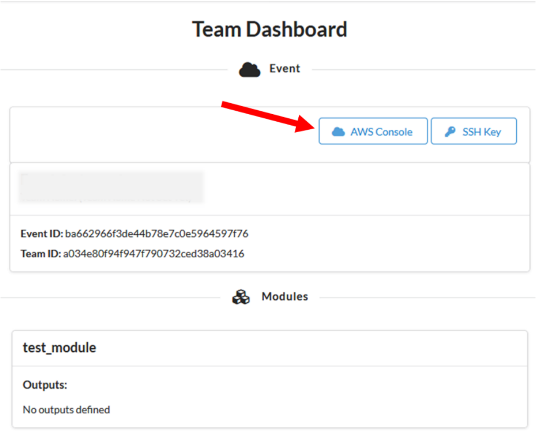
Threat Detection and Incident Response Workshop

1. Get Started Using the Lab Environment

This workshop should be completed in a dedicated AWS account. If you are attending a formal AWS event, you will have been sent an access code (or 'hash') that grants you permission to use a dedicated AWS account for this workshop.

1.1 Go to https://dashboard.eventengine.run/, enter the access code and click to **Accept Terms & Login**.
1.2 Pick the sign-in method you prefer. (Recommended: OTP)
1.3 Click on **AWS Console**, then **Open AWS Console** to login into your dedicated AWS environment.



Team Dashboard

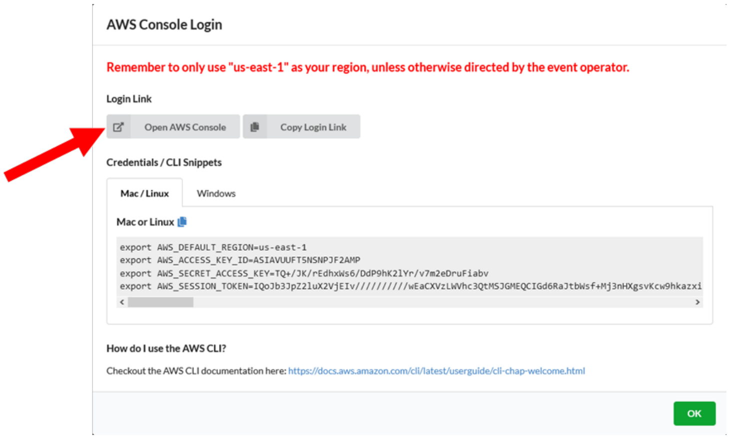
[redacted]

Event ID: ba662966f3de44b78e7c0e5964597f76
Team ID: a034e80f94f947f790732ced38a03416

test_module

Outputs:

No outputs defined



AWS Console Login

Remember to only use "us-east-1" as your region, unless otherwise directed by the event operator.

Login Link

Credentials / CLI Snippets

Mac or Linux

```
export AWS_DEFAULT_REGION=us-east-1
export AWS_ACCESS_KEY_ID=ASIAVUUFT5NSNPJF2AMP
export AWS_SECRET_ACCESS_KEY=TQ+/JK/rEdhxWs6/DdP9hK2lYr/v7m2eDruFiabv
export AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEIv//////////wEaCXVzLWVhc3QtMSJGMEQCIGd6RaJtbWsf+Mj3nHXgsvKcw9hkazxi
```

How do I use the AWS CLI?

Checkout the AWS CLI documentation here: https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html

1.4 Follow this link to set up your environment using CloudFormation.

The link will pre-load the page with an Amazon S3 URL. Just click **Next** at the bottom of the page.

https://console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/new?stackName=SecurityHubWorkshop&templateURL=https://sa-security-specialist-workshops-us-west-2.s3-us-west-2.amazonaws.com/security-hub-workshop/templates/sechub-workshop-setup-template.json

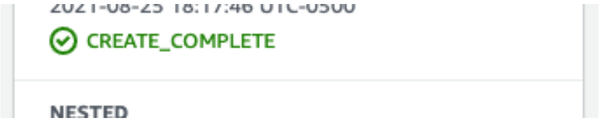
1.5 On the Specify stack details page, there are 5 drop-down options under Parameters.

Select "**Yes-…**" for all five parameters. Leave everything else on the page as it is and click **Next**.

1.6 On the Configure stack options page, just click **Next**.

1.7 On the Review page, check the two boxes under Capabilities and click **Create Stack**.

1.8 It takes 5-10 minutes to complete. Refresh the page until you see that each of the Nested stacks show a status of **CREATE_COMPLETE**. There are 6 nested stacks total.



2021-08-25 18:17:46 UTC-0500

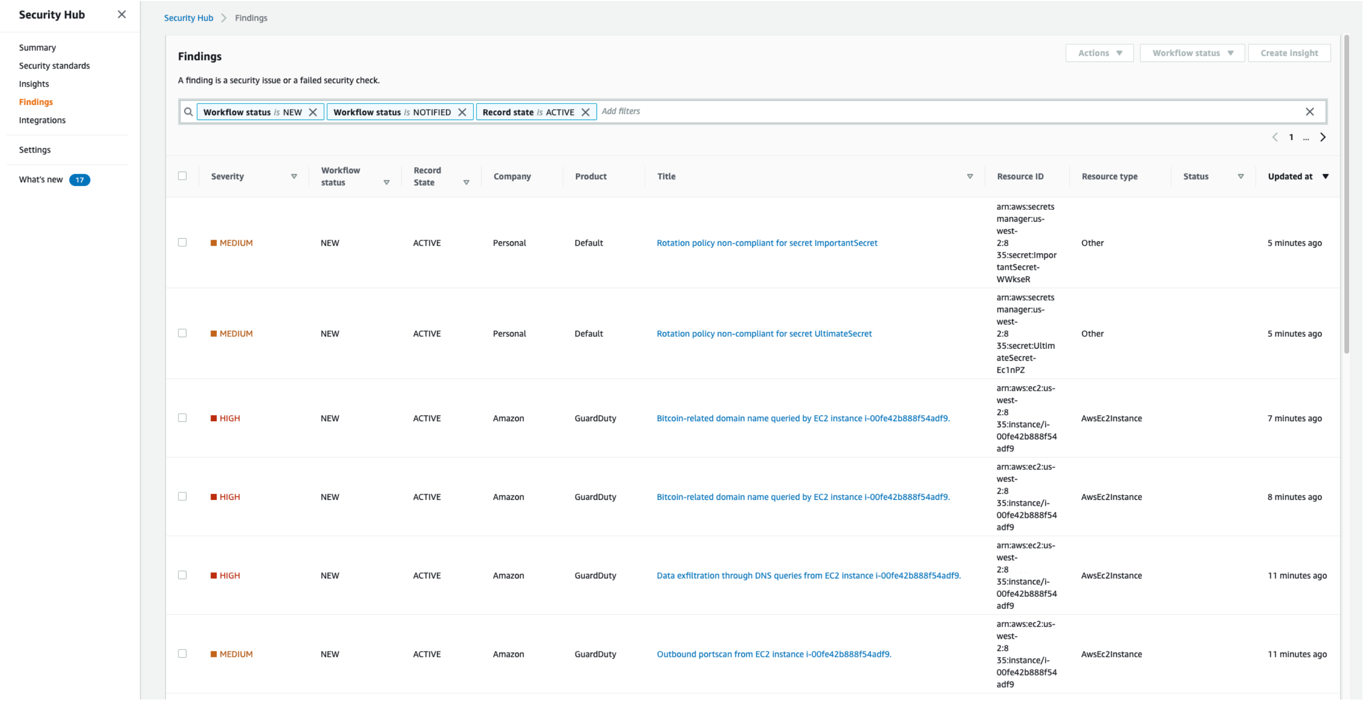
2. Explore AWS Security Hub

AWS Security Hub gives you a comprehensive view of your security alerts and security posture across your AWS accounts. There are a range of powerful security tools at your disposal, from firewalls and endpoint protection to vulnerability and compliance scanners. But oftentimes this leaves your team switching back-and-forth between these tools to deal with hundreds, and sometimes thousands, of security alerts every day. With Security Hub, you now have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Systems Manager, and AWS Firewall Manager, as well as from AWS Partner Network (APN) solutions. AWS Security Hub continuously monitors your environment using automated security checks based on the AWS best practices and industry standards that your organization follows. You can also take action on these security findings by investigating them in Amazon Detective or by using Amazon CloudWatch Event rules to send the findings to ticketing, chat, Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR), and incident management tools or to custom remediation playbooks.

