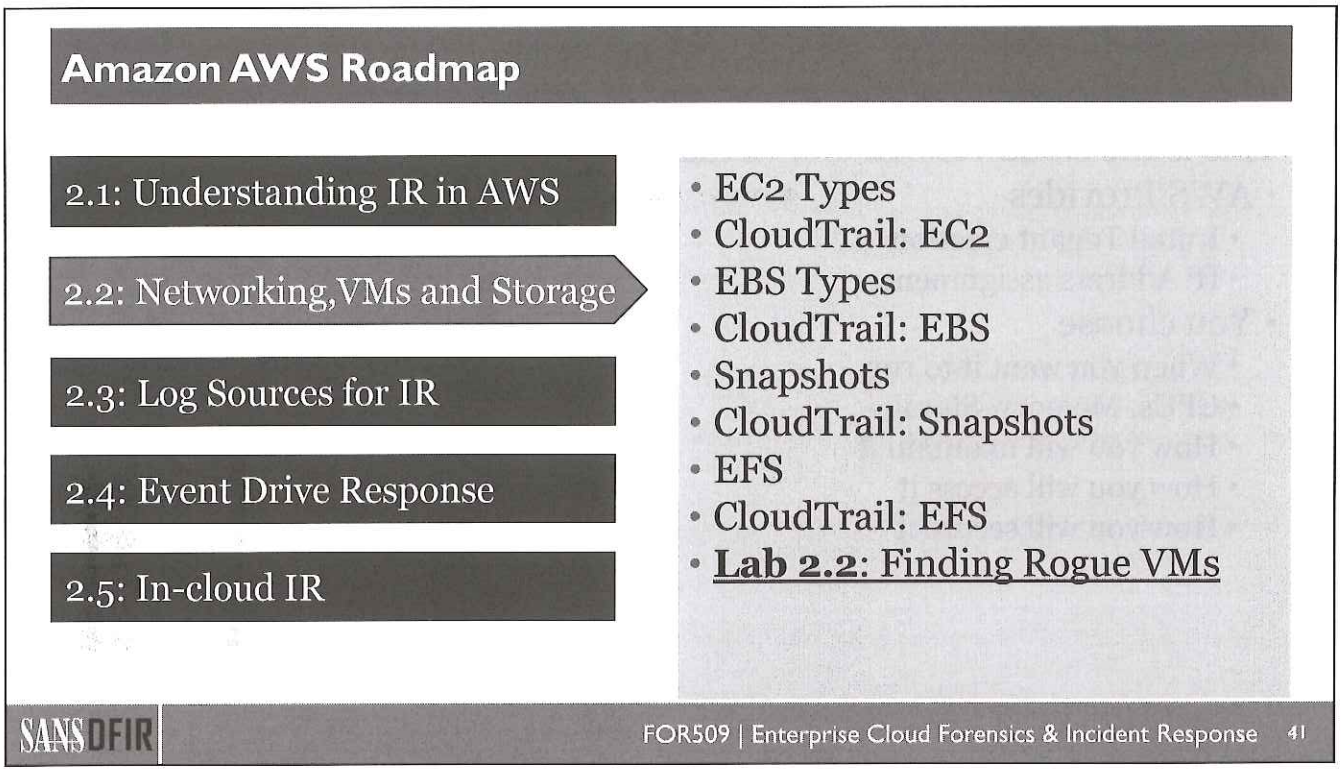
Guard Duty (2)



This page intentionally left blank.



This page intentionally left blank.

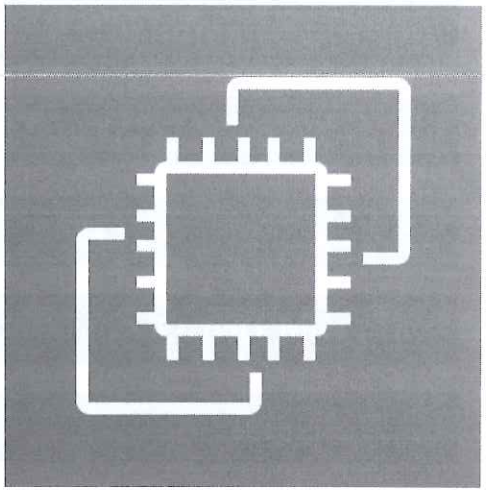


This page intentionally left blank.

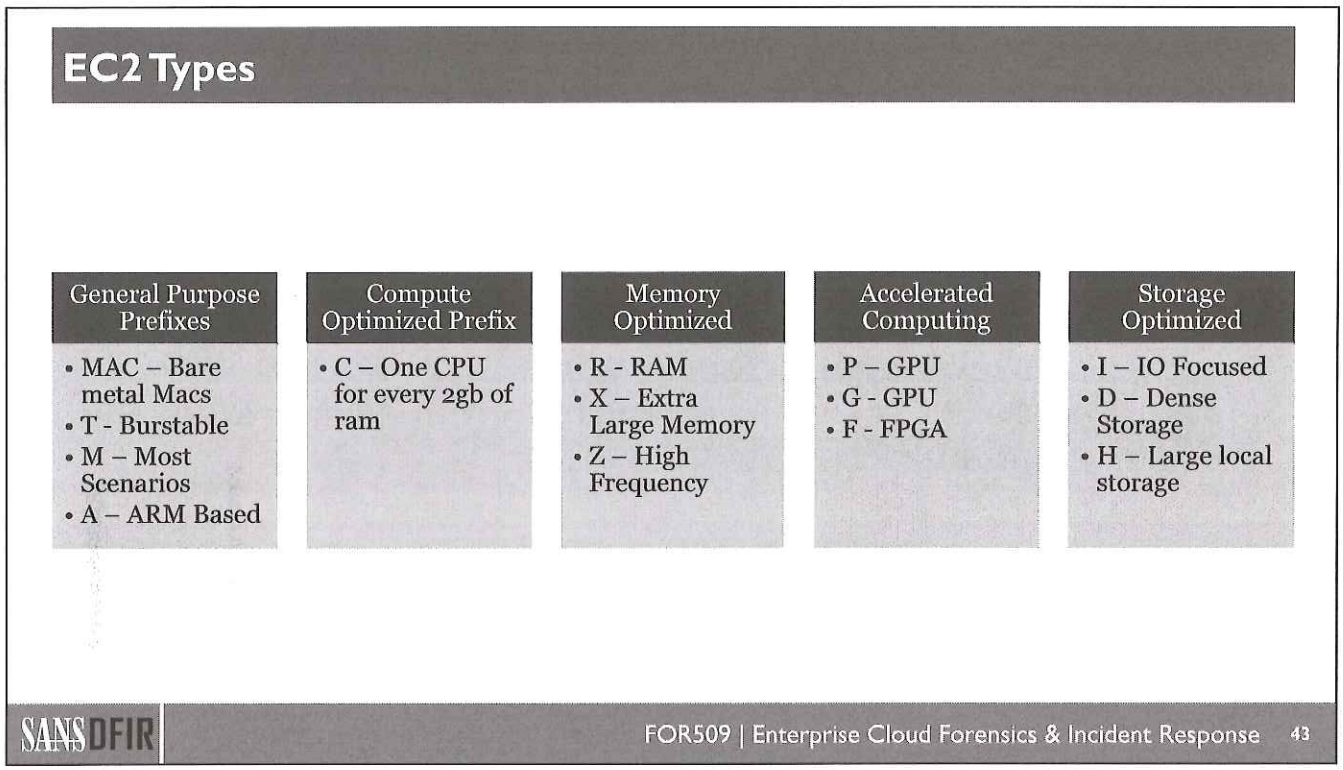
EC2 – Elastic Compute Cloud

This is the cloud version of a virtual machine

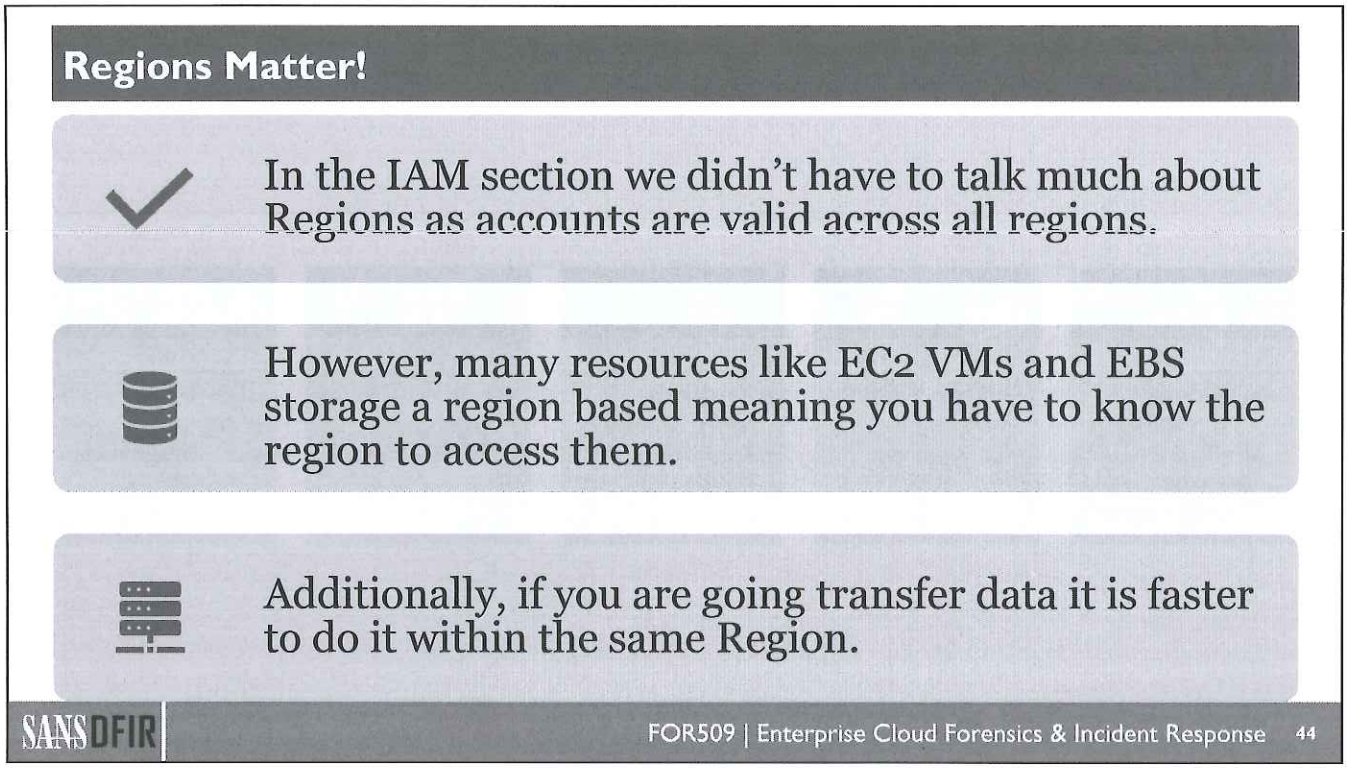
- AWS Provides
  - Initial Tenant creation
  - IP Address assignment
- You choose
  - When you want it to run
  - CPUs, Memory, Storage
  - How you will maintain it
  - How you will access it
  - How you will secure it



This page intentionally left blank.

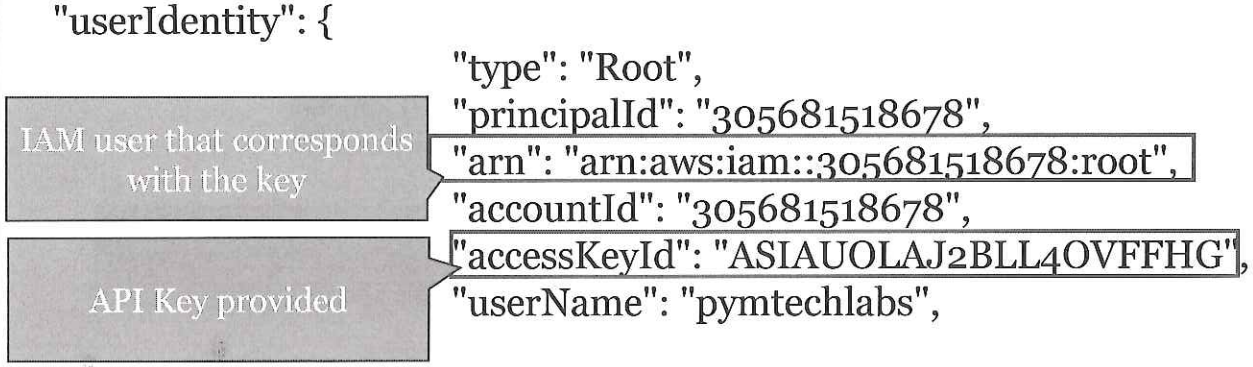


This page intentionally left blank.

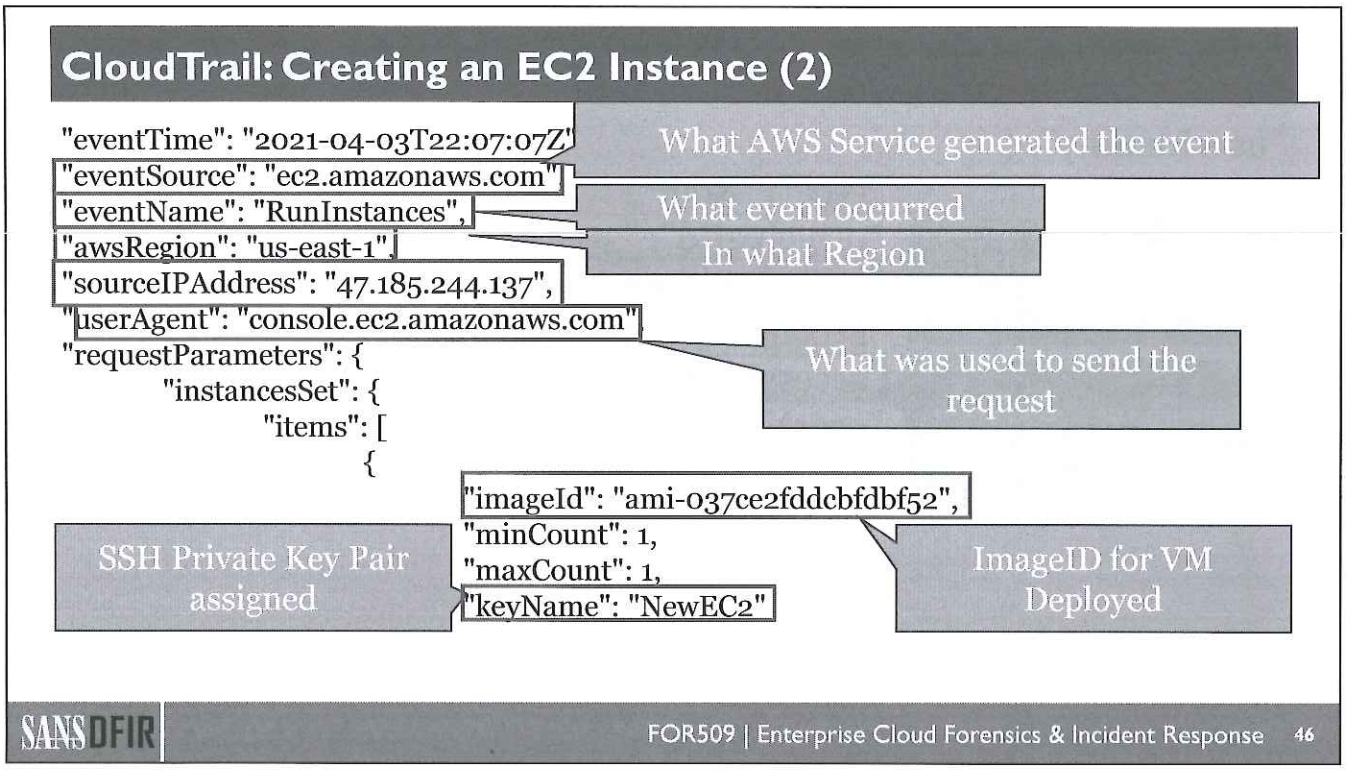


This page intentionally left blank.

CloudTrail: Creating an EC2 Instance (1)



This page intentionally left blank.



This page intentionally left blank.

CloudTrail: Creating an EC2 Instance (3)


```
"attributes": {
                "mfaAuthenticated": "true",
                "creationDate": "2021-04-01T12:03:50Z"
                        "groupSet": {
                                "items": [
                                        {
                                        "groupId": "sg-00b98f2f5d3339900"
                                        },
                                        {
                                        "groupId": "sg-044c410b2327cc21f"
                                        }
                                        ]
                                },
                "userData": "<sensitiveDataRemoved>",
                "instanceType": "t2.micro",
```


The type of EC2 VM that was created

This page intentionally left blank.

CloudTrail: Creating an EC2 Instance with GPU

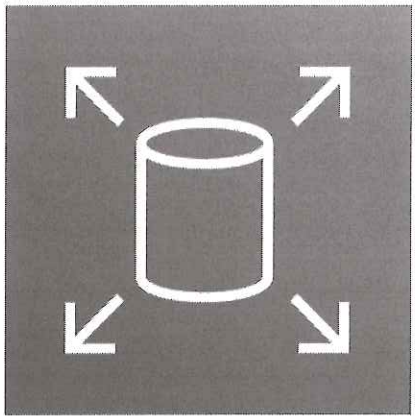

```
"attributes": {
                    "mfaAuthenticated": "true",
                    "creationDate": "2021-04-03T18:03:51Z"
                        "groupSet": {
                "items": [
                    {
                        "groupId": "sg-00b98f2f5d3339900"
                    },
                    {
                        "groupId": "sg-044c410b2327cc21f"
                    }
                ]
            },
            "userData": "<sensitiveDataRemoved>",
            "instanceType": "g4ad.4xlarge",
```


A GPU Enabled VM was created

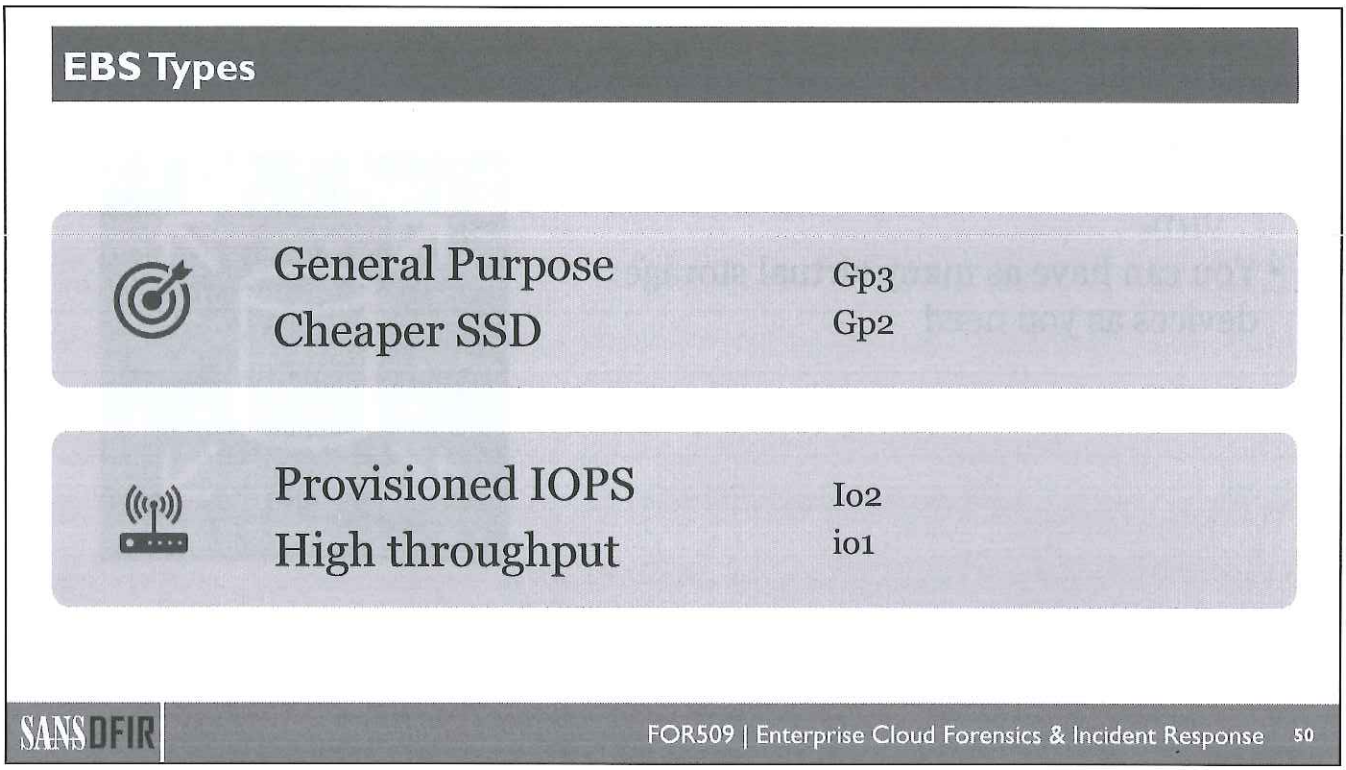
This page intentionally left blank.

