re:Invent 2019

ARC319

Security Vulnerability Identification and Remediation

Copyright © 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved.

This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.

All trademarks are the property of their owners.

© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.

Table of Contents

© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.

Prerequisites

This exercise requires access to Amazon Web Services. (AWS) console. You will be provided with a pre-provisioned AWS account and console access. As this is a 300-level workshop, it is assumed that you already have the knowledge required to satisfy the prerequisites for the workshop.

In the event you are conducting this exercise without a pre-provisioned account ensure the IAM user you are leveraging has full admin rights.

© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.

Problem Statement

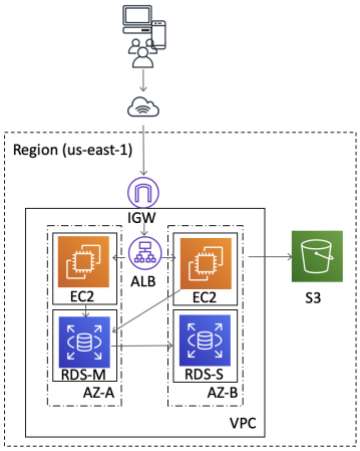
You are the lead DevSecOps engineer for a large global conglomerate. Various business lines are grown primarily through mergers and acquisitions. Your company just bought a new startup that specializes in an online blogging platform; and you have been asked to implement the technology stack that was acquired. The technology stack was done as infrastructure as code in a CloudFormation Template. This will be cake…. Right?

This workshop focuses on integrating the new web platform and ensuring a proper security posture is maintained. The lab will involve learning how to monitor, alert, and remediate security events in your AWS environments; primarily focusing on AWS Config and AWS Security Hub.

*****ARC319 will provide scripts and templates that intentionally create security holes, to be remediated. These templates should ONLY be deployed into temporary/sandbox AWS accounts and not into your corporate environment or anywhere with sensitive data.**

© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.

Solution Overview



The solution diagram, shown above, is to be deployed into the AWS region eu-central-1 (Frankfurt); and the architecture provides a WordPress environment to host the online blogging platform. AWS services included are Amazon EC2, Amazon S3, and Amazon RDS.

In the workshop, you will need to ensure that the new technology stack fits within your company's security posture. Your company is fairly new to AWS but has heard about services like AWS Config, AWS Security Hub, Amazon GuardDuty, and Amazon Macie to help secure their environment. This lab will focus on the **AWS Config** and **AWS Security Hub** for detective controls and remediation.

© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.

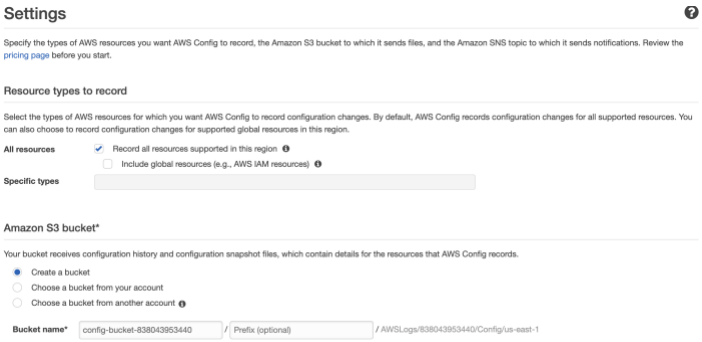
Task 1 – Enable AWS Config and AWS Security Hub

AWS Security Hub requires AWS Config to be turned on. Let's do that first.

Enable AWS Config

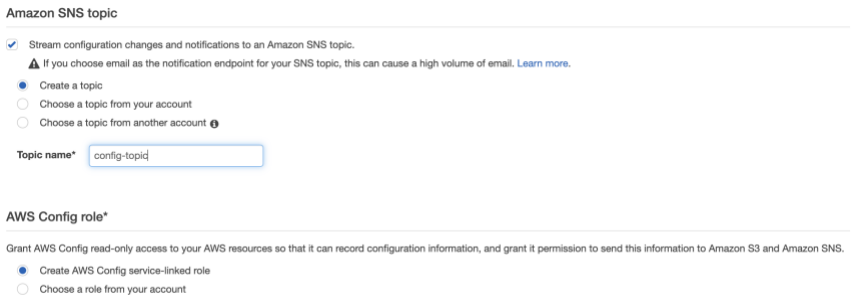
1. Log into the AWS console with the link and credentials provided by the lab instructor
2. Ensure your region is eu-central-1 (Frankfurt); (in the top right navigation bar)
3. Navigate to the AWS Config service (click services at the top; Config is under 'Management & Governance')
4. If you get the screen below, click 'Get Started'

5. In 'Step 1: Settings' ensure the following options are configured
    a. Resource types to record; "Record all resources supported in this region" Checked
    b. Amazon S3 bucket; 'Create Bucket' Checked



© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.