2.1 Open **AWS Security Hub**. https://console.aws.amazon.com/securityhub

2.2 Click on **Findings** from the left-hand navigation pane.

Security Hub imports findings AWS security services, third-party product integrations that you enable, and custom integrations you build. Security Hub consumes these findings using a standard findings format called AWS Security Finding Format (ASFF), which eliminates the need for time-consuming data conversion efforts. Security Hub then correlates the findings across integrated products to prioritize the most important ones.



Findings

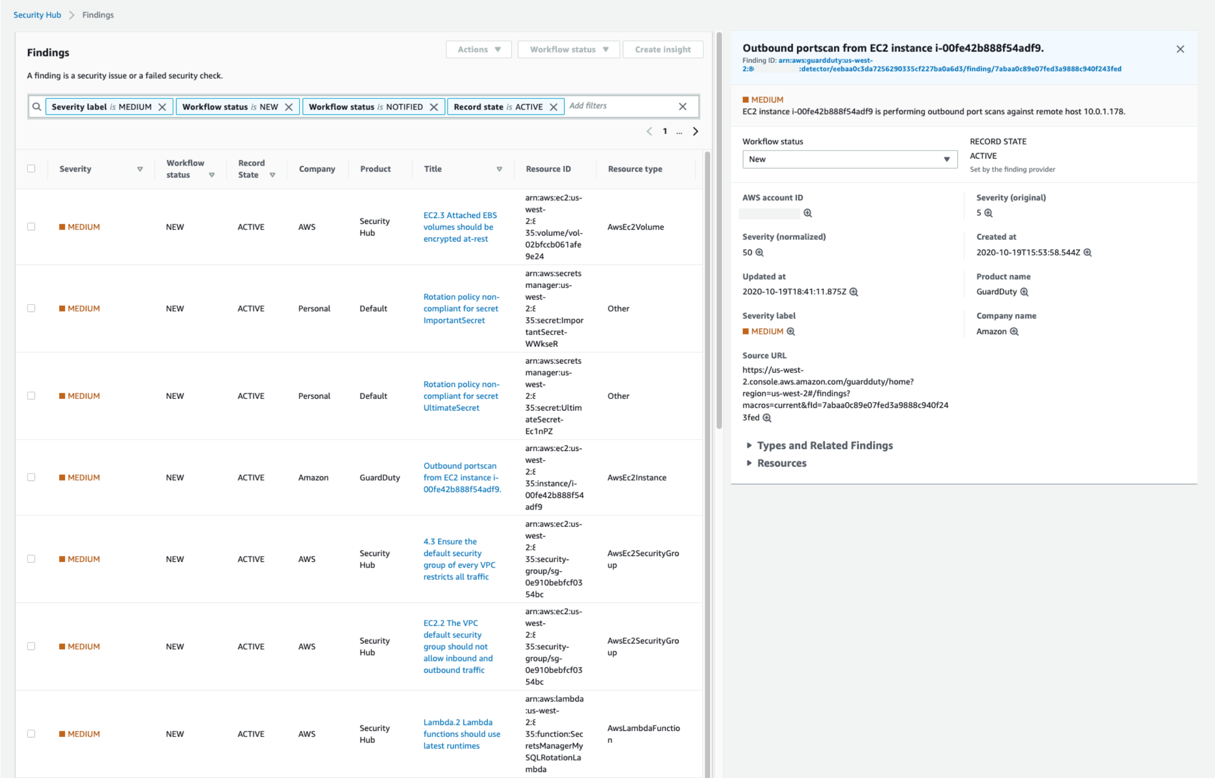
A finding is a security issue or a failed security check.

Workflow status *is* NEW | Workflow status *is* NOTIFIED | Record state *is* ACTIVE

□	Severity	Workflow status	Record State	Company	Product	Title	Resource ID	Resource type	Status	Updated at
□	MEDIUM	NEW	ACTIVE	Personal	Default	Rotation policy non-compliant for secret ImportantSecret	arn:aws:secretsmanager:us-west-2:835:secret:ImportantSecret-WWkseR	Other		5 minutes ago
□	MEDIUM	NEW	ACTIVE	Personal	Default	Rotation policy non-compliant for secret UltimateSecret	arn:aws:secretsmanager:us-west-2:835:secret:UltimateSecret-Ec1nPZ	Other		5 minutes ago
□	HIGH	NEW	ACTIVE	Amazon	GuardDuty	Bitcoin-related domain name queried by EC2 instance i-00fe42b888f54adf9.	arn:aws:ec2:us-west-2:835:instance/i-00fe42b888f54adf9	AwsEc2Instance		7 minutes ago
□	HIGH	NEW	ACTIVE	Amazon	GuardDuty	Bitcoin-related domain name queried by EC2 instance i-00fe42b888f54adf9.	arn:aws:ec2:us-west-2:835:instance/i-00fe42b888f54adf9	AwsEc2Instance		8 minutes ago
□	HIGH	NEW	ACTIVE	Amazon	GuardDuty	Data exfiltration through DNS queries from EC2 instance i-00fe42b888f54adf9.	arn:aws:ec2:us-west-2:835:instance/i-00fe42b888f54adf9	AwsEc2Instance		11 minutes ago
□	MEDIUM	NEW	ACTIVE	Amazon	GuardDuty	Outbound portscan from EC2 instance i-00fe42b888f54adf9.	arn:aws:ec2:us-west-2:835:instance/i-00fe42b888f54adf9	AwsEc2Instance		11 minutes ago

2.3 Click on the **Title** of any finding to see more information in the finding details pane.

Review the information available here.



Security Hub > Findings

Findings

A finding is a security issue or a failed security check.

Severity label *is* MEDIUM ✕ | Workflow status *is* NEW ✕ | Workflow status *is* NOTIFIED ✕ | Record state *is* ACTIVE ✕ | *Add filters*

□	Severity	Workflow status	Record State	Company	Product	Title	Resource ID	Resource type
□	MEDIUM	NEW	ACTIVE	AWS	Security Hub	EC2.3 Attached EBS volumes should be encrypted at-rest	arn:aws:ec2:us-west-2:8[redacted]35:volume/vol-02bfccb061afe9e24	AwsEc2Volume
□	MEDIUM	NEW	ACTIVE	Personal	Default	Rotation policy non-compliant for secret ImportantSecret	arn:aws:secretsmanager:us-west-2:8[redacted]35:secret:ImportantSecret-WWkseR	Other
□	MEDIUM	NEW	ACTIVE	Personal	Default	Rotation policy non-compliant for secret UltimateSecret	arn:aws:secretsmanager:us-west-2:8[redacted]35:secret:UltimateSecret-Ec1nPZ	Other
□	MEDIUM	NEW	ACTIVE	Amazon	GuardDuty	Outbound portscan from EC2 instance i-00fe42b888f54adf9.	arn:aws:ec2:us-west-2:8[redacted]35:instance/i-00fe42b888f54adf9	AwsEc2Instance
□	MEDIUM	NEW	ACTIVE	AWS	Security Hub	4.3 Ensure the default security group of every VPC restricts all traffic	arn:aws:ec2:us-west-2:8[redacted]35:security-group/sg-0e910bebfcf0354bc	AwsEc2SecurityGroup
□	MEDIUM	NEW	ACTIVE	AWS	Security Hub	EC2.2 The VPC default security group should not allow inbound and outbound traffic	arn:aws:ec2:us-west-2:8[redacted]35:security-group/sg-0e910bebfcf0354bc	AwsEc2SecurityGroup
□	MEDIUM	NEW	ACTIVE	AWS	Security Hub	Lambda.2 Lambda functions should use latest runtimes	arn:aws:lambda:us-west-2:8[redacted]35:function:SecretsManagerMySQLRotationLambda	AwsLambdaFunction

Outbound portscan from EC2 instance i-00fe42b888f54adf9.

Finding ID: arn:aws:guardduty:us-west-2:8[redacted]:detector/eebaa0c3da7256290335cf227ba0a6d3/finding/7abaa0c89e07fed3a9888c940f243fed

MEDIUM
EC2 instance i-00fe42b888f54adf9 is performing outbound port scans against remote host 10.0.1.178.

