Deploying CIS Benchmarks with Auto Remediation for Amazon AWS Services

A Project Report

submitted by

Ayush Bajirao

(301558706)

Brij Bhatia

(301553818)

Divya Thomas

(301564401)

Poornima

(301559076)

under the supervision of

Reza Bagheri

in partial fulfillment of

the requirements for the degree of

Master of Professional Computer Science

December 2022

Contents

Chapter 1

Introduction

1.1 Introduction

The CIS Foundations Benchmarks provide prescriptive guidance for configuring, deploying, and securing services in public cloud environments including best practices for cloud security. In this project, we are analyzing CIS Amazon Web Services (AWS) Foundations Benchmark. The AWS CIS Foundations Benchmark is a compliance standard that provides guidelines specifically for implementing security controls, hardening and monitoring AWS accounts.

CIS created the AWS Foundations Benchmark, a set of security configuration best practices for Amazon Web Service (AWS). These best practices offer highly specific, detailed guidelines for implementing security controls in AWS services and validating their effectiveness.

1.2 What is CIS?

The Center for Internet Security (CIS) is a non-profit security research body that develops best practices for securing IT systems and data, including cloud security best practices. The CIS Benchmarks draw on the expertise of cybersecurity and IT professionals from government, business, and academia from around the world.

1.3 What are CIS Benchmarks?

CIS Benchmarks from the Center of Internet Security (CIS) are a set of globally recognized and consensus-driven best practices to help security practitioners implement and manage their cybersecurity defenses. Developed with a global community of security experts, the guidelines help organizations proactively safeguard against emerging risks. Companies implement the CIS Benchmark guidelines to limit configuration-based security vulnerabilities in their digital assets.

1.4 What is the CIS AWS Foundations Benchmark?

The CIS AWS Foundations Benchmark is a compliance standard for securing Amazon Web Services resources. The benchmark offers prescriptive instructions for configuring AWS services in accordance with industry best practices. In May 2018, the Center for Internet Security (CIS) published version 1.2.0. CIS AWS recommendations are decided upon by consensus of independent security experts.

1.5 Why is CIS AWS Compliance Important?

Any organization that uses cloud resources provided by Amazon Web Services can help safeguard sensitive IT systems and data by complying with the CIS AWS Foundations Benchmark. Cloud misconfigurations and cyber attacks are a constant concern for organizations that operate in the cloud, so security is of utmost importance.

CIS notes that the benchmark is for anyone who plans to ”develop, deploy, assess, or secure solutions in Amazon Web Services,” so DevOps personnel, security analysts, and compliance analysts in particular can benefit from evaluating their infrastructure against the benchmark and adhering to its recommendations.

When you implement CIS Benchmarks, you can better secure your legacy systems against common and emerging risks by taking steps such as these:

- Disabling unused ports
- Removing unnecessary app permissions
- Limiting administrative privileges

IT systems and applications also perform better when you disable unnecessary services.

1.6 CIS Benchmarks example

By adopting CIS Benchmarks, your organization can gain several cybersecurity benefits, such as the following:

- Expert cybersecurity guidelines: CIS Benchmarks provide organizations with a framework of security configurations that are expert-vetted and proven. Companies can avoid trial-and-error scenarios that put security at risk and benefit from the expertise of a diverse IT and cybersecurity community.
- Globally recognized security standards: CIS Benchmarks are the only best practice guides that are globally recognized and accepted by governments, businesses, research, and academic institutions alike. Thanks to the global and diverse community that works on a consensus-based decision-making model, CIS Benchmarks have far wider applicability and acceptability than regional laws and security standards.
- Cost-effective threat prevention: The CIS Benchmark documentation is freely available for anyone to download and implement. Your company can get up-to-date, step-by-step instructions for all kinds of IT systems at no cost. You can achieve IT governance and avert financial and reputational damage from preventable cyberthreats.
- Regulatory compliance: CIS Benchmarks align with major security and data privacy frameworks such as these:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)

Implementing CIS Benchmarks is a big step toward achieving compliance for organizations that operate in heavily regulated industries. They can prevent compliance failures due to misconfigured IT systems.

1.7 CIS AWS Foundations Benchmark Compliance

The CIS AWS Foundations Benchmark is composed of 4 sections with a total of 49 controls known as "recommendations." The 4 sections include:

1. **Identity and Access Management**
   The first section contains recommendations for configuring IAM-related options. For example, CIS AWS 1.11 encourages users to "Ensure IAM password policy expires passwords within 90 days or less." Regular password changes can limit the risk of a breach due to stolen or compromised passwords, reuse of the same password in different systems, and other potentially dangerous situations. Organizations can promote password hygiene by creating a password policy that requires users to create a new password every 90 days or less.

2. **Logging**
   The second section contains recommendations for configuring account logging features. CIS AWS 2.7 suggests that users "Ensure CloudTrail logs are encrypted at rest using KMS CMKs." Using KMS customer master keys to encrypt CloudTrail log files provides additional confidentiality controls on log data. For each CloudTrail trail, enable encryption and specify a KMS key ID.

3. **Monitoring**
   The third section contains recommendations for configuring AWS log metric filters and alarms to monitor services. To comply with CIS AWS 3.1, "Ensure

a log metric filter and alarm exist for unauthorized API calls," you can direct CloudTrail logs to CloudWatch logs and establish a corresponding metric filter and alarm. Monitoring API calls can help decrease the time needed to detect malicious activity, so set up a metric filter, alarm, SNS topic, and subscription to track suspicious calls.

4. **Networking**
   The fourth section contains recommendations for configuring security-related VPC attributes. For example, CIS AWS 4.1, "Ensure no security groups allow ingress from 0.0.0.0/0 to port 22," helps prevent the internet at large from accessing your servers through SSH. You can achieve this by auditing your security groups and removing any inbound rules that allow unrestricted traffic to port 22.

1.8 How are CIS Benchmarks developed?

CIS communities follow a unique consensus-based process to develop, approve, and maintain CIS Benchmarks for different target systems. Overall, the CIS Benchmark development process looks like this:

- The community identifies the need for a specific benchmark.
- They establish the scope of the benchmark.
- Volunteers create discussion threads on the CIS WorkBench community website.
- Experts from the specific IT systemâs CIS community spend time reviewing and discussing the working draft.
- The experts create, discuss, and test their recommendations until they reach a consensus.
- They finalize the benchmark and publish it on the CIS website.
- More volunteers from the community join in on the CIS Benchmark discussion.

