INTEGRATING SECURITY INTO THE IAC PIPELINE II

Group 3

LIST OF MEMBERS

- Violette Naa Adoley Allotey
- Samuel Nartey
- Riverson Atta
- Marie-Pearl Otoo
- Samuel Ayim
- Nick Anderson
- Benard Solodzi
- Clement Owusu Bempah
- Priscilla Antwiwaa Duah
- Rose Anyama Owusu
- Sudais Abdul Hamid
- Eugene Essuman
- Faustina Ayornu

INTRO EDUCTION

CI/CD pipelines automate software delivery processes, ensuring rapid and reliable deployments. Trend Micro's Cloud One - Conformity Template Scanner helps enforce security best practices by scanning your CloudFormation templates for potential issues before deployment.

WHAT WE DID STEP-BY-STEP CODECOMMIT

1. Cloned the GitHub repo using git clone to work locally.
2. Modified the code, updating CloudFormation templates and pipeline configurations.
3. Staged changes with git add . and committed them using git commit -m "message".
4. Pushed updates back to GitHub with git push origin main.
5. Verified changes in the repo and confirmed CI/CD pipeline execution.

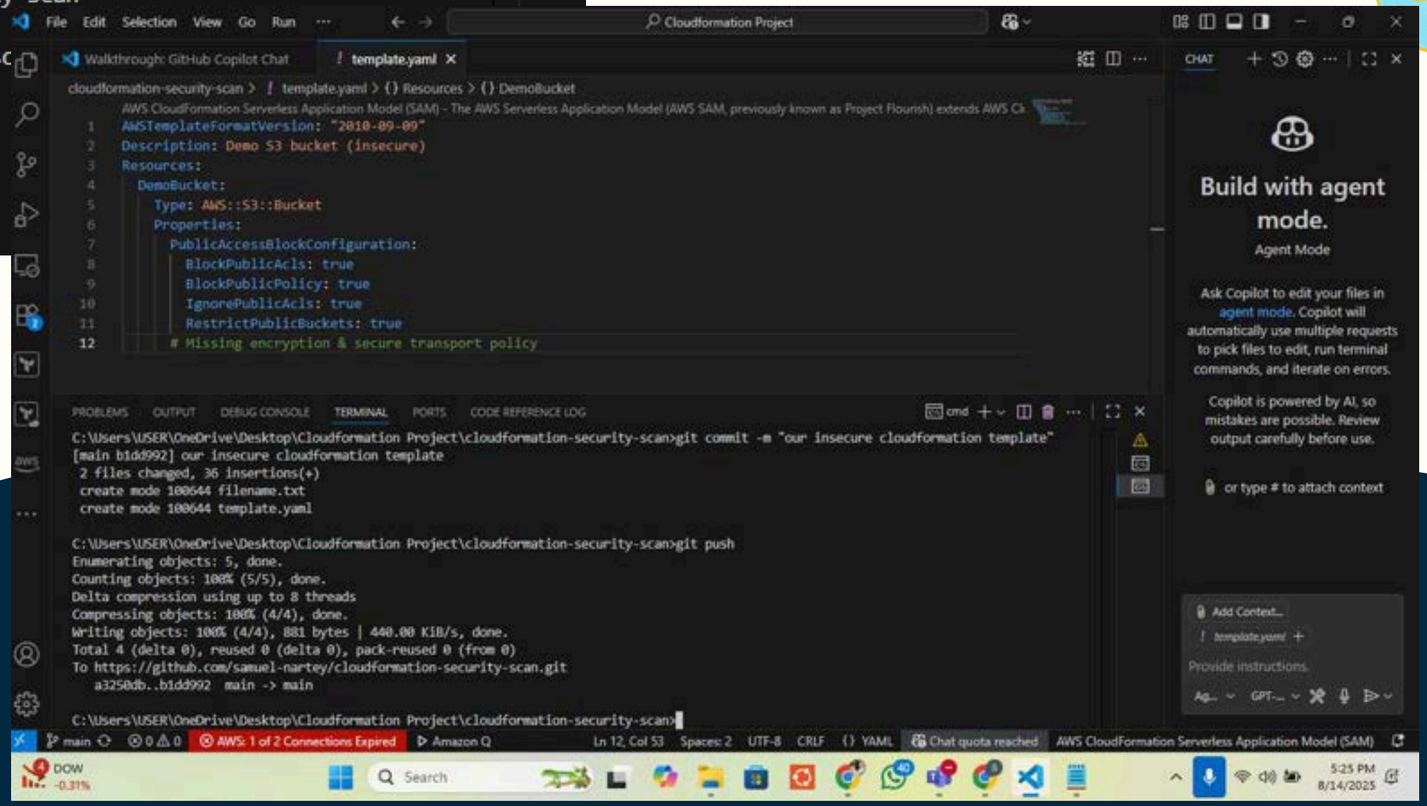
Key Improvements:

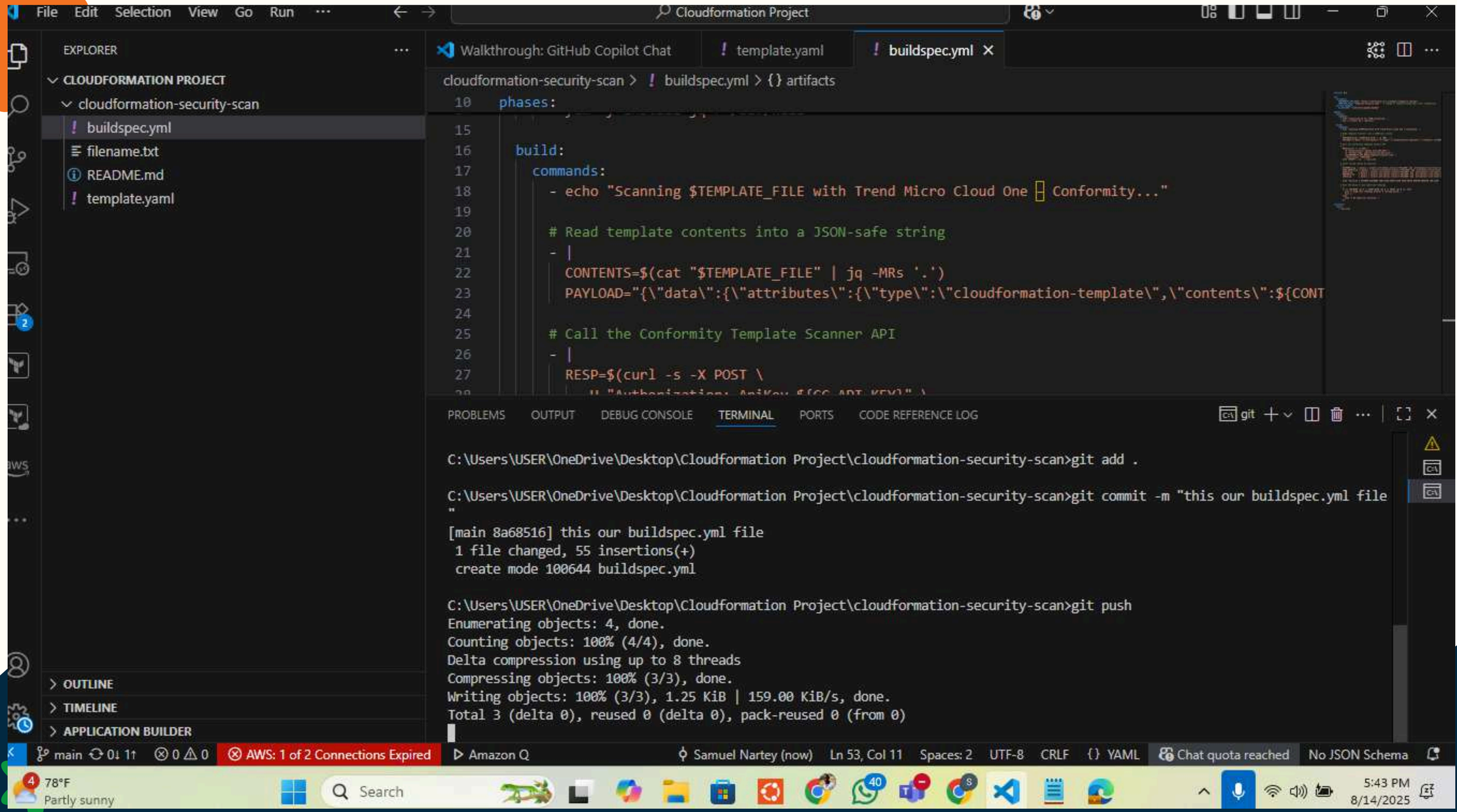
- Migrated from CodeCommit to GitHub for better collaboration.
- Established a secure, automated scanning workflow.
- Maintained version control best practices.

This streamlined our infrastructure-as-code process while ensuring security compliance.

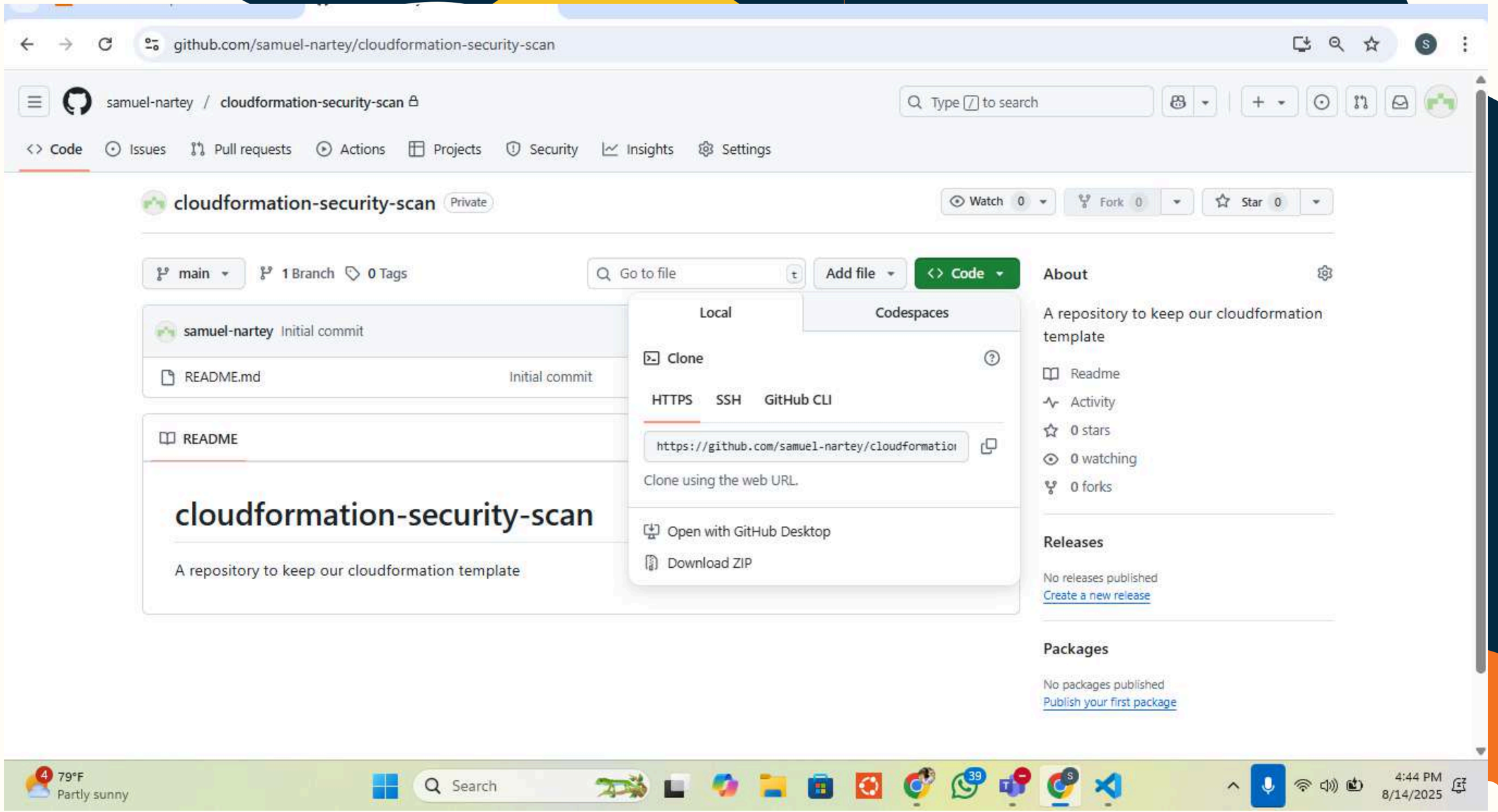
Cloning our github project repo using git clone and commiting/pushing our code back to our gitub repo using ,git add . git -m "commit message" and git push

```
C:\Users\USER\OneDrive\Desktop\Cloudformation Project>git clone https://github.com/your-username/cloudformation-secur
ity-scan.git
Cloning into 'cloudformation-security-scan'...
remote: Repository not found.
fatal: repository 'https://github.com/your-username/cloudformation-security-scan.git/' not found

C:\Users\USER\OneDrive\Desktop\Cloudformation Project>git clone https://github.com/samuel-nartey/cloudformation-secur
ity-scan.git
Cloning into 'cloudformation-security-scan'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (3/3), done.

C:\Users\USER\OneDrive\Desktop\Cloudformation Project>cd cloudformation-security-scan

C:\Users\USER\OneDrive\Desktop\Cloudformation Project\cloudformation-security-sc
```