EBS – Elastic Block Store

- Virtual Storage for EC2
  - In virtual machine terms – VMDKs, VDIs, VHDs
- You can have as many virtual storage devices as you need

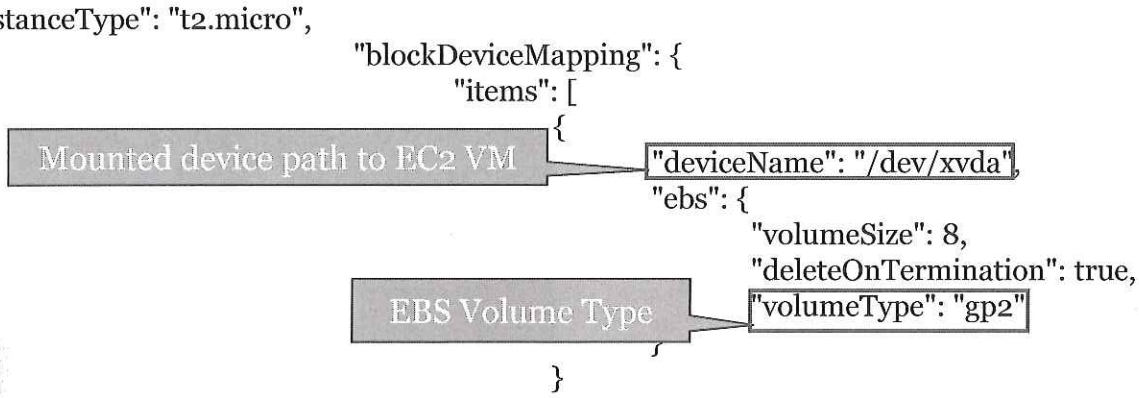


This page intentionally left blank.



This page intentionally left blank.

CloudTrail: Creation of EBS



This page intentionally left blank.

Snapshots

- Creates a disk image of the current state of the disk through the hypervisor
- First snapshot contains all data
- Subsequent snapshots only contain differences on a per block basis
- Copying snapshots between regions will get hit with a data transfer charge ($.01 - $.02 per GC)

This page intentionally left blank.

Snapshot Pricing

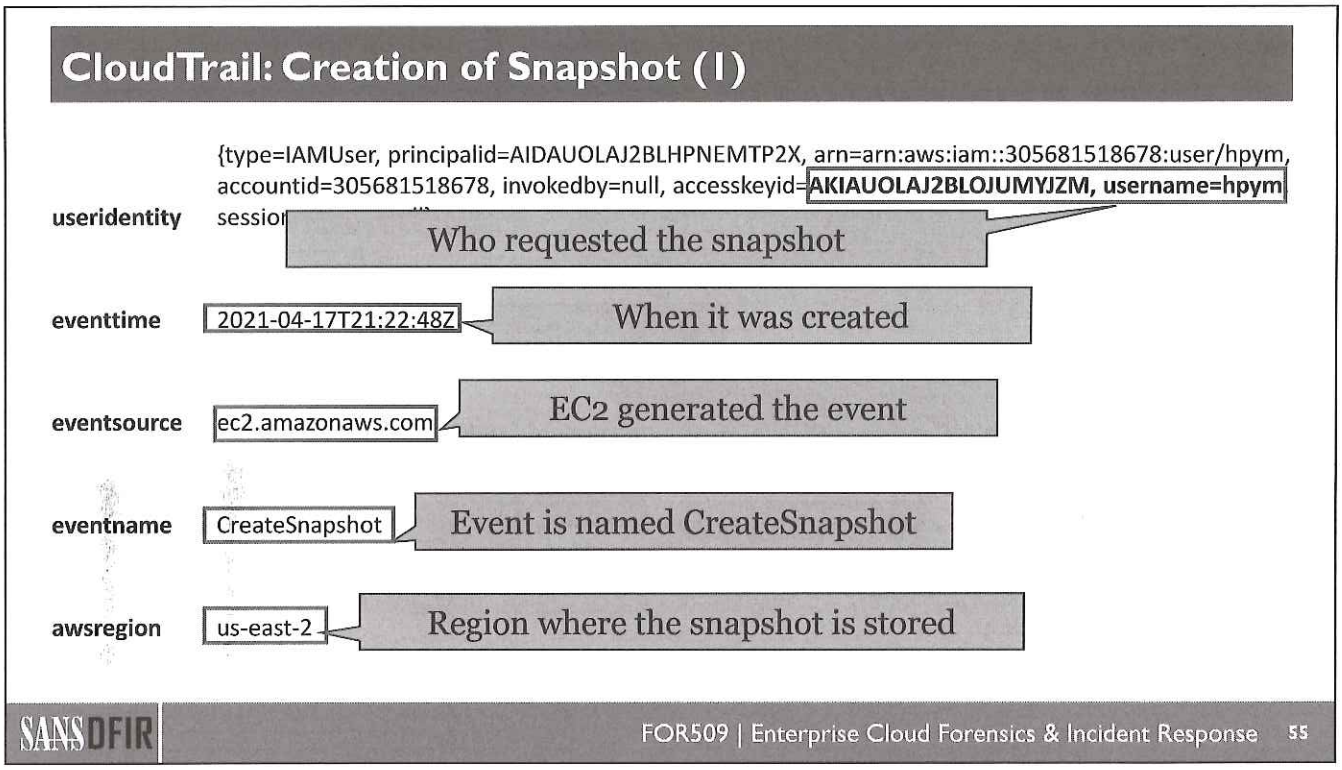
- Storage – Storage is charged on total space allocated, free space is not included
  - Free Tier
    - 1GB of snapshot storage
  - Paid Tier
    - $.05 GB/month of data sored
- Fast Snapshot Restoration
  - $.75 per 1 DSU hour (Data Service Hours)
- Direct Block Access
  - List Blocks - $.0006 per thousand requests
  - Get Blocks - $.003 per thousand units
  - Put Blocks -$.006 per thousand units

This page intentionally left blank.

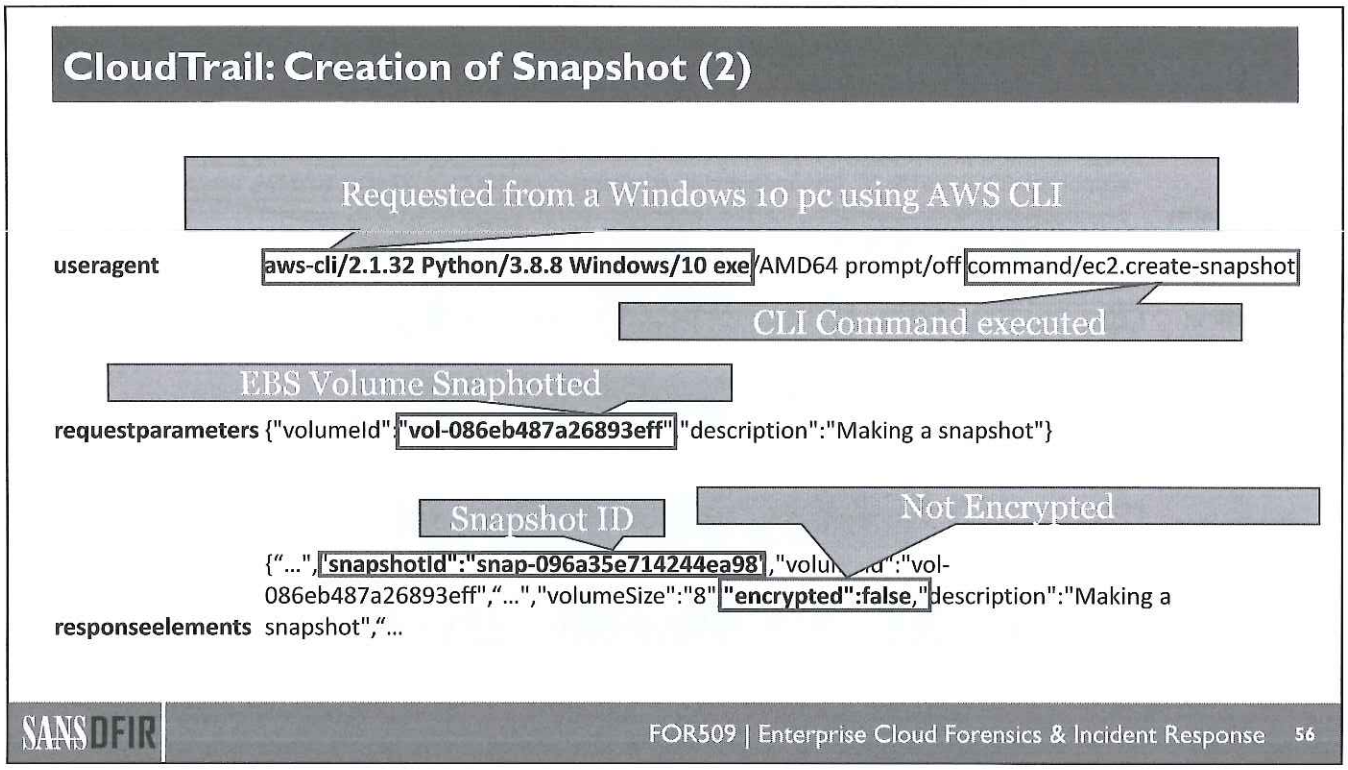
Making a snapshot with the CLI

```
aws ec2 create-snapshot --volume-id <volumeid>
     --description "Making a snapshot"
{
    "Description": "Making a snapshot",
    "Encrypted": false,
    "OwnerId": "305681518678",
    "Progress": "",
    "SnapshotId": "snap-096a35e714244ea98",
    "StartTime": "2021-04-17T21:22:48+00:00",
    "State": "pending",
    "VolumeId": "<volumeid>",
    "VolumeSize": 8,
    "Tags": []
}
```

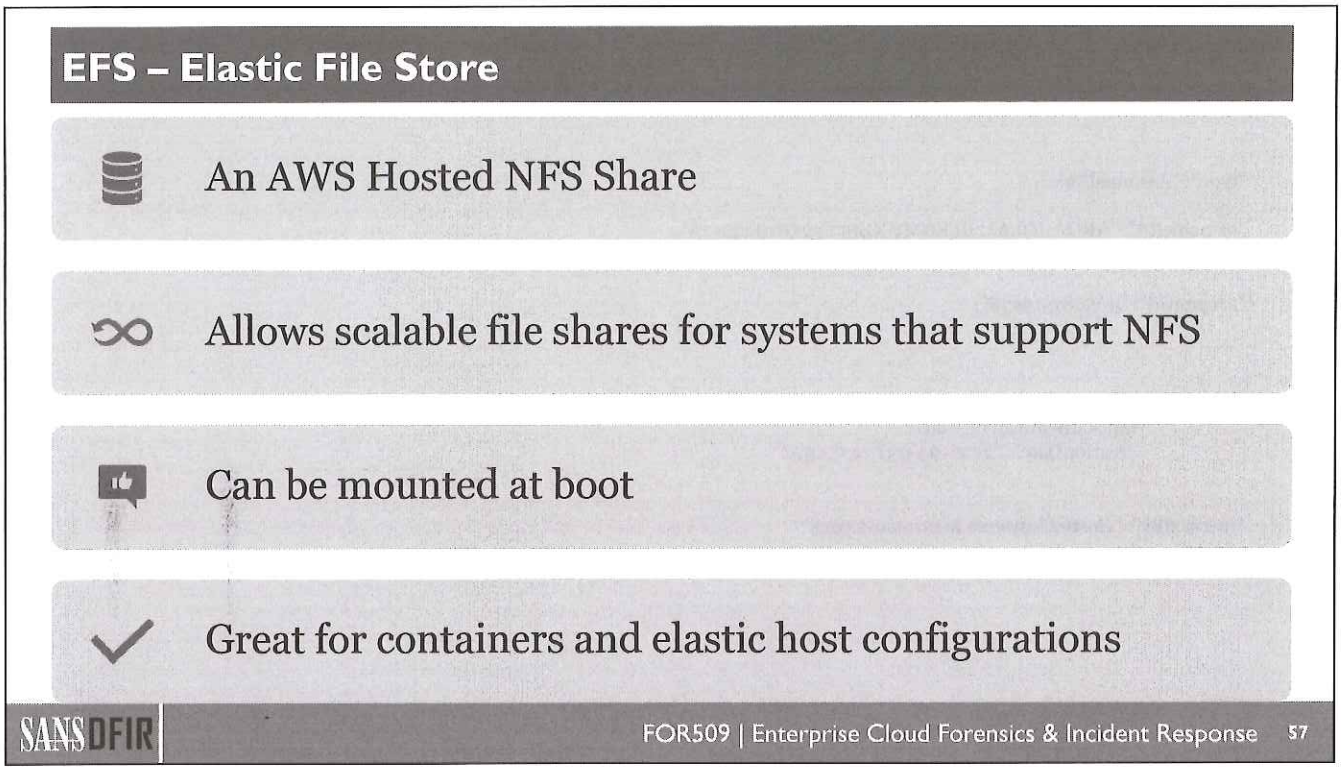

This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.

CloudTrail: Mounting EFS (1)


```
"type": "AssumedRole",

"principalId": "AROAUOLAJ2BLEGMUX2J52:523670242123",
    "arn": "arn:aws:sts::305681518678:assumed-role/AWSServiceRoleForAmazonElasticFileSystem/523670242123",

"accountId": "305681518678",

            ...

"attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2021-04-03T22:03:52Z"
            },

"invokedBy": "elasticfilesystem.amazonaws.com"
```


This page intentionally left blank.

CloudTrail: Mounting EFS (2)

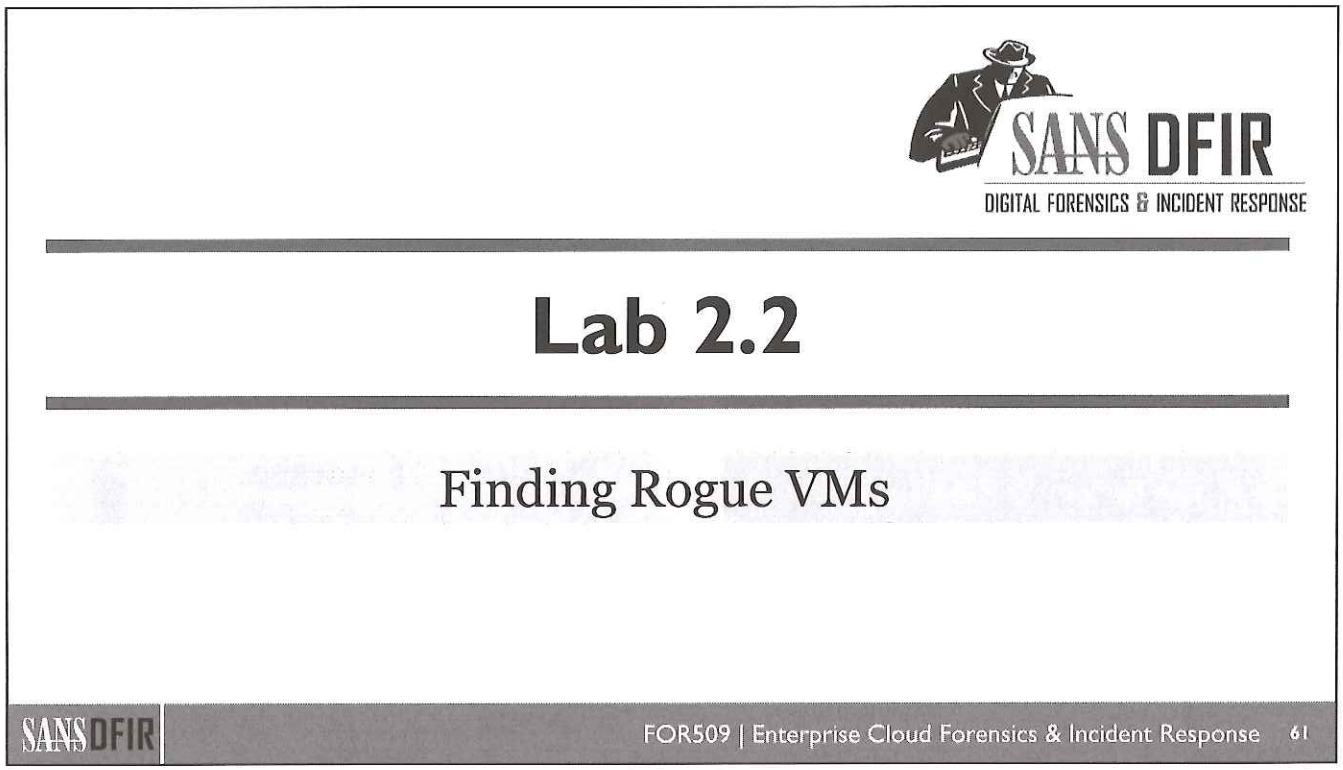

```
},
                "eventTime": "2021-04-03T22:03:53Z",
                "eventSource": "ec2.amazonaws.com",
                "eventName": "CreateNetworkInterface",
                "awsRegion": "us-east-1",
                "sourceIPAddress": "elasticfilesystem.amazonaws.com",
                "userAgent": "elasticfilesystem.amazonaws.com",
                "requestParameters": {
                        "subnetId": "subnet-0fceba79524beb4ed",
                        "description": "EFS mount target for fs-747766c1 (fsmt-7bd116ce)",
                        "groupSet": {},
                        "privateIpAddressesSet": {}
                },
```


This page intentionally left blank.