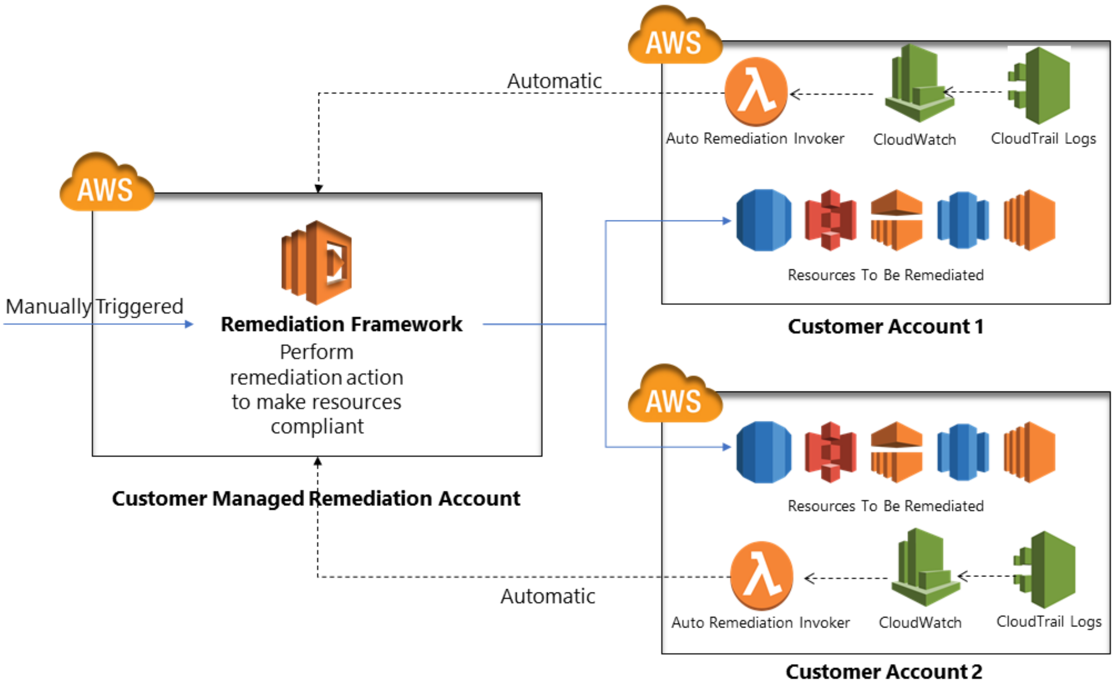
- The consensus team considers the feedback from those who implement the benchmark.
- They make revisions and updates in the new versions of the CIS Benchmark.

1.9 How our solution works?

This remediation solution is designed to continuously perform remediation in near real-time of non-compliant AWS resources. It helps to set up security configurations whenever new resources get created in AWS account.

The remediation framework uses Cloudwatch event rules, CloudTrail, CloudWatch log group, the remediation lambda functions, and the appropriate IAM roles.

1. AWS account administrator resources in AWS account.
2. CloudTrail and CloudWatch event bus collects the events occurred in AWS account and trigger appropriate event rule.
3. CloudWatch event rule trigger the auto-remediation in near real-time in its region.
4. Remediation functions setup required security configuration on the resources.

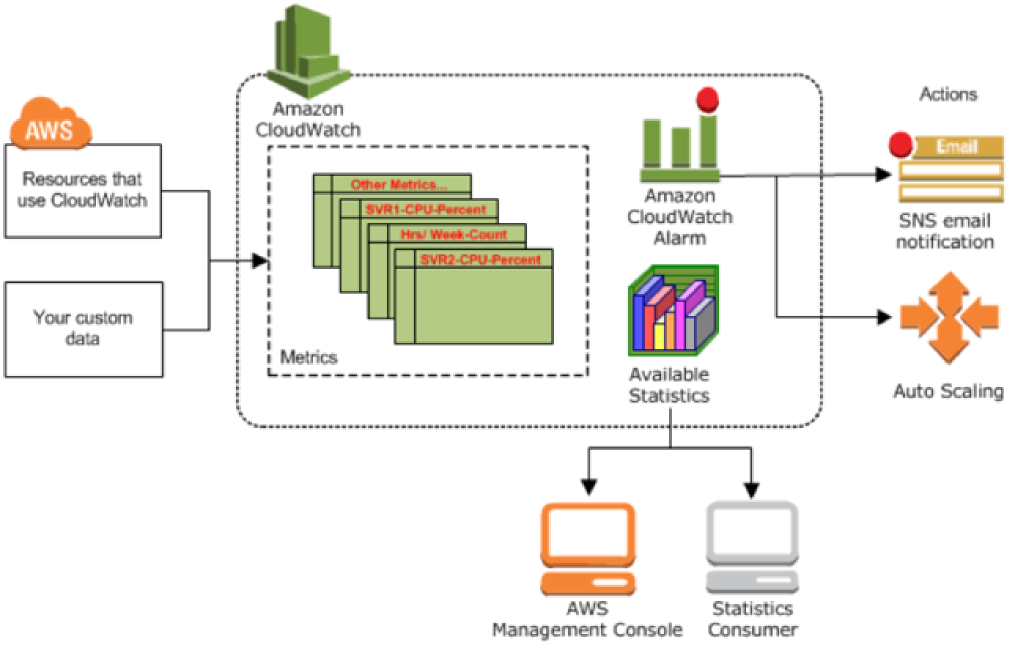

AWS
Automatic
Auto Remediation Invoker
CloudWatch
CloudTrail Logs
AWS
Manually Triggered
Remediation Framework
Perform remediation action to make resources compliant
Resources To Be Remediated
Customer Account 1
AWS
Resources To Be Remediated
Customer Managed Remediation Account
Automatic
Auto Remediation Invoker
CloudWatch
CloudTrail Logs
Customer Account 2

Chapter 2

Amazon Web Services Components

2.1 CloudWatch

CloudWatch is an AWS monitoring and management service which is designed for the purpose of maintaining the services and resources which are used. It is used to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in Amazon Web Services resources. It can monitor Amazon Web Services resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by applications and services, and any log files generated by applications.



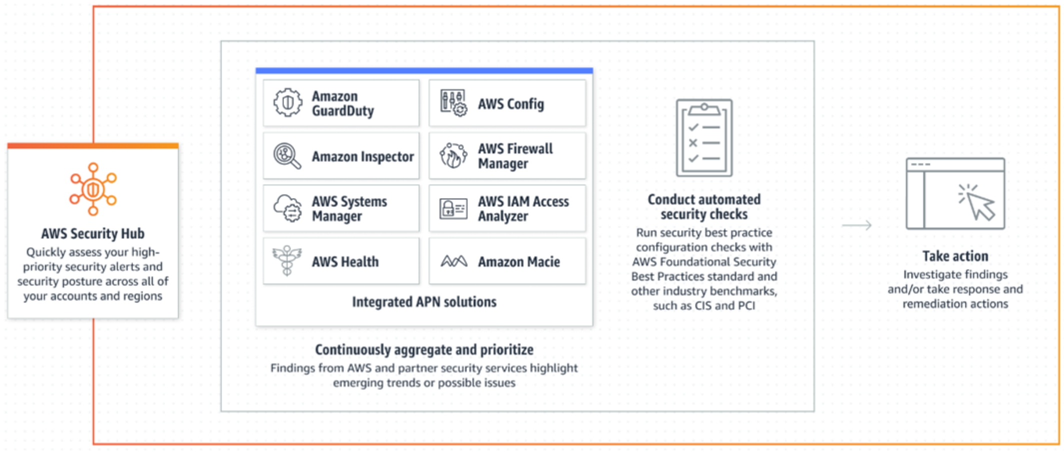
Amazon CloudWatch can be accessed via API, command-line interface, AWS SDKs, and the AWS Management Console. It receives and provides metrics for all Amazon EC2 instances and should work with any operating system currently supported by the Amazon EC2 service. It integrates with AWS Identity and Access Management (IAM) which helps to specify which CloudWatch actions a user in an AWS Account can perform. For example, create an IAM policy that gives only certain users in an organization permission to use GetMetricStatistics. They could then use the action to retrieve data about the cloud resources.

2.2 Amazon CloudWatch Log

CloudWatch Logs helps users to access, monitor and store log files from EC2 instances, CloudTrail, Lambda functions, and other sources. It helps to troubleshoot systems and applications and also offers near real-time monitoring and users can search for specific phrases, values, or patterns.

2.3 AWS Security Hub

AWS Security Hub is a cloud security posture management service that performs security best practice checks, aggregates alerts, and enables automated remediation. Security Hub collects security data from across AWS accounts, services, and supported third-party partner products and helps to analyze security trends and identify the highest priority security issues. Security Hub provides a pre-built dashboard to help organize and prioritize any issues or alerts for AWS environments discovered from security checks. Security Hub in general saves time by creating accurate reports on security gaps in AWS environment.