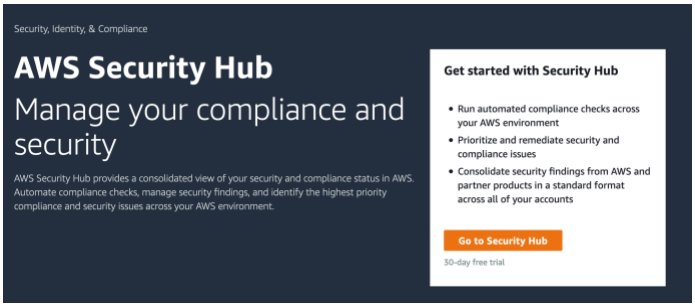
6. Continue configuring settings as indicated below
    a. Amazon SNS topic; “Create a topic” checked; leave the “Topic name” as default
    b. AWS Config role; “Create AWS Config service-linked role”



7. Click “Next”
8. On “Step 2: Rules” don’t select any (we’ll create these later)
9. Click “Skip”
10. On “Step 3: Review” click “Confirm”

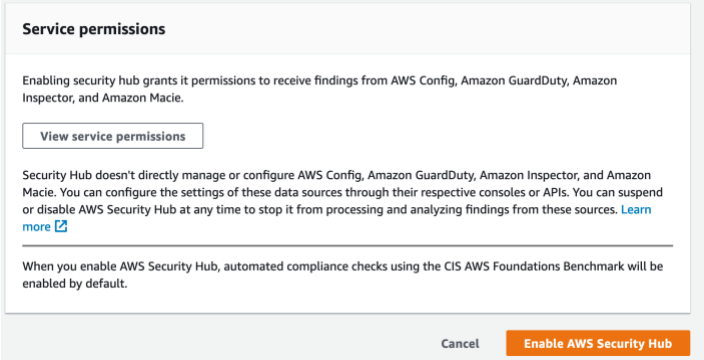
Enable AWS Security Hub

1. Navigate to the AWS Security Hub service (click services at the top; Security Hub is under ‘Security, Identity, & Compliance’)
2. Ensure your region is eu-central-1 (Frankfurt); (in the top right navigation bar)
3. If you get the screen below, click ‘Go to Security Hub’



4. On the next screen click ‘Enable AWS Security Hub’

© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.



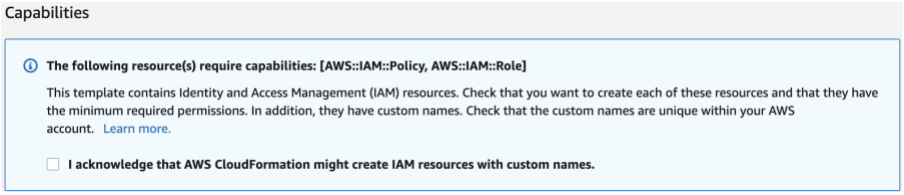
Task 2 – Create AWS Config rules/remediations

Launch the AWS Config CloudFormation stack in eu-central-1 (Frankfurt):

Launch Stack

The link opens the CloudFormation console in your account eu-central-1 region.

1. In 'Specify Template', click Next. (details should be pre-populated)
2. Under 'Specify Stack Details'
    a. Enter an email that you have access to in MyEmailAddress; this will be used for remediation notifications
    b. Review, but leave the defaults for TagCostCenterValue, TagWorkloadValue, and TagOwnerValue
3. In the Options section, scroll down to the bottom and click Next.
4. In the Review section, scroll down to the bottom, check the "I acknowledge…" checkbox and click Create. You may have to click the refresh button in CloudFormation console for the stack to appear; it should show CREATE_IN_PROGRESS under Status.