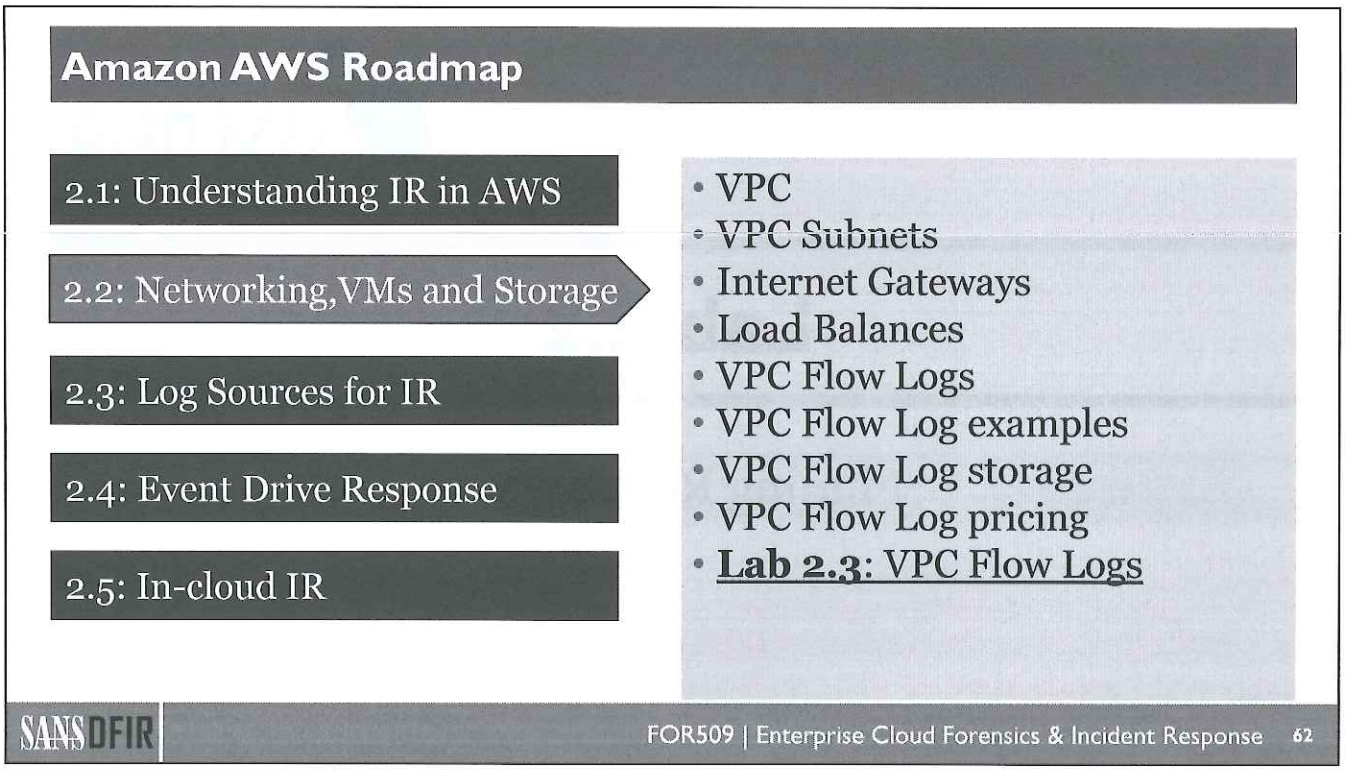
CloudTrail: Mounting EFS (3)


```
"responseElements": {
                        "requestId": "cfcf5ad0-8855-4e27-936d-c4bf6abda234",
                        "networkInterface": {
                                "networkInterfaceId": "eni-0bb4b98b581305086",
                                "subnetId": "subnet-0feeba79524beb4ed",
                                "vpcId": "vpc-09edf30a76f46ad91",
                                "availabilityZone": "us-east-1e",
                                "description": "EFS mount target for fs-747766c1 (fsmt-7bd116ce)",
                                ...
                                "macAddress": "06:62:de:b6:ca:15",
                                "privateIpAddress": "172.31.54.64",
                                "privateDnsName": "ip-172-31-54-64.ec2.internal",
                                "sourceDestCheck": true,
```


This page intentionally left blank.



This page intentionally left blank.

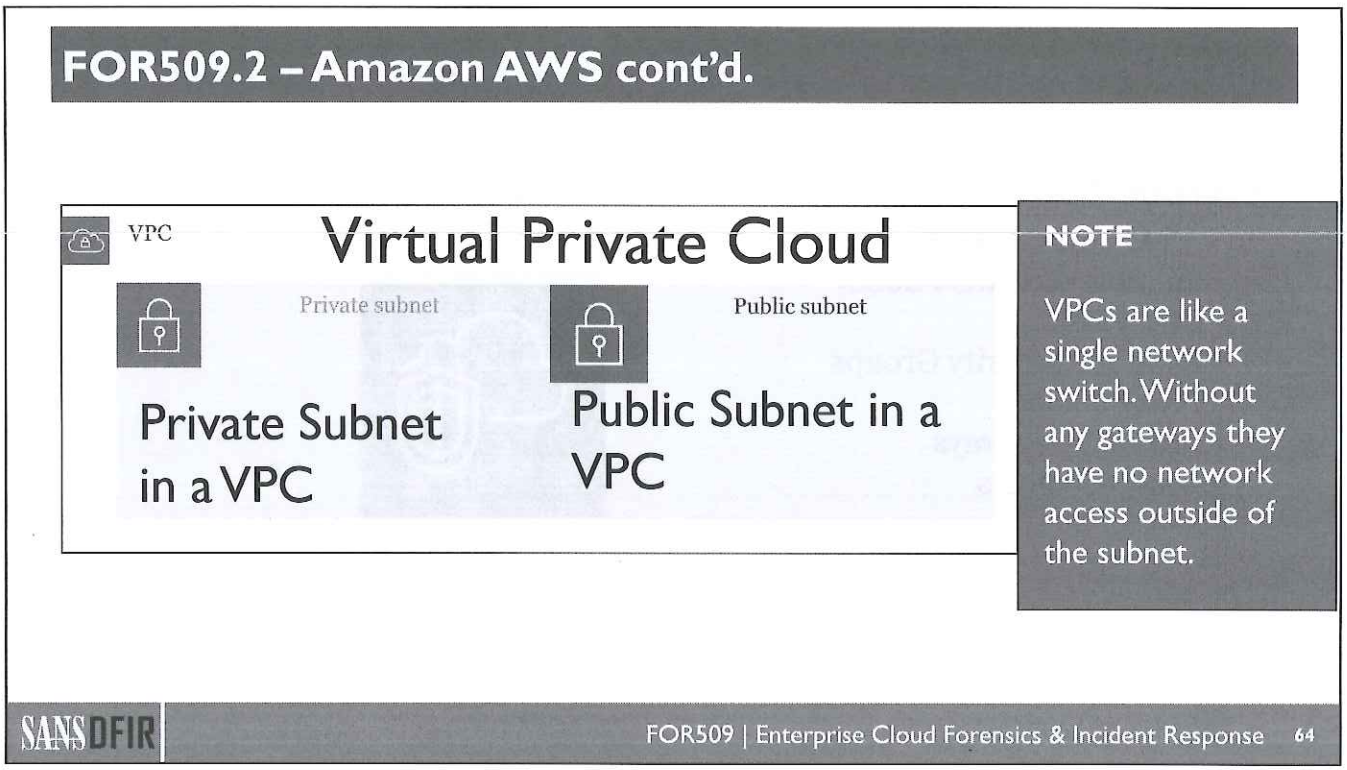


This page intentionally left blank.

Virtual Private Cloud

- A collection of resources grouped into a group
- A VPC can contain
  - Subnets (Private/Public)
  - EC2 VMs
  - Network Security Groups
  - Proxy Servers
  - Internet Gateways
  - Load Balancers

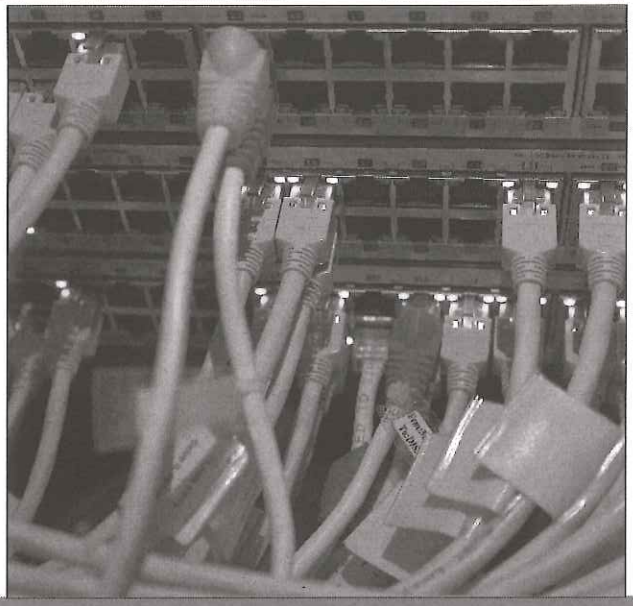
This page intentionally left blank.



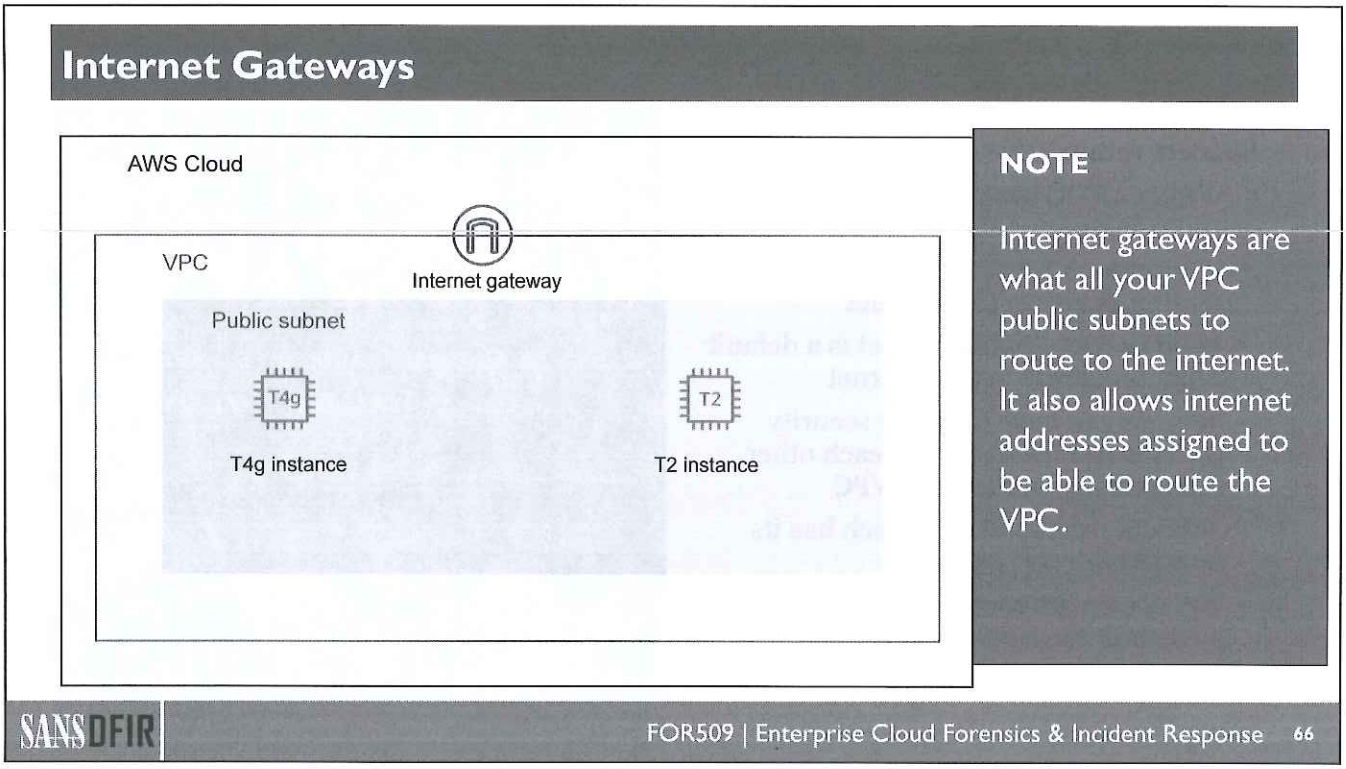
This page intentionally left blank.

VPC Subnets

- Subnets within VPCs
  - Within a VPC you can have both public and private subnets
  - What makes a private subnet is no direct routing ability to the internet
  - What makes a public subnet is a default route that leads to the internet
  - Subnets can have different security policies and features than each other than still live in the same VPC
  - Subnets are like VLANs, each has its own IP address space
  - You can create routes between subnets, by default they are isolated



This page intentionally left blank.



This page intentionally left blank.

AWS Load Balancers

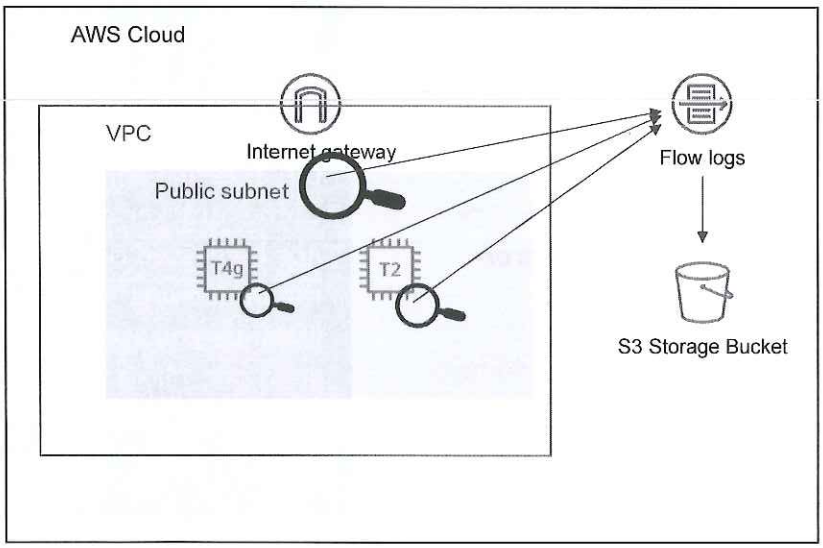
- AWS load balancers work one of four ways:
  - Application load balancer
    - Understands HTTP and can route requests between sets of web servers
  - Classic load balancer
    - Balances traffic by routing traffic based on weights or rotation
  - Network load balancer
    - Balances loads across multiple VPCs

NOTE

If a AWS load balancer is in place the external address of the attacker may not be passed on to the underlying instance you are analyzing. Make sure to get load balancer logs!

This page intentionally left blank.

VPC Flow Logs



NOTE

Flow logs can be enabled at the:

- VPC
- Subnet
- Network interface

They put no load on your network and are collected out of band.

You can enable them at any time.

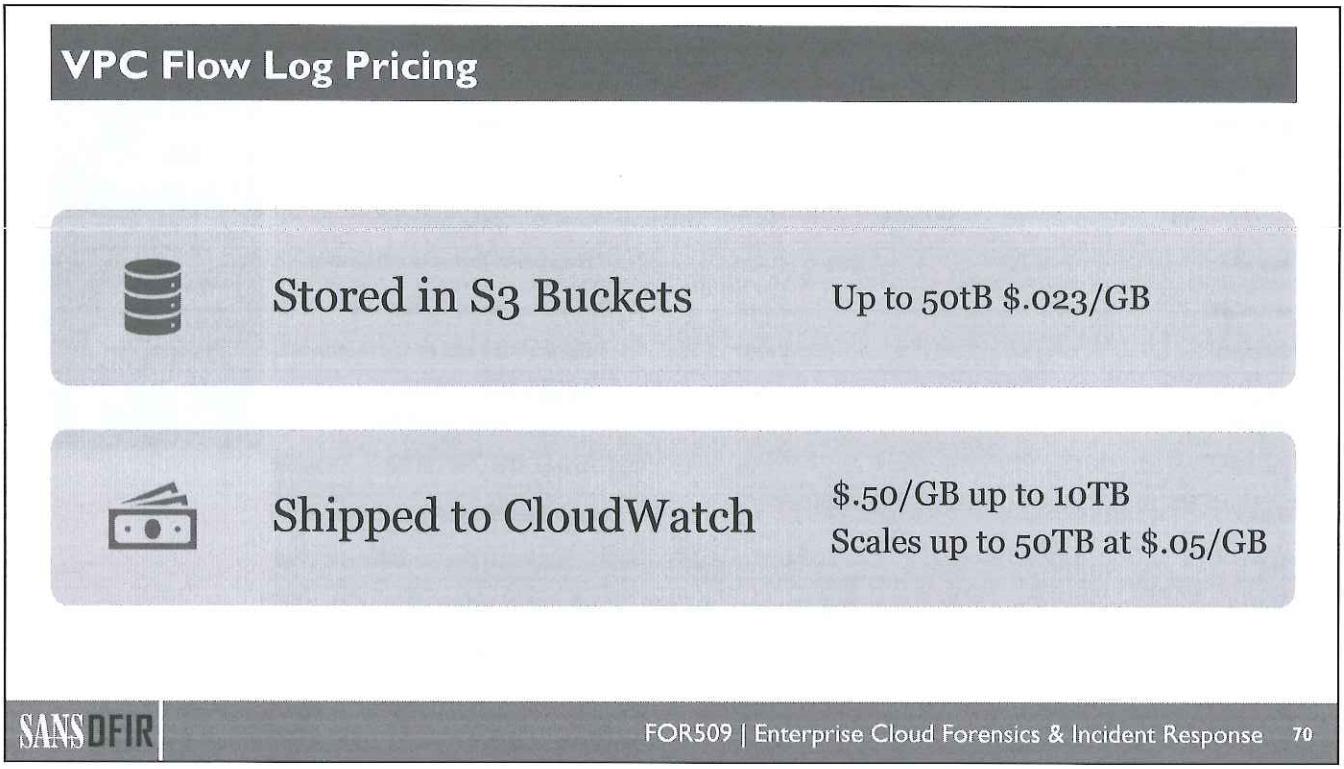
This page intentionally left blank.