AWS Security Hub
Quickly assess your high-priority security alerts and security posture across all of your accounts and regions
Amazon GuardDuty
AWS Config
Amazon Inspector
AWS Firewall Manager
AWS Systems Manager
AWS IAM Access Analyzer
AWS Health
Amazon Macie
Integrated APN solutions
Continuously aggregate and prioritize
Findings from AWS and partner security services highlight emerging trends or possible issues
Conduct automated security checks
Run security best practice configuration checks with AWS Foundational Security Best Practices standard and other industry benchmarks, such as CIS and PCI
Take action
Investigate findings and/or take response and remediation actions

Reduce the time and effort to collect information: collect and prioritize security findings results across multiple accounts from integrated AWS services and third-party partner products.

Automation capability: automate remediation of specific findings, and define custom actions to be taken when the specific findings are received. The findings can also be sent to the ticketing system or automatic remediation software.

Best practices and standards security checks: Security Hub runs continuous security checks following AWS best practices and industry standards, provides the results of these checks as scores, and identifies AWS accounts and resources that require attention.

Consolidated view across AWS accounts: consolidate security findings from multiple AWS accounts and helps to easily identify potential threats and take necessary action.

Findings aggregation across AWS regions: view findings across multiple regions by setting an aggregation region and then linking other AWS regions to it.

2.4 EventBridge

EventBridge is a serverless service that uses events to connect application components together, making it easier for you to build scalable event-driven applications. EventBridge receives an event, an indicator of a change in environment, and applies a rule to route the event to a target. Rules match events to targets based on either the structure of the event, called an event pattern, or on a schedule. All events that come to EventBridge are associated with an event bus. Rules are tied to a single event bus, so they can only be applied to events on that event bus.

2.5 EventBridge Building Blocks

1. **Events**

   An event is a real-time change in a system, data, or environment. This change can be either in your application or in an AWS service or a SaaS partner service.

2. **Event sources**

   An event source is used to ingest events from a SaaS partner, AWS Services, or your own applications.

3. **Event buses**

   An event bus is a pipeline that receives events. Rules associated with the event bus evaluate events as they arrive. Each rule checks whether an event matches the ruleâs criteria.

4. **Rules**

   A rule matches incoming events and sends them to targets for processing. A single rule can send an event to multiple targets, which then run in parallel. Rules are based either on an event pattern or a schedule.

   An **event** pattern defines the event structure and the fields that a rule matches.

   Rules that are based on a **schedule** perform an action at regular intervals.

5. **Targets**

   A target is a resource or endpoint that EventBridge sends an event to when the event matches the event pattern defined for a rule. The rule processes the event data and sends the pertinent information to the target.

2.6 CloudFormation

AWS CloudFormation is a service that gives developers and businesses an easy way to create a collection of related AWS and third-party resources, and provision and manage them in an orderly and predictable fashion.

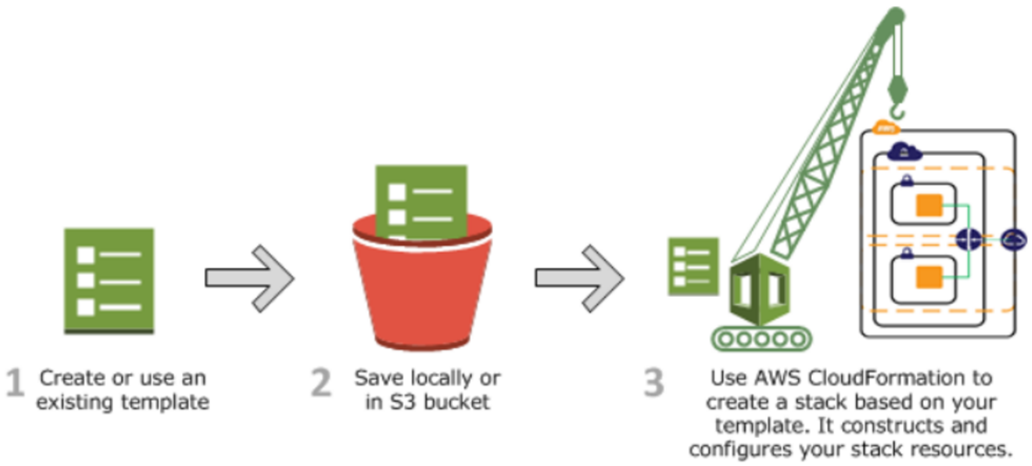
Developers can deploy and update, compute many other resources in a simple, declarative style that abstracts away the complexity of specific resource APIs. AWS CloudFormation is designed to allow resource lifecycles to be managed repeatedly, predictable, and safely, while allowing for automatic rollbacks, automated state management, and management of resources across accounts and regions. Recent enhancements and options allow for multiple ways to create resources, including using AWS CDK for coding in higher-level languages, importing existing resources, detecting configuration drift, and a new Registry that makes it easier to create custom types that inherit many core CloudFormation benefits.

CloudFormation introduces four concepts: A template is a JSON or YAML declarative code file that describes the intended state of all the resources needed to deploy an application. A stack implements and manages the group of resources outlined in the template and allows the state and dependencies of those resources to be managed together. A change set is a preview of changes that will be executed by stack operations to create, update, or remove resources. A stack set is a group of stacks you manage together that can replicate a group. The following diagram summarizes the CloudFormation workflow for creating stacks.

1. Use the AWS Cloud Formation Designer or own text editor to create or modify a CloudFormation template in JSON or YAML format.

2. Save the template locally or in an Amazon S3 bucket. If you created a template, save it with a file extension like: .json, .yaml, or .txt.

3. Create a CloudFormation stack by specifying the location of template file, such as a path on local computer or an Amazon S3 URL.


1 Create or use an existing template
2 Save locally or in S3 bucket
3 Use AWS CloudFormation to create a stack based on your template. It constructs and configures your stack resources.

2.7 Identity and Access Management

AWS Identity and Access Management (IAM) is a web service that helps the user to securely control access to AWS resources. With IAM, users can centrally manage permissions that control which AWS resources users can access. IAM is used to control who is authenticated (signed in) and authorized (has permissions) to use resources.IAM grants granular access to specific Google Cloud resources and helps prevent access to other resources. IAM lets users adopt the security principle of least privilege, which states that nobody should have more permissions than they actually need. In IAM, permission to access a resource isn't granted directly to the end user.

Instead, permissions are grouped into roles, and roles are granted to authenticated principals. An allow policy, also known as an IAM policy, defines and enforces what roles are granted to which principals. Each allow policy is attached to a resource.When an authenticated principal attempts to access a resource, IAM checks the resource's allow policy to determine whether the action is permitted.

IAM features used in the project are:

- **Shared access to your AWS account:**
  You can grant other people permission to administer and use resources in your AWS account without having to share the password or access key.
- **Granular permissions:**

You can grant different permissions to different people for different resources. to access your billing information but nothing else.

- **Secure access to AWS resources for applications that run on Amazon EC2:**
  IAM features can be used to securely provide credentials for applications that run on EC2 instances. These credentials provide permissions for applications to access other AWS resources.

- **Multi-factor authentication (MFA):**
  User can add two-factor authentication to his account and to individual users for extra security. With MFA you or your users must provide not only a password or access key to work with your account, but also a code from a specially configured device.

- **Identity federation:**
  You can allow users who already have passwords elsewhere to get temporary access to your AWS account.