File Edit Selection View Go Run
Cloudformation Project
EXPLORER
CLOUDFORMATION PROJECT
cloudformation-security-scan
buildspec.yml
filename.txt
README.md
template.yaml
Walkthrough: GitHub Copilot Chat
template.yaml
buildspec.yml
cloudformation-security-scan > buildspec.yml > {} artifacts
10 phases:
15
16 build:
17 commands:
18 - echo "Scanning $TEMPLATE_FILE with Trend Micro Cloud One Conformity..."
19
20 # Read template contents into a JSON-safe string
21 - |
22 CONTENTS=$(cat "$TEMPLATE_FILE" | jq -MRs '.')
23 PAYLOAD="{\"data\":{\"attributes\":{\"type\":\"cloudformation-template\",\"contents\":${CONT
24
25 # Call the Conformity Template Scanner API
26 - |
27 RESP=$(curl -s -X POST \
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS CODE REFERENCE LOG
git
C:\Users\USER\OneDrive\Desktop\Cloudformation Project\cloudformation-security-scan>git add .
C:\Users\USER\OneDrive\Desktop\Cloudformation Project\cloudformation-security-scan>git commit -m "this our buildspec.yml file
"
[main 8a68516] this our buildspec.yml file
1 file changed, 55 insertions(+)
create mode 100644 buildspec.yml
C:\Users\USER\OneDrive\Desktop\Cloudformation Project\cloudformation-security-scan>git push
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 8 threads
Compressing objects: 100% (3/3), done.
Writing objects: 100% (3/3), 1.25 KiB | 159.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
OUTLINE
TIMELINE
APPLICATION BUILDER
main 0↓ 1↑ 0 0
AWS: 1 of 2 Connections Expired
Amazon Q
Samuel Nartey (now) Ln 53, Col 11 Spaces: 2 UTF-8 CRLF {} YAML
Chat quota reached
No JSON Schema
78°F
Partly sunny
Search
5:43 PM
8/14/2025

GITHUB
REPO CREATION


github.com/samuel-nartey/cloudformation-security-scan
samuel-nartey / cloudformation-security-scan
Type / to search
Code
Issues
Pull requests
Actions
Projects
Security
Insights
Settings
cloudformation-security-scan
Private
Watch 0
Fork 0
Star 0
main
1 Branch
0 Tags
Go to file
Add file
Code
Local
Codespaces
Clone
HTTPS
SSH
GitHub CLI
https://github.com/samuel-nartey/cloudformatio
Clone using the web URL.
Open with GitHub Desktop
Download ZIP
samuel-nartey Initial commit
README.md
Initial commit
README
cloudformation-security-scan
A repository to keep our cloudformation template
About
A repository to keep our cloudformation template
Readme
Activity
0 stars
0 watching
0 forks
Releases
No releases published
Create a new release
Packages
No packages published
Publish your first package
79°F
Partly sunny
Search
4:44 PM
8/14/2025

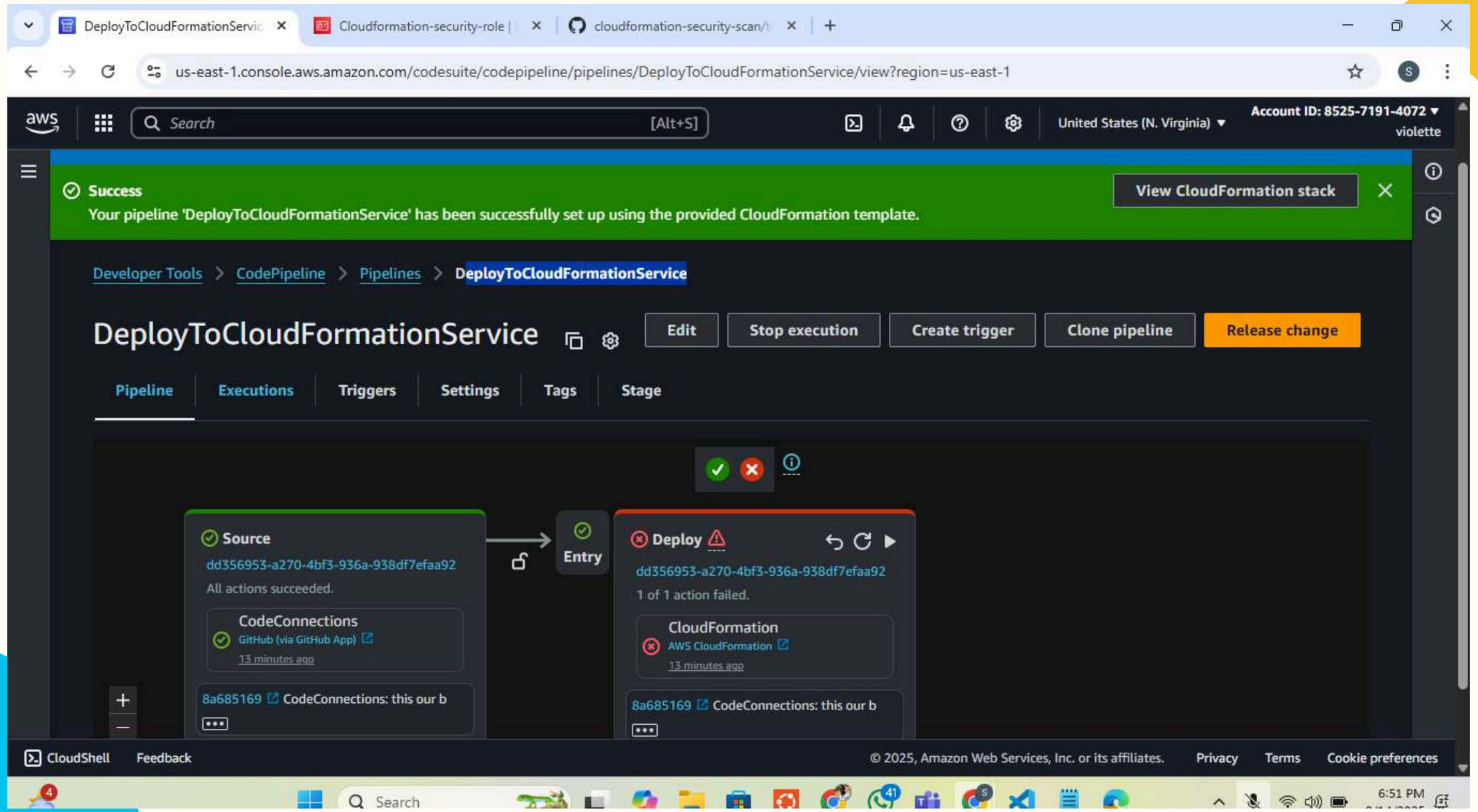
1. CodePipeline Successfully Checked Out the latest code from our GitHub repository during execution.
2. The Build Stage Passed, with the Conformity Template Scanner validating the CloudFormation template.
3. Deployment Failed
4. We Reviewed Pipeline Logs in AWS CodeBuild/CodePipeline to identify the root cause..