VPC Flow Log Examples

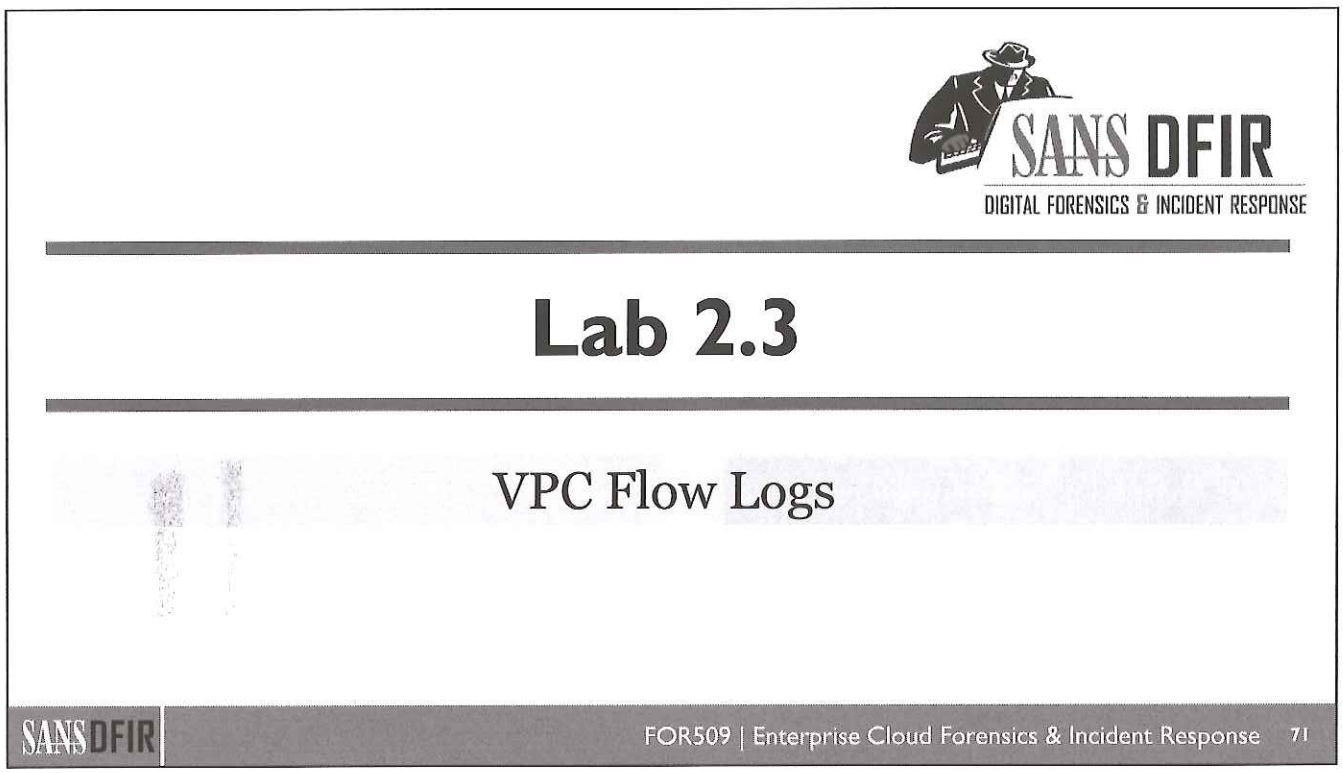
version	*2*	The version of AWS Flow Log
account-id	*305681518678.00*	The AWS Account that this was generated in
interface-id	*eni-06fa0119bda73bdc5*	The virtual network interface that was contacted
srcaddr	*209.17.96.130*	The system that sent the connection
dstaddr	*10.0.2.99*	The system the connection was sent to
dstport	*61087*	The port that was on the destination
srcport	*990*	The port used by the sending system
protocol	*6*	The protocol number in use
packets	*1*	The number of packets in this connection
bytes	*44*	The number of bytes in this connection
start	*1618617647*	A unix time stamp of when this connection started
end	*1618617703*	A unix time stamp of when this connection ended
action	*ACCEPT*	What action the network security group took
log-status	*OK*	OK

NOTE
Flow logs record sessions every 10 minutes by default

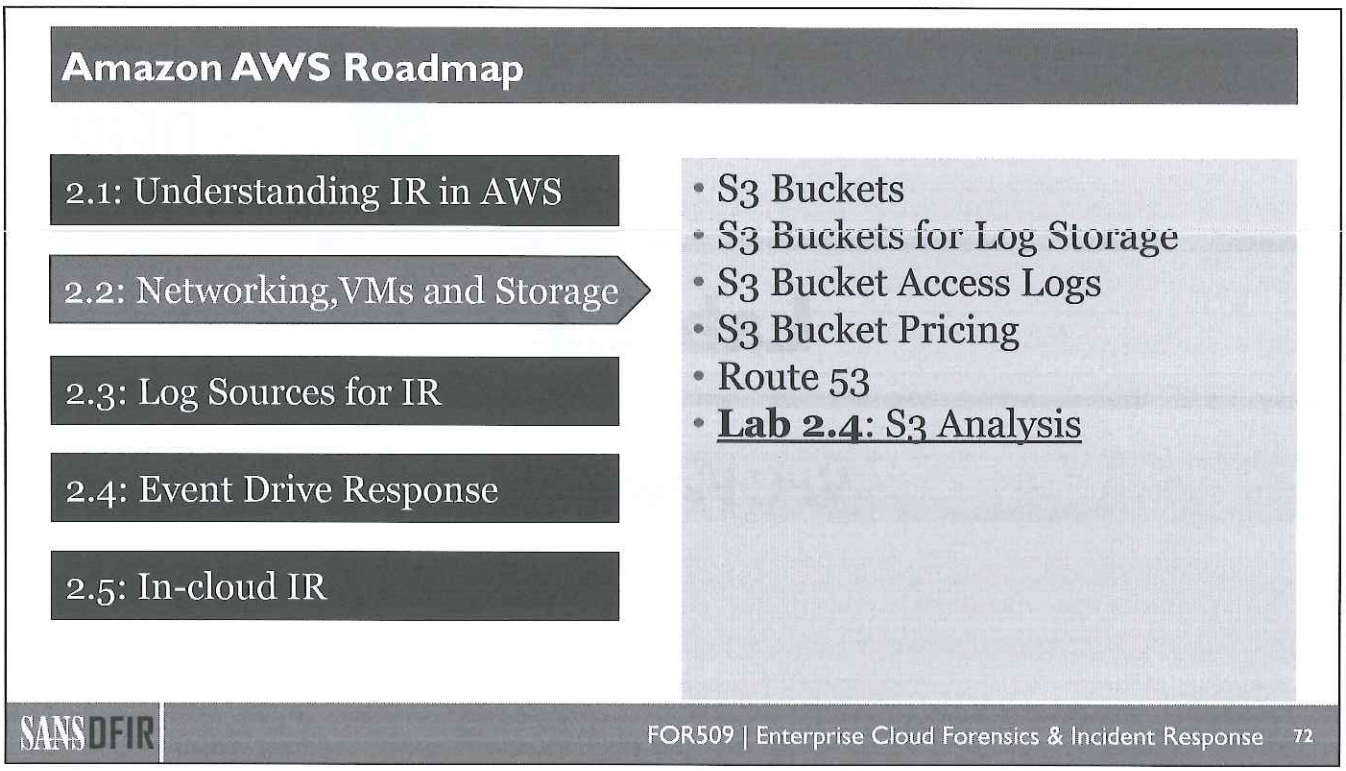
This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.

S3 Buckets

Those things you keep reading about in the news

A file share you can upload to with a web browser

S3 Names are Universal

- That means only one customer can have a s3 bucket name in all of amazon

This page intentionally left blank.

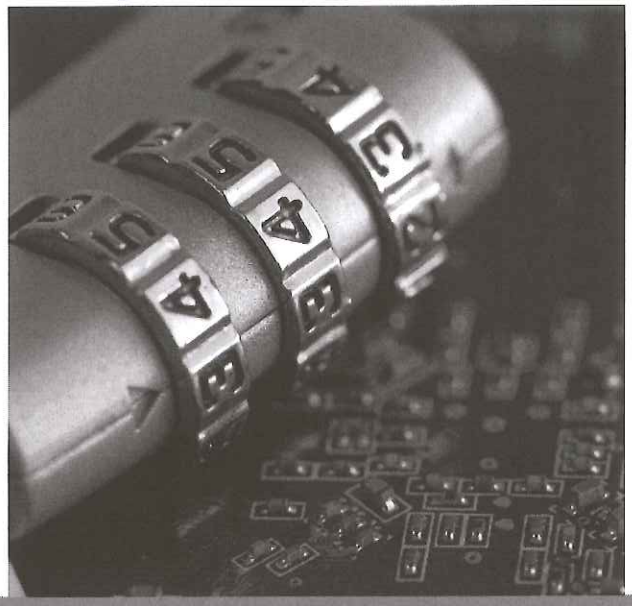
S3 Buckets – Restrictions of access

- Public
  - Anyone can access the contents
- AWS User
  - Any AWS user can access
- Org User
  - A specified user(s) can access the contents
- IAM Roles
  - Specific roles can access the contents
- Tokens in URL strings
  - Anyone with the correct link, in the specified time, can access the contents

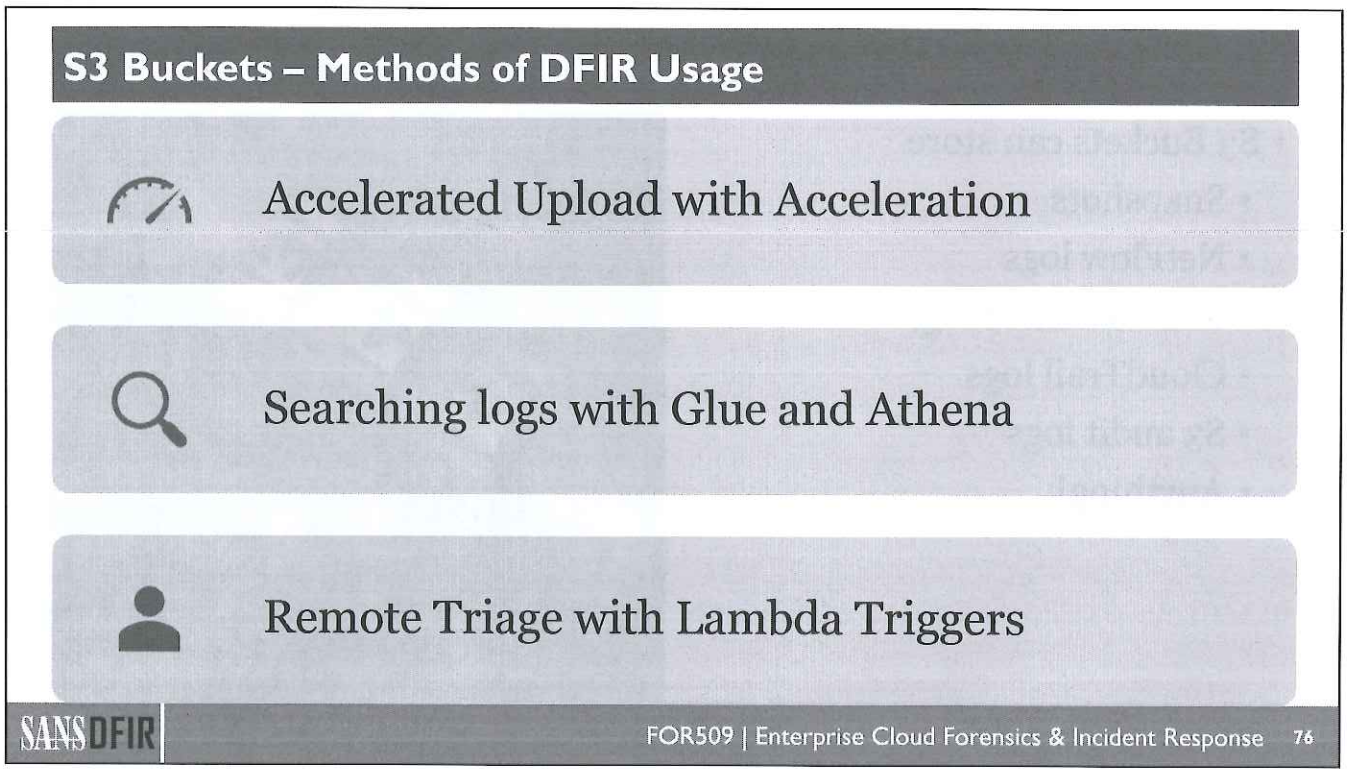
This page intentionally left blank.

S3 Buckets – Cornerstone of AWS IR

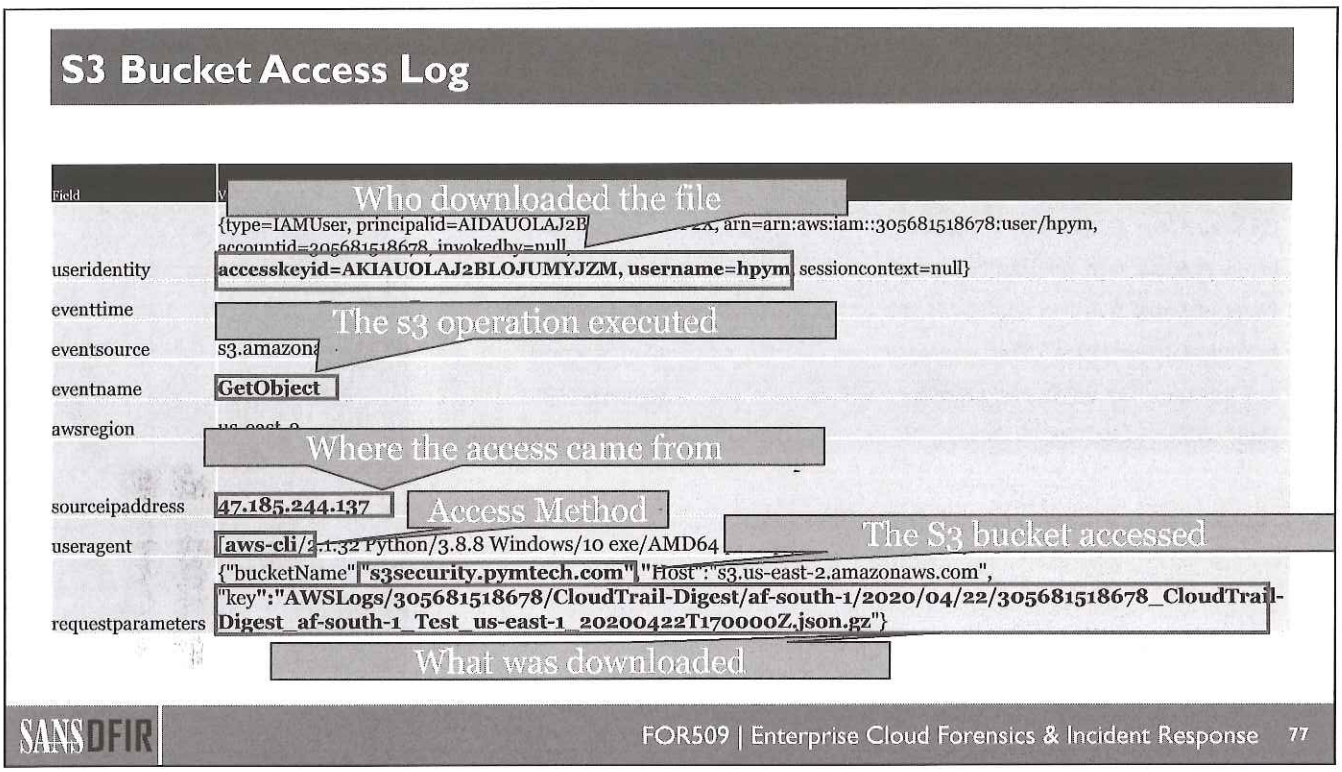
- S3 Buckets can store
  - Snapshots
  - NetFlow logs
  - Load balancer logs
  - CloudTrail logs
  - S3 audit logs
  - Anything!



This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.

S3 Access Log Storage Pricing

S3 Intelligent Tiering	Cost per GB
Frequent Access Tier, First 50 TB / Month	$0.023 per GB
Frequent Access Tier, Next 450 TB / Month	$0.022 per GB
Frequent Access Tier, Over 500 TB / Month	$0.021 per GB
Infrequent Access Tier, All Storage / Month	$0.0125 per GB
Archive Access Tier, All Storage / Month	$0.004 per GB
Deep Archive Access Tier, All Storage / Month	$0.00099 per GB

NOTE
S3 data access logs won't appear in the CloudTrail console.

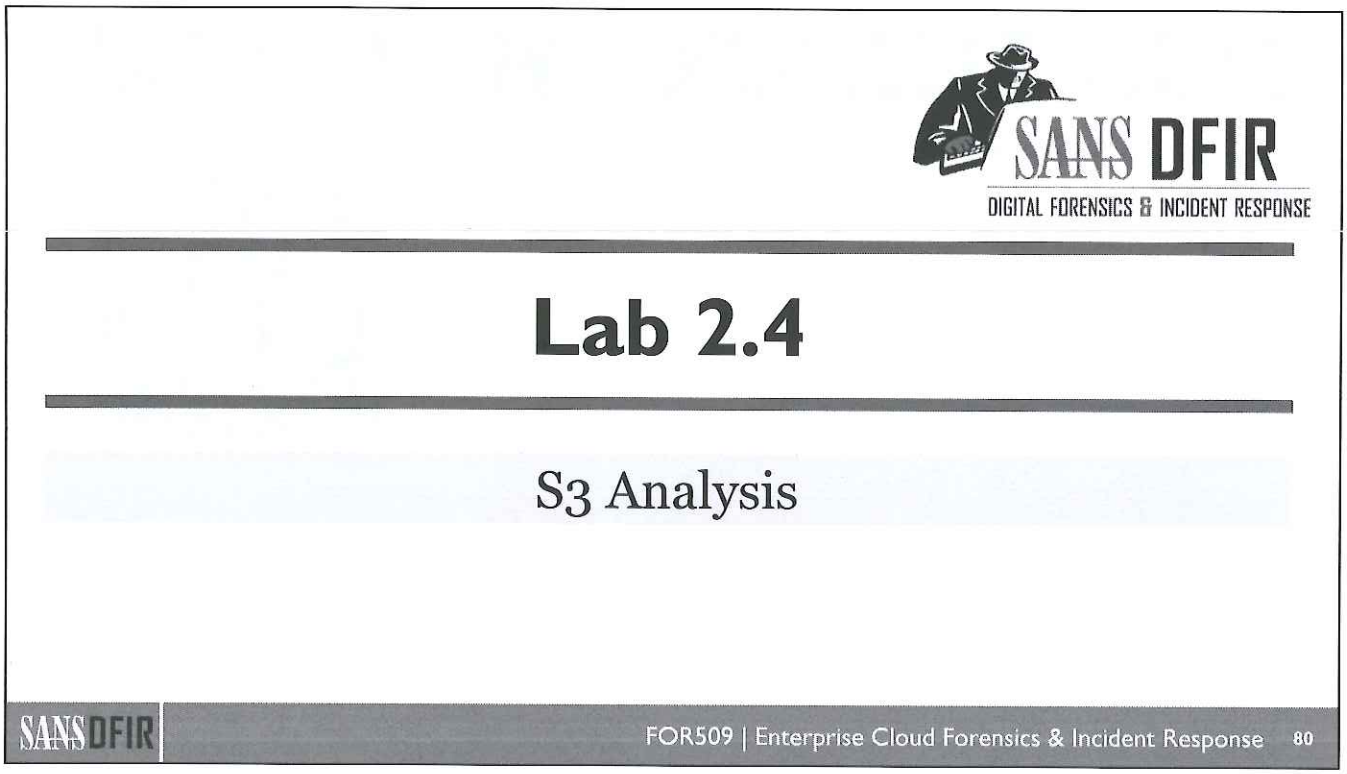
You have to parse the CloudTrail logs in a tool like Athena to view data/object logs. API Events will appear in the CloudTrail console.