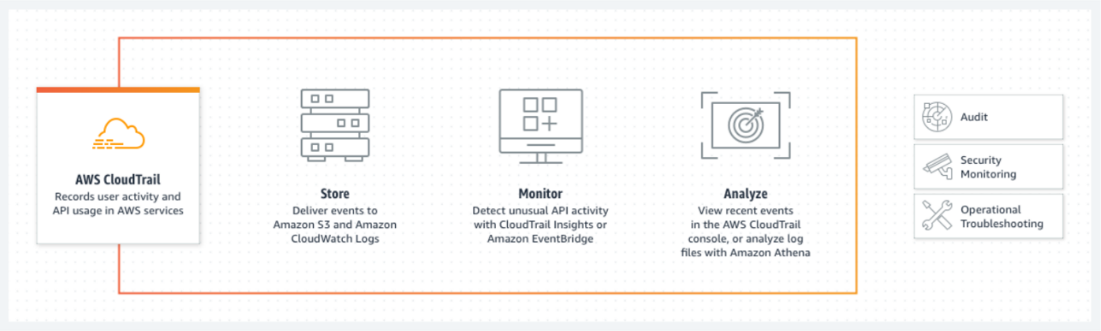
2.8 Simple Notification Service

Amazon Simple Notification Service (Amazon SNS) is a managed service that provides message delivery from publishers to subscribers (also known as producers and consumers). Publishers communicate asynchronously with subscribers by sending messages to a topic, which is a logical access point and communication channel. Clients can subscribe to the SNS topic and receive published messages using a supported endpoint type, such as Amazon Kinesis Data Firehose, Amazon SQS, AWS Lambda, HTTP, email, mobile push notifications, and mobile text messages (SMS). events.It provides Application-to-application messaging, Application-to-person notifications, Message durability,Message analytics, filtering and security.

2.9 CloudTrail

AWS CloudTrail helps you enable governance, compliance, and operational and risk auditing of the AWS account.CloudTrail helps to get a history of AWS API calls and related events for the AWS account. Its tracking includes calls made by using the AWS Management Console, AWS SDKs, command-line tools, APIs and higher-level AWS services (such as AWS CloudFormation). CloudTrail helps to identify which users and accounts called AWS for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred.It is enabled on AWS accounts when users create it.CloudTrail is per AWS account and per region for all the services supporting it. AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing AWS CloudTrail Insights can be enabled on a trail to help identify and respond to unusual activity.

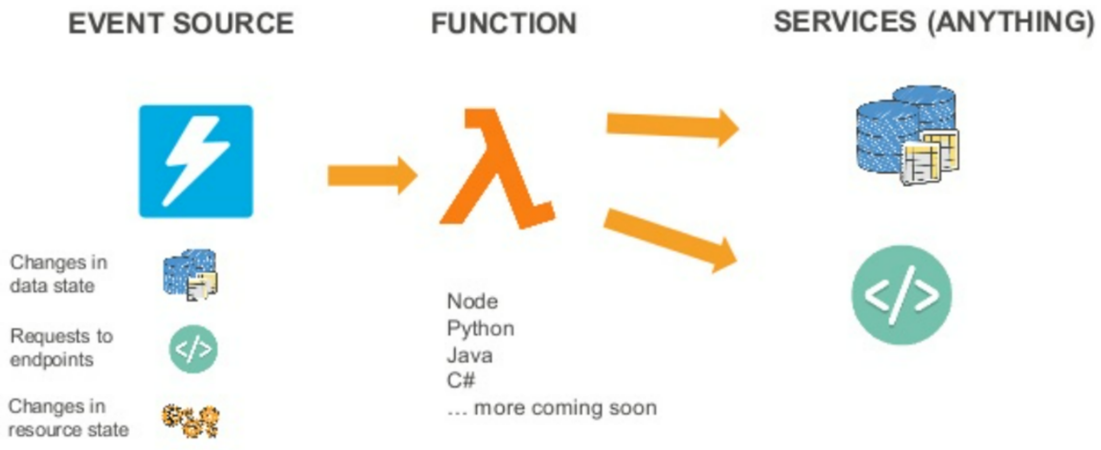
AWS CloudTrail captures AWS API calls and related events made by or on behalf of an AWS account and delivers log files to a specified S3 bucket. S3 lifecycle rules can be applied to archive or delete log files automatically.Log files contain API calls from all of the accountâs CloudTrail-supported services. Log files from all the regions can be delivered to a single S3 bucket and are encrypted, by default, using S3 server-side encryption (SSE). Encryption can be configured with AWS KMS. CloudTrail typically delivers log files within 15 minutes of an API call and publishes new log files multiple times an hour, usually about every 5 mins. It can be configured, optionally, to deliver events to a log group to be monitored by CloudWatch Logs.SNS notifications can be configured to be sent each time a log file is delivered to your bucket.A trail, which is a configuration, needs to be created that enables logging of the AWS API activity and related events in your account. Trail can be created with CloudTrail console, AWS CLI, or CloudTrail API.Turning on a trail means creating a trail and starting logging. IAM can control which AWS users can create, configure, or delete trails, start and stop logging, and access the buckets containing log information. Log file integrity validation can be enabled to verify that log files have remained unchanged since CloudTrail delivered them.CloudTrail Lake helps run fine-grained SQL-based queries on your events.


AWS CloudTrail
Records user activity and API usage in AWS services
Store
Deliver events to Amazon S3 and Amazon CloudWatch Logs
Monitor
Detect unusual API activity with CloudTrail Insights or Amazon EventBridge
Analyze
View recent events in the AWS CloudTrail console, or analyze log files with Amazon Athena
Audit
Security Monitoring
Operational Troubleshooting

2.10 Lambda Function

AWS Lambda is a compute service that lets you run code without provisioning or managing servers. Lambda runs your code on a high-availability compute infrastructure and performs all of the administration of the compute resources, including server and operating system maintenance, capacity provisioning and automatic scaling, and logging. With Lambda, you can run code for virtually any type of application or backend service.

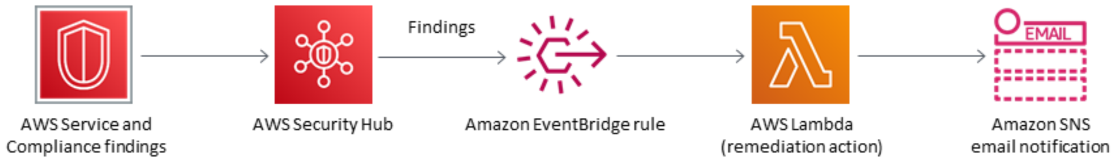
Each Lambda function runs in its own container. When a function is created, Lambda packages it into a new container and then executes that container on a multi-tenant cluster of machines managed by AWS.Before the functions start running, each functionâs container is allocated its necessary RAM and CPU capacity. Once the functions finish running, the RAM allocated at the beginning is multiplied by the amount of time the function spent running. The customers then get charged based on the allocated memory and the amount of run time the function took to complete.The entire infrastructure layer of AWS Lambda is managed by AWS.



