ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MIJAR, MOODBIDRI D.K. -574225

KARNATAKA

CYBERSECURITY FINISHING SCHOOL

(Organized by CySecK and Co-Organizer by Trisakha Foundation)

PROJECT REPORT ON

"INCIDENT RESPONSE SIMULATION: TABLETOP EXERCISE"

Submitted by:

Name: LAXMISH V HEGDE

Team: POWER_RANGERS

Table of Content

LIST OF FIGURES

ABSTRACT

In today's digital landscape, organizations face ever-evolving cyber threats that necessitate robust incident response capabilities. Cloud environments, particularly Amazon Web Services (AWS), present unique challenges and opportunities in incident detection, containment, and recovery. This abstract outlines a tabletop exercise approach tailored specifically for AWS environments to enhance incident response readiness. The tabletop exercise simulates a realistic security incident scenario within an AWS infrastructure, engaging key stakeholders across departments. Participants are tasked with navigating through the incident lifecycle, from initial detection to post-incident analysis, leveraging AWS tools and services to mitigate the threat effectively. Through guided discussions and real-time decision-making, participants identify roles, responsibilities, and response procedures pertinent to the incident scenario. They utilize AWS CloudTrail, Amazon GuardDuty, and other monitoring tools to detect anomalous activities and potential breaches. Containment and mitigation strategies are employed using AWS IAM, VPC Security Groups, and WAF to limit the impact and prevent further escalation. The exercise emphasizes collaboration, communication, and coordination among cross-functional teams, mirroring real-world incident response dynamics. Participants leverage AWSservices like CloudWatch Logs, AWS Config, and Security Hub for forensic analysis, enabling informed decision-making and root cause identification. Post-exercise, a comprehensive debriefing session fosters reflection, knowledge sharing, and lessons learned. Insights gleaned from the exercise inform updates to the incident response plan, AWSinfrastructure configurations, and organizational policies, driving continuous improvement in incident response capabilities. This abstract serves as a blueprint for organizations seeking to strengthen their incident response posture in AWS through structured tabletop exercises. By proactively testing and refining response procedures in a simulated environment, organizations can better prepare for the inevitable challenges of cybersecurity incidents in the cloud era.

CHAPTER 01

INTRODUCTION

Security is the top priority at AWS. AWS customers benefit from data centres and network architecture built to help support the needs of the most security-sensitive organizations. AWS has a shared responsibility model: AWS manages the security of the cloud, and customers are responsible for security in the cloud. This means that you have full control of your security implementation, including access to several tools and services to help meet your security objectives. These capabilities help you establish a security baseline for applications running in the AWS Cloud. When a deviation from the baseline occurs, such as by a misconfiguration or changing external factors, you will need to respond and investigate. To successfully do so, you need to understand the basic concepts of security incident response within your AWS environment and the requirements to prepare, educate, and train cloud teams before security issues occur. It is important to know which controls and capabilities you can use, review topical examples for resolving potential concerns, and identify remediation methods that use automation to improve response speed and consistency. Additionally, you should understand your compliance and regulatory requirements as they relate to building a security incident response program to fulfil those requirements. Security incident response can be complex, so we encourage you to implement an iterative approach: begin with the core security services, build foundational detection and response capabilities, then develop playbooks to create an initial library of incident response mechanisms upon which to iterate and improve.

CHAPTER 02

ASPECTS OF AWS INCIDENT RESPONSE

All AWS users within an organization should have a basic understanding of security incident response processes, and security staff should understand how to respond to security issues. Education, training, and experience are vital to a successful cloud incident response program and are ideally implemented well in advance of having to handle a possible security incident. The foundation of a successful incident response program in the cloud is Preparation, Operations, and Post-Incident Activity. To understand each of these aspects, consider the following descriptions:

• Preparation– Prepare your incident response team to detect and respond to incidents within AWS by enabling detective controls and verifying appropriate access to the necessary tools and cloud services. Additionally, prepare the necessary playbooks, both manual and automated, to verify reliable and consistent responses.

• Operations– Operate on security events and potential incidents following NIST's phases of incident response: detect, analyse, contain, eradicate, and recover.

• Post-incident activity– Iterate on the outcome of your security events and simulations to improve the efficacy of your response, increase value derived from response and investigation, and further reduce risk. You have to learn from incidents and have strong ownership of improvement activities. Each of these aspects are explored and detailed in this guide. The following diagram shows the flow of these aspects, aligning with the previously mentioned NIST incident response lifecycle, but with operations encompassing detection and analysis with containment, eradication, and recovery.

