## Lab Objective and Due Date:

Understand and practice the creation of a secure DevSecOps environment in AWS. This lab is due **April 8, 2024.**

## Pre-Lab Setup:

1. AWS Account Setup, including setting up an AWS Organization.
2. [Resource Allocation](https://aws.amazon.com/getting-started/hands-on/control-your-costs-free-tier-budgets/): Assign budget limits and monitor usage to prevent unexpected costs.

## Lab Exercise:

Complete the [AWS-Designed Lab here](https://devops.awssecworkshops.com/) and answer the following questions.

## Lab Notes and Hints:

1. NOTE: Please use the Python 3.12 runtime in your Lambda functions.
2. HINT: Almost all of the action here happens in the “resources.json” file in the /code/ folder of this codebase.
3. HINT: In the “finding AWS Keys” module you will encounter an additional issue beyond credentials in the resources.json file. It has to do with “EncryptedVolume” configurations in EBS.
4. HINT: Remove the second Action from your StaticCodeAnalysis stage before beginning. It will fail after you’ve removed the credentials from resources.json.

## Deliverables:

### Evidence to Provide

1. Provide a screenshot proving you completed each module in the lab. The screenshot should show a working DevSecOps pipeline being processed.

MODULE-1

A screenshot of a computer

Description automatically generated

A screenshot of a computer

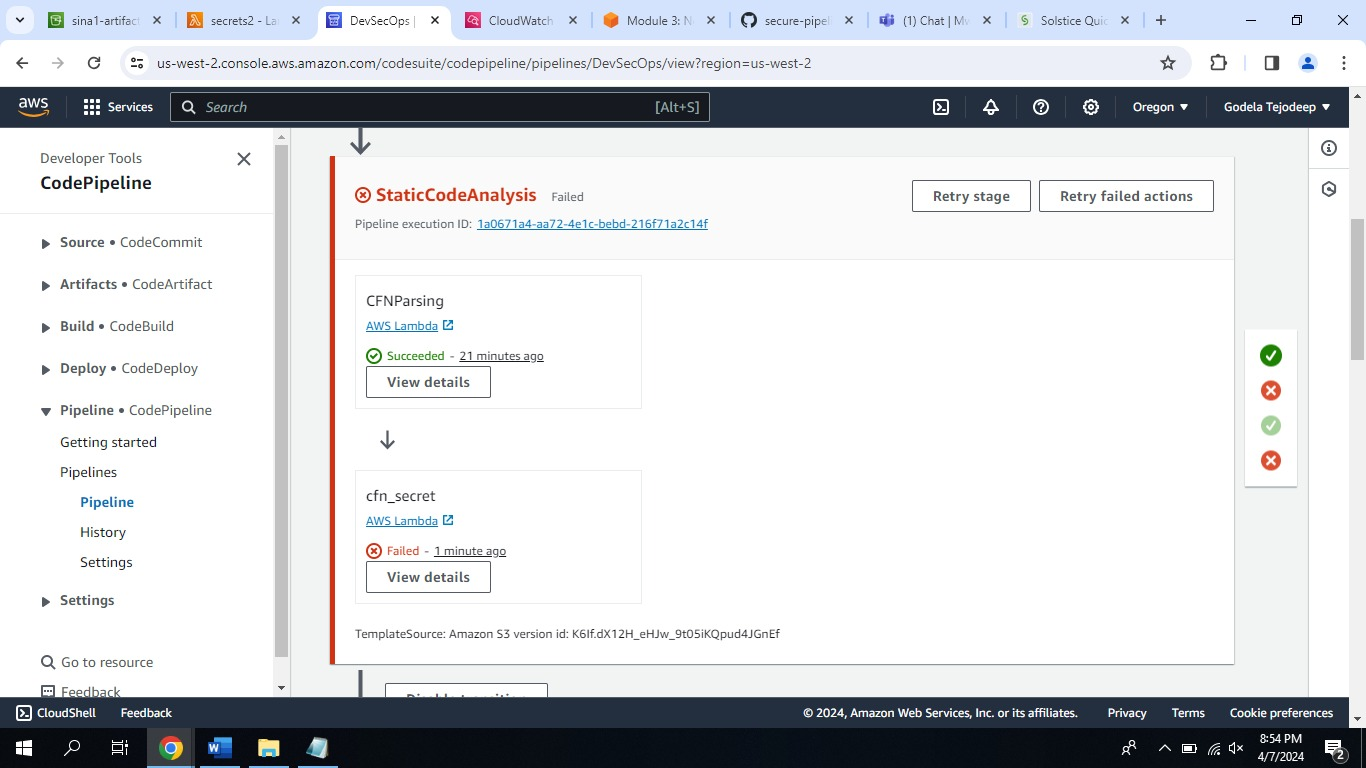
Description automatically generated