EVENT SOURCE
FUNCTION
SERVICES (ANYTHING)
Changes in data state
Requests to endpoints
Changes in resource state
Node
Python
Java
C#
… more coming soon

Chapter 3

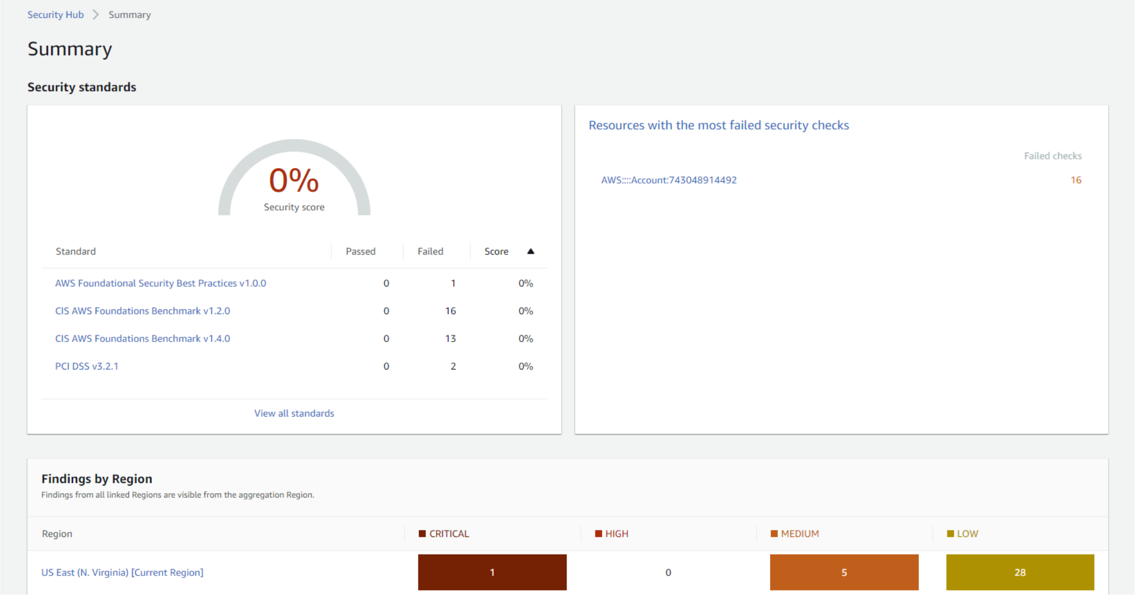
Integration


AWS Service and Compliance findings
AWS Security Hub
Findings
Amazon EventBridge rule
AWS Lambda (remediation action)
EMAIL
Amazon SNS email notification

The idea to remediate all the Compliance findings is from the above-mentioned flowchart. The findings from Security Hub displays all the requirements that are met and the ones that aren't. Based on those findings, we start to remediate the issues in order to make the account compliant to the CIS policies.

Our findings are then sent as events to the lambda function using an event bridge rule which is configured to take custom actions and that will be taken as the event input for the lambda function. This is then repeated for all the findings from Security hub in order to resolve all the failed compliance issues.

3.1 Security Hub



Summary

Security standards

0%
Security score

Standard	Passed	Failed	Score ▲
AWS Foundational Security Best Practices v1.0.0	0	1	0%
CIS AWS Foundations Benchmark v1.2.0	0	16	0%
CIS AWS Foundations Benchmark v1.4.0	0	13	0%
PCI DSS v3.2.1	0	2	0%

Resources with the most failed security checks

	Failed checks
AWS::::Account:743048914492	16

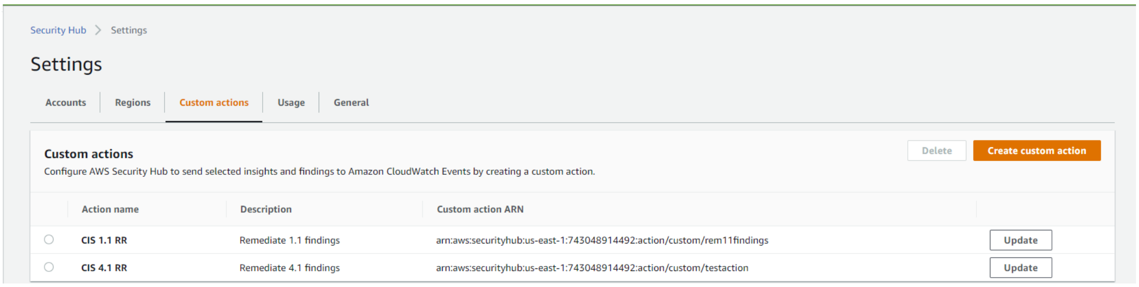
Findings by Region

Findings from all linked Regions are visible from the aggregation Region.

Region	CRITICAL	HIGH	MEDIUM	LOW
US East (N. Virginia) [Current Region]	1	0	5	28

The Security Hub Dashboard displays all the failed compliance status for a particular account. A custom action can be then created and then attached to the Event Bridge rule in order to remediate particular finding.

3.2 Custom Actions



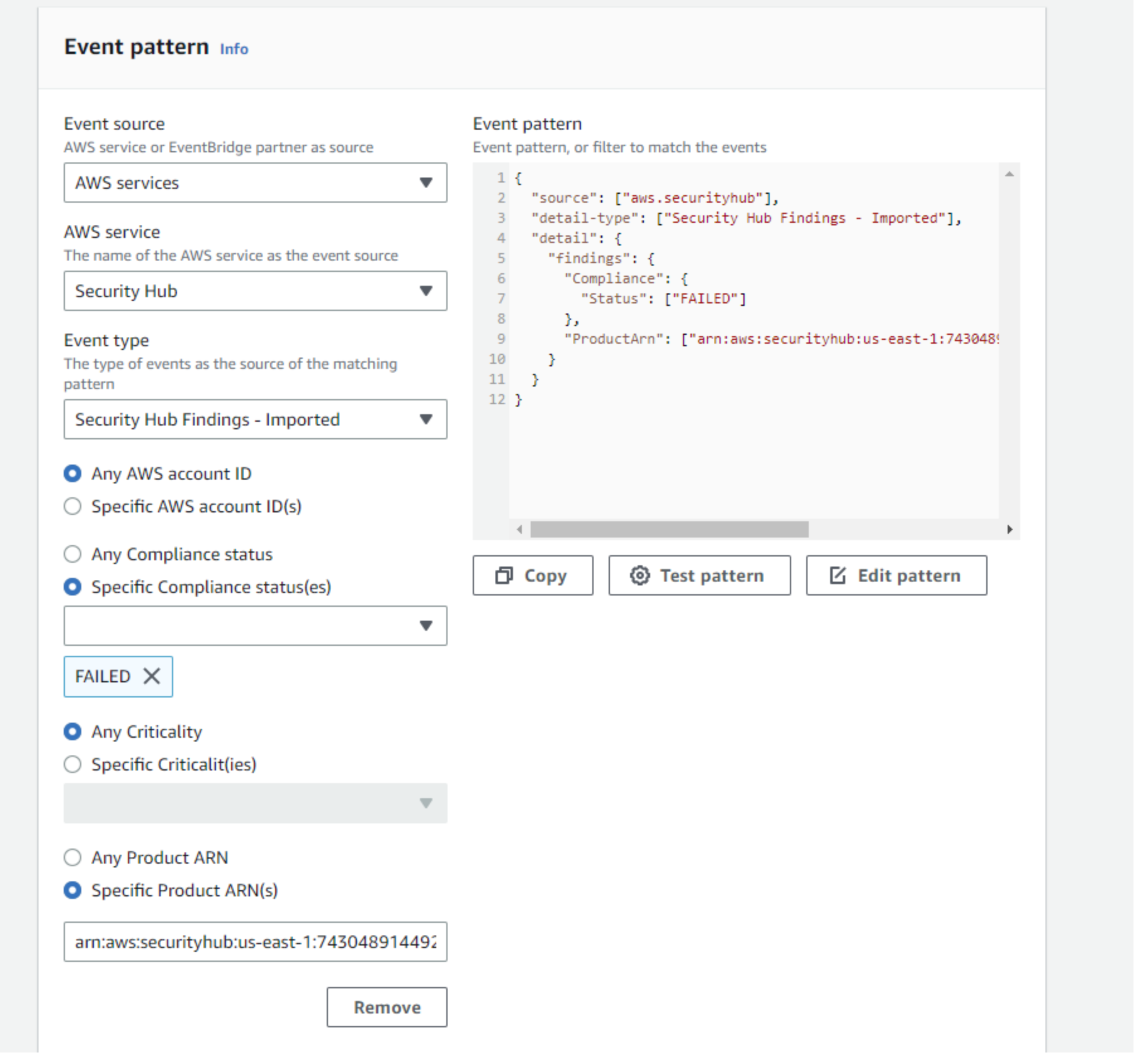
Settings

Custom actions

Configure AWS Security Hub to send selected insights and findings to Amazon CloudWatch Events by creating a custom action.