This page intentionally left blank.

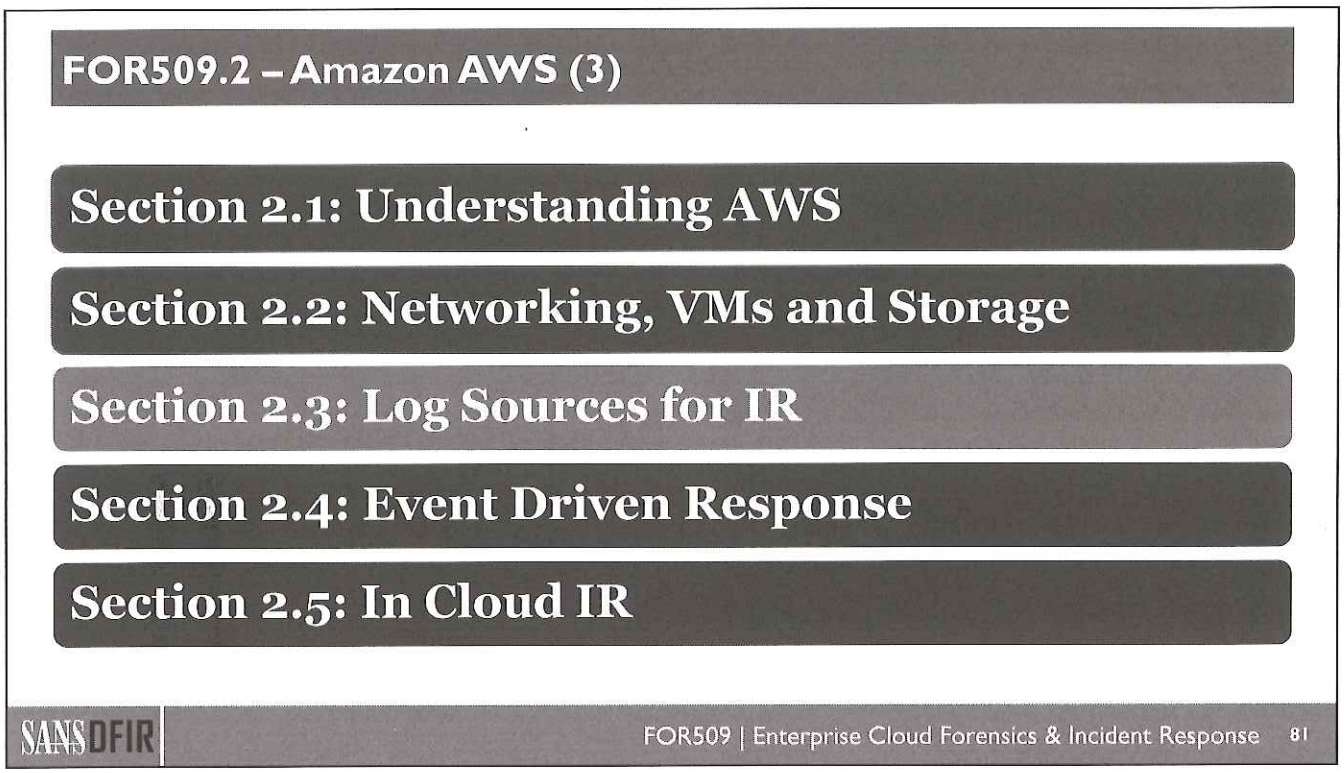
Route 53 – AWS DNS

- Amazon's Hosted DNS Service
- DNS Zone Query Logging
  - Log queries made to your hosted DNS Domains
- Route 53 Resolver Query Logs
  - Log all DNS queries made within your VPC

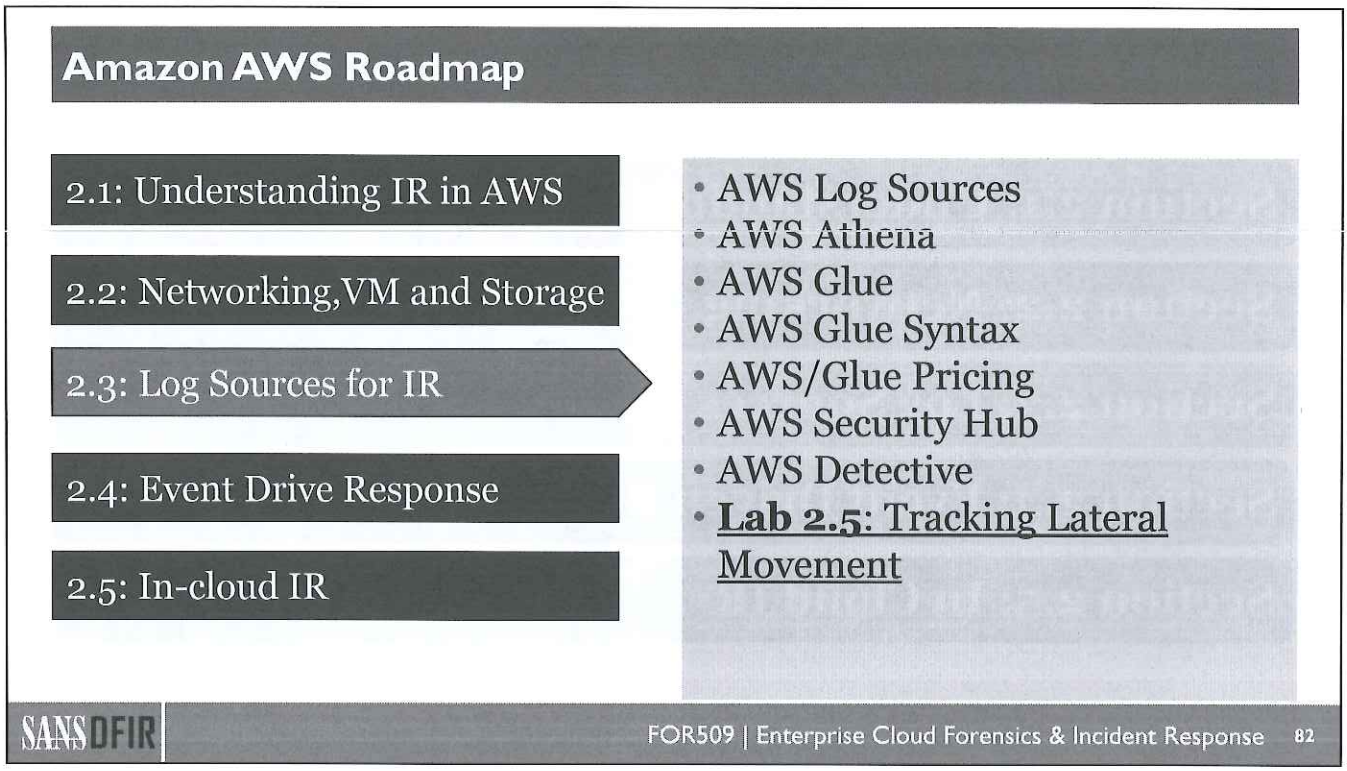
This page intentionally left blank.



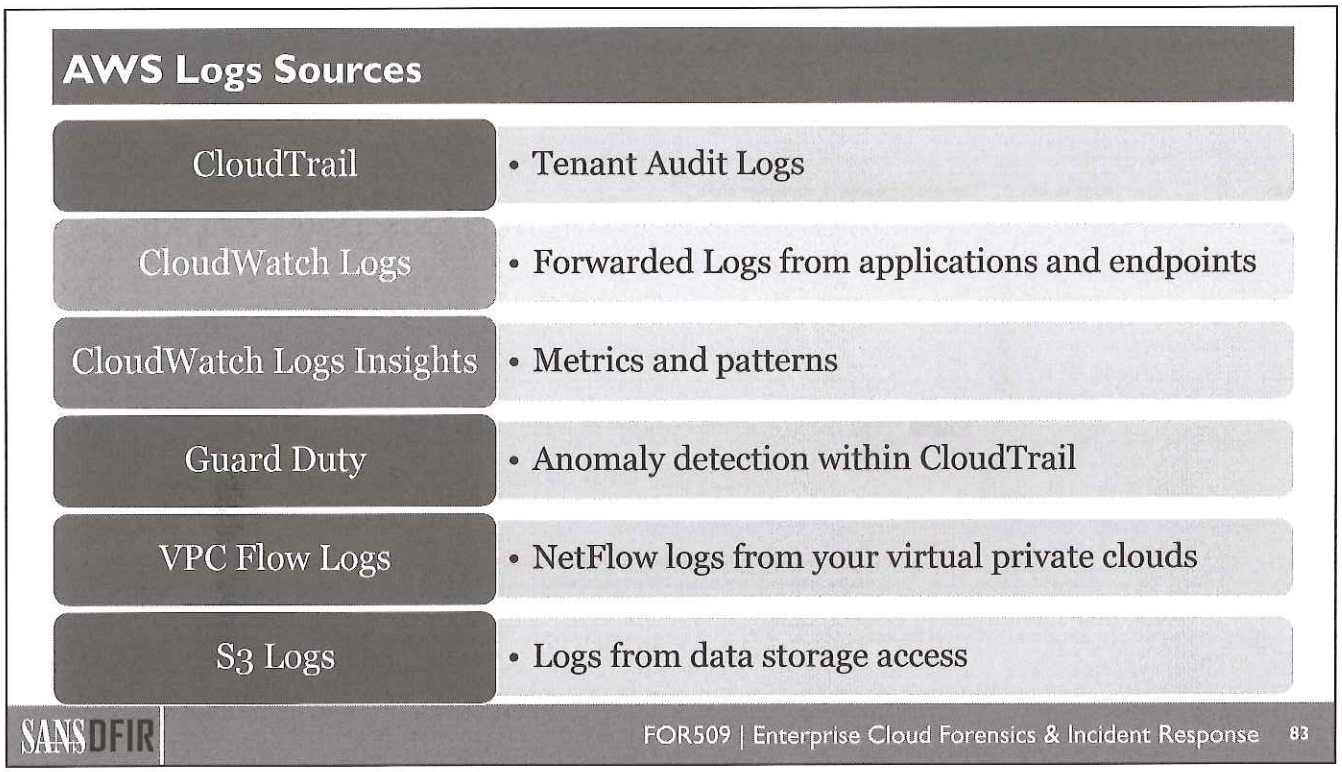
This page intentionally left blank.



This page intentionally left blank.

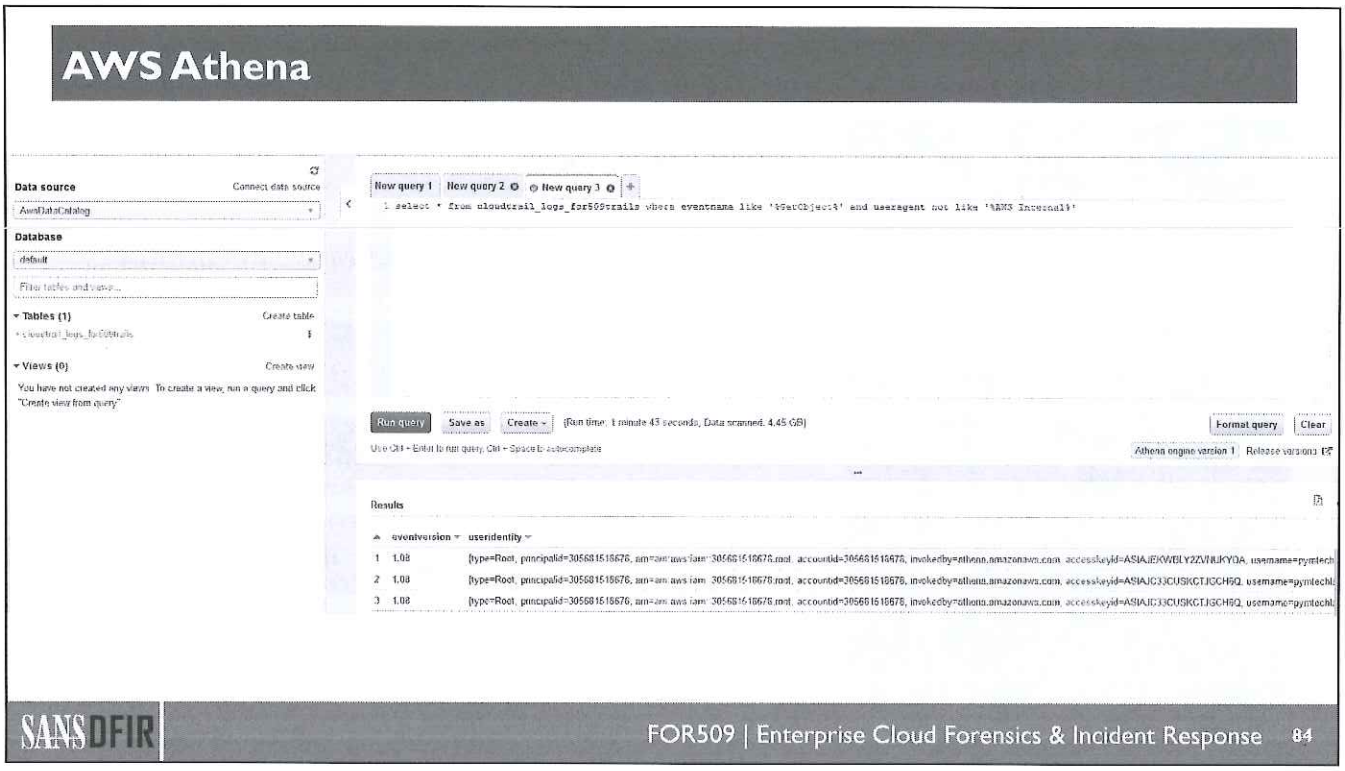


This page intentionally left blank.

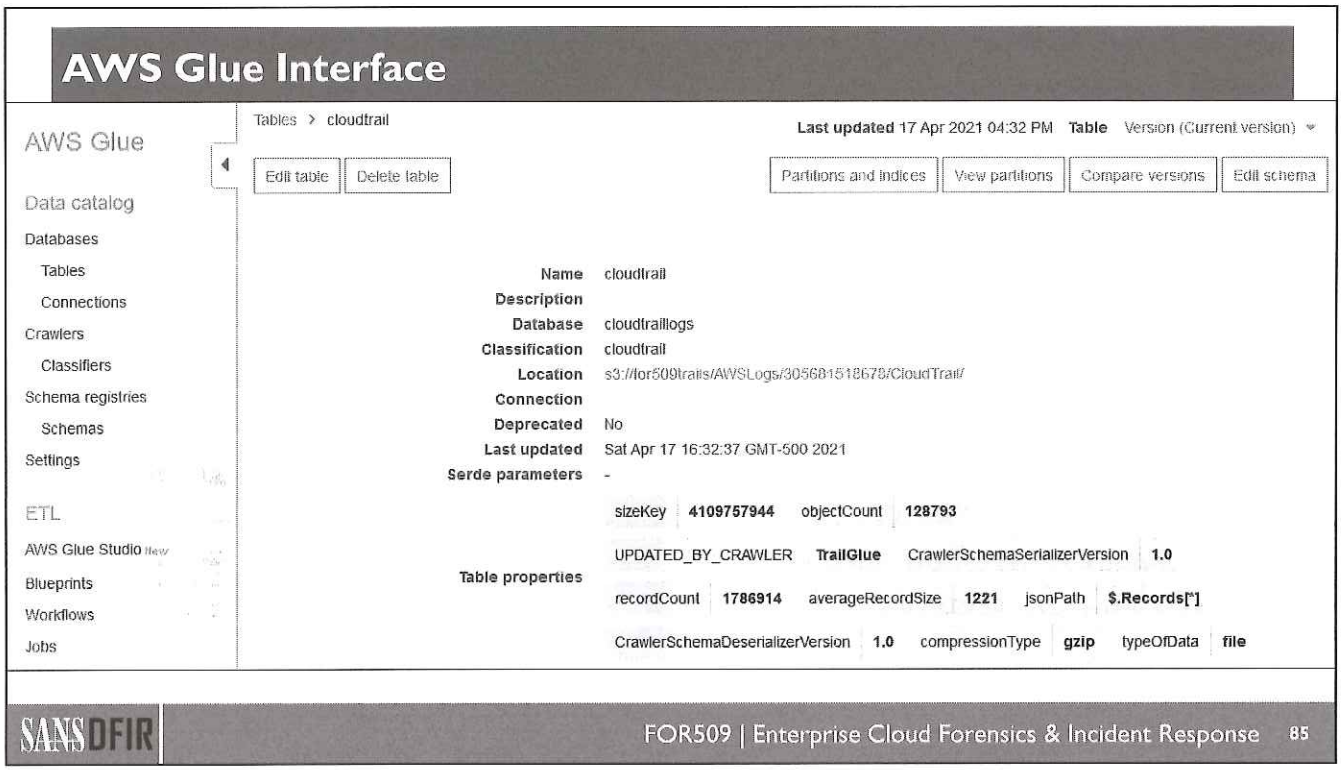


1. Tenant logs
2. Network logs
3. Storage logs

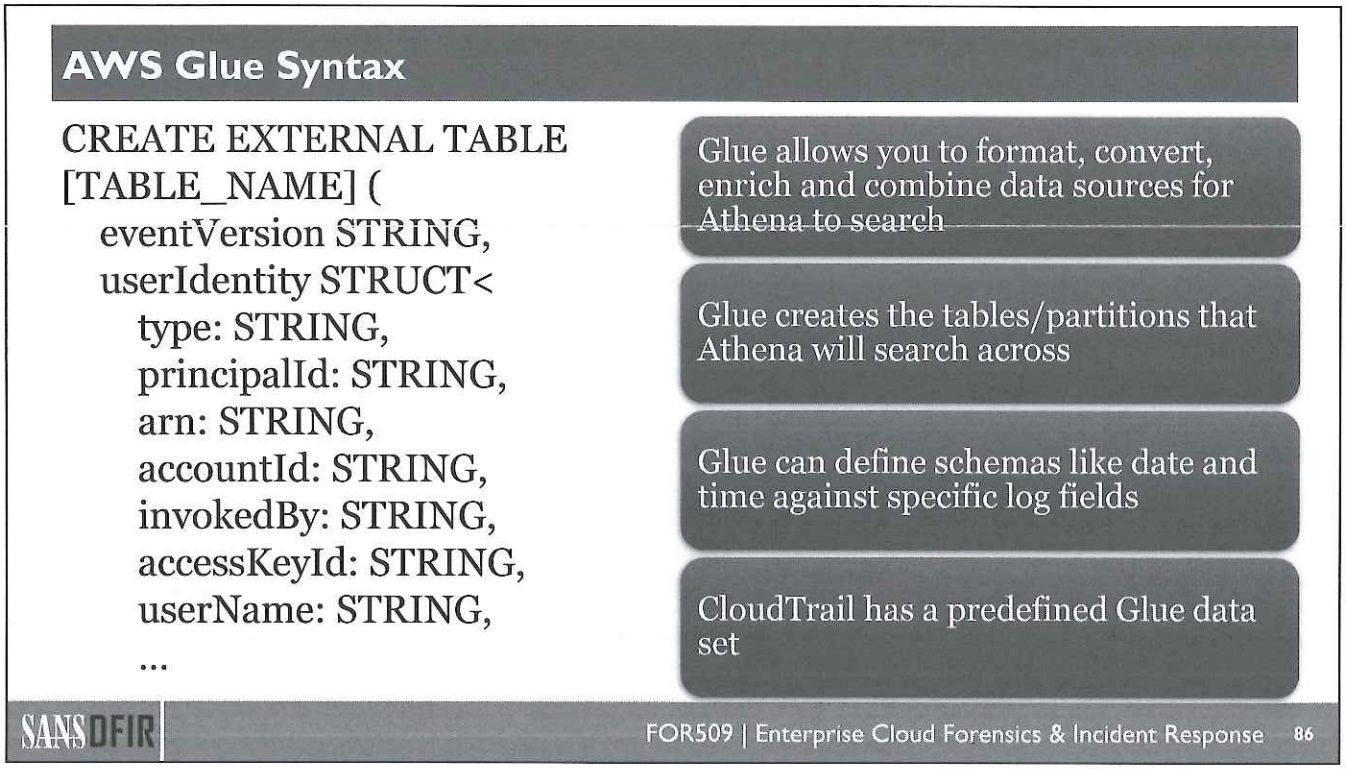
Can I do it in one slide for all three clouds???