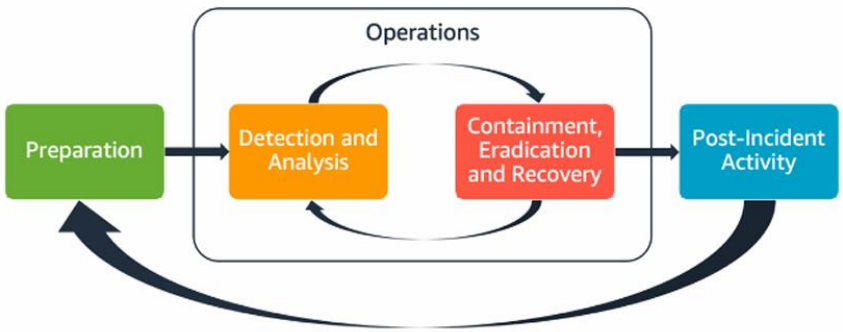

FIG (i): OPERATIONS OF INCIDENT RESPONCE

CHAPTER 03

CLOUD SECURITY INCIDENT DOMAINS

To effectively prepare for and respond to security events in your AWS environment, you need to understand the commons types of cloud security incidents. There are three domains within the customer's responsibility where security incidents might occur: service, infrastructure, and application. Different domains require different knowledge, tools, and response processes. Consider these domains:

• Service domain– Incidents in the service domain might affect your AWS account, AWS Identity and Access Management (IAM) permissions, resource metadata, billing, or other areas. A service domain event is one that you respond to exclusively with AWS API mechanisms, or where you Cloud security incident domains 5 AWS Security Incident Response Guide AWS Technical Guide have root causes associated with your configuration or resource permissions, and might have related service-oriented logging.

• Infrastructure domain– Incidents in the infrastructure domain include data or network-related activity, such as processes and data on your Amazon Elastic Compute Cloud (Amazon EC2) instances, traffic to your Amazon EC2 instances within the virtual private cloud (VPC), and other areas, such as containers or other future services. Your response to infrastructure domain events often involves acquiring incident-related data for forensic analysis. It likely includes interaction with the operating system of an instance, and, in various cases, might also involve AWS API mechanisms. In the infrastructure domain, you can use a combination of AWS APIs and digital forensics/incident response (DFIR) tooling within a guest operating system, such as an Amazon EC2 instance dedicated to performing forensic analysis and investigations. Infrastructure domain incidents might involve analysing network packet captures, disk blocks on an Amazon Elastic Block Store (Amazon EBS) volume, or volatile memory acquired from an instance.

• Application domain– Incidents in the application domain occur in the application code or in software deployed to the services or infrastructure. This domain should be included in your cloud threat detection and response playbooks and might incorporate similar responses to those in the infrastructure domain. With appropriate and thoughtful application architecture, you can manage this domain with cloud tools by using automated acquisition, recovery, and deployment. In these domains, consider the actors who might act against AWS accounts,

resources, or data. Whether internal or external, use a risk framework to determine specific risks to the organization and prepare accordingly. Additionally, you should develop threat models, which can help with your incident response planning and thoughtful architecture buildings.

CHAPTER 04

ALERT SOURCES

You should consider using the following sources to define alerts:

• Findings– AWS services such as Amazon GuardDuty, AWS Security Hub, Amazon Macie, Amazon Inspector, AWS Config, IAM Access Analyzer, and Network Access Analyzer generate findings that can be used to craft alerts.

• Logs– AWSservice, infrastructure, and application logs stored in Amazon S3 buckets and CloudWatch log groups can be parsed and correlated to generate alerts.

• Billing activity– A sudden change in billing activity can indicate a security event. Follow the documentation on Creating a billing alarm to monitor your estimated AWS charges to monitor for this.

• Cyber threat intelligence– If you subscribe to a third-party cyber threat intelligence feed, you can correlate that information with other logging and monitoring tools to identify potential indicators of events.

• Partner tools– Partners in the AWS Partner Network (APN) offer top-tier products that can help you meet your security objectives. For incident response, partner products with endpoint detection and response (EDR) or SIEM can help support your incident response objectives. For more information, see Security Partner Solutions and Security Solutions in the AWS Marketplace. Detection 34 AWSSecurity Incident Response Guide AWS Technical Guide

• AWS trust and safety– AWS Support might contact customers if we identify abusive or malicious activity.

• One-time contact– Because it can be your customers, developers, or other staff in your organization who notice something unusual, it’s important to have a well-known, well-publicized method of contacting your security team. Popular choices include ticketing systems, contact email addresses, and web forms. If your organization works with the general public, you might also need a public-facing security contact mechanism

CHAPTER 05

SOURCE CONTAINMENT

Source containment is the use and application of filtering or routing within an environment to prevent access to resources from a specific source IP address or network range. Examples of source containment using AWS services are highlighted here:

• Security groups– Creating and applying isolation security groups to Amazon EC2 instances or removing rules from an existing security group can help to contain unauthorized traffic to an Amazon EC2 instance or AWS resource. It is important to note that existing tracked connections won't be shut down as a result of changing security groups– only future traffic will be effectively blocked by the new security group.