	Action name	Description	Custom action ARN	
○	CIS 1.1 RR	Remediate 1.1 findings	arn:aws:securityhub:us-east-1:743048914492:action/custom/rem11findings	Update
○	CIS 4.1 RR	Remediate 4.1 findings	arn:aws:securityhub:us-east-1:743048914492:action/custom/testaction	Update

3.3 Eventbridge Rules



Event pattern Info

Event source
AWS service or EventBridge partner as source
AWS services ▼

AWS service
The name of the AWS service as the event source
Security Hub ▼

Event type
The type of events as the source of the matching pattern
Security Hub Findings - Imported ▼

● Any AWS account ID
○ Specific AWS account ID(s)

○ Any Compliance status
● Specific Compliance status(es)

FAILED ✕

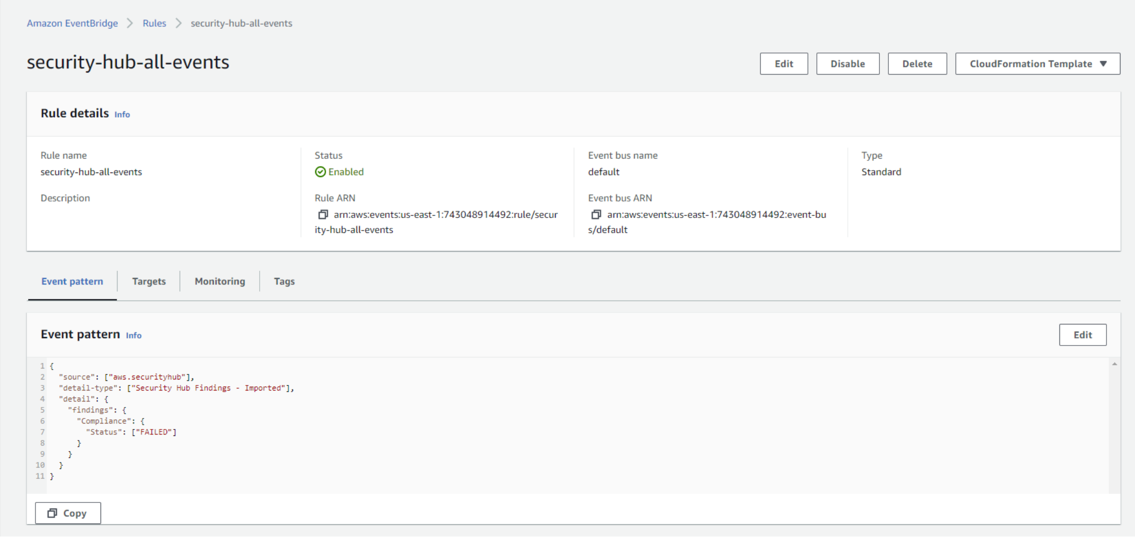
● Any Criticality
○ Specific Criticalit(ies)

○ Any Product ARN
● Specific Product ARN(s)

arn:aws:securityhub:us-east-1:74304891449

Event pattern
Event pattern, or filter to match the events

```
{
  "source": ["aws.securityhub"],
  "detail-type": ["Security Hub Findings - Imported"],
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED"]
      },
      "ProductArn": ["arn:aws:securityhub:us-east-1:743048
    }
  }
}
```



Amazon EventBridge > Rules > security-hub-all-events

security-hub-all-events

Rule details Info

Rule name
security-hub-all-events

Description

Status
Enabled

Rule ARN
arn:aws:events:us-east-1:743048914492:rule/security-hub-all-events

Event bus name
default

Event bus ARN
arn:aws:events:us-east-1:743048914492:event-bus/default

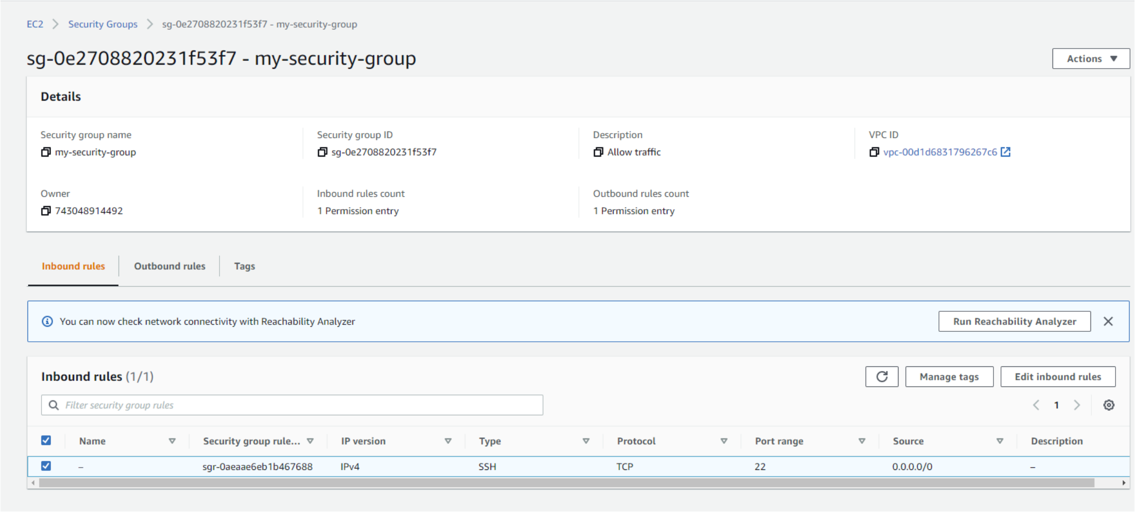
Type
Standard

Event pattern Info

```
{
  "source": ["aws.securityhub"],
  "detail-type": ["Security Hub Findings - Imported"],
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED"]
      }
    }
  }
}
```

After creating the custom rule, and selecting the compliance status as Failed, we will only get the compliance benchmarks that are not met. This is then used with the lambda function where the input provided is used as a event to test the Lambda function.

3.4 Security Group with Inbound Rule


EC2 > Security Groups > sg-0e2708820231f53f7 - my-security-group
Actions ▼
Inbound rules
Outbound rules
Tags
Run Reachability Analyzer
Manage tags
Edit inbound rules
1