Workflow status: New ▼

RECORD STATE: ACTIVE
Set by the finding provider

AWS account ID: [redacted]

Severity (original): 5

Severity (normalized): 50

Created at: 2020-10-19T15:53:58.544Z

Updated at: 2020-10-19T18:41:11.875Z

Product name: GuardDuty

Severity label: MEDIUM

Company name: Amazon

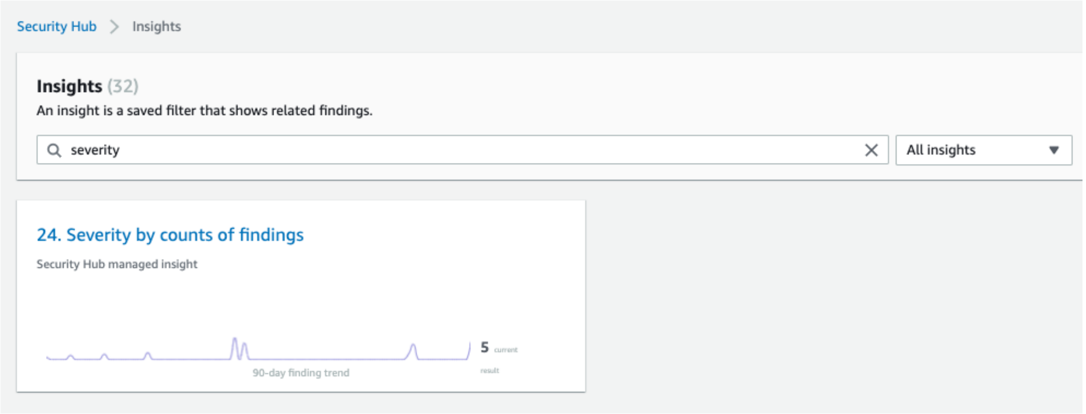
Source URL: https://us-west-2.console.aws.amazon.com/guardduty/home?region=us-west-2#/findings?macros=current&fId=7abaa0c89e07fed3a9888c940f243fed

▸ Types and Related Findings
▸ Resources

2.4 Next, click on **Insights** from the left-hand navigation pane.

A Security Hub Insight is a collection of related findings defined by an aggregation statement and optional filters. An insight identifies a security area that requires attention and intervention. Security Hub offers several managed (default) insights that you can't modify or delete. You can also create custom insights to track security issues unique to your AWS environment and usage.

2.5 In the Insights search bar, type "**severity**".



Security Hub > Insights

Insights (32)

An insight is a saved filter that shows related findings.

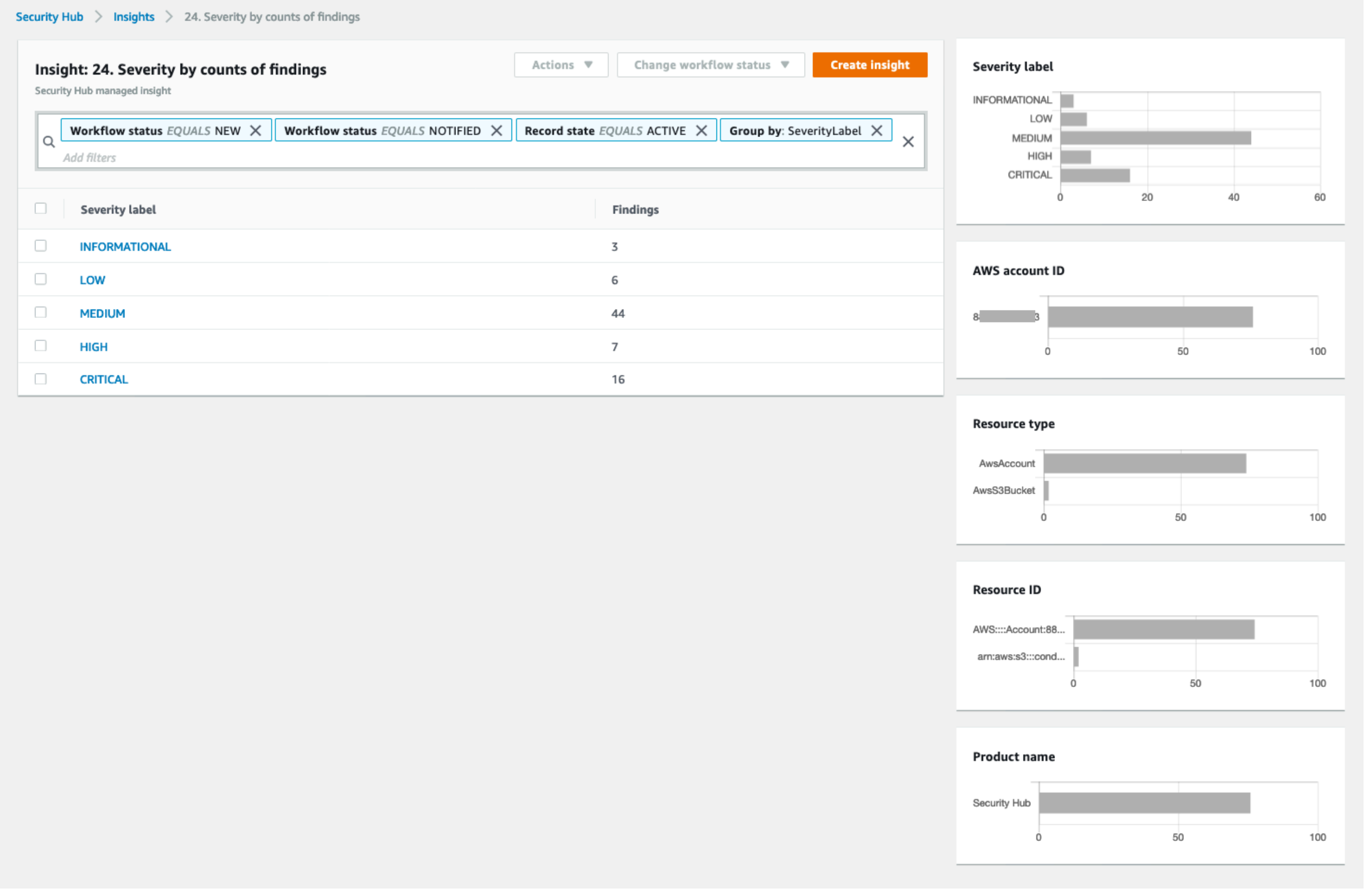
Search: severity ✕ | All insights ▼

24. Severity by counts of findings

Security Hub managed insight

2.6 Click on the title of the Insight, “**Severity by counts of findings**”.

This insight displays the numbers of findings for this account, and corresponding graphs.



Security Hub > Insights > 24. Severity by counts of findings

Insight: 24. Severity by counts of findings

Security Hub managed insight

Workflow status *EQUALS* NEW ✕ **Workflow status** *EQUALS* NOTIFIED ✕ **Record state** *EQUALS* ACTIVE ✕ **Group by**: SeverityLabel ✕