SUCCESSFUL

CHECKOUT BY CODE PIPELINE

SUCCESSFUL

CHECKOUT BY CODE PIPELINE

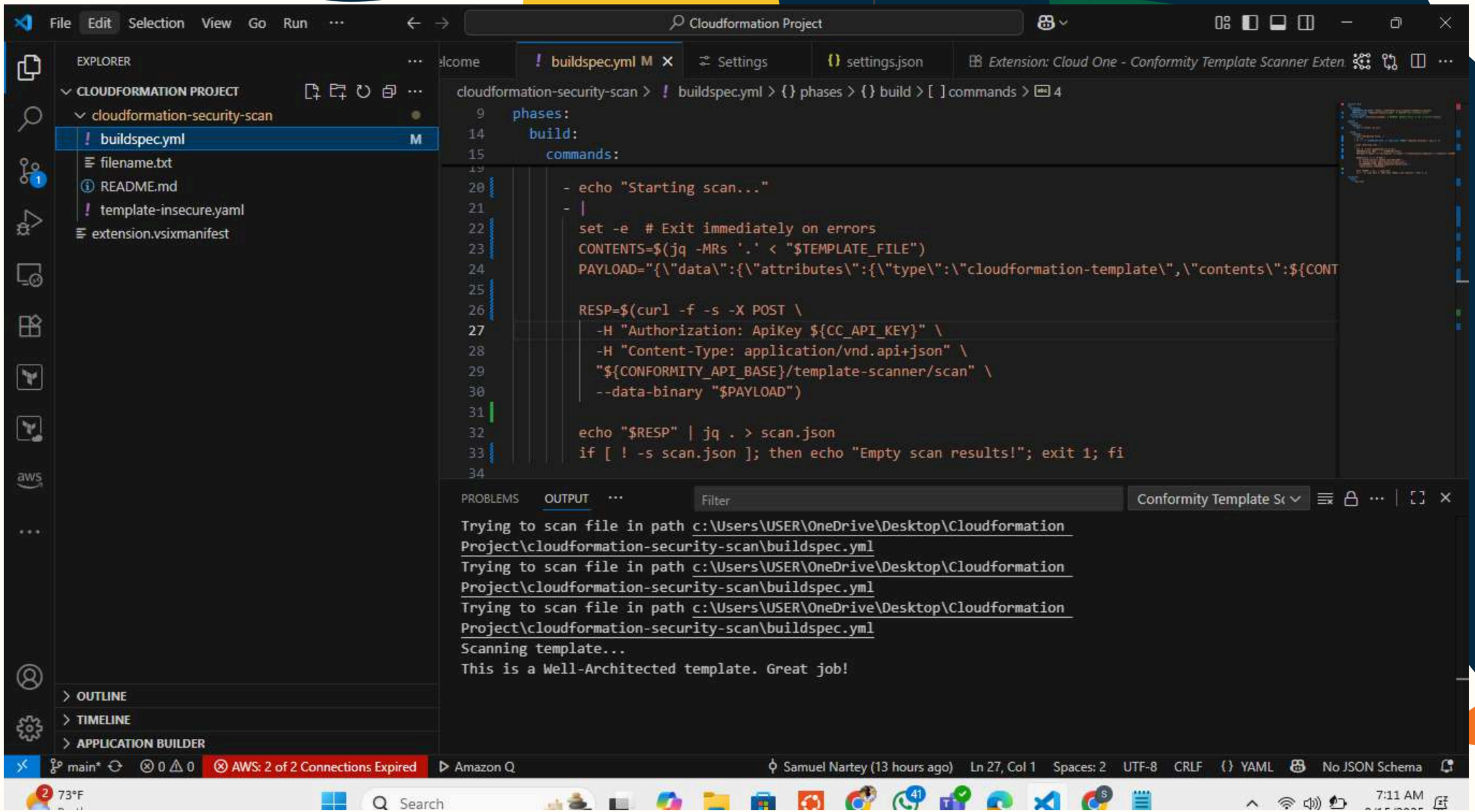

DeployToCloudFormationServic
Cloudformation-security-role |
cloudformation-security-scan/t
us-east-1.console.aws.amazon.com/codesuite/codepipeline/pipelines/DeployToCloudFormationService/view?region=us-east-1
aws
Search
[Alt+S]
United States (N. Virginia)
Account ID: 8525-7191-4072
violette
Success
Your pipeline 'DeployToCloudFormationService' has been successfully set up using the provided CloudFormation template.
View CloudFormation stack
Developer Tools
CodePipeline
Pipelines
DeployToCloudFormationService
DeployToCloudFormationService
Edit
Stop execution
Create trigger
Clone pipeline
Release change
Pipeline
Executions
Triggers
Settings
Tags
Stage
Source
dd356953-a270-4bf3-936a-938df7efaa92
All actions succeeded.
CodeConnections
GitHub (via GitHub App)
13 minutes ago
8a685169
CodeConnections: this our b
Entry
Deploy
dd356953-a270-4bf3-936a-938df7efaa92
1 of 1 action failed.
CloudFormation
AWS CloudFormation
13 minutes ago
8a685169
CodeConnections: this our b
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
6:51 PM