This page intentionally left blank.



This page intentionally left blank.

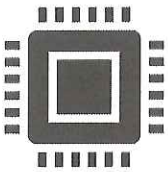


This page intentionally left blank.

AWS Athena/Glue Pricing

Athena Searching

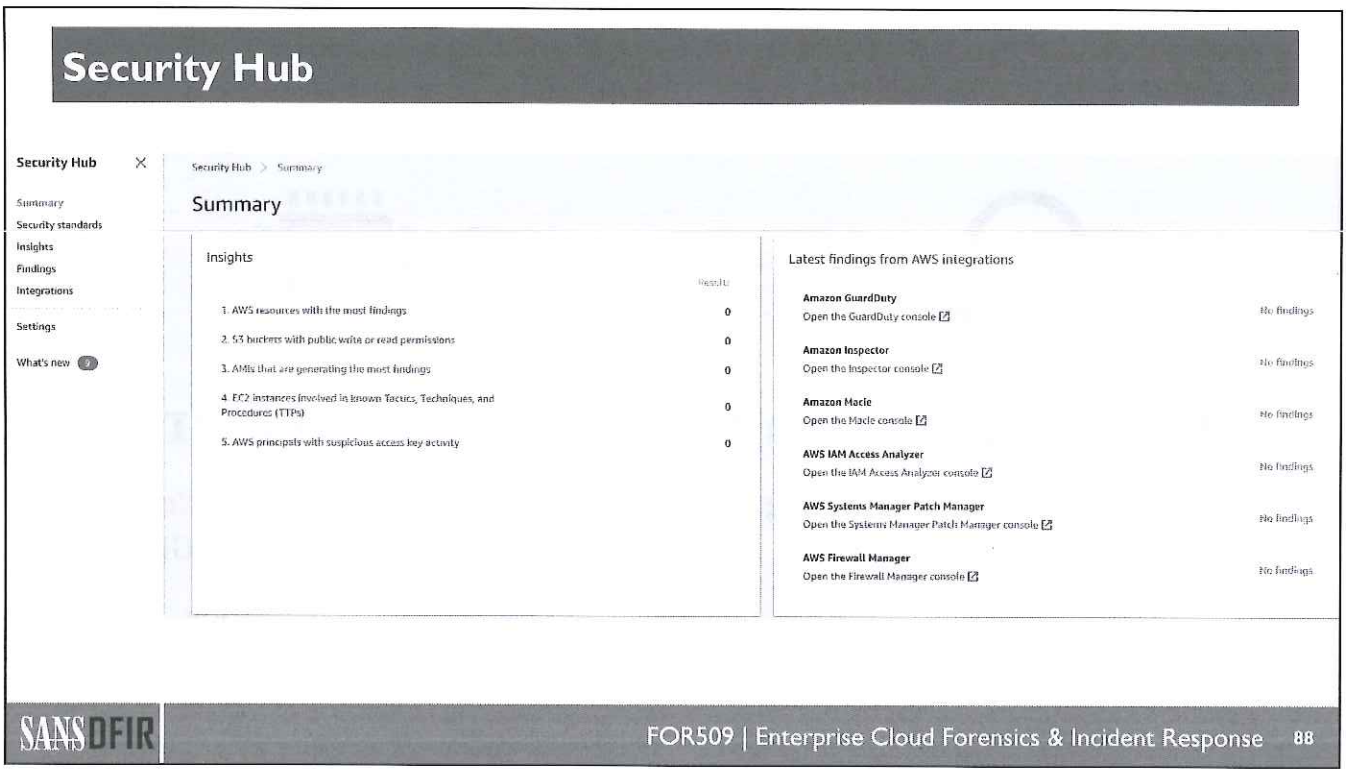
$5 per TB scanned while searching
Failed queries are not charged



Glue Crawling

$0.44 per DPU (Data Process Unit) hour
DPUs have 4 CPUs and 16GB of memory.
10 minute minimum billed

This page intentionally left blank.

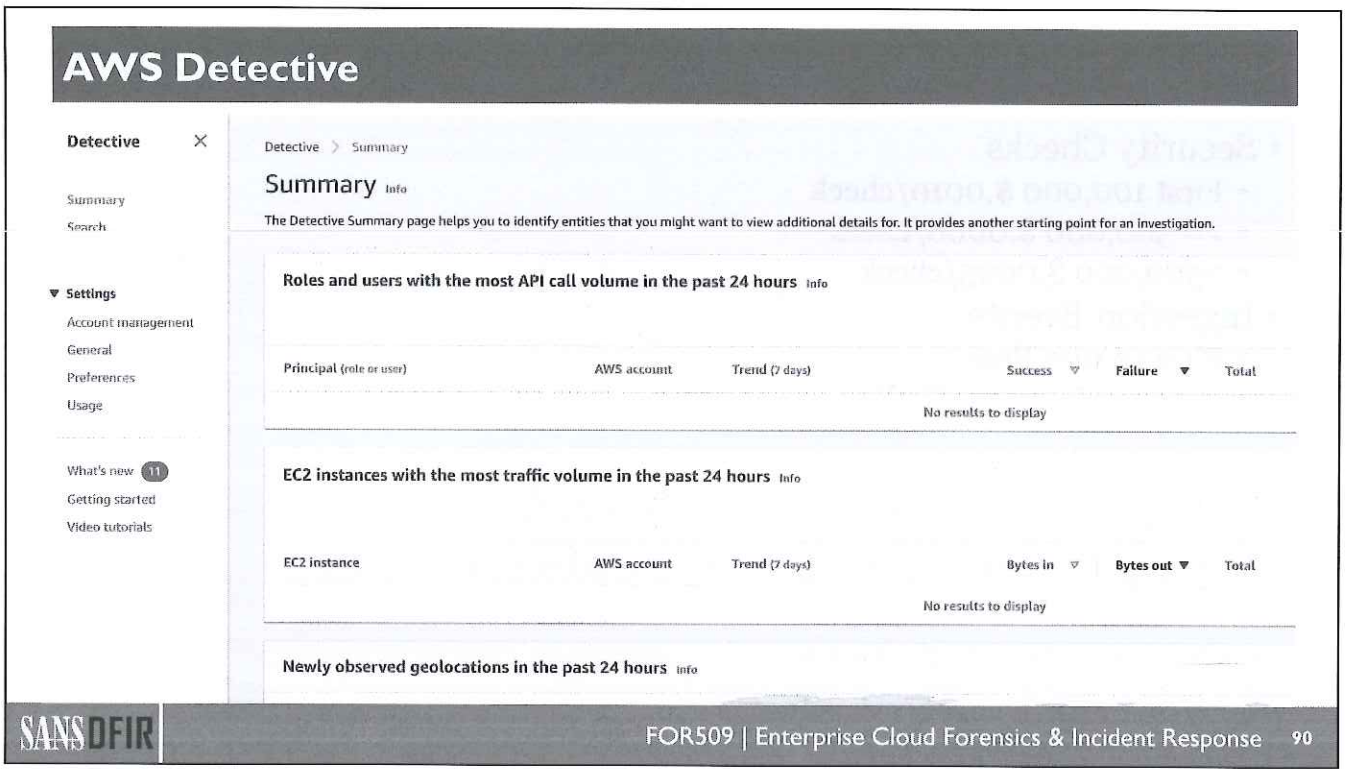


This page intentionally left blank.

Security Hub Pricing

- Security Checks
  - First 100,000 $.0010/check
  - >= 500,000 $.0008/check
  - >500,000 $.0005/check
- Ingestion Events
  - First 10,000 Free
  - >10,000 $.00003/finding

This page intentionally left blank.

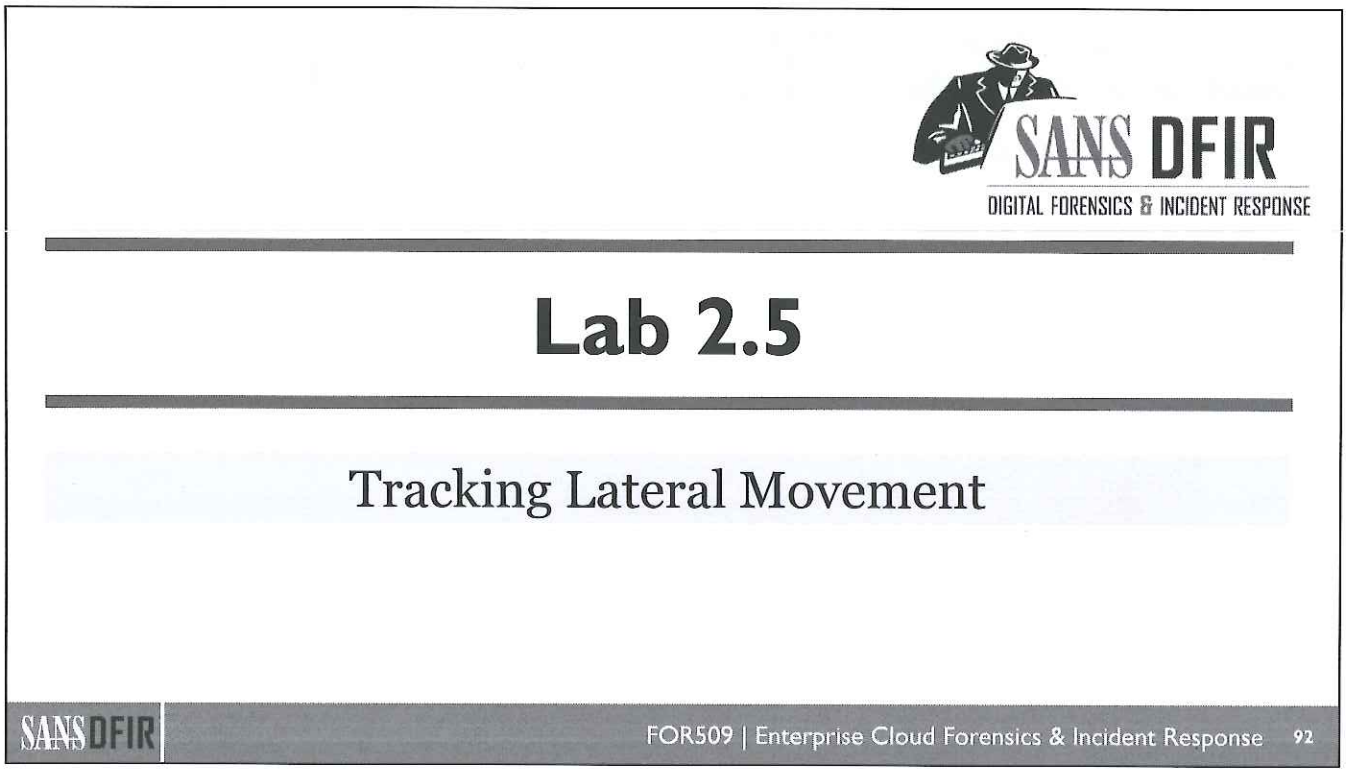


This page intentionally left blank.

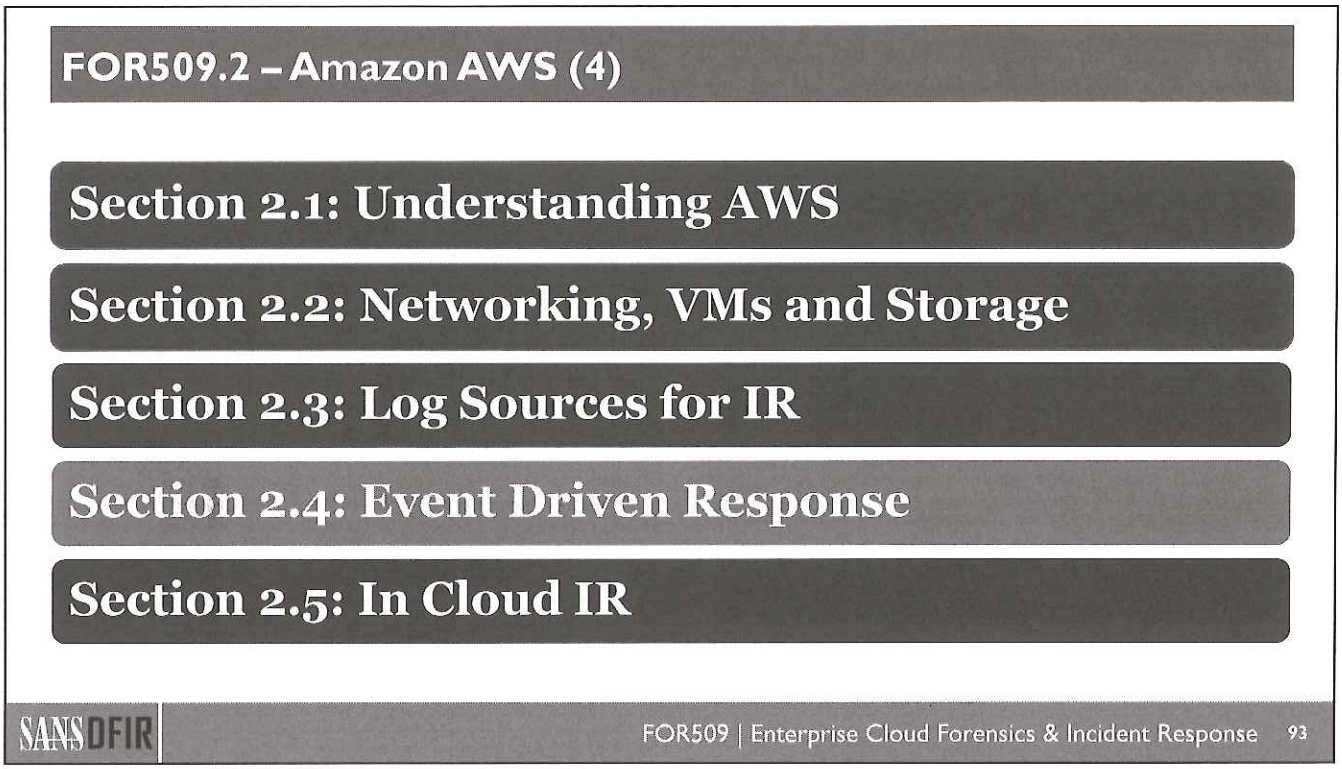
AWS Detective Pricing

- Ingested Logs per GB
  - <= 1,000 GB $2/GB
  - <= 5,000 GB $1/GB
  - <=10,000GB $.50/GB
  - >10,000GB $.25/GB

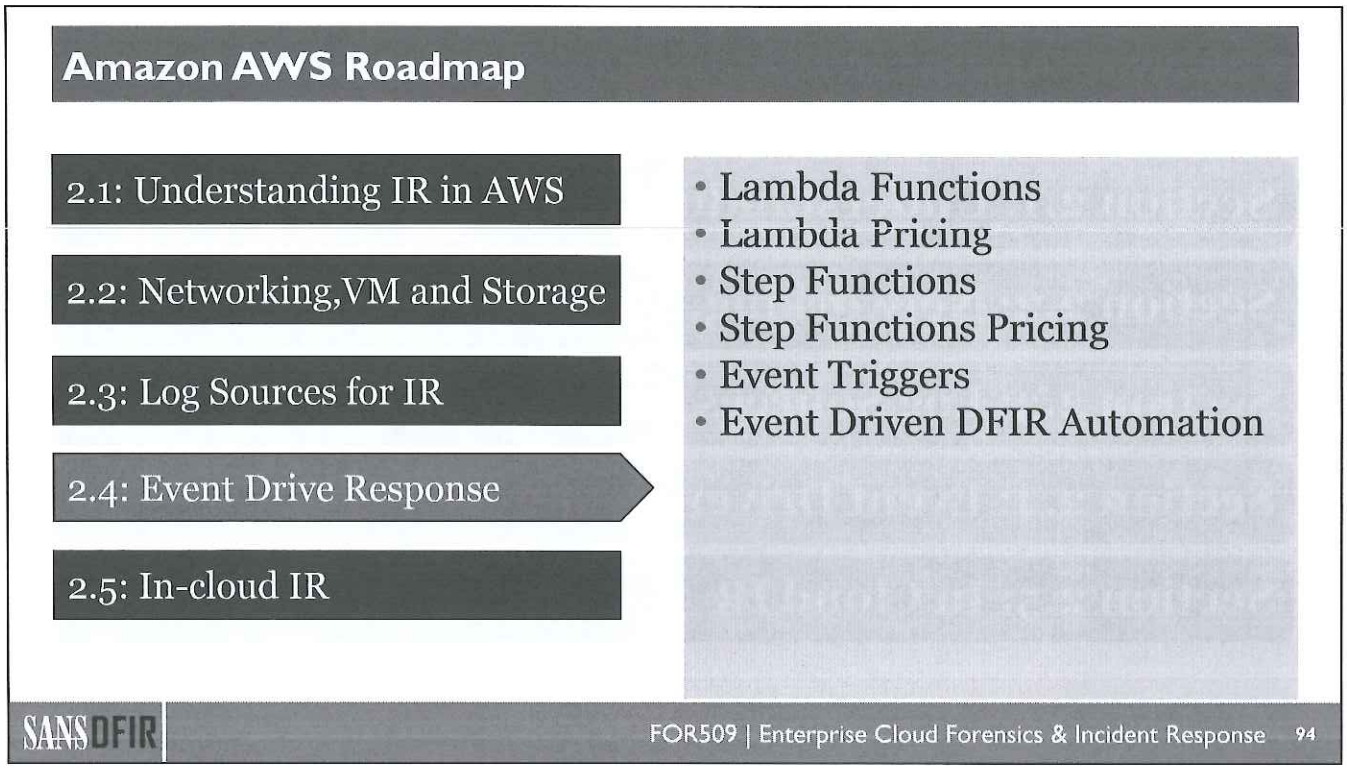
This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.