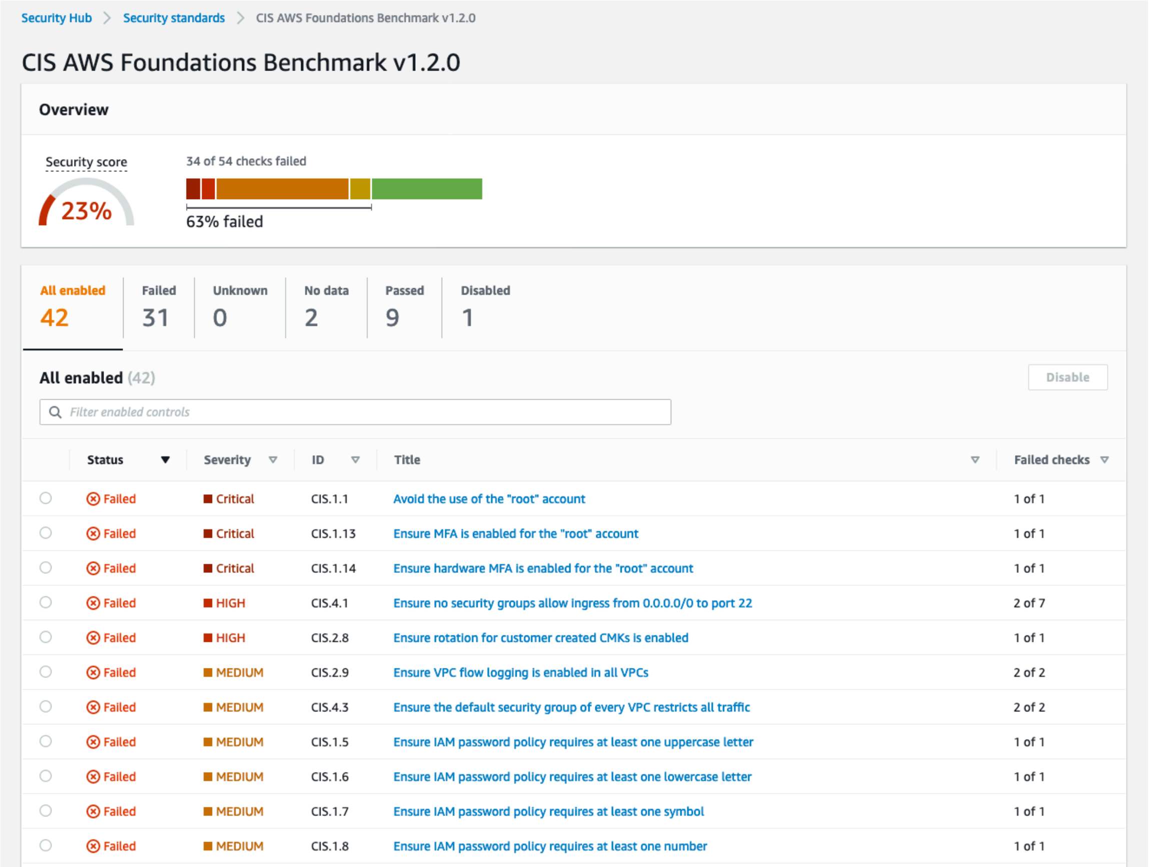
Add filters

□	Severity label	Findings
□	INFORMATIONAL	3
□	LOW	6
□	MEDIUM	44
□	HIGH	7
□	CRITICAL	16

2.7 Click on **Security Standards** from the left-hand navigation pane.

Security standards provide a set of related controls to determine compliance with regulatory frameworks, industry best practices, or company policies. For a standard in Security Hub, you can view the list of controls and determine whether to enable or disable a standard for your account. You can also see the overall security score for the standard. Administrator accounts see aggregated scores and statuses across their member accounts.

2.8 Click **View Results** for CIS AWS Foundations Benchmark v1.2.0.



Security Hub > Security standards > CIS AWS Foundations Benchmark v1.2.0

CIS AWS Foundations Benchmark v1.2.0

Overview

Security score 23%

34 of 54 checks failed

63% failed

All enabled	Failed	Unknown	No data	Passed	Disabled
42	31	0	2	9	1

All enabled (42)

Filter enabled controls

Disable

	Status	Severity	ID	Title	Failed checks
○	Failed	Critical	CIS.1.1	Avoid the use of the "root" account	1 of 1
○	Failed	Critical	CIS.1.13	Ensure MFA is enabled for the "root" account	1 of 1
○	Failed	Critical	CIS.1.14	Ensure hardware MFA is enabled for the "root" account	1 of 1
○	Failed	HIGH	CIS.4.1	Ensure no security groups allow ingress from 0.0.0.0/0 to port 22	2 of 7
○	Failed	HIGH	CIS.2.8	Ensure rotation for customer created CMKs is enabled	1 of 1
○	Failed	MEDIUM	CIS.2.9	Ensure VPC flow logging is enabled in all VPCs	2 of 2
○	Failed	MEDIUM	CIS.4.3	Ensure the default security group of every VPC restricts all traffic	2 of 2
○	Failed	MEDIUM	CIS.1.5	Ensure IAM password policy requires at least one uppercase letter	1 of 1
○	Failed	MEDIUM	CIS.1.6	Ensure IAM password policy requires at least one lowercase letter	1 of 1
○	Failed	MEDIUM	CIS.1.7	Ensure IAM password policy requires at least one symbol	1 of 1
○	Failed	MEDIUM	CIS.1.8	Ensure IAM password policy requires at least one number	1 of 1

2.9 In the **Filter Enabled Controls** search bar, type “**CMK**” and hit enter to search.

CMK stands for customer master key.

2.10 Click the title of the control “**Ensure rotation for customer created CMKs is enabled**”.

Here you can see resources that have failed and passed the check. At the top of the page, there is also a link to “Remediation Instructions”.

3. Creating an Integration for Security Alerts

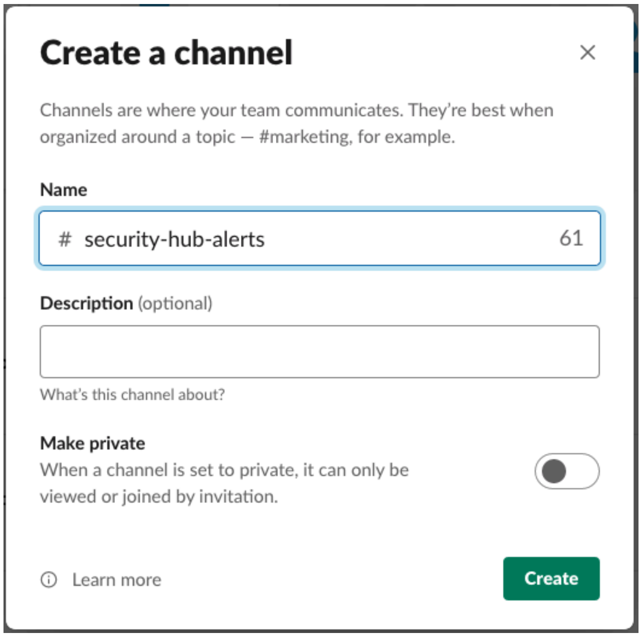
AWS Security Hub continuously monitors your environment using automated security checks based on the AWS best practices and industry standards that your organization follows. You can also take action on these security findings by using Amazon CloudWatch Event rules to send the findings to ticketing, chat, Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR), and incident management tools or to custom remediation playbooks.

Set up a Slack channel for receiving alerts of high priority findings.

3.1 Use the following link to create a new Slack Workspace for yourself.

https://get.slack.help/hc/en-us/articles/206845317-Create-a-Slack-workspace

3.2 Create a new channel in your Slack Workspace and name it “security-hub-alerts”.



Create a channel

Channels are where your team communicates. They're best when organized around a topic — #marketing, for example.

Name: # security-hub-alerts 61

Description (optional): What's this channel about?

Make private: When a channel is set to private, it can only be viewed or joined by invitation.

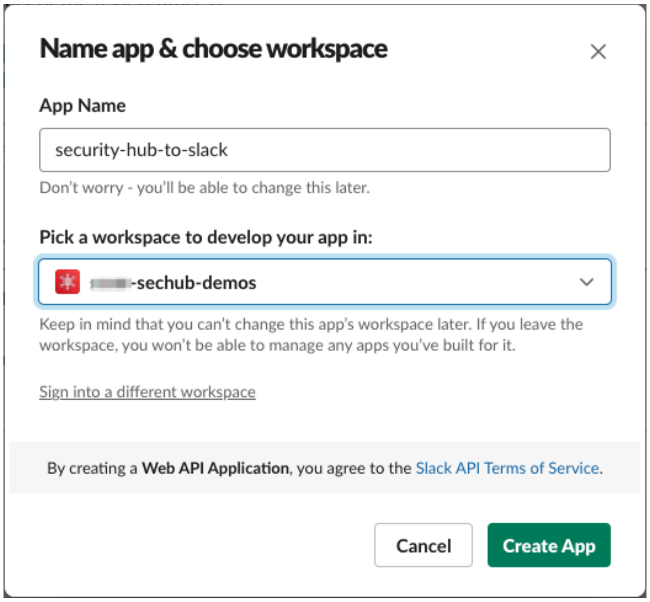
3.3 Then navigate to https://api.slack.com.

3.4 Click on **Create an App** button.

3.5 In the Create an app popup choose **From scratch**.

3.6 Fill in the following details for your app:

- App Name: security-hub-to-slack
- Development Slack Workspace: Choose the Slack workspace that will receive the Security Hub findings (this is the one you created)



Name app & choose workspace

App Name

security-hub-to-slack

Don't worry - you'll be able to change this later.

Pick a workspace to develop your app in:

[redacted]-sechub-demos

Keep in mind that you can't change this app's workspace later. If you leave the workspace, you won't be able to manage any apps you've built for it.

Sign into a different workspace

By creating a **Web API Application**, you agree to the Slack API Terms of Service.