sg-0e2708820231f53f7 - my-security-group

Details

Security group name: my-security-group

Security group ID: sg-0e2708820231f53f7

Description: Allow traffic

VPC ID: vpc-00d1d6831796267c6

Owner: 743048914492

Inbound rules count: 1 Permission entry

Outbound rules count: 1 Permission entry

You can now check network connectivity with Reachability Analyzer

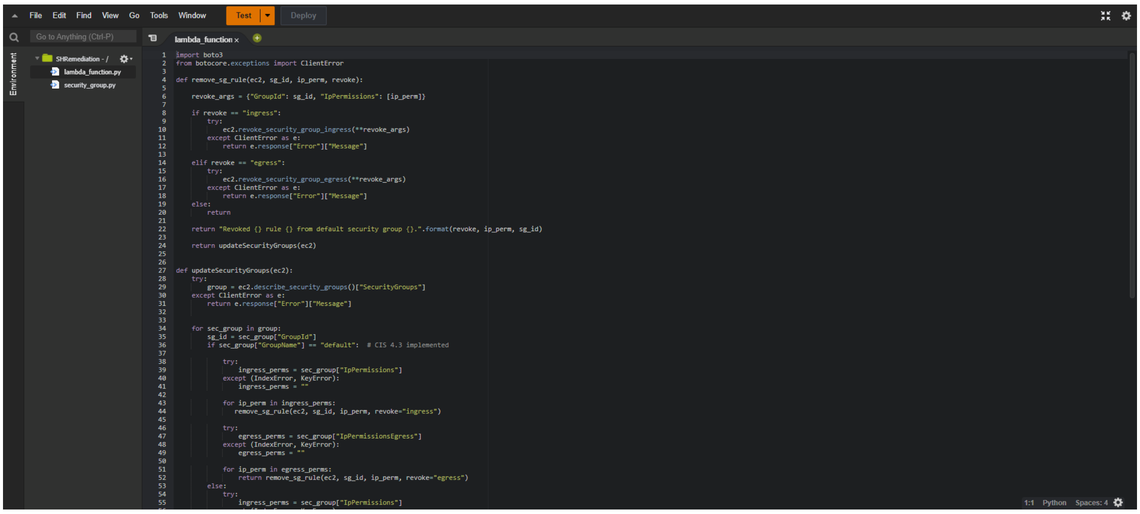
Inbound rules (1/1)

Filter security group rules

☑	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
☑	–	sgr-0aeaae6eb1b467688	IPv4	SSH	TCP	22	0.0.0.0/0	–

For this case, we are going to resolve the Security Group compliance that allows traffic from all sources to SSH into a service that has this service group attached which is in defiance of the compliance of the AWS CIS policy.

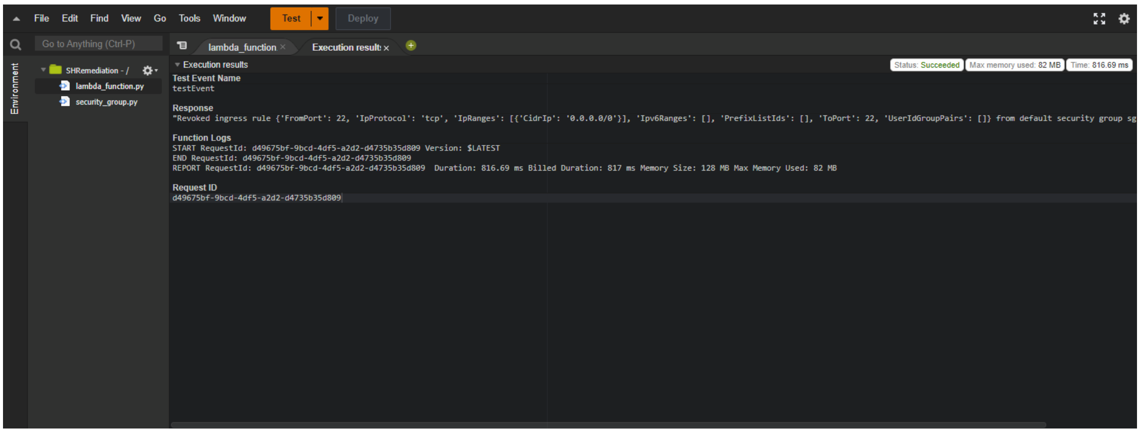
3.5 Lambda Function to Remediate Security Group Findings



```python
import boto3
from botocore.exceptions import ClientError

def remove_sg_rule(ec2, sg_id, ip_perm, revoke):

    revoke_args = {"GroupId": sg_id, "IpPermissions": [ip_perm]}

    if revoke == "ingress":
        try:
            ec2.revoke_security_group_ingress(**revoke_args)
        except ClientError as e:
            return e.response["Error"]["Message"]

    elif revoke == "egress":
        try:
            ec2.revoke_security_group_egress(**revoke_args)
        except ClientError as e:
            return e.response["Error"]["Message"]
    else:
        return

    return "Revoked {} rule {} from default security group {}.".format(revoke, ip_perm, sg_id)

    return updateSecurityGroups(ec2)


def updateSecurityGroups(ec2):
    try:
        group = ec2.describe_security_groups()["SecurityGroups"]
    except ClientError as e:
        return e.response["Error"]["Message"]


    for sec_group in group:
        sg_id = sec_group["GroupId"]
        if sec_group["GroupName"] == "default":  # CIS 4.3 implemented

            try:
                ingress_perms = sec_group["IpPermissions"]
            except (IndexError, KeyError):
                ingress_perms = ""

            for ip_perm in ingress_perms:
               remove_sg_rule(ec2, sg_id, ip_perm, revoke="ingress")

            try:
                egress_perms = sec_group["IpPermissionsEgress"]
            except (IndexError, KeyError):
                egress_perms = ""

            for ip_perm in egress_perms:
                return remove_sg_rule(ec2, sg_id, ip_perm, revoke="egress")
        else:
            try:
                ingress_perms = sec_group["IpPermissions"]
```

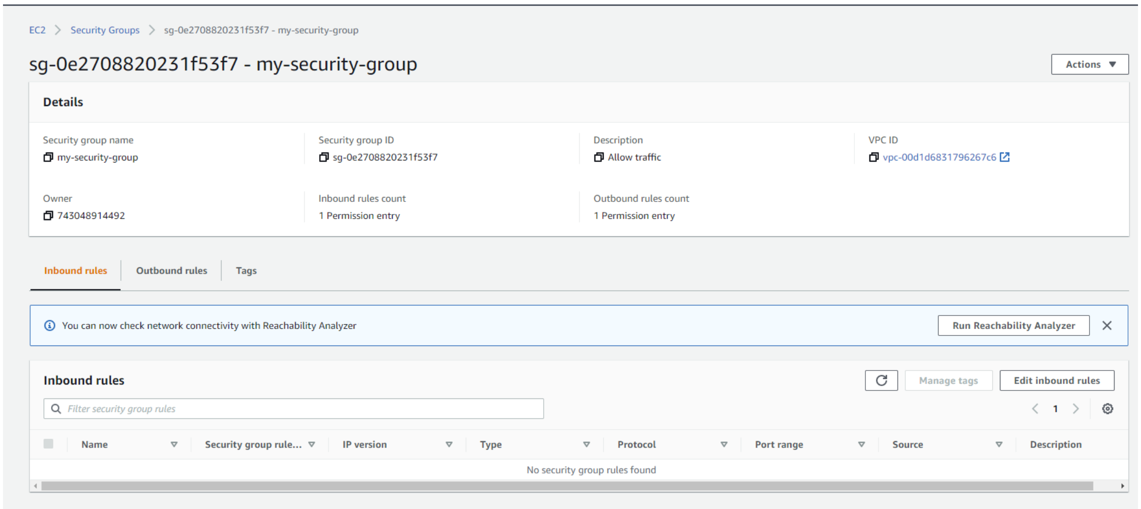
After our triggers have been set, we can then run the lambda function. This then gives us the response that informs us that the inbound rule for the security group has been removed.

3.6 Inbound Rule has been Remediated



```
Test Event Name
testEvent

Response
"Revoked ingress rule {'FromPort': 22, 'IpProtocol': 'tcp', 'IpRanges': [{'CidrIp': '0.0.0.0/0'}], 'Ipv6Ranges': [], 'PrefixListIds': [], 'ToPort': 22, 'UserIdGroupPairs': []} from default security group sg

Function Logs
START RequestId: d49675bf-9bcd-4df5-a2d2-d4735b35d809 Version: $LATEST
END RequestId: d49675bf-9bcd-4df5-a2d2-d4735b35d809
REPORT RequestId: d49675bf-9bcd-4df5-a2d2-d4735b35d809  Duration: 816.69 ms Billed Duration: 817 ms Memory Size: 128 MB Max Memory Used: 82 MB

Request ID
d49675bf-9bcd-4df5-a2d2-d4735b35d809
```

The ingress rule has now been revoked, which then makes the security group compliant.