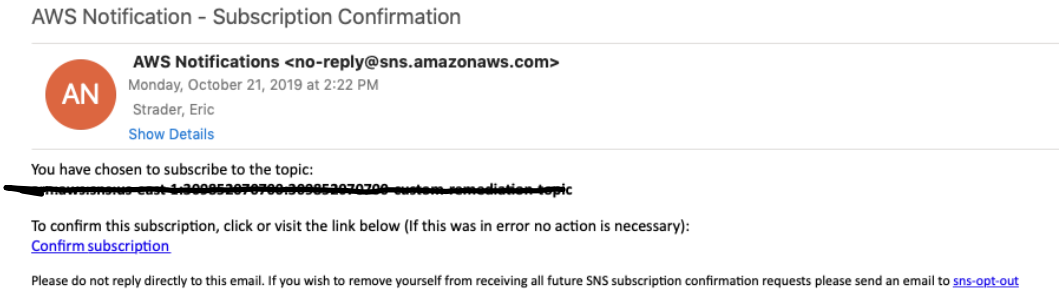


While the stacks are being built, we will discuss details around creating AWS Config rules and options that exist for remediation.

Once the stack creation has completed, do the following;

© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.

1. Check the resources output within the CloudFormation stack and copy the **'IAMRoleArn'** (you will need this later)
2. check the email addressed you entered in the stack details. You should see an email from AWS Notifications titled 'AWS Notification – Subscription Confirmation.' Open this email and click 'Confirm subscription.'



Task 3 – Deploy the Three Tier Web App CloudFormation Template

*****The steps below will deploy an environment with intentional security vulnerabilities, this template should ONLY be deployed into temporary/sandbox AWS accounts and not into your corporate environment or anywhere with sensitive data.**

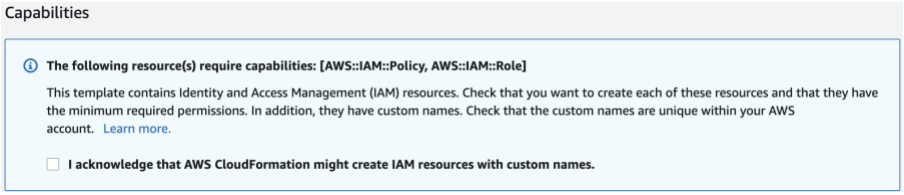
Launch the AWS Three Tier Web App CloudFormation stack in us-east-1 (N. Virginia):

Launch Stack

The link opens the CloudFormation console in your account in us-east-1 region.

1. In 'Specify Template', click Next.
2. In 'Specify Stack Details' click Next
3. In the Options section, scroll down to the bottom and click Next.
4. In the Review section, scroll down to the bottom, check the "I acknowledge…" checkbox and click Create. You may have to click the refresh button in CloudFormation console for the stack to appear; it should show CREATE_IN_PROGRESS under Status.

© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.



The creation of this stack can take up to 5 minutes. While the CloudFormation stack is being created we'll review the CloudFormation Template.

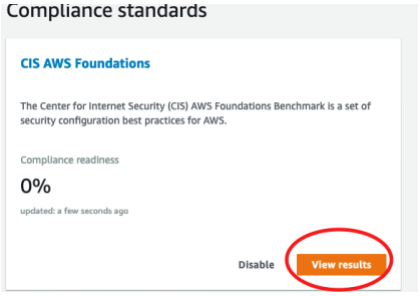
Discussion: Do you see anything that might generate security concerns? (Hint… Hint… Look at lines 295 and 350.)

Task 4 – Check your security findings

1. Navigate to the AWS Security Hub service (click services at the top; Security Hub is under 'Security, Identity, & Compliance')
2. Scroll through the 'Summary' section
3. Click on the 'Integrations' link on the left side and explore the different AWS Services and 3rd party solutions that integrate with Security Hub.

Discussion – AWS Security Hub is a centralized service to review aggregated and normalized findings. What other AWS Security services (and 3rd party solutions) could integrate?

4. Click on 'Compliance Standards'
5. Click on View Results



6. The foundational controls that are displayed are based on CIS Hardening; providing greater visibility and allowing you to identify additional vulnerabilities.
7. In the 'Filter Controls' search box type 'S3'

We can see a large number of findings are listed. This is great for an environment that is regularly monitored, unfortunately yours is not. In addition, what about internally mandated controls (versus CIS) like encrypted S3 buckets?

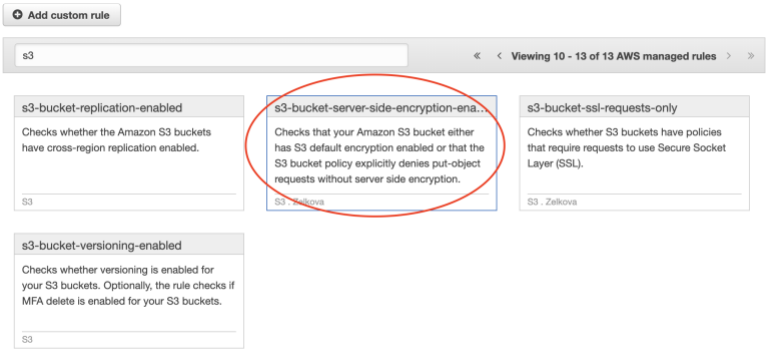
© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.