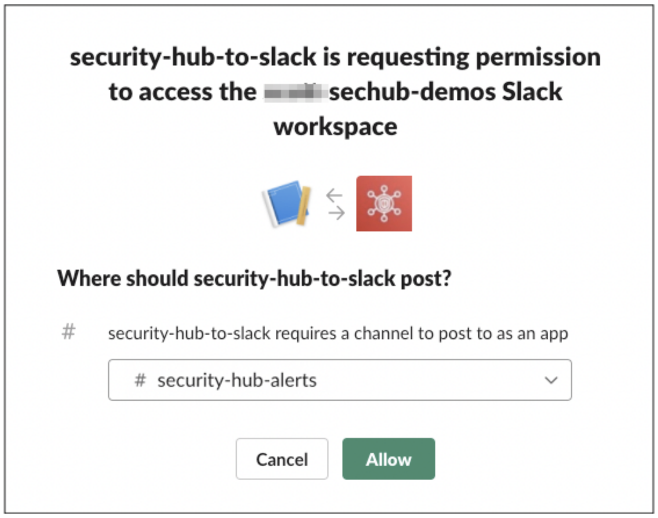
3.7 Click the **Create App** Button.

3.8 Select **Incoming Webhooks**.

3.9 At the **Activate Incoming Webhooks** screen, move the slider from OFF to ON.

3.10 At the bottom of the screen choose **Add New Webhook to Workspace**.

3.11 In the screen asking where your app should post, choose the channel that you created in an earlier step.



security-hub-to-slack is requesting permission to access the [redacted] sechub-demos Slack workspace

Where should security-hub-to-slack post?

security-hub-to-slack requires a channel to post to as an app

# security-hub-alerts

3.12 On the next screen, scroll down to the Webhook URL section and save the URL as you will need it later to complete your setup.

To create the event-driven integration for sending findings to Slack, we'll leverage Amazon EventBridge. Amazon EventBridge is a serverless event bus that makes it easier to build event-driven applications at scale using events generated from your applications, integrated Software-as-a-Service (SaaS) applications, and AWS services.

3.13 Open **Amazon EventBridge**. https://console.aws.amazon.com/events/home

3.14 Click **Create Rule**.

3.15 Type "**SendToSlack**" in the Name field.

3.16 Under Define Pattern, select "**Event pattern**".

3.17 Under "Event matching pattern", select "**Pre-defined pattern by service**".

3.18 Under "Service provider", select "**AWS**".

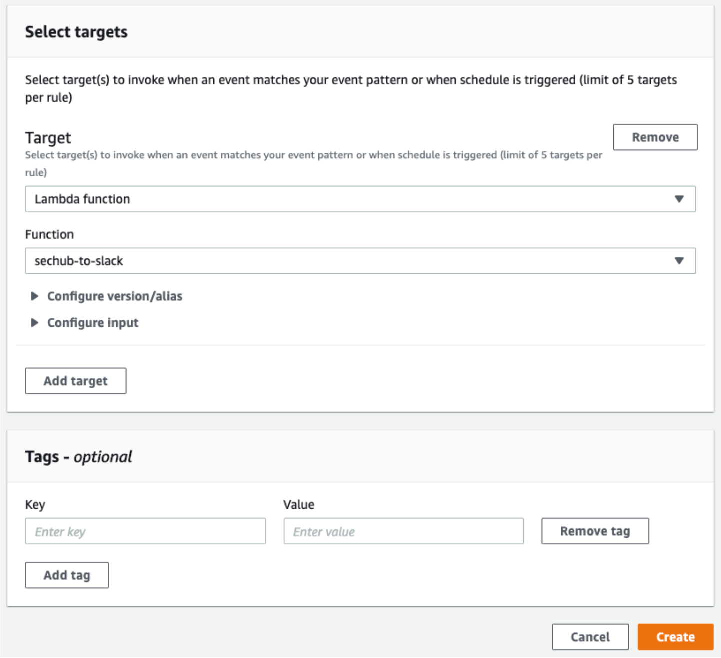
3.19 Under "Service name", select "**Security Hub**".

3.20 Under "Event type", select "**Security Hub Findings – Imported**".

3.21 Now you are presented several additional options. Review the different filters available. For now, leave all of these as default. You may come back and add filters later to limit what alerts your receive.

3.22 Scroll down to the section "Select Targets" and pick "**Lambda function**". Under "Function" select "**sechub-to-slack**". This lambda function was created by the CloudFormation template.

3.23 At the bottom of the page, click **Create**.



Select targets

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

Target

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

Lambda function

Function

sechub-to-slack

Tags - *optional*

Key: *Enter key*

Value: *Enter value*

Now we need to update the Lambda Function to send messages to the Slack channel you created. The function "sechub-to-slack" was created for us, but you need to update the environment variables of your lambda function so that notifications can be sent to the correct Slack workspace.

3.24 Navigate to the Lambda console. https://console.aws.amazon.com/lambda

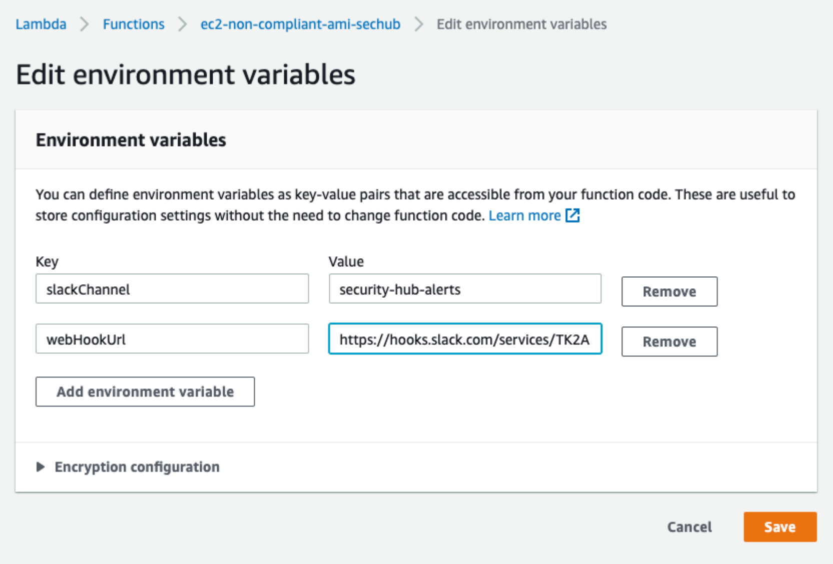
3.25 Search the functions for "**sechub-to-slack**" and click the name of the function.

3.26 Click on the "**Configuration**" tab above the function code. Then click "**Environment variables**" from the tabs on the left.

3.27 Click **Edit** in the Environment variables pane.

3.28 Fill in the two missing values, the name of your Slack channel and the webHookUrl for your Slack Channel.

3.29 Click **Save**.


Lambda > Functions > ec2-non-compliant-ami-sechub > Edit environment variables
Remove
Remove
Add environment variable
▶ Encryption configuration
Cancel
Save

Edit environment variables

Environment variables

You can define environment variables as key-value pairs that are accessible from your function code. These are useful to store configuration settings without the need to change function code. Learn more

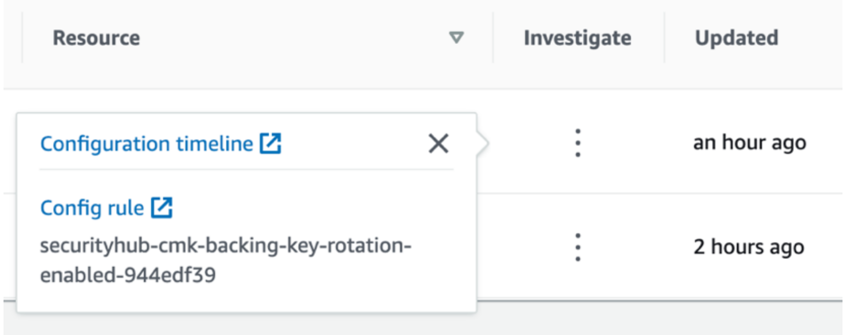
Key	Value
slackChannel	security-hub-alerts
webHookUrl	https://hooks.slack.com/services/TK2A

Your Slack channel and integration are set up! Keep the Slack channel open and watch for findings to appear there as you continue the workshop. Let's practice investigating findings.

4. Investigating Misconfigured Resources

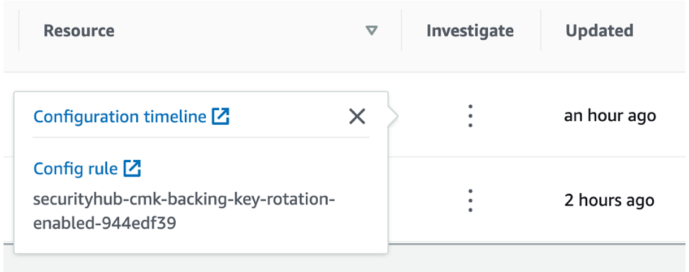
Return to the check for "Ensure rotation for customer created CMKs is enabled" in the CIS AWS Foundations Benchmark v1.2.0. Security Standard from earlier.