• Policies– Amazon S3 bucket policies can be configured to block or allow traffic from an IP address, a network range, or a VPC endpoint. Policies create the ability to block suspicious addresses and access to the Amazon S3 bucket. Additional information on bucket policies can be found at Adding a bucket policy using the Amazon S3 console.

• AWSWAF–Web access control lists (web ACLs) can be configured on AWS WAF to provide fine-grained control over web requests that resources respond to. You can add an IP address or network range to an IP set configured on AWS WAF, and apply match conditions, such as block, to the IP set. This will block web requests to a resource if the IP address or network ranges from the originating traffic match those configured in the IP set rules. An example of source containment can be seen in the following diagram with an incident response analyst modifying a security group of an Amazon EC2 instance in order to restrict new connections to only certain IP addresses. As stated in the security groups bullet, existing tracked connections won't be shut down as a result of changing security groups.

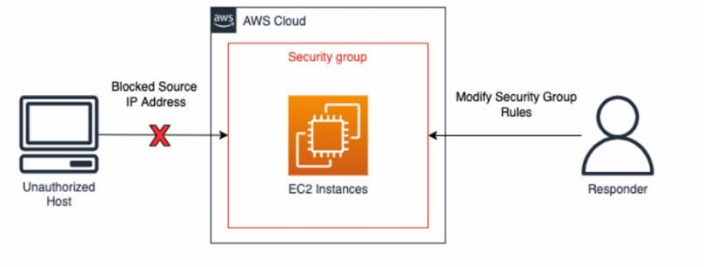

FIG (ii): SOURCE CONTAINMENT EXAMPLE

CHAPTER 06