MODULE-2

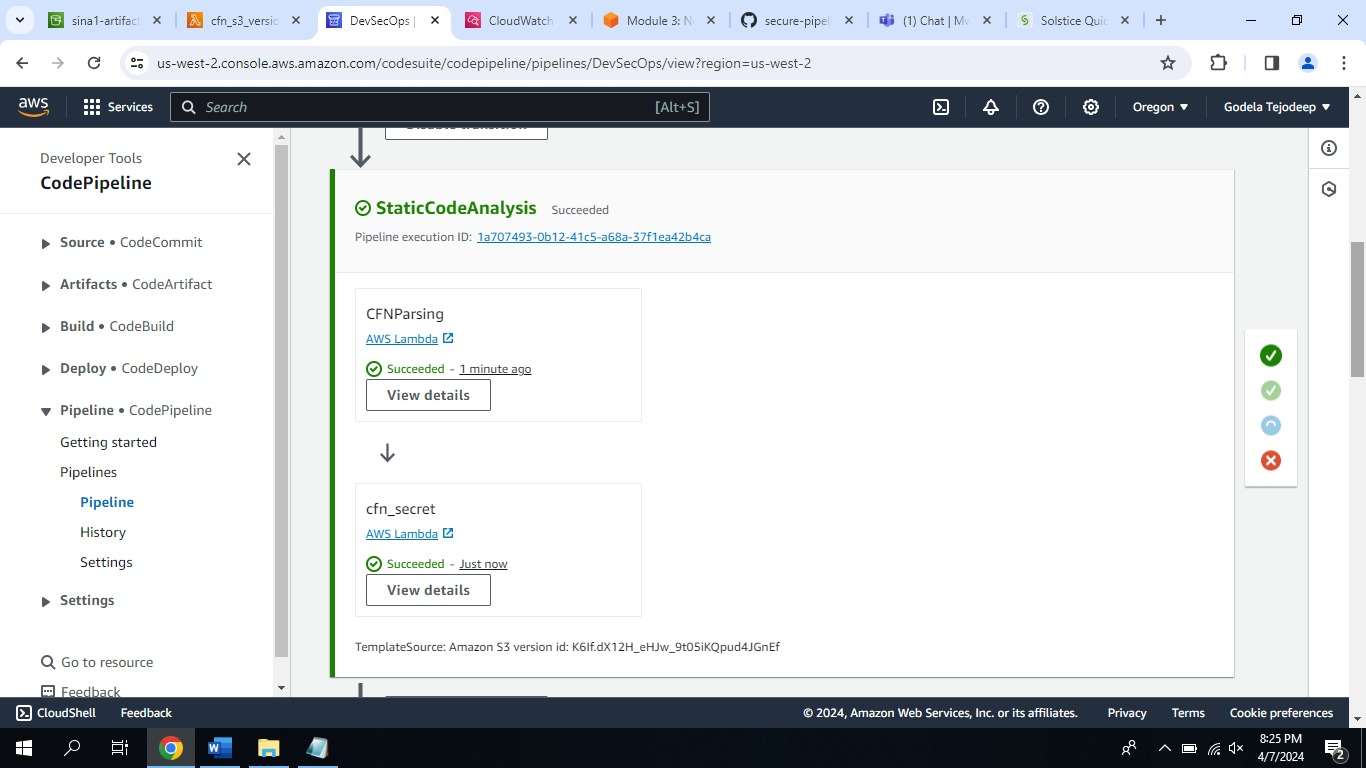
A screenshot of a computer

Description automatically generated

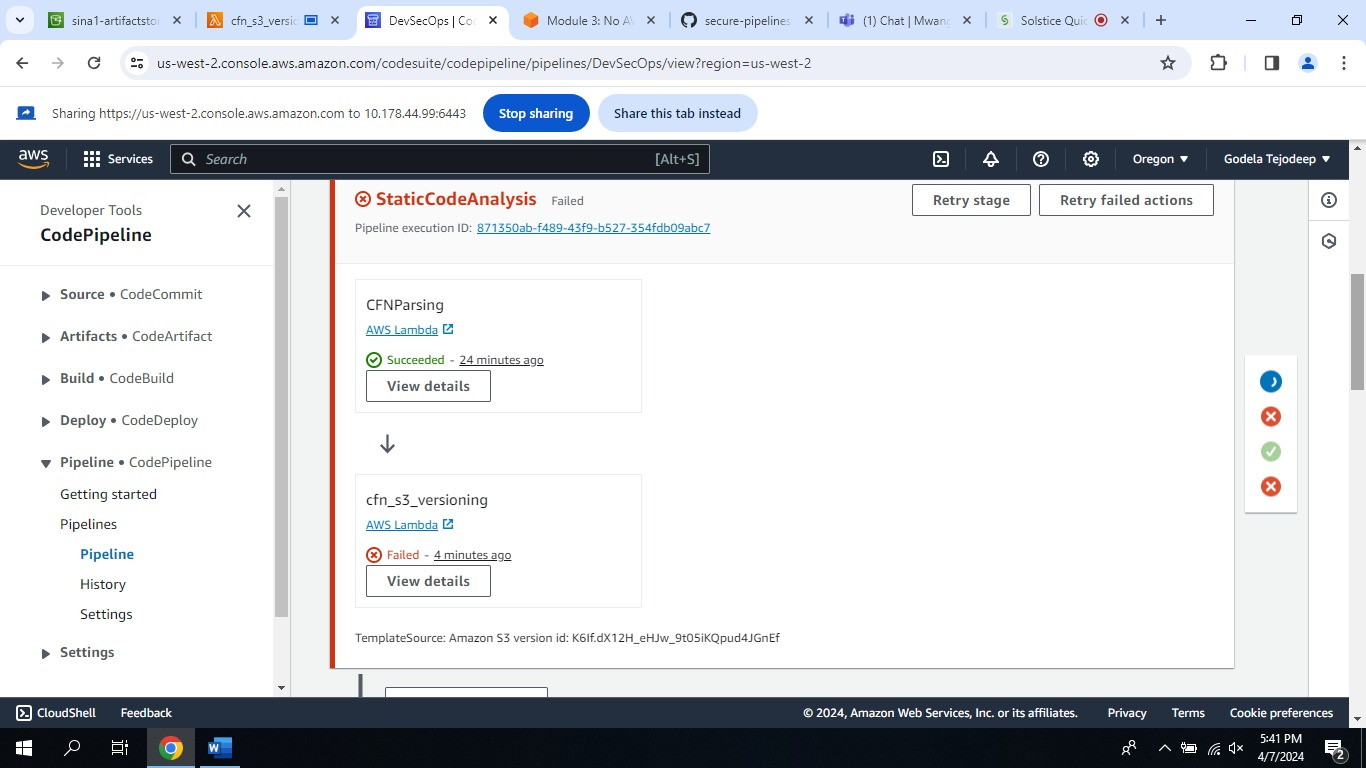
Module-3



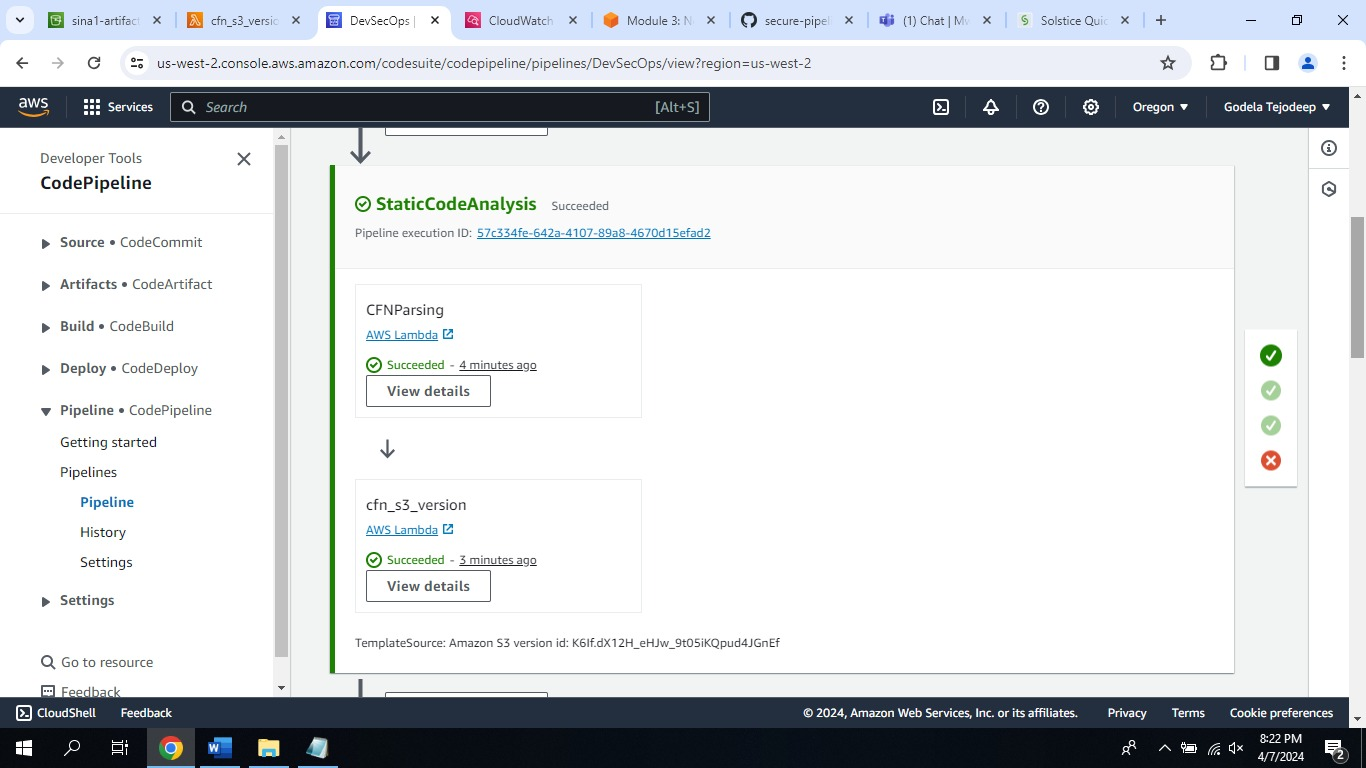
MODULE-4



MODULE-5

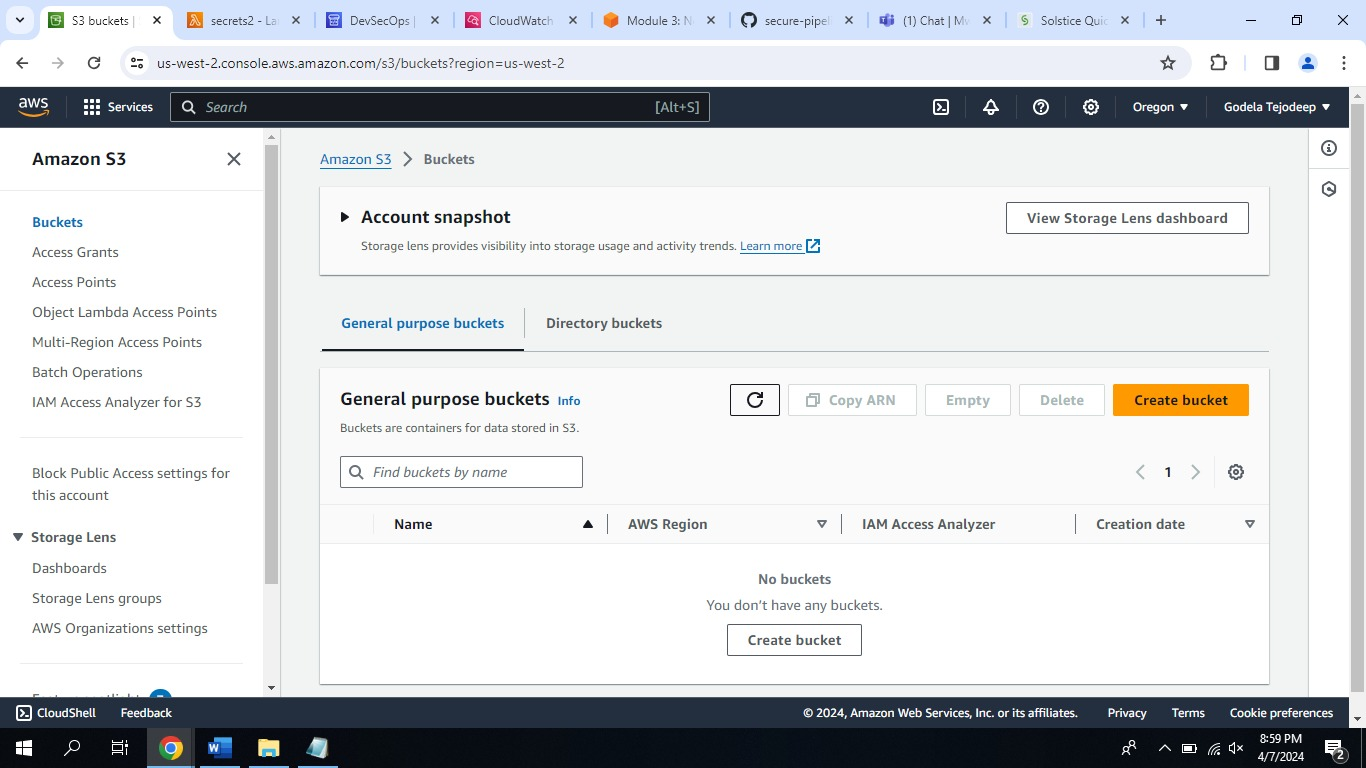


MODULE-6

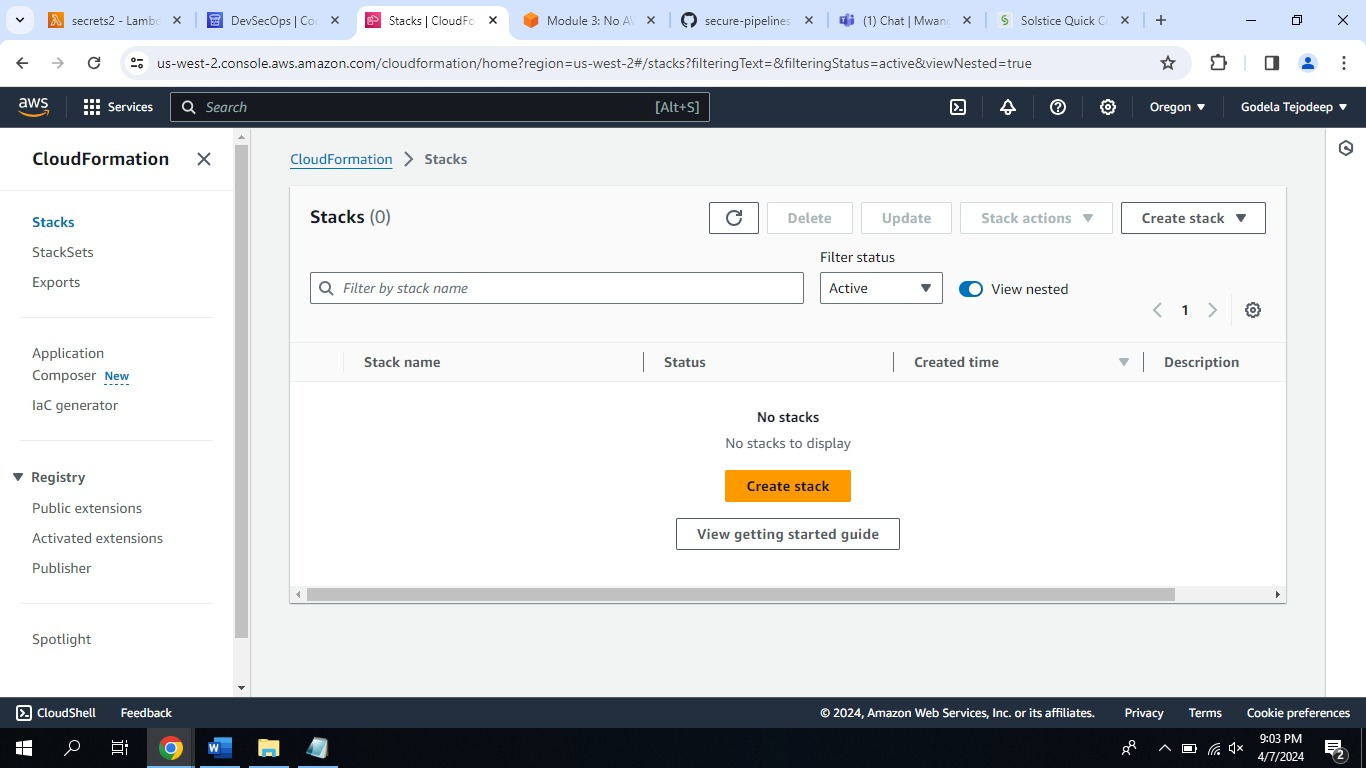


MODULE-7

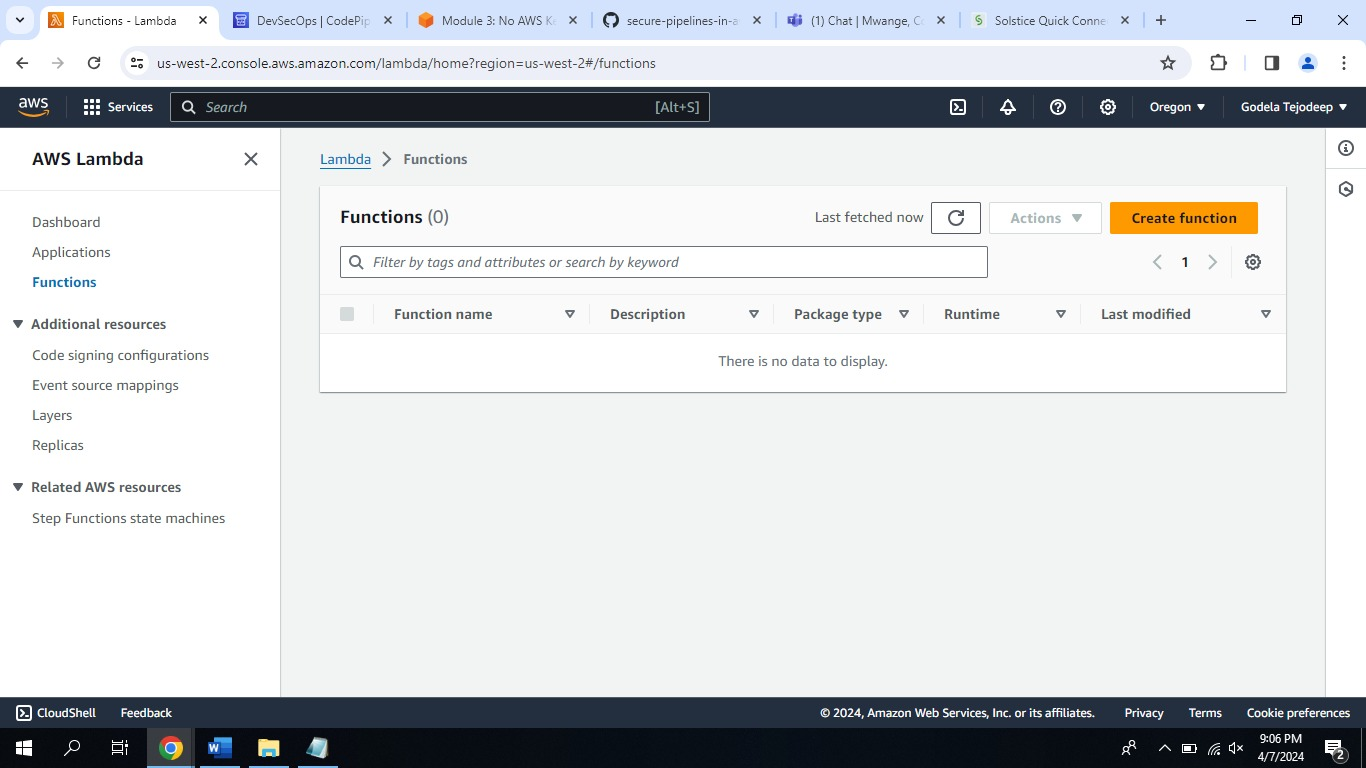
CLEANING S3 BUCKETS



CLEANING CLOUD FORMATION STACK



CLEANING LAMBDA FUNCTIONS



### Questions to Answer

1. How does DevSecOps fit into Governance, Risk and Compliance?

Answer: As we can see DEVSECOPS has a hierarchy

S3Buckets à CloudFormation Stack à Lambda à Pipeline

As we know that if any Transaction before fails, we can see the pipeline failing and starting from start to avoid risk.