Discussion: How could you enable automated remediation for these findings or add new controls?

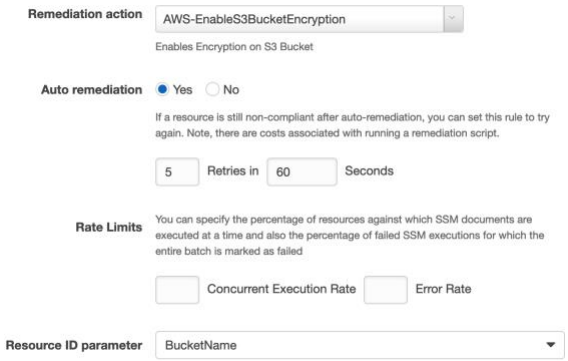
Task 5 – Create a new AWS Config Rule

1. Navigate to the AWS Config service (click services at the top; Config is under 'Management & Governance')
2. In the left side navigation pane, select rules
3. Select 'Add Rule'

4. Search for 's3-bucket-server' and select 's3-bucket-server-side-encryption-ena…'



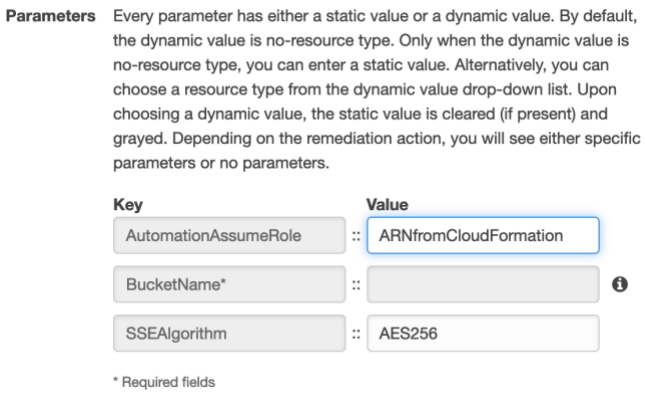
5. Leave the defaults up until the 'Choose Remediation Section'
6. Modify the following settings
    a. Remediation Action: choose 'AWS-EnableS3BucketEncryption'
    b. Change Auto Remediation to 'Yes'
    c. Resource ID Parameter: choose 'BucketName'



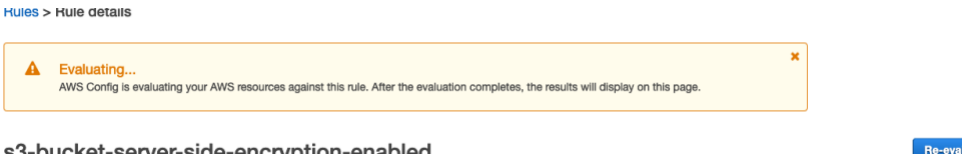
7. In the parameters section change AutomationAssumeRole to the arn of the IAM role created in the Task 3 ('IAMRoleArn' Noted earlier)

© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.

8. Leave SSE Algorithm as ‘AES256’



9. Click Save
10. In the ‘rules’ window select the rule titled ‘S3-bucket-server-side-encryption-enabled’
    a. It may take a couple minutes for the rule to evaluate, if you receive the following message wait 1-2 minutes and refresh the screen



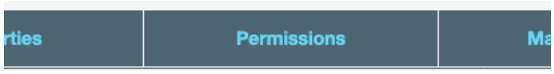
11. Check the action status and verify that encryption was turned on for your S3 Bucket with an ‘Action executed successfully’ message

Task 6 – Review the AWS Config deployed rules

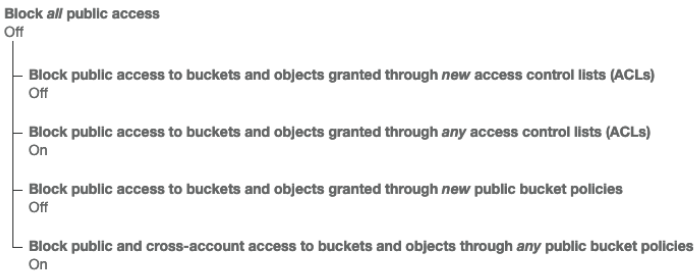
1. Navigate to the AWS Config service (click services at the top; Config is under ‘Management & Governance’)
2. In the left navigation pane click on Rules
3. Look at the rule titled ‘S3_BUCKET_PUBLIC_READ_PROHIBITED’
    a. Click the rule name
    b. Click Edit
    c. Explore the remediation actions
    d. We see that this rule is being remediated with a Systems Manager pre-defined remediation
    e. Click Cancel
    f. Go back into the rule (clicking on the name) and check the ‘Compliance Status’ section at the bottom
        i. If resources aren’t populated yet, move on and come back to check after subsequent steps.

© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.

ii. If resources exist, click on the resource name
iii. Click the 'Manage Resource' button in the top right
iv. Once in the corresponding S3 bucket, click the 'Permissions' tab



v. View the 'Block public access' rule and validate that it looks like the following screenshot



vi. Congratulations, your config rule has blocked public access!

***Note - *It may could take some time for the rule to evaluate/remediate, feel free to use the 're-evaulate' button at the top of the rule or check back later in the lab*

4. Now look at the rule that includes 'REQUIRED_TAGS' in the name
    a. Click the rule name
        i. Click Edit for the rule (top right)
        ii. Notice that the remediation is 'AWS-PublisSNSNotification'
        iii. This rule doesn't have a corresponding AWS Systems Manager pre-defined remediation; it is being remediated with a custom Lambda Function triggered via an SNS topic.
5. Open AWS Lambda (click services at the top; Lambda is under 'Compute')
    a. Open the Lambda function where the name includes 'RequiredTags'
    b. Review the Lambda function to understand how it is remediating inconsistent/non-existent tags
6. Go back to the config rule and click the name of one of the resources that has been remediated (under 'Rules' | Compliance Status section)
    a. Explore this section by looking at the compliance timelines

    b. Now go back to the 'resources' screen for the resource you selected and choose 'Manage Resource' in top right

© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.

c. Validate that the tags have been updated in the corresponding resource, they should be as follows
    i. CostCenter = 900124-984
    ii. Owner = Brad Pitt (but not THAT Brad Pitt)
    iii. Workload=WordPress
d. Now check your email (email used when you deployed the CloudFormation Stack) and validate that you received notifications regarding missing required tags.

***Note - *It may could take some time for the rule to evaluate/remediate*

Task 7 – Additional Testing

Now that you have deployed the environment and remediated the security vulnerabilities through a combination of AWS Config and AWS Security Hub test out deploying resources with known vulnerabilities.

Example

- Create a new S3 bucket not encrypted with public read/write settings
- Create a new resource with improper tags on it

Once deployed go back in and check the settings.

Do the vulnerabilities still exist?

Task 8 – Cleanup

As these are temporary accounts, environments will be deleted upon completion. However; best practices would indicate to delete each deployed CloudFormation stack to avoid incurring additional costs. If you encounter errors with deleting the Config.yaml CloudFormation Stack, go to AWS config open any rule that hasn't been deleted > click edit > click delete rule (bottom of page). Once you have done this try to delete the CloudFormation Stack again.

If you have the AWS CLI configured or are familiar with a Node JS development environment, you can use the material https://github.com/collinforrester/aws-config-helpers#aws-config-helpers to help clean up.

Manually disable Security Hub and Config as follows

- Disable Security Hub (settings > general > disable)
- Disable Config (settings > edit > uncheck Enable Recorder > save)

© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.

Task 9 – Optional (further reading/discussion)

- AWS Config
- AWS Security Hub
- CIS Hardening
- Amazon Macie
- Amazon GuardDuty

Appendix A: Troubleshooting common issues

Problem: My CloudFormation stack shows failed after I attempt to delete it.
Fix: Sometimes Config Rules with remediations fail to delete through the CloudFormation process. If you experience this, go into AWS Config and delete the rules, then delete the CloudFormation stack; it will then succeed.

Problem: I created a new AWS Config rule but the remediation isn't working.
Fix: Verify that you used the IAMRoleArn from the Config CloudFormation deployment. Additionally, if you chose a different remediation you will need to update the IAM role with proper policies.

Problem: I don't see the stack that I deployed.
Fix: Verify that you are working in the eu-central-1.

Problem: I have created an AWS Config rule but it is not finding any resources out of compliance?
Fix: Depending on the type of rule and size of the account it can take some time for the rule to evaluate/remediate. Check back in later.

© 2019 Amazon Web Services, Inc. and its affiliates. All rights reserved.