INSTALLED MICRO CLOUD

1. Configured the VSCode Environment by installing the Trend Micro Cloud One Conformity plugin and setting up API credentials.
2. Performed Local Template Scans on all CloudFormation templates before committing changes using the VSCode extension's scan functionality.
3. Identified and Resolved Security Issues during development by:
    - Analyzing scan results in VSCode's Problems tab
    - Addressing all critical and high-severity findings
    - Validating fixes with subsequent scans
4. Verified Clean Scans before staging changes with git add.
5. Only Committed Code that passed all Conformity security checks.

SUCCESSFUL SCANNING

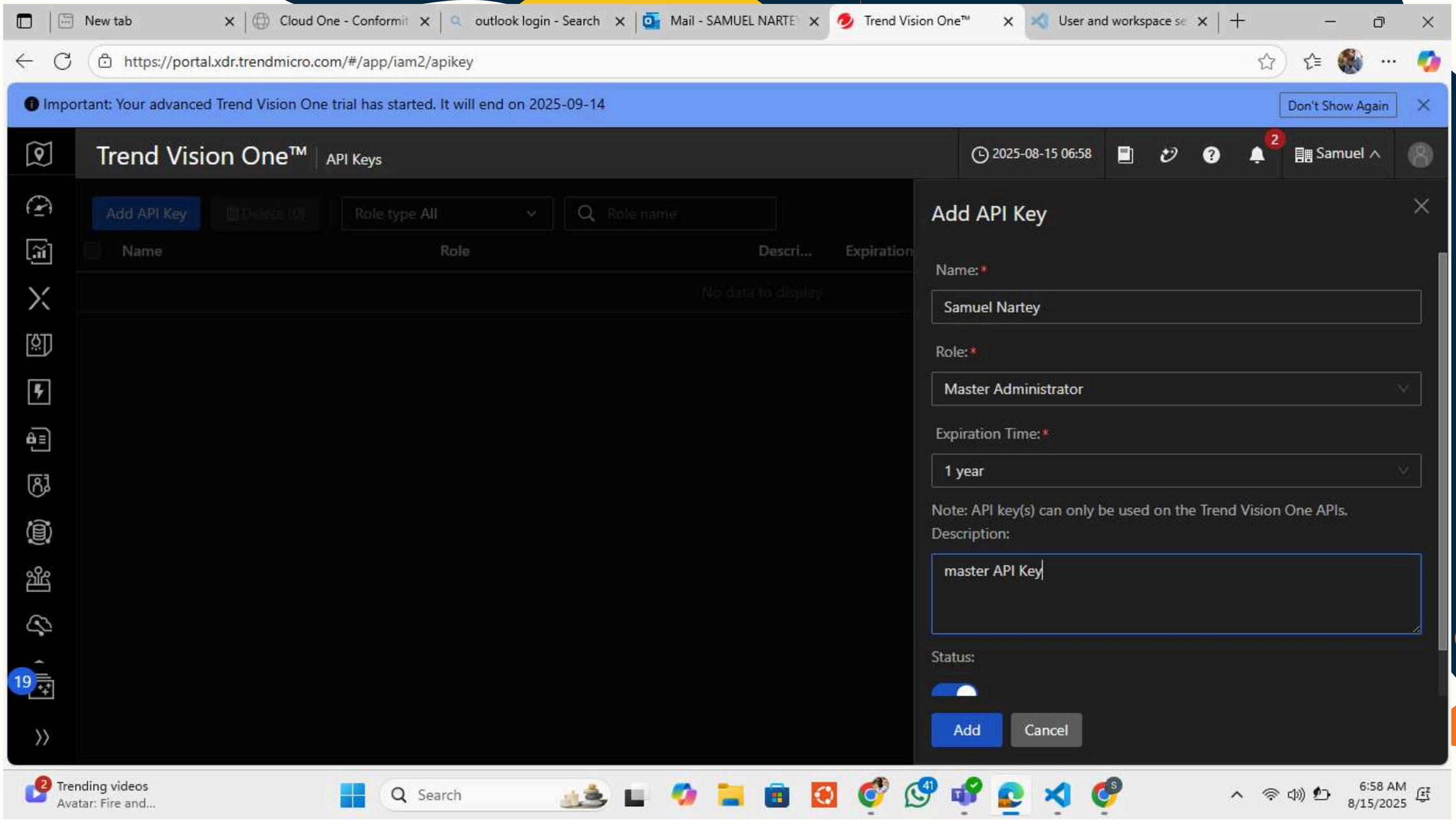
Successful scaning of template using trend one conformity scanner in vscode before commititng