4.1 Click on **Security Standards** from the left-hand navigation pane.
4.2 Click **View Results** for CIS AWS Foundations Benchmark v1.2.0.
4.3 In the **Filter Enabled Controls** search bar, type "CMK" and hit enter to search.
4.4 Click the title of the control "**Ensure rotation for customer created CMKs is enabled**". Notice there is a resource listed with a FAILED status. One of your keys does not have rotation enabled.
4.5 Click on the three dots corresponding to the finding to Investigate. A popup will appear with options to view the "Configuration timeline" or view the "Config rule".



securityhub-cmk-backing-key-rotation-enabled-944edf39

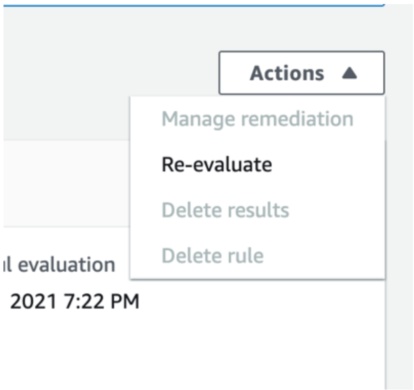
4.6 Click to view the **Configuration timeline**. This will open the configuration timeline for the resource in AWS Config. From here you can review configuration and compliance changes over time or click into specific related CloudTrail events.
4.7 In this case, you want to enable key rotation for the customer master key (CMK). Navigate to the Key Management Service Console: https://console.aws.amazon.com/kms
4.8 In the left navigation, click **Customer Managed Keys**.
4.9 Then click the Key ID for your CMK. This will open the configuration for your key.
4.10 Click the tab titled, **Key rotation**.
4.11 Check the box for "Automatically rotate this CMK every year" and click **Save**.
4.12 You have enabled rotation for the non-compliant key. Return to check in Security Hub to see if it updated. https://us-west-2.console.aws.amazon.com/securityhub/home?region=us-west-2#/standards/cis-aws-foundations-benchmark-1.2.0/CIS.2.8
4.13 If the check is still listed as FAILED for your key (most likely), click the 3 dots to investigate again, but this time click **Config Rule**.



securityhub-cmk-backing-key-rotation-enabled-944edf39

4.14 Clicking on “Config Rule” brought you to the rule in AWS Config that is used to evaluate if the resource is in compliance. Notice that the “Trigger type” is “Periodic: 12 hours”. You can either wait for the rule to evaluate again on schedule, or manually trigger the rule to evaluate.

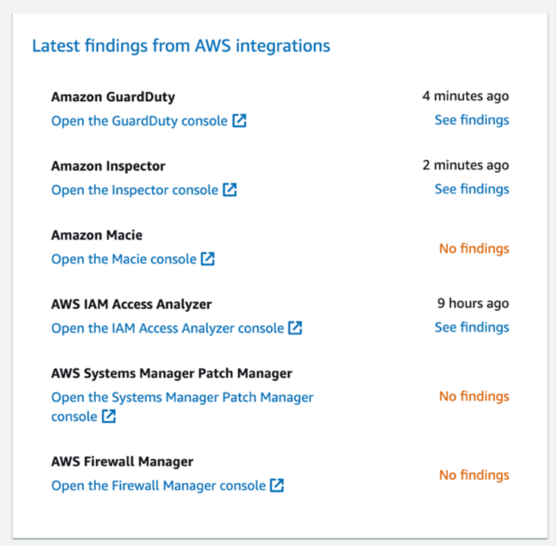
On the right side of the screen, click **Actions** and then select **Re-evaluate**. Wait a minute and refresh the page. It may take a couple minutes. Once the rule re-evaluates, you’ll notice that the timestamp for “Last successful evaluation” changed, and the resource will no longer be listed as noncompliant. This will also update in Security Hub.



5. Identifying Public Resources

5.1 Return to the Security Hub dashboard. https://us-west-2.console.aws.amazon.com/securityhub/home?region=us-west-2#/summary

5.2 Near the bottom of the page, you should notice that Security Hub has received findings from Amazon GuardDuty, Amazon Inspector, and AWS IAM Access Analyzer. Click **See Findings** next to AWS IAM Access Analyzer.



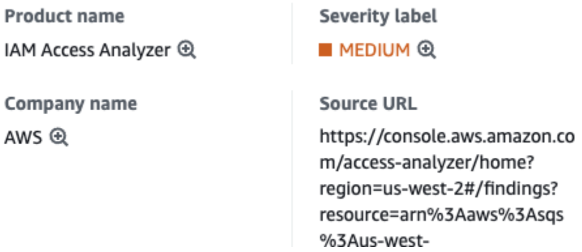
Latest findings from AWS integrations

Amazon GuardDuty Open the GuardDuty console	4 minutes ago See findings
Amazon Inspector Open the Inspector console	2 minutes ago See findings
Amazon Macie Open the Macie console	No findings
AWS IAM Access Analyzer Open the IAM Access Analyzer console	9 hours ago See findings
AWS Systems Manager Patch Manager Open the Systems Manager Patch Manager console	No findings
AWS Firewall Manager Open the Firewall Manager console	No findings

5.3 This opens the findings page within Security Hub with filters added so you only see findings from IAM Access Analyzer. Notice that there is a finding for an SQS Queue. Can you determine what the issue is and how to resolve it?

Hint: Click the title of the finding. Read the section on Remediation.

5.4 Copy and paste the **Source URL** from the finding into a new browser window to investigate the finding in IAM Access Analyzer. Or navigate to IAM Access Analyzer by following the link, https://console.aws.amazon.com/access-analyzer



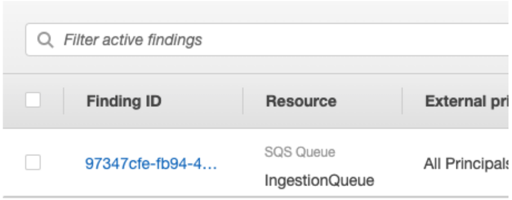
Product name
IAM Access Analyzer

Severity label
MEDIUM

Company name
AWS

Source URL
https://console.aws.amazon.com/access-analyzer/home?region=us-west-2#/findings?resource=arn%3Aaws%3Asqs%3Aus-west-

5.5 Once you are in in IAM Access Analyzer, you'll notice one finding for the public SQS queue.



Filter active findings

□	Finding ID	Resource	External pri
□	97347cfe-fb94-4…	SQS Queue IngestionQueue	All Principals

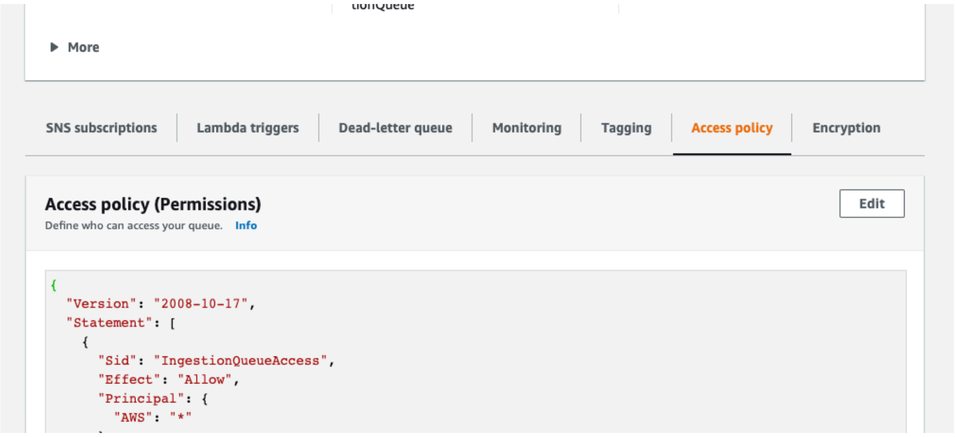
5.6 Click the Finding ID to open the Finding page.

From the Finding page in IAM Access Analyzer, you can see more information on the finding, including Access level. You can also Archive the finding if it is intentional, follow the link to the SQS console to re-configure the resource, or Rescan if you already reconfigured the resource.