Lambda Functions

- Lambda is AWS's version of Serverless functions
- Lambda functions can be written in several languages
  - Java
  - Go
  - PowerShell
  - Node.js
  - C#
  - Python
  - and Ruby

This page intentionally left blank.

Lambda Pricing

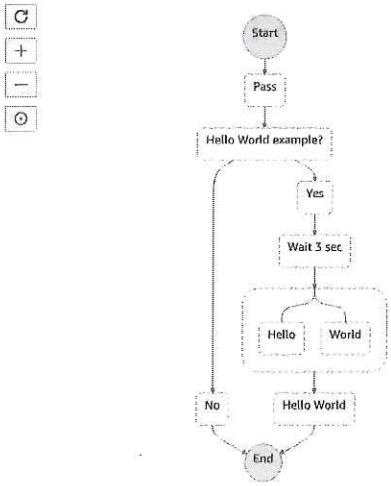
$.20 per 1 Million Requests

Also charged $0.0000166667 for every GB of ram used per second the function runs

This page intentionally left blank.

Step Functions

- Step functions allows you to chain lambda functions into a workflow where the prior output is the input for the next step.
- This allows you to divide your workflow into fast and cheap running lambda functions and build a larger IR automation tool.



This page intentionally left blank.

Step Functions Pricing

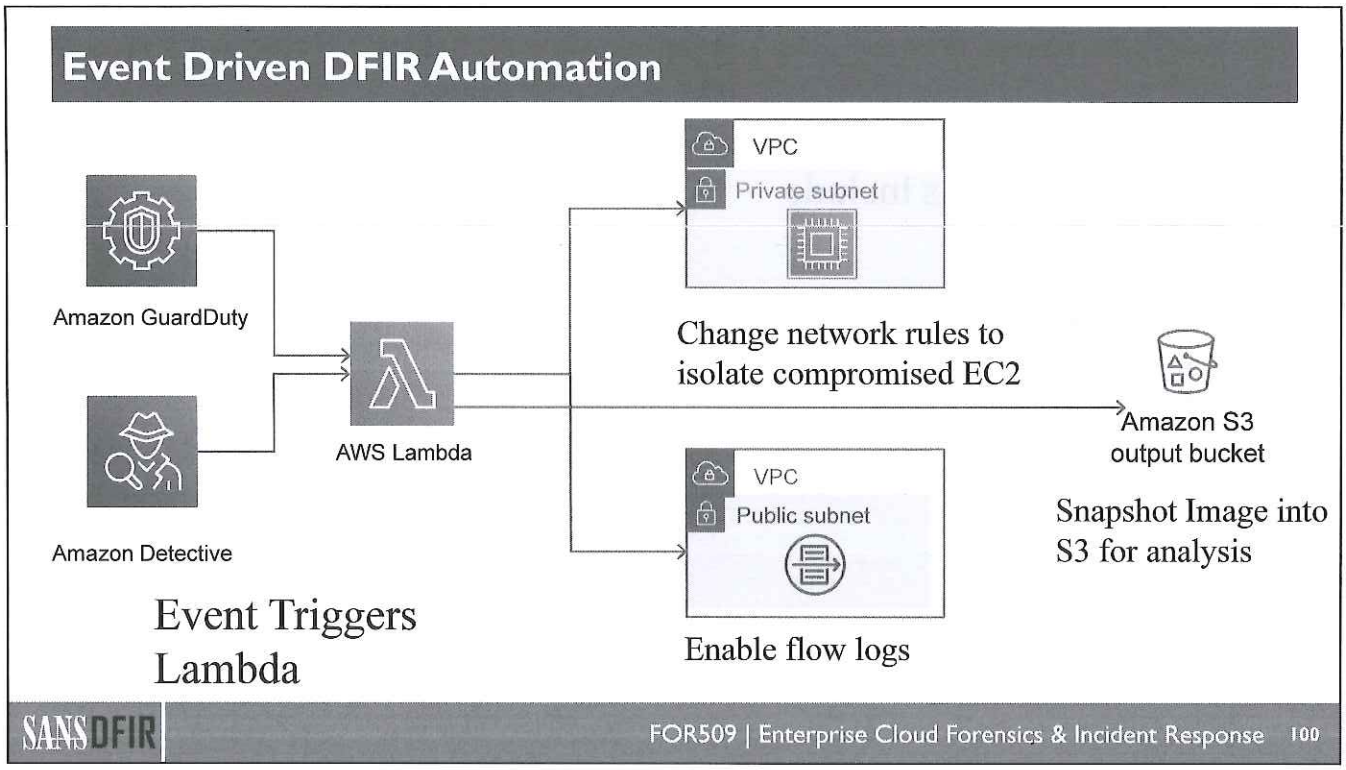
- 4,000 State Transitions are Free per month
- More than 4,000 state transactions are $.025 per 1,000 state transactions

This page intentionally left blank.

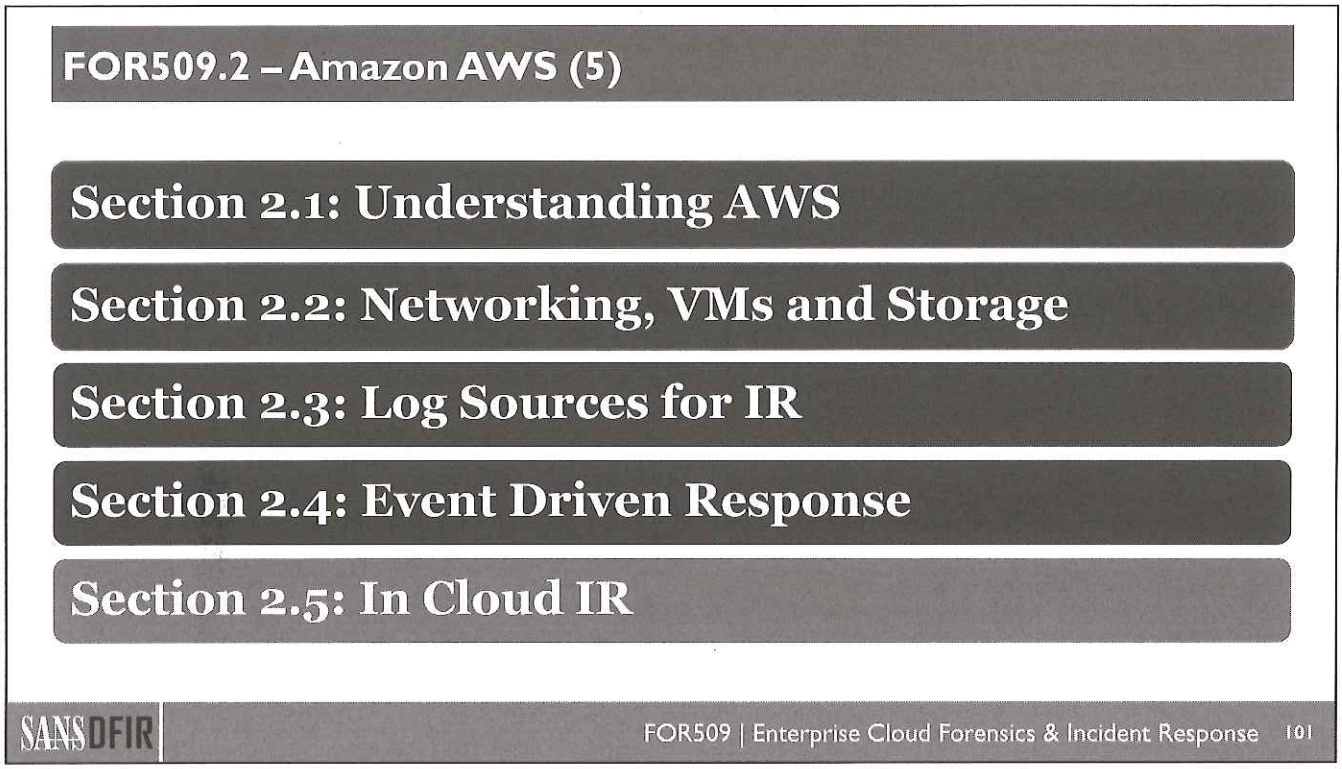
Event Triggers

- Lambda functions can be triggered with AWS events
- Examples of Events include
  - S3 Uploads
  - CloudTrail events
  - EC2 Changes
  - EFS Changes
  - Amazon Config changes

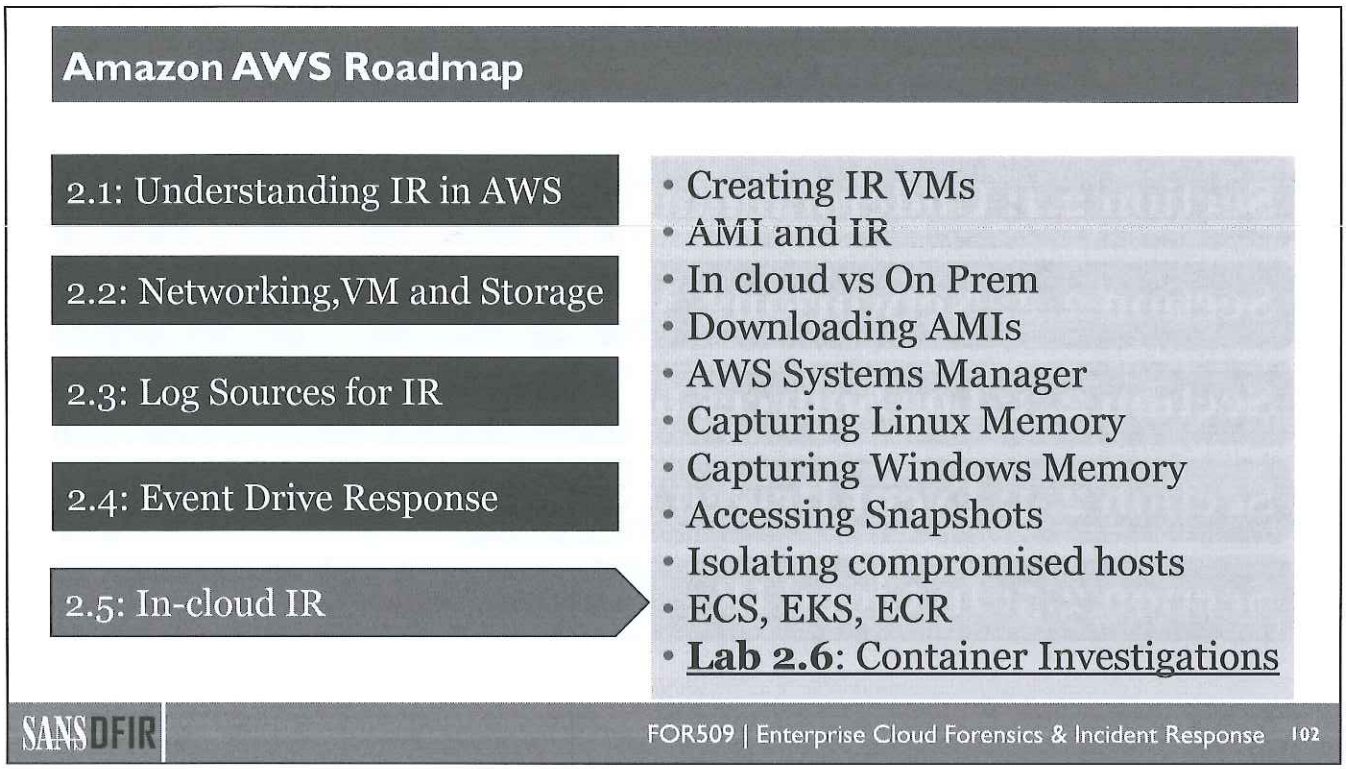
This page intentionally left blank.



This page intentionally left blank.



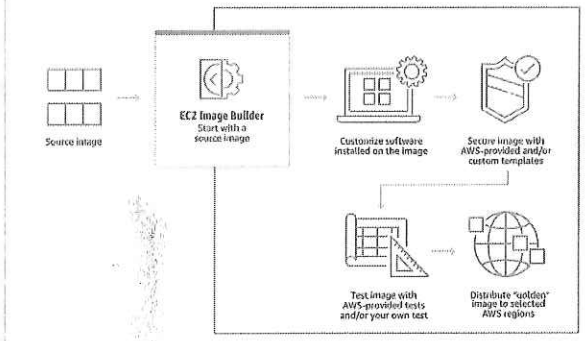
This page intentionally left blank.



This page intentionally left blank.

Creating IR VMs

How it works



Amazon makes it easy to create a custom IR VM

The EC2 Image Builder lets you pick a base image (Windows, Linux, etc..)

You can then configure the base system and then upload them as a template for your organization to deploy on demand anywhere in the world.

This page intentionally left blank.

AMIs and IR

- AMIs can be examined in two ways
  - Within AWS
    - You can snapshot the running system and attach it to a DFIR AMI that is running
    - Run all of your tools against the Snapshots
    - Snapshots are basically raw disks that can be accessed like a DD Image
  - Outside of AWS
    - You can snapshot the running system and then download the data
    - You can power off the running system and download the AMI
    - The time to download could be longer than it takes to do the examination within AWS

This page intentionally left blank.

In cloud vs. On Prem AMI examination

In Cloud

- Pros
  - Fastest time to access data
  - Able to process and load data using Amazon provided services:
    - Elastic auto scaling clusters
    - Athena for log searching
    - Containers for scalable processing
  - On demand DFIR lab anywhere in the world
- Cons
  - Cost for every examination
  - If the entire organization is compromised your DFIR account may be too

On Prem

- Pros
  - After initial investment in hardware, software and people there is no cost per incident to run the DFIR systems.
  - Isolated labs can be outside of compromised cloud environment
- Cons
  - Time to download cloud data
  - Time to process data
  - Data speeds can be slower on international transfers
  - Infrastructure maintenance costs

This page intentionally left blank.

Downloading AMIs

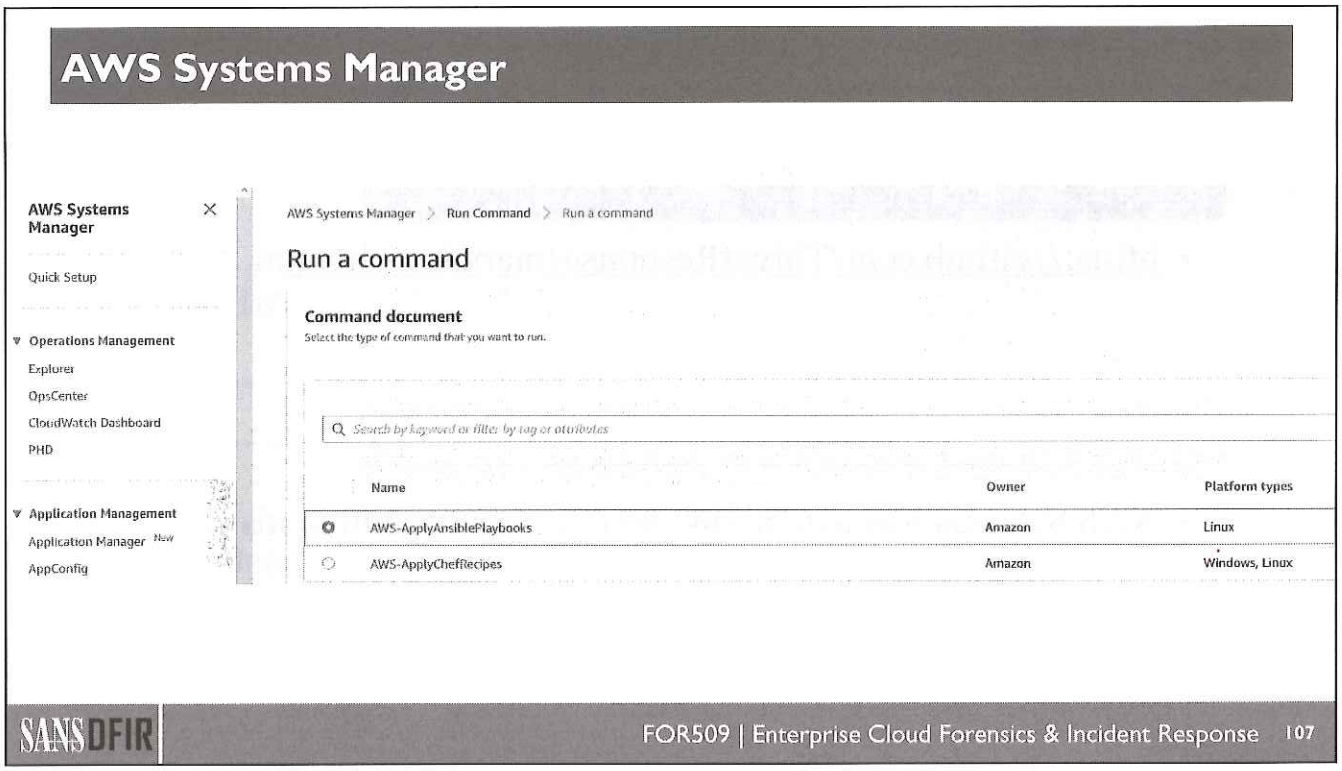
- Requires an S3 bucket to write to
- Requires the AWS CLI
- Exporting an Instance

```
aws ec2 create-instance-export-task --instance-id instance-id --target-environment vmware --export-to-s3-task file://C:\file.json
```

- Exporting an AMI

```
aws ec2 export-image --image-id ami-id --disk-image-format VMDK --s3-export-location S3Bucket=my-export-bucket,S3Prefix=exports/
```


This page intentionally left blank.



This page intentionally left blank.