IMPLEMENTATION AND RESULT

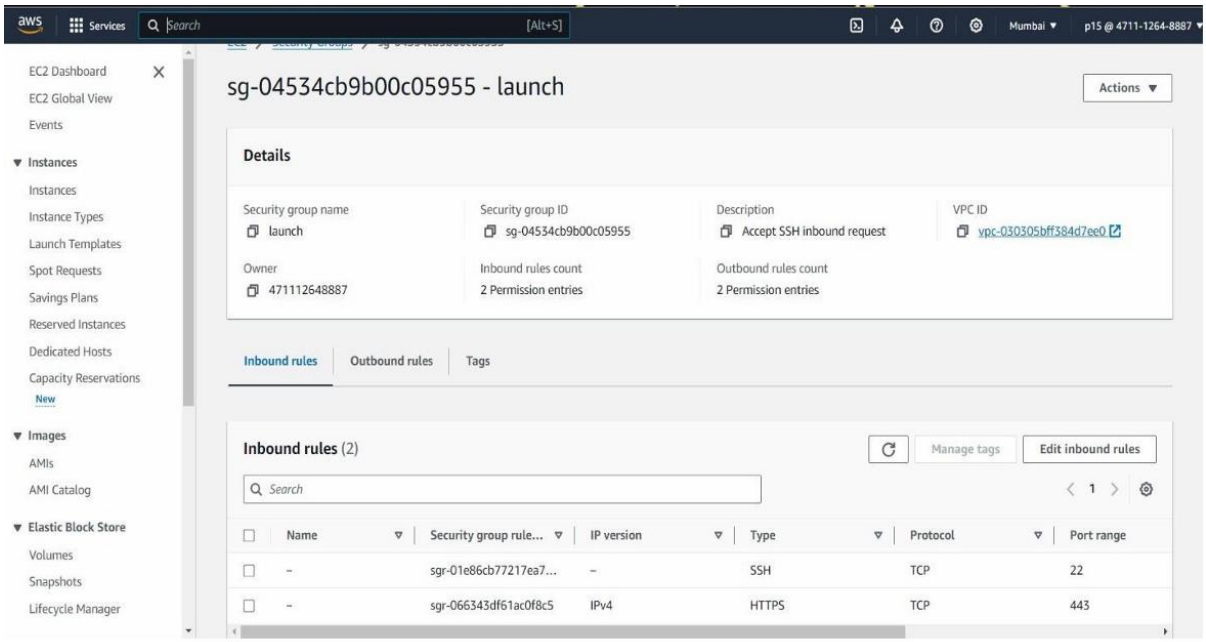

FIG (iii): SECURITY GROUP INBOUND GROUP

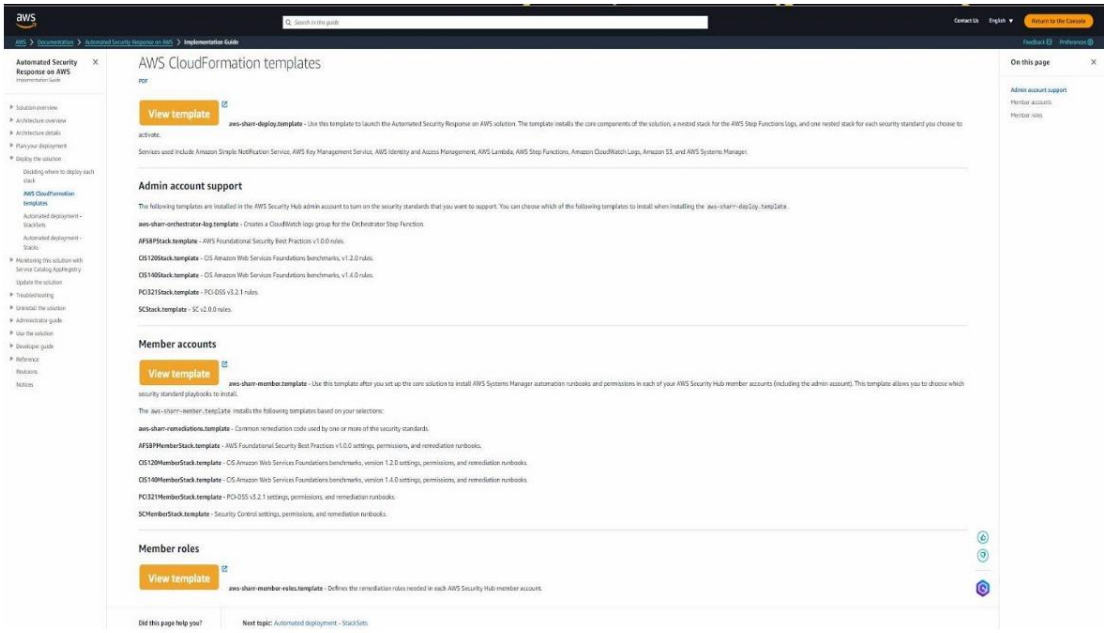

FIG (iv): CLOUD FORMATION TEMPLATE

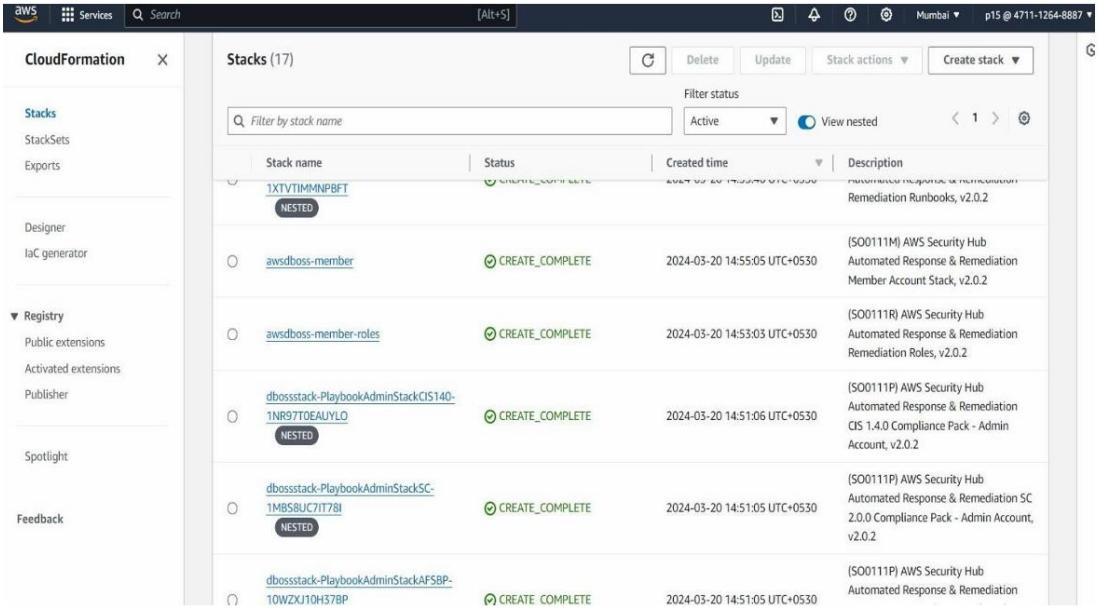

FIG (v): CLOUD FORMATION STACKS

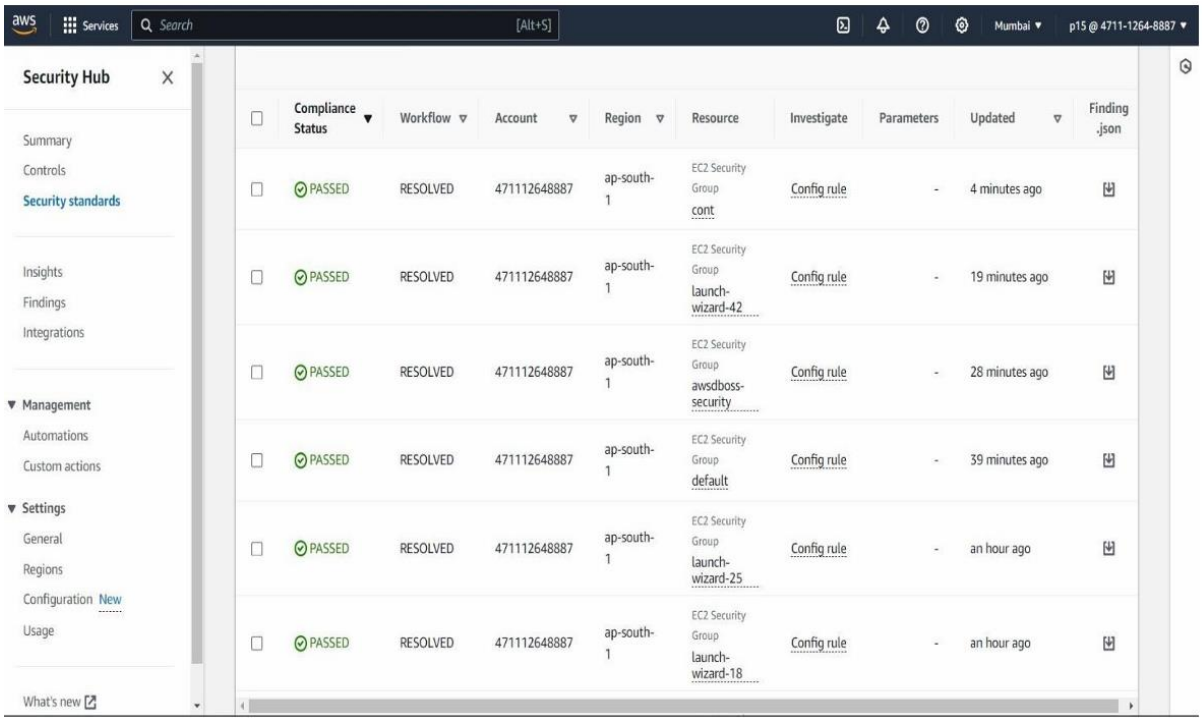

FIG (vi): SECURITY HUB

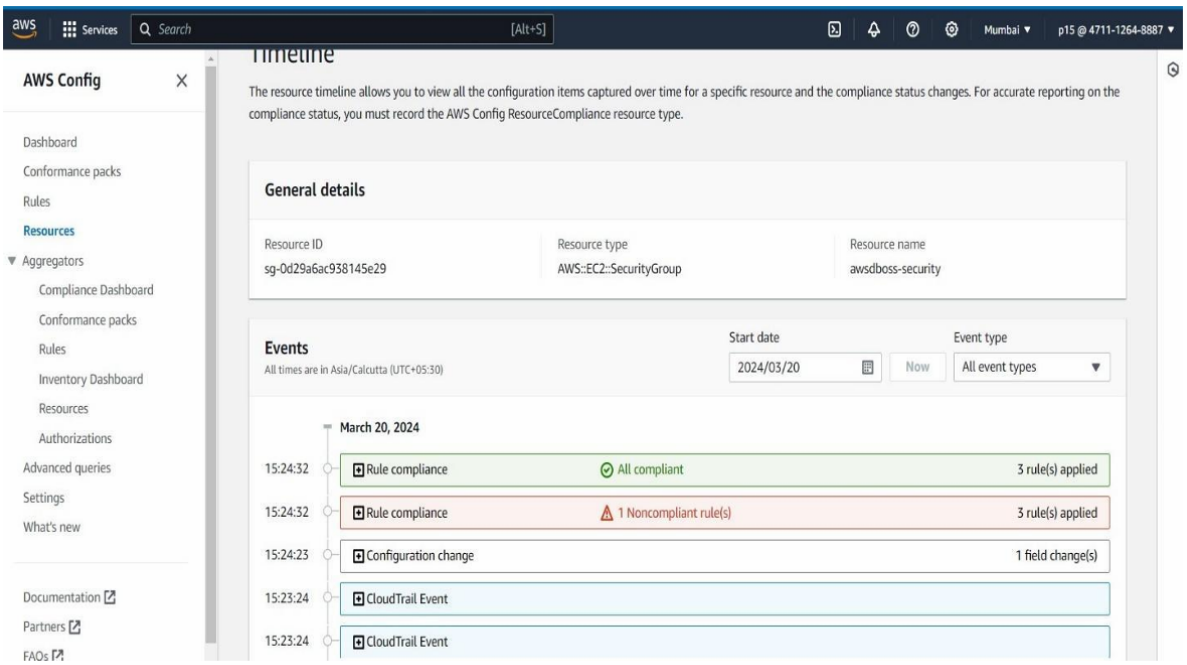

FIG (vii): SECURITY HUB TIMELINE

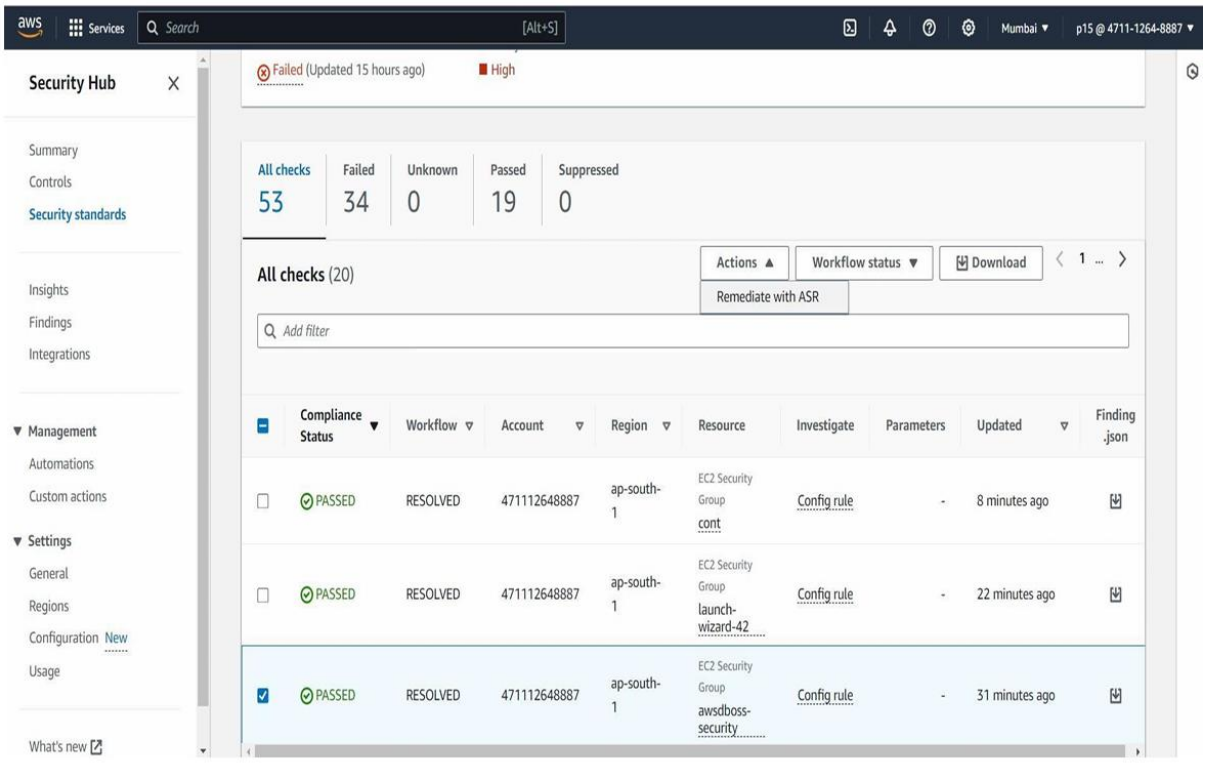