File Edit Selection View Go Run
Cloudformation Project
EXPLORER
CLOUDFORMATION PROJECT
cloudformation-security-scan
buildspec.yml M
filename.txt
README.md
template-insecure.yaml
extension.vsixmanifest
buildspec.yml M
Settings
settings.json
Extension: Cloud One - Conformity Template Scanner Exten
cloudformation-security-scan > buildspec.yml > {} phases > {} build > [ ] commands > 4
phases:
build:
commands:
- echo "Starting scan..."
- |
set -e # Exit immediately on errors
CONTENTS=$(jq -MRs '.' < "$TEMPLATE_FILE")
PAYLOAD="{\"data\":{\"attributes\":{\"type\":\"cloudformation-template\",\"contents\":${CONT
RESP=$(curl -f -s -X POST \
-H "Authorization: ApiKey ${CC_API_KEY}" \
-H "Content-Type: application/vnd.api+json" \
"${CONFORMITY_API_BASE}/template-scanner/scan" \
--data-binary "$PAYLOAD")
echo "$RESP" | jq . > scan.json
if [! -s scan.json]; then echo "Empty scan results!"; exit 1; fi
PROBLEMS
OUTPUT
Filter
Conformity Template Sc
Trying to scan file in path c:\Users\USER\OneDrive\Desktop\Cloudformation Project\cloudformation-security-scan\buildspec.yml
Trying to scan file in path c:\Users\USER\OneDrive\Desktop\Cloudformation Project\cloudformation-security-scan\buildspec.yml
Trying to scan file in path c:\Users\USER\OneDrive\Desktop\Cloudformation Project\cloudformation-security-scan\buildspec.yml
Scanning template...
This is a Well-Architected template. Great job!
OUTLINE
TIMELINE
APPLICATION BUILDER
main*
0 0
AWS: 2 of 2 Connections Expired
Amazon Q
Samuel Nartey (13 hours ago)
Ln 27, Col 1
Spaces: 2
UTF-8
CRLF
YAML
No JSON Schema
73°F
Search
7:11 AM