Capturing Linux Memory

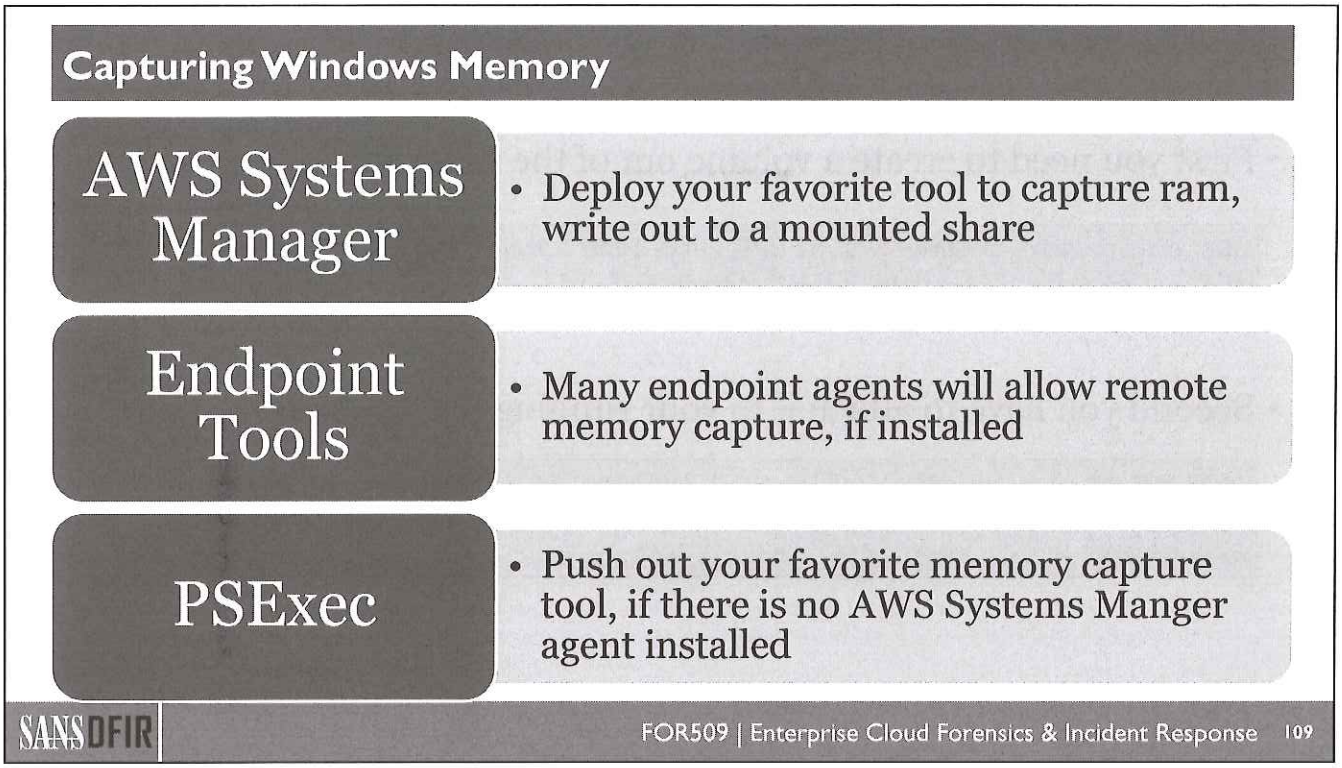
Margarita Shotgun

- https://github.com/ThreatResponse/margaritashotgun
- Logs into a running EC2 instance via SSH and runs LiME to capture memory

AVML and AWS Systems Manager

- AWS Systems Manager allows you to execute commands across instances that have the system manager agent installed
- AVML can be statically compiled meaning it does not require compromised systems have kernel headers

This page intentionally left blank.



This page intentionally left blank.

Accessing Snapshots from DFIR AMIs

- First you need to create a volume out of the snapshot

```
aws ec2 create-volume --availability-zone <zone where your DFIR
AMI is running>  --snapshot-id <snapshot-id>
```

- Second you have to attach it to your running EC2 instance

```
aws ec2 attach-volume --volume-id <volume id returned from prior
command> --instance-id <your DFIR EC2 instance> --device
</dev/sdX>
```


This page intentionally left blank.

Isolating Compromised Hosts

- Need to isolate a compromised host?
  - Virtual firewalls can be configured on demand
  - Lambda to change ec2 security group

```
def modifyInstanceAttribute(instanceId,securityGroupId):
          response = ec2Client.modify_instance_attribute(
                    Groups=[securityGroupId], InstanceId=instanceId)
```

  - Lambda to place it in the isolated security group

```
def createSecurityGroup(groupName, descriptionString, vpcId):
resource = boto3.resource('ec2')
securityGroupId = resource.create_security_group(GroupName=groupName,
          Description=descriptionString, VpcId=vpcId)
          securityGroupId.revoke_egress(IpPermissions= [{'IpProtocol': '-
1','IpRanges':     [{'CidrIp': '0.0.0.0/0'}],'Ipv6Ranges':
[],'PrefixListIds': [],'UserIdGroupPairs': []}])
          return securityGroupId.
```


Reference: https://aws.amazon.com/blogs/security/automate-amazon-ec2-instance-isolation-by-using-tags/

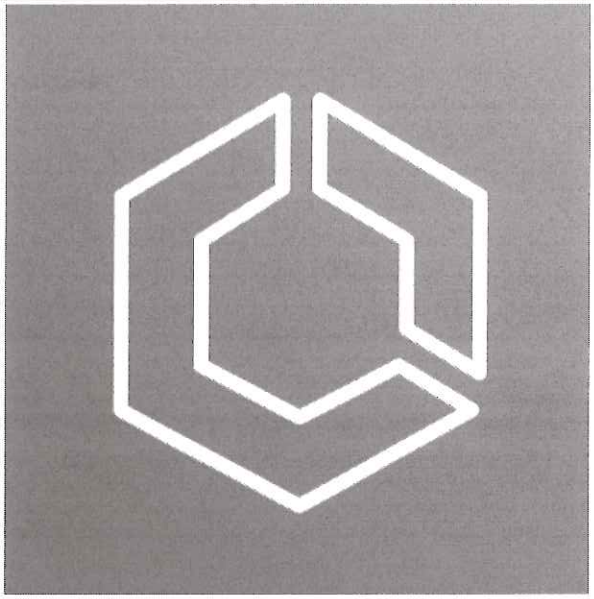
Regions and Response

- Regions Matter!
- Every region is physically resident in the country it's named after
- Transferring data between regions:
  - Takes time
  - Costs money
- Consider spinning up your DFIR AMIs in the region where you want to analyze the data

This page intentionally left blank.

ECS - Elastic Container Service

- Amazon's version of Kubernetes
- Allows for a lower overhead container cluster
- Runs docker containers at scale and manages spinning up more as needed.



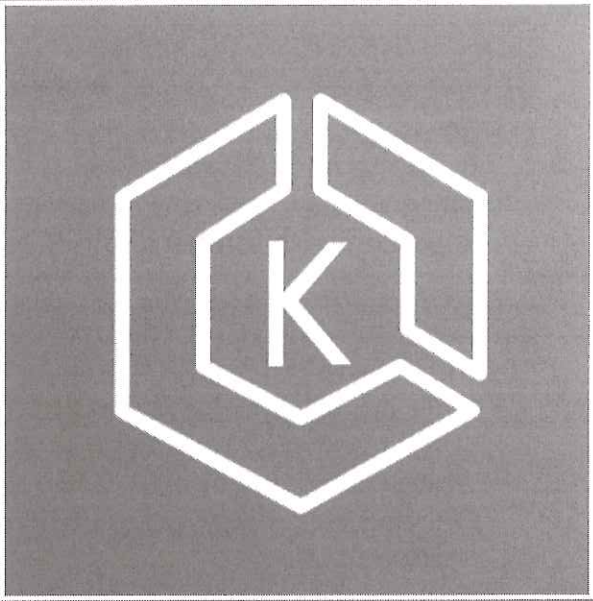
This page intentionally left blank.

Container Registry

This page intentionally left blank.

EKS – Elastic Kubernetes Service

- The real Kubernetes
  - Requires more administration than ECS
  - Can spin up any number of containers from the container registry



This page intentionally left blank.

Most Common Container Investigations

Vulnerable applications from the AWS Marketplace

- Many developers will launch preconfigured container applications from the AWS Marketplace
- Many of these preconfigured applications are out of date and can be launched with known exploitable services

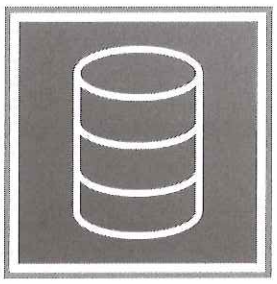
Stolen IAM roles through the Metadata service

- Once an attacker has access to the container environment, they can reach the Metadata service unless the NSG prevents it
- Always available at http://169.254.169.254/latest/meta-data/
- Once accessed IAM roles and credentials applied to the instance can be stolen

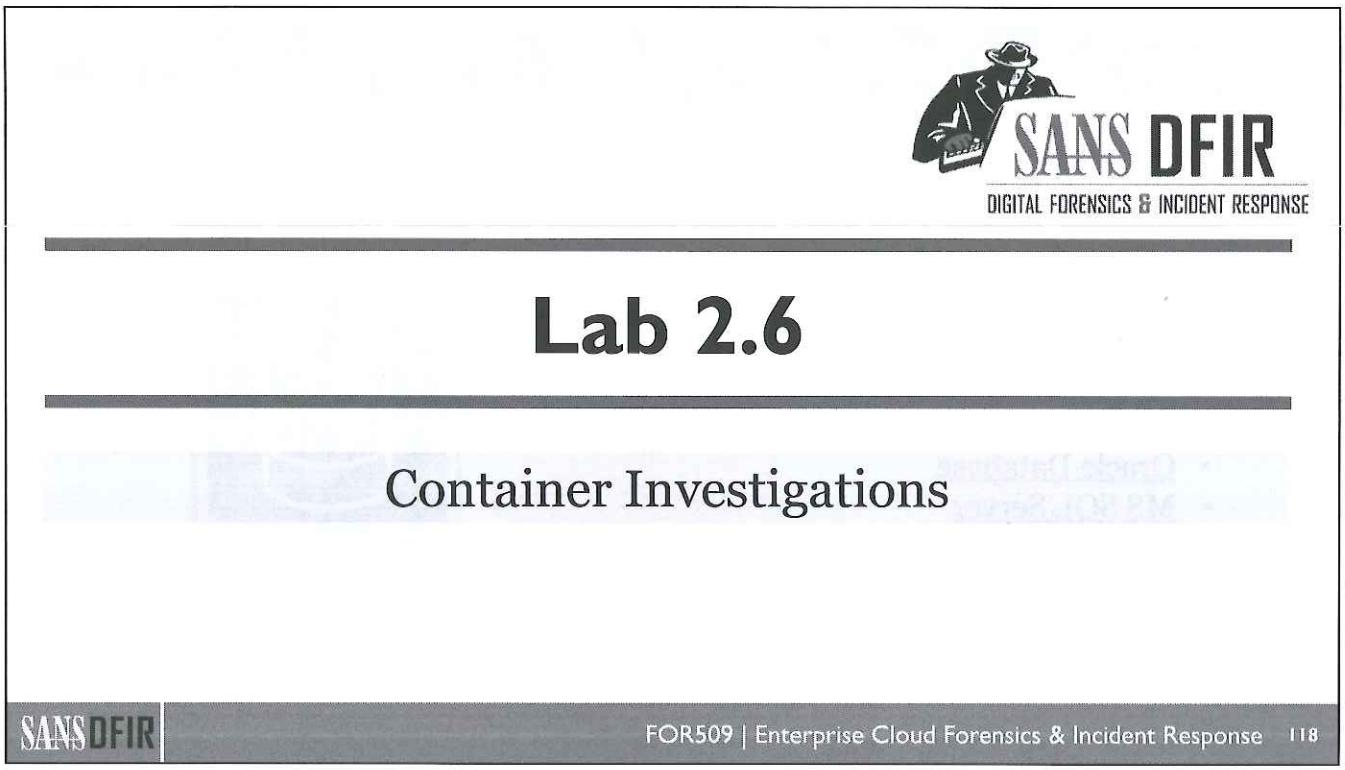
This page intentionally left blank.

Amazon Hosted Databases

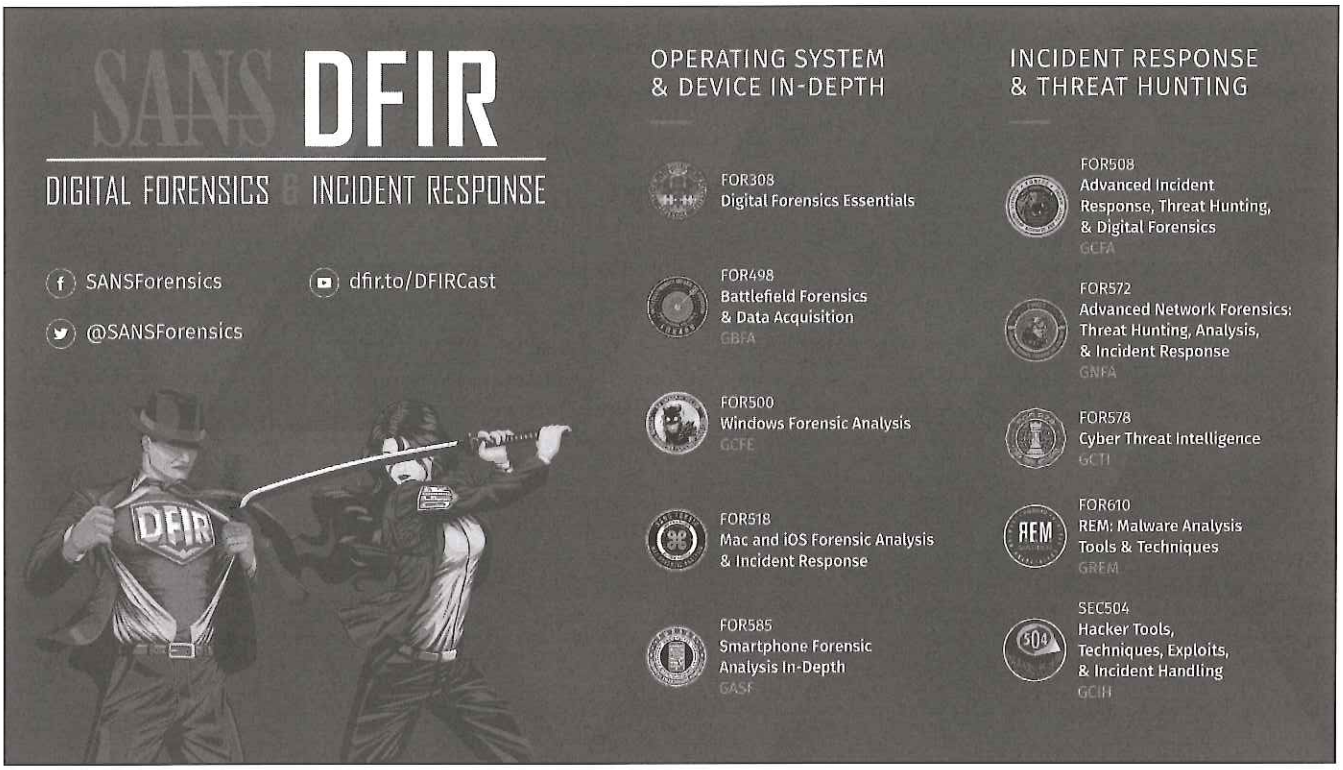
- Rather than running a database in EC2 Amazon provides hosted databases where you only must manage the data within them.
- Databases supported:
  - Amazon Aurora
  - PostgreSQL
  - MySQL
  - MariaDB
  - Oracle Database
  - MS SQL Server



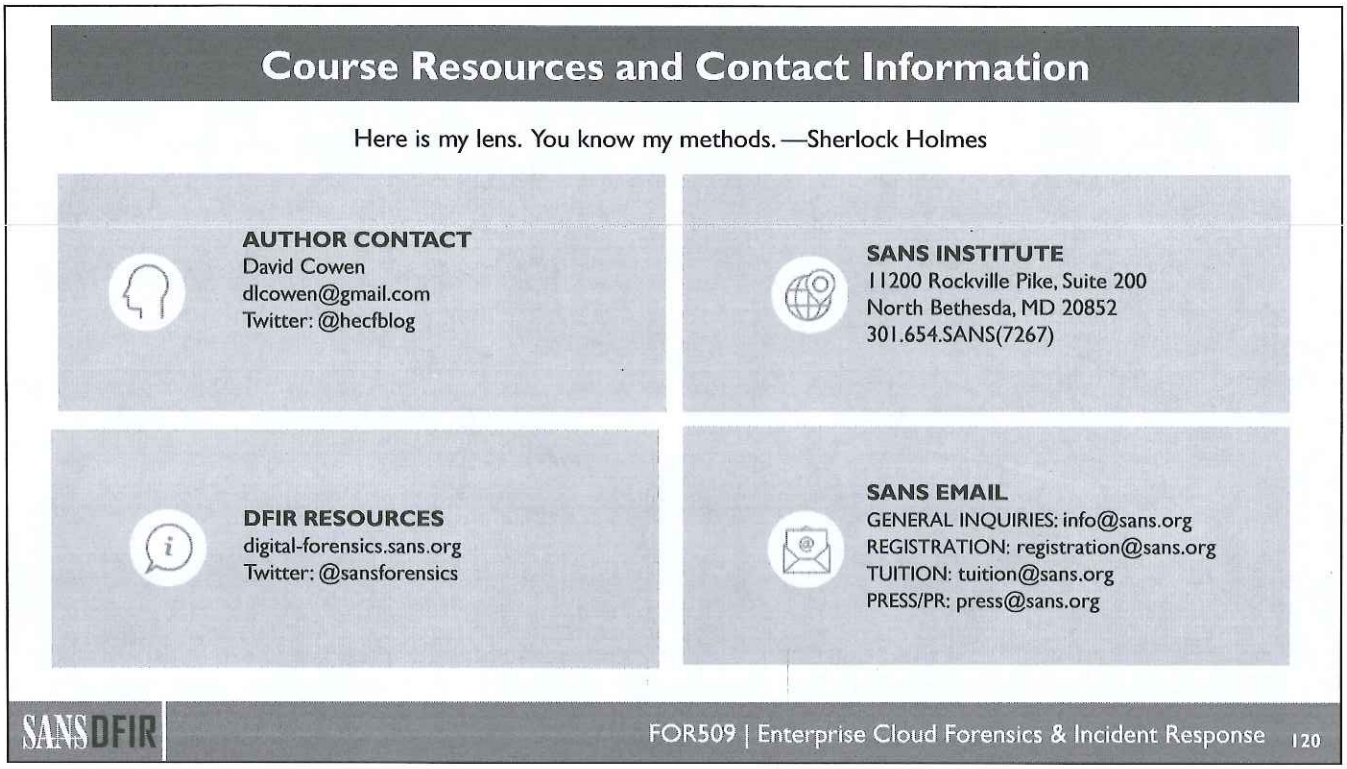
This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.



Author: David Cowen
Email: dlcowen@gmail.com
Twitter: @hecfblog

"As usual, SANS courses pay for themselves by Day 2. By Day 3, you are itching to get back to the office to use what you've learned."
Ken Evans, Hewlett Packard Enterprise - Digital Investigation Services

SANS Programs
sans.org/programs

GIAC Certifications
Graduate Degree Programs
NetWars & CyberCity Ranges
Cyber Guardian
Security Awareness Training
CyberTalent Management
Group/Enterprise Purchase Arrangements
DoDD 8140
Community of Interest for NetSec
Cybersecurity Innovation Awards

Search SANSInstitute

SANS Free Resources
sans.org/security-resources

- E-Newsletters
  NewsBites: Bi-weekly digest of top news
  OUCH!: Monthly security awareness newsletter
  @RISK: Weekly summary of threats & mitigations
- Internet Storm Center
- CIS Critical Security Controls
- Blogs
- Security Posters
- Webcasts
- InfoSec Reading Room
- Top 25 Software Errors
- Security Policies
- Intrusion Detection FAQ
- Tip of the Day
- 20 Coolest Careers
- Security Glossary

SANS Institute
8120 Woodmont Avenue | Suite 310
Bethesda, MD 20814
301.654.SANS(7267)
info@sans.org