FIG (viii): EVENT BRIDGE ACTION

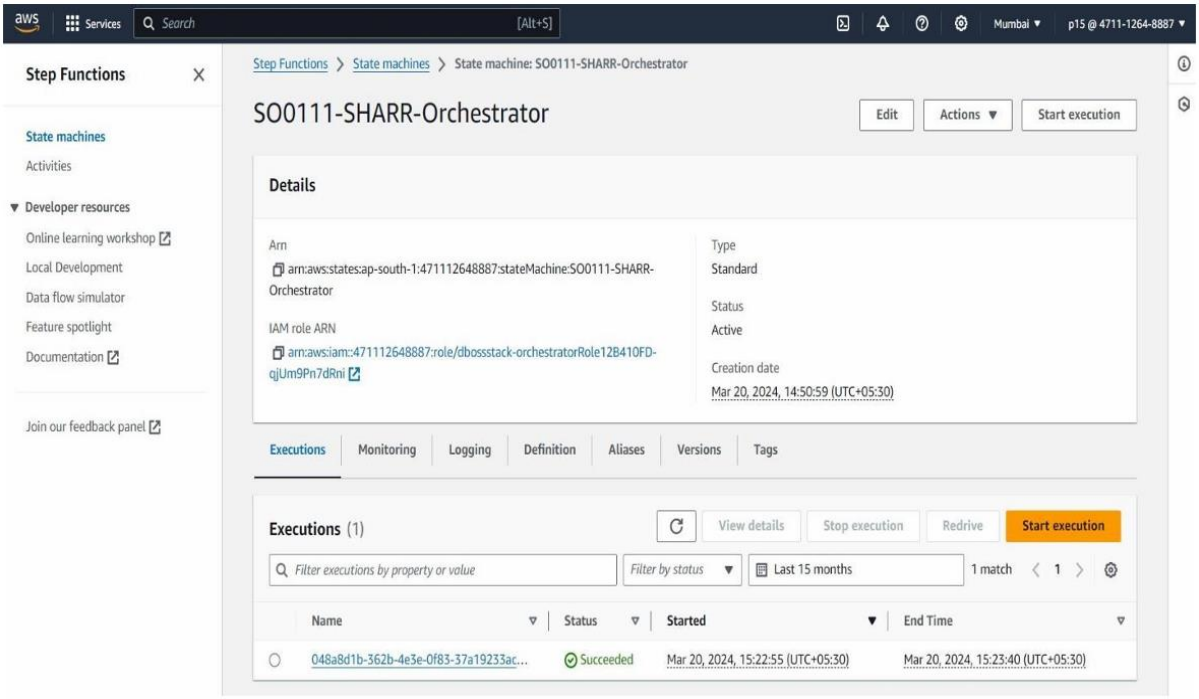

FIG (ix): EVENT BRIDGE ACTION HAPPENING

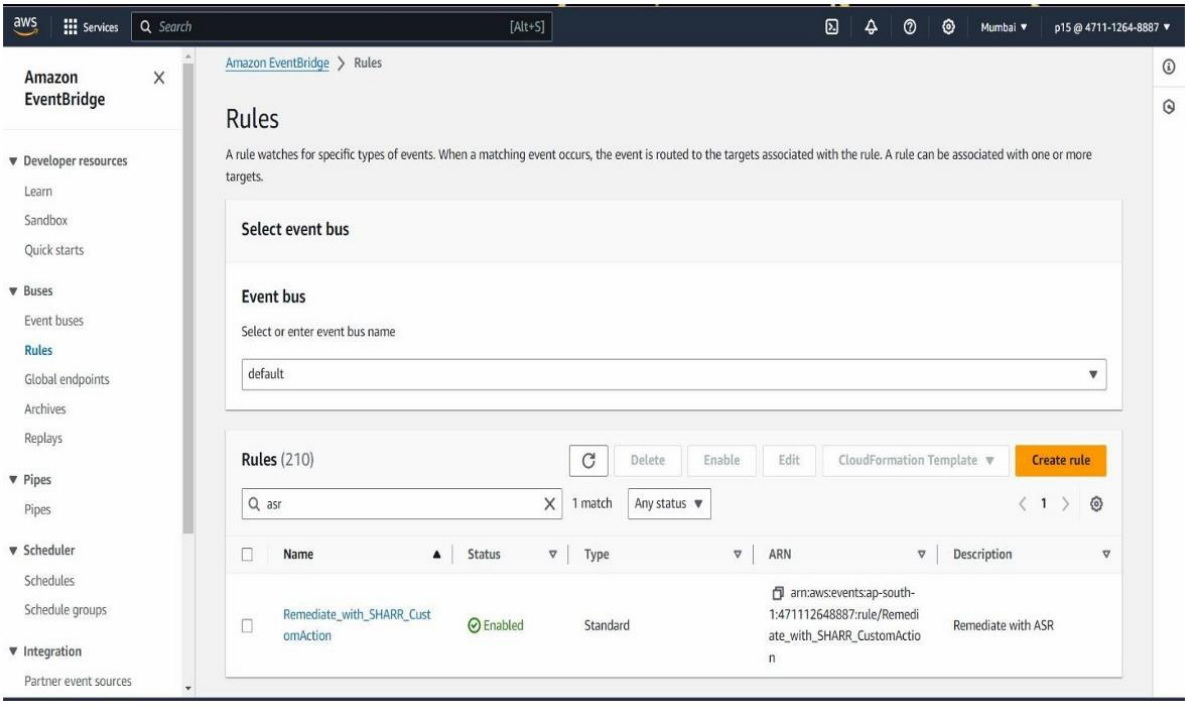

FIG (x): EVENT BRIDGE RULES

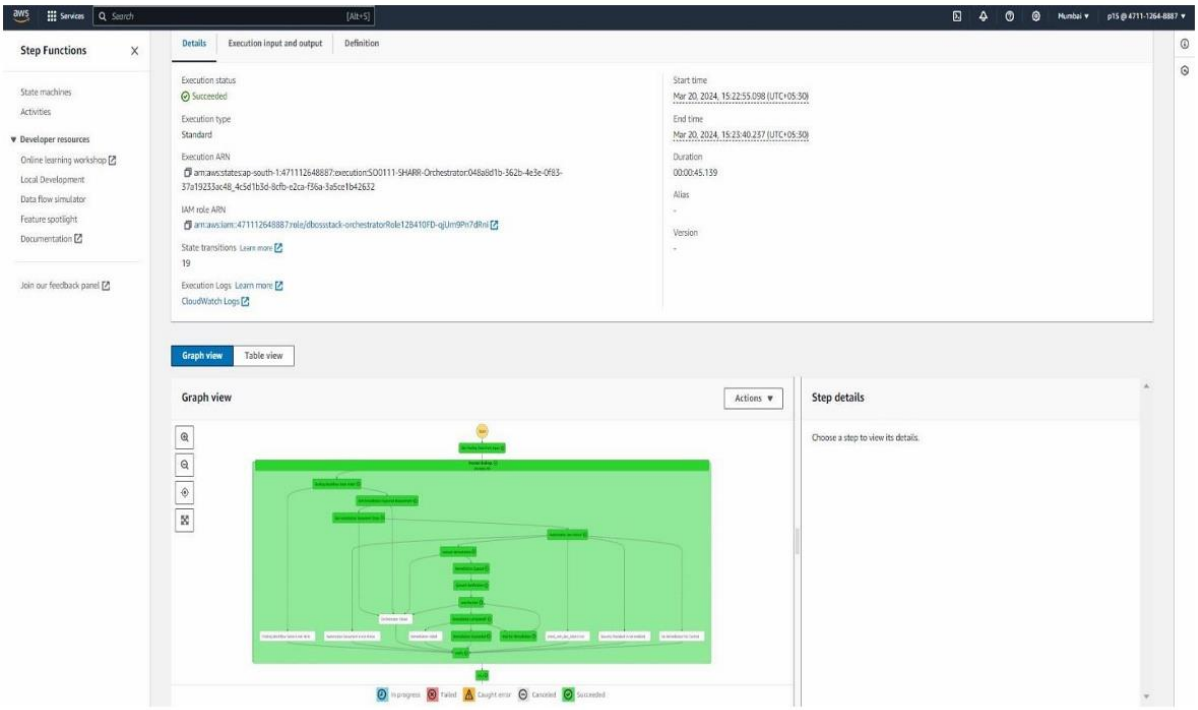

FIG (xi): AWS EVENT GRAPH

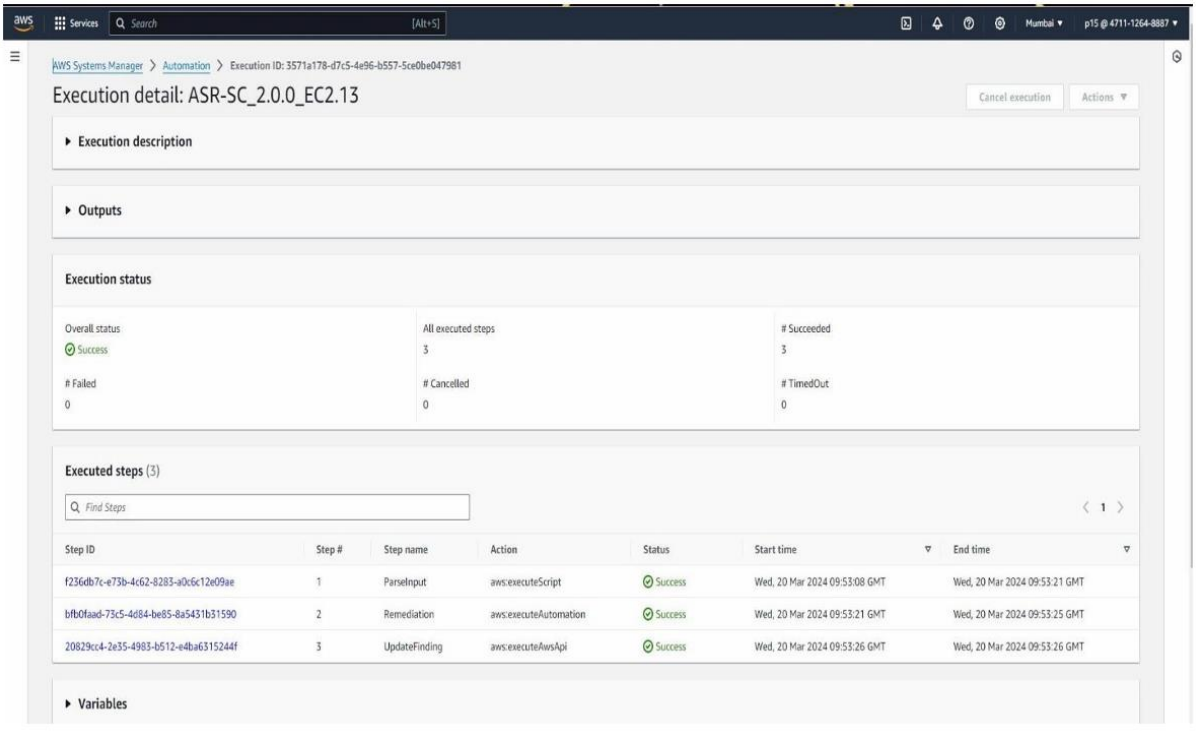

FIG (xi): AWS EVENT AUTOMATION

CHAPTER 06

CONCLUSION

As you continue your cloud journey, it is important for you to consider the fundamental security incident response concepts for your AWS environment. You can combine the available controls, cloud capabilities, and remediation options to help you improve the security of your cloud environment. You can also start small and iterate as you adopt automation capabilities that improve your response speed, so you are better prepared when security events occur.