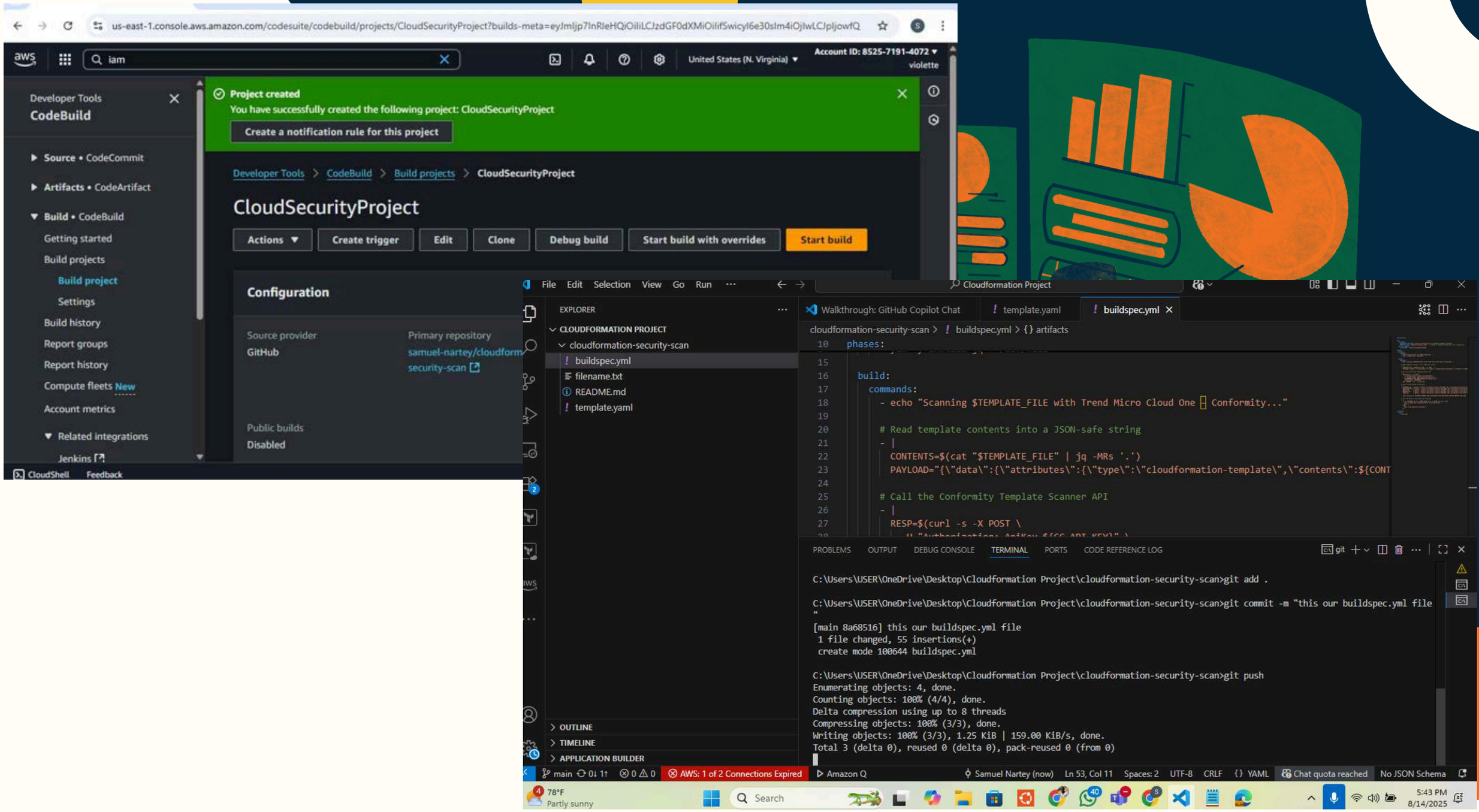
CREATING AN API KEY

creating an API key for trend one confromity scanner

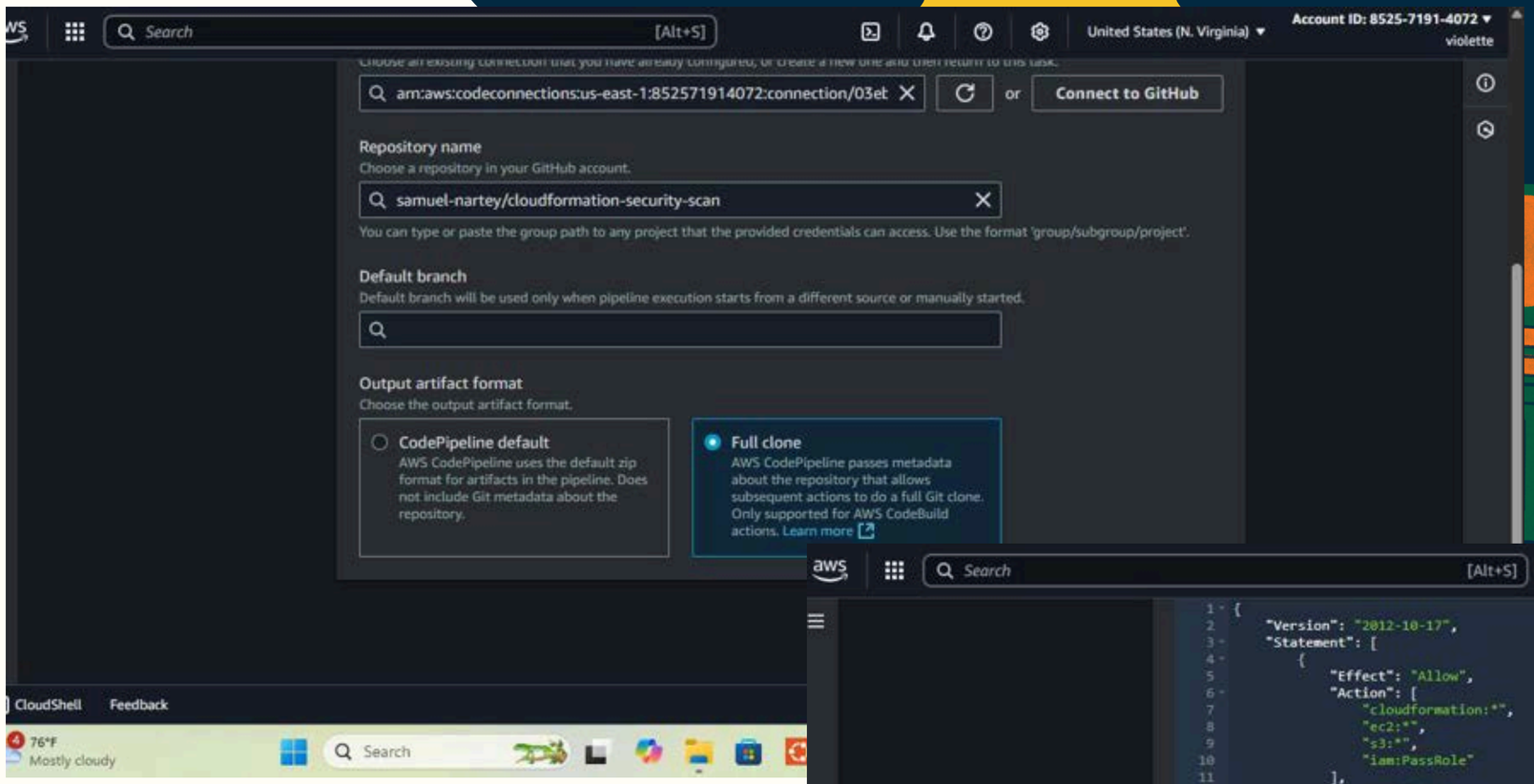
1. Logged into Cloud One Console
2. We accessed the Cloud One dashboard using our team credentials.
3. Navigated to Conformity Section
4. Selected "Conformity" from the Cloud One services menu.
5. Opened API Key Management
6. Went to "Account Settings" → "API Keys" section.
7. Generated New API Key
8. Clicked "Generate API Key"
9. Named it "CICD-Pipeline-Scanner" for clear identification
1. Set appropriate expiration period (we chose 1 year)
2. Assigned "Full Access" permissions for scanning functionality
3. Securely Stored the Key
4. Copied the generated key immediately (as it's only shown once)
5. Stored it in AWS Secrets Manager for pipeline access
6. Shared securely with team members via encrypted channels
7. Configured Access
8. Added the key to our CI/CD environment variables
9. Set it up in VSCode plugin settings for local scanning
10. Updated our buildspec.yaml to use the key during pipeline scans