EC2 > Security Groups > sg-0e2708820231f53f7 - my-security-group
Actions ▼
Inbound rules
Outbound rules
Tags
Run Reachability Analyzer
Manage tags
Edit inbound rules
1

sg-0e2708820231f53f7 - my-security-group

Details

Security group name: my-security-group

Security group ID: sg-0e2708820231f53f7

Description: Allow traffic

VPC ID: vpc-00d1d6831796267c6

Owner: 743048914492

Inbound rules count: 1 Permission entry

Outbound rules count: 1 Permission entry

You can now check network connectivity with Reachability Analyzer

Inbound rules

Filter security group rules

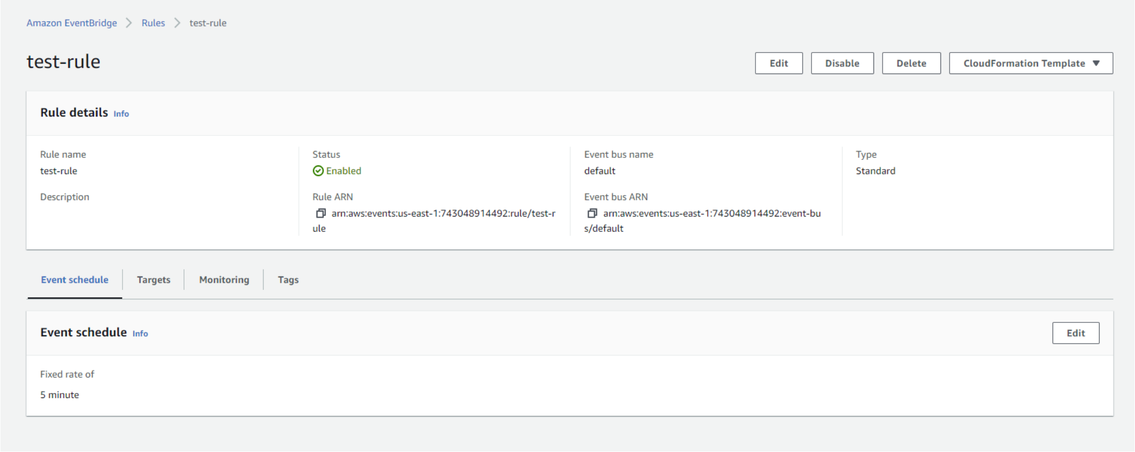
Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description

No security group rules found

This is then noticed after 12 hours in Security Hub.

Automation of the lambda function can be done using EventBridge rules. This can be added as a trigger to the lambda function.

3.7 EventBridge rule for Automation of Lambda Function



test-rule

Rule details

Rule name: test-rule

Status: Enabled

Event bus name: default

Type: Standard

Description

Rule ARN: arn:aws:events:us-east-1:743048914492:rule/test-rule

Event bus ARN: arn:aws:events:us-east-1:743048914492:event-bus/default

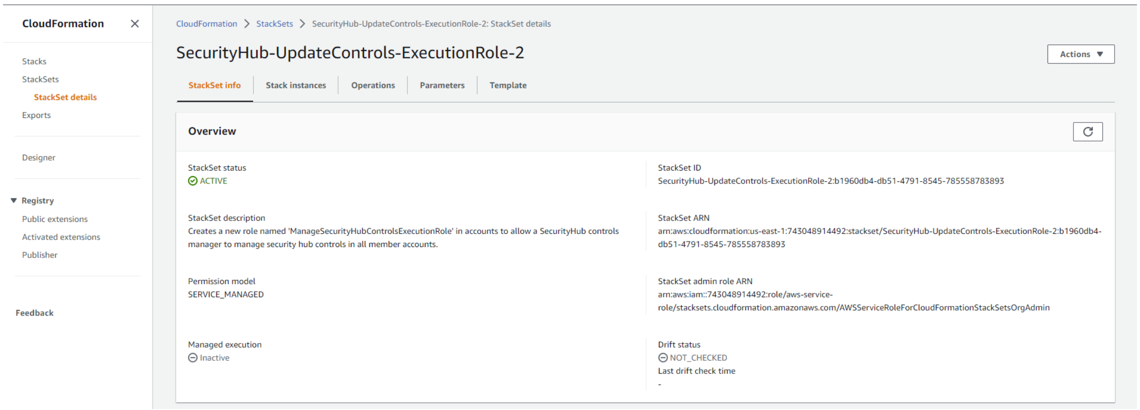
Event schedule

Fixed rate of

5 minute

This can be extended for more than a single user. But first, a role containing permissions to assume the access needs to be deployed to the user accounts in the organization. This can be done using CloudFormation Stacksets.

3.8 CloudFormation StackSet for Role Deployment



SecurityHub-UpdateControls-ExecutionRole-2

Overview

StackSet status
✓ ACTIVE

StackSet ID
SecurityHub-UpdateControls-ExecutionRole-2:b1960db4-db51-4791-8545-785558783893

StackSet description
Creates a new role named 'ManageSecurityHubControlsExecutionRole' in accounts to allow a SecurityHub controls manager to manage security hub controls in all member accounts.

StackSet ARN
arn:aws:cloudformation:us-east-1:743048914492:stackset/SecurityHub-UpdateControls-ExecutionRole-2:b1960db4-db51-4791-8545-785558783893

Permission model
SERVICE_MANAGED

StackSet admin role ARN
arn:aws:iam::743048914492:role/aws-service-role/stacksets.cloudformation.amazonaws.com/AWSServiceRoleForCloudFormationStackSetsOrgAdmin

Managed execution
⊖ Inactive

Drift status
⊖ NOT_CHECKED
Last drift check time
-

Chapter 4

Conclusion

4.1 Conclusion

The purpose of this project is to secure the cloud environment by automating the remediation. In this project, first, each control of the CIS benchmark is audited, analyzed, and remediated. After that, the AWS CIS benchmark is monitored and audited using SecurityHub. And finally, EventBridge is used to integrate SecurityHub and Lambda functions to implement the remediation playbook for custom action or auto-remediation. By creating custom actions mapped to specific finding types and by developing a corresponding Lambda function for that custom action, can achieve targeted, automated remediation for the Security hub findings.

4.2 Future Work

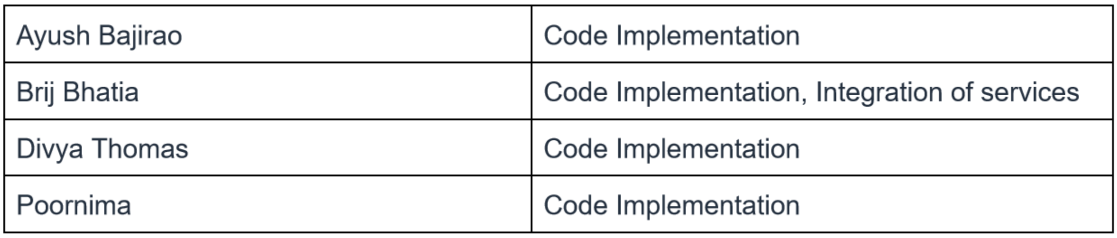
This project has a lot of prospective future work possibilities such as:

1. Implement all CIS controls that cannot be implemented directly (eg. 1.1, 1.2)

2. Implement newly released CIS v1.4.0 controls.

3. Implement CIS Benchmarks in other public cloud providers like Azure, Google Cloud Platform.

4.3 Responsibilities



Ayush Bajirao	Code Implementation
Brij Bhatia	Code Implementation, Integration of services
Divya Thomas	Code Implementation
Poornima	Code Implementation