In the Governance perspective in module 3 and Module 5 [AWS Keys and Versioning] in Lambda function in the segment of existing roles we need to select only Pipeline role for successful execution all other roles fail in the pipeline. Using IAM roles we can restrict and Govern the Pipelines

If we don’t follow the protocols or Guidance of an operation Pipeline fails. If we miss any resources in JSON file or even the indentation, we can see the fails and if we follow the Modules we can finish the task successfully.

1. How does DevSecOps contribute to the early detection and mitigation of vulnerabilities in the software development lifecycle?

Answer: As we can see PIPELINE has a hierarchy

Commit à StaticCodeAnalysis à Test Deployment à Production Deployment

Commit has s3 bucket which has our resources to test stack and Lambdas.

Static code analysis has two parts, CNFParsing and Lambda function which is our code/project and once this is success the pipeline checks the project. If there are any errors, we will get taken back to commit.

Test Deployment will check for IAM roles and Manual approval else back to Static code analysis and need to check lambdas and s3 buckets.

Production Deployment checks the size and stack behavior and output artifacts of the project any errors back to Teat Deployment.

In conclusion every time pipeline fails, we will start from S3Buckets à CloudFormation Stack à Lambda à Pipeline. So we can rewrite the project with better parameters avoiding basic mistakes so DEVSECOPS is like a sandbox for the projects by helping in early detection and mitigation of vulnerabilities in the software development lifecycle.

1. How do data privacy laws impact the design and operation of a DevSecOps pipeline, especially when dealing with personally identifiable information (PII) in cloud environments?

Answer: DevSecOps pipelines are significantly impacted by data privacy requirements, particularly when processing personal data in the cloud. These regulations, such as the CCPA and GDPR, specify how personal data must be gathered, stored, and protected. Limiting the quantity of personal information gathered and encrypting it to prevent hackers from accessing it are crucial.

To ensure that only the appropriate individuals may view this data, we also need to restrict who has access to it. We occasionally use techniques, such as using fictitious names in place of genuine ones, to protect data. Additionally, we must be cautious about how long we save data and make sure that it is deleted as soon as it is no longer needed.

In conclusion when doing lab in CloudFormation Stack in US-East so I can see the Pipeline created but I has no access because my S3 was in US-West so in this way we can create different access controls for people from EU because of GDPR. Using IAM roles for specific projects containing PII data.