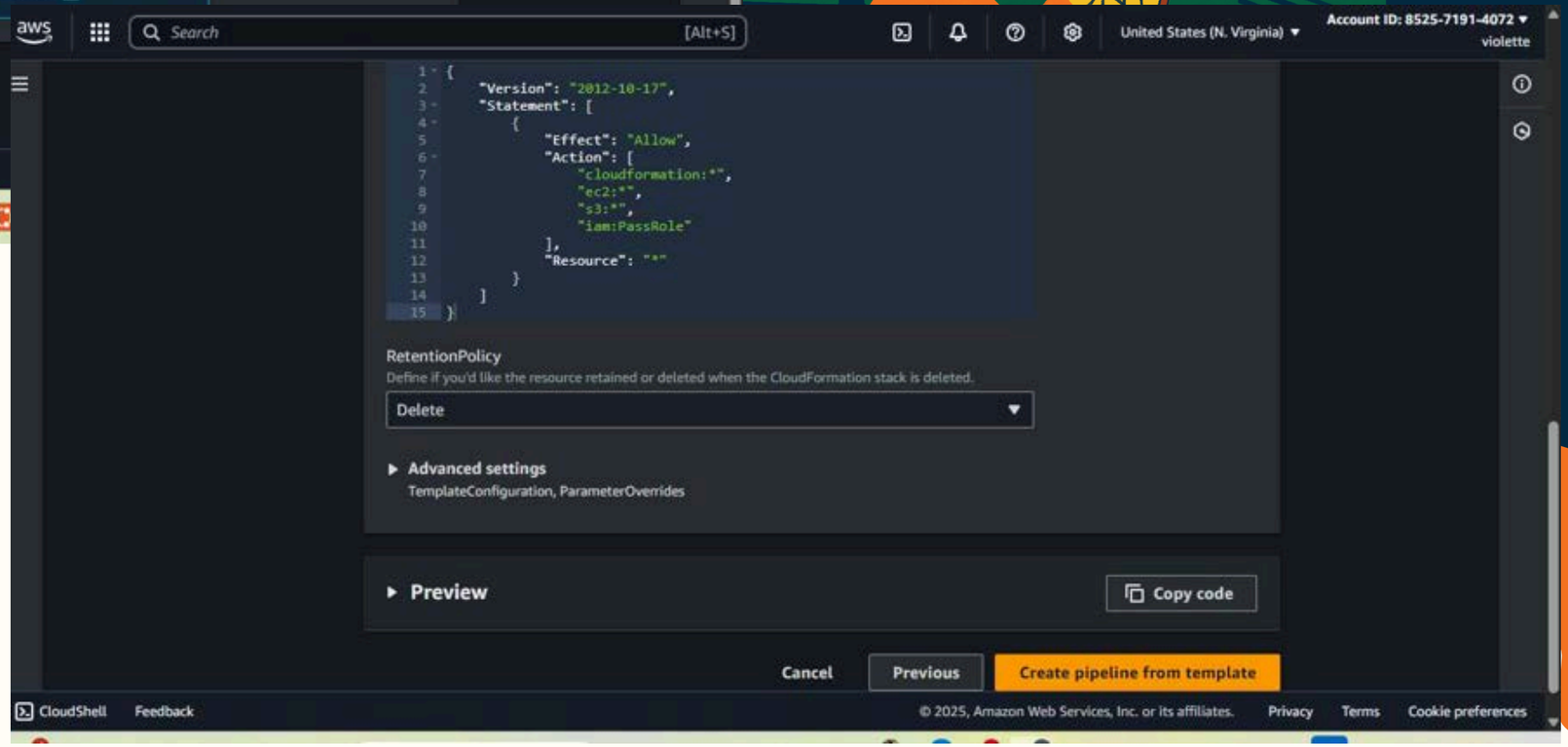

New tab
Cloud One - Conformit
outlook login - Search
Mail - SAMUEL NARTE
Trend Vision One™
User and workspace se
https://portal.xdr.trendmicro.com/#/app/iam2/apikey
Important: Your advanced Trend Vision One trial has started. It will end on 2025-09-14
Don't Show Again
Trend Vision One™
API Keys
2025-08-15 06:58
Samuel
Add API Key
Delete (0)
Role type All
Role name
Name
Role
Descri...
Expiration
No data to display
Add API Key
Name: *
Samuel Nartey
Role: *
Master Administrator
Expiration Time: *
1 year
Note: API key(s) can only be used on the Trend Vision One APIs.
Description:
master API Key
Status:
Add
Cancel
19
Trending videos
Avatar: Fire and...
Search
6:58 AM
8/15/2025

CONFIGURING OF CODEBUILD


us-east-1.console.aws.amazon.com/codesuite/codebuild/projects/CloudSecurityProject?builds-meta=eyJmIjp7InRleHQiOiIiLCJzdGF0dXMiOiIifSwicyI6e30sIm4iOjIwLCJpIjowfQ
aws
iam
United States (N. Virginia)
Account ID: 8525-7191-4072
violette
Developer Tools
CodeBuild
Source • CodeCommit
Artifacts • CodeArtifact
Build • CodeBuild
Getting started
Build projects
Build project
Settings
Build history
Report groups
Report history
Compute fleets New
Account metrics
Related integrations
Jenkins
Project created
You have successfully created the following project: CloudSecurityProject
Create a notification rule for this project
Developer Tools > CodeBuild > Build projects > CloudSecurityProject
CloudSecurityProject
Actions
Create trigger
Edit
Clone
Debug build
Start build with overrides
Start build
Configuration
Source provider
GitHub
Primary repository
samuel-nartey/cloudform
security-scan
Public builds
Disabled
CloudShell
Feedback
File Edit Selection View Go Run
Cloudformation Project
EXPLORER
CLOUDFORMATION PROJECT
cloudformation-security-scan
buildspec.yml
filename.txt
README.md
template.yaml
Walkthrough: GitHub Copilot Chat
template.yaml
buildspec.yml
cloudformation-security-scan > buildspec.yml > {} artifacts
10 phases:
16 build:
17 commands:
18 - echo "Scanning $TEMPLATE_FILE with Trend Micro Cloud One Conformity..."
20 # Read template contents into a JSON-safe string
22 CONTENTS=$(cat "$TEMPLATE_FILE" | jq -MRs '.')
23 PAYLOAD="{\"data\":{\"attributes\":{\"type\":\"cloudformation-template\",\"contents\":${CONT
25 # Call the Conformity Template Scanner API
27 RESP=$(curl -s -X POST \
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS CODE REFERENCE LOG
C:\Users\USER\OneDrive\Desktop\Cloudformation Project\cloudformation-security-scan>git add .
C:\Users\USER\OneDrive\Desktop\Cloudformation Project\cloudformation-security-scan>git commit -m "this our buildspec.yml file
"
[main 8a68516] this our buildspec.yml file
1 file changed, 55 insertions(+)
create mode 100644 buildspec.yml
C:\Users\USER\OneDrive\Desktop\Cloudformation Project\cloudformation-security-scan>git push
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 8 threads
Compressing objects: 100% (3/3), done.
Writing objects: 100% (3/3), 1.25 KiB | 159.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
OUTLINE
TIMELINE
APPLICATION BUILDER
main
AWS: 1 of 2 Connections Expired
Amazon Q
Samuel Nartey (now)
Ln 53, Col 11
Spaces: 2
UTF-8
CRLF
YAML
Chat quota reached
No JSON Schema
78°F
Partly sunny
Search
5:43 PM
8/14/2025

CONFIGURING CODEPIPELINE


Search
[Alt+S]
United States (N. Virginia)
Account ID: 8525-7191-4072
violette
arn:aws:codeconnections:us-east-1:852571914072:connection/03et
or
Connect to GitHub
Repository name
Choose a repository in your GitHub account.
samuel-nartey/cloudformation-security-scan
You can type or paste the group path to any project that the provided credentials can access. Use the format 'group/subgroup/project'.
Default branch
Default branch will be used only when pipeline execution starts from a different source or manually started.
Output artifact format
Choose the output artifact format.
CodePipeline default
AWS CodePipeline uses the default zip format for artifacts in the pipeline. Does not include Git metadata about the repository.
Full clone
AWS CodePipeline passes metadata about the repository that allows subsequent actions to do a full Git clone. Only supported for AWS CodeBuild actions. Learn more
CloudShell
Feedback
76°F
Mostly cloudy
Search


aws
Search
[Alt+S]
United States (N. Virginia)
Account ID: 8525-7191-4072
violette
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"cloudformation:*",
"ec2:*",
"s3:*",
"iam:PassRole"
],
"Resource": "*"
}
]
}
RetentionPolicy
Define if you'd like the resource retained or deleted when the CloudFormation stack is deleted.
Delete
Advanced settings
TemplateConfiguration, ParameterOverrides
Preview
Copy code
Cancel
Previous
Create pipeline from template
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

CONCLUSION

Despite implementing Trend Micro Cloud One Conformity scanning in our CI/CD pipeline, we encountered deployment challenges that prevented successful execution. While the scanning process worked as intended. These hurdles revealed gaps that we'll address later. .

THANK YOU