5.7 Reconfigure the service to remove public access. Navigate to Amazon SQS by clicking the **Go to SQS Console** button.

5.8 Click the name of the queue **IngestionQueue**.

5.9 From this page, modify the Access policy. Click the **Access policy** tab, and then click the **Edit** button.



Access policy (Permissions)

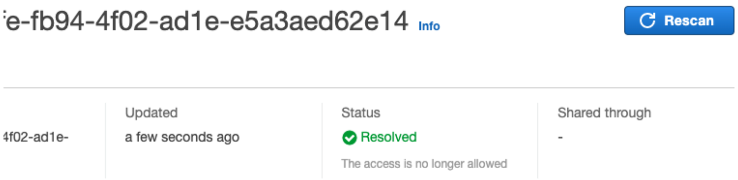
Define who can access your queue.

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "IngestionQueueAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
```

5.10 For the purposes of this workshop, just delete the entire access policy and click **Save** at the bottom of the page. Leave everything else as is. This will replace the public access policy with the default policy.

5.11 To rescan the finding using IAM Access Analyzer, return to IAM Access Analyzer and open the finding again. https://console.aws.amazon.com/access-analyzer

5.12 Check the Status of the finding. It may already show "Resolved". If not, click **Rescan**.



'e-fb94-4f02-ad1e-e5a3aed62e14

	Updated	Status	Shared through
4f02-ad1e-	a few seconds ago	✓ Resolved The access is no longer allowed	-

If you return to Security Hub and look for the finding, you'll see that the record state has updated to "ARCHIVED".

6. Automating Remediation

After Security Hub has detected configuration that needs attention, the next step is take action and resolve the finding. This section will walk you through how to create a custom action in Security Hub which will trigger an EventBridge rule. In this scenario, the EventBridge rule will invoke a Lambda function to change the security group on an EC2 instance that is associated with a Security Hub finding.

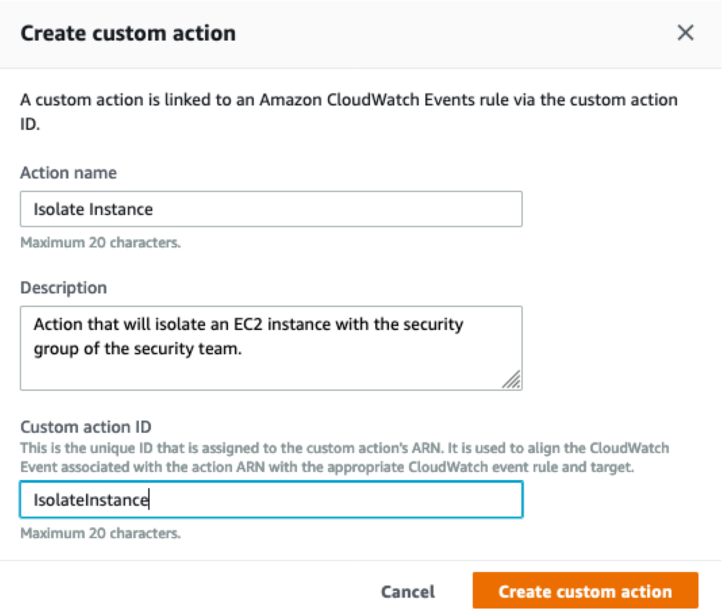
6.1 Navigate to the Security Hub console.

6.2 In the left-hand navigation pane choose **Settings**.

6.3 Choose the **Custom actions** tab.

6.4 Click the **Create custom action** button.

6.5 Enter an Action Name, Action Description, and an Action ID that are representative of an action that would isolate an EC2 instance.



Create custom action

A custom action is linked to an Amazon CloudWatch Events rule via the custom action ID.

Action name: Isolate Instance

Maximum 20 characters.

Description: Action that will isolate an EC2 instance with the security group of the security team.

Custom action ID

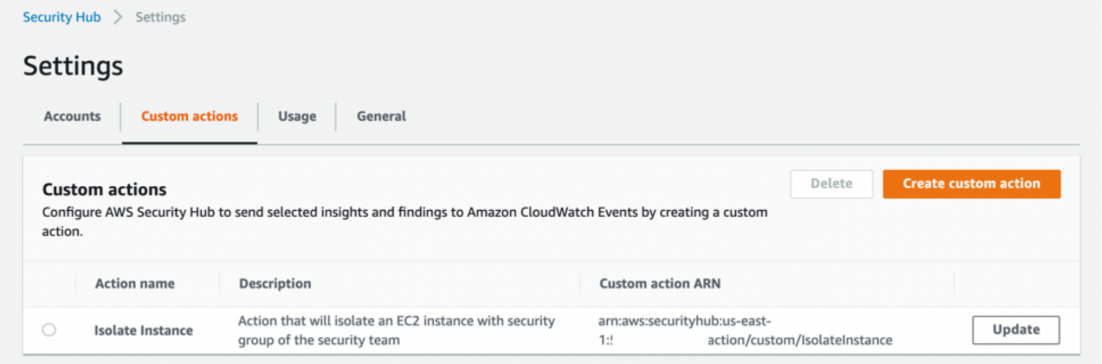
This is the unique ID that is assigned to the custom action's ARN. It is used to align the CloudWatch Event associated with the action ARN with the appropriate CloudWatch event rule and target.

IsolateInstance

Maximum 20 characters.

6.6 Click **Create custom action**.

6.7 Copy the Custom action ARN that was generated for your custom finding.



Custom actions

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

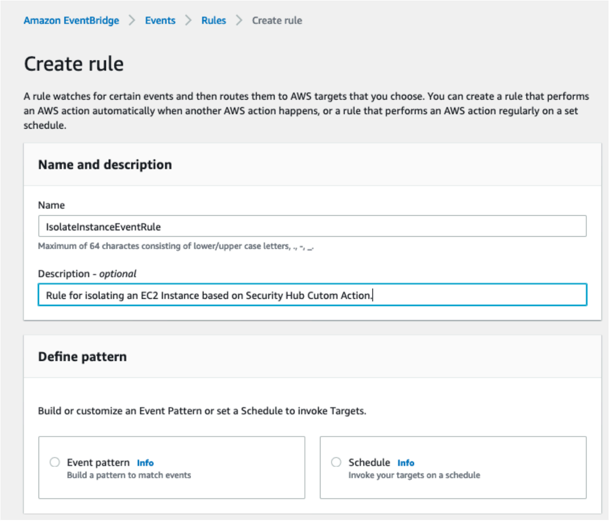
	Action name	Description	Custom action ARN	
○	Isolate Instance	Action that will isolate an EC2 instance with security group of the security team	arn:aws:securityhub:us-east-1:! action/custom/IsolateInstance	Update

In this section, you will define an EventBridge rule that will match events (findings) coming from Security Hub which were forwarded by the custom action you defined above.

6.8 Navigate to the **Amazon EventBridge** Console.

6.9 Click on the **Create rule** on the right side.

6.10 In the Create rule page give your rule a **name** and a **description** that represents the rule's purpose.



Create rule

A rule watches for certain events and then routes them to AWS targets that you choose. You can create a rule that performs an AWS action automatically when another AWS action happens, or a rule that performs an AWS action regularly on a set schedule.

Name and description

Name: IsolateInstanceEventRule

Maximum of 64 charactes consisting of lower/upper case letters, ., -, _.

Description - *optional*: Rule for isolating an EC2 Instance based on Security Hub Cutom Action.

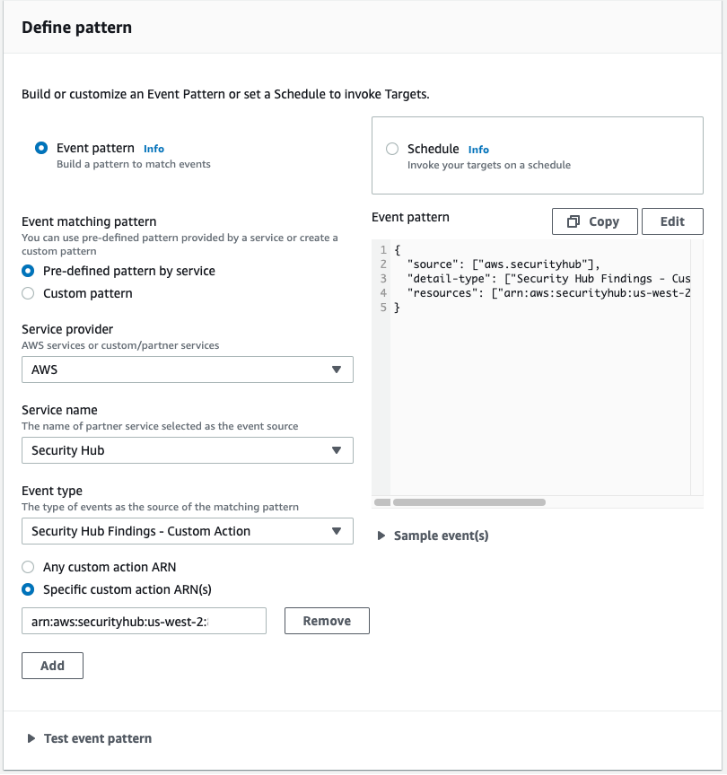
Define pattern

Build or customize an Event Pattern or set a Schedule to invoke Targets.

○ Event pattern Info — Build a pattern to match events

○ Schedule Info — Invoke your targets on a schedule

6.11 Under Define pattern, select **Event pattern**.
6.12 Select **Pre-defined pattern by service**.
6.13 In the drop down for **Service Provider**, select **AWS** for the service provider.
6.14 In the drop down for **Service Name**, select or type and select **Security Hub**.
6.15 In the drop down for **Event type** choose **Security Hub Finding – Custom Action**.
6.16 Select the **Specific custom action ARN(s)** radio button. Enter the ARN for the custom action that you created earlier.



Define pattern

Build or customize an Event Pattern or set a Schedule to invoke Targets.

● Event pattern Info — Build a pattern to match events

○ Schedule Info — Invoke your targets on a schedule

Event matching pattern

You can use pre-defined pattern provided by a service or create a custom pattern

● Pre-defined pattern by service

○ Custom pattern

Service provider

AWS services or custom/partner services

AWS ▼

Service name

The name of partner service selected as the event source

Security Hub ▼

Event type

The type of events as the source of the matching pattern

Security Hub Findings - Custom Action ▼

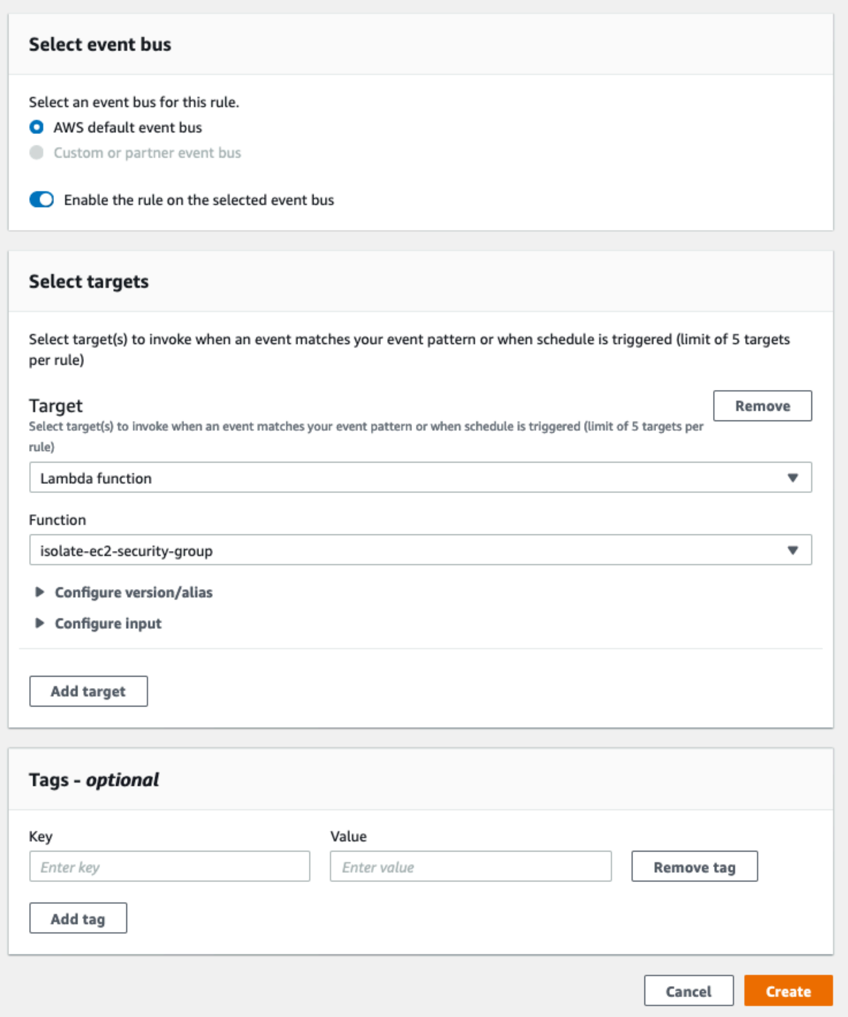
○ Any custom action ARN

● Specific custom action ARN(s)

arn:aws:securityhub:us-west-2:

```
{
  "source": ["aws.securityhub"],
  "detail-type": ["Security Hub Findings - Cus
  "resources": ["arn:aws:securityhub:us-west-2
}
```

6.17 Under Select targets, ensure **Lambda function** is populated in the top drop down and then select **isolate-ec2-security-group** Lambda function.



Select event bus

Select an event bus for this rule.

● AWS default event bus

○ Custom or partner event bus

Enable the rule on the selected event bus

Select targets

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

Target

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

Lambda function

Function

isolate-ec2-security-group

Tags - *optional*

Key: Enter key

Value: Enter value

6.18 Click **Create** to complete creation of the Event Bridge rule.

6.19 Now you will test the response action starting from a Security Finding for an EC2 instance. Navigate to the Security Hub Dashboard.

6.20 In the left-hand navigation pane choose **Findings**.

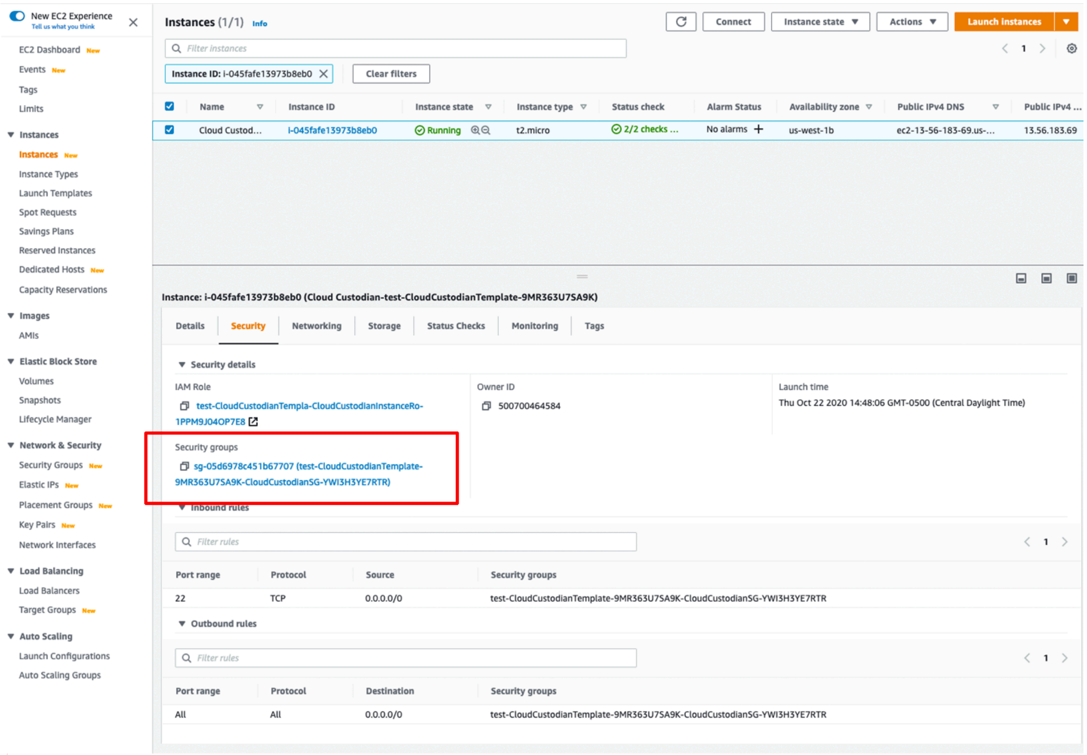
6.21 If you do not see a finding with the resource type of AwsEc2Instance, add a filter for **Resource Type** and enter **AwsEc2Instance** (case sensitive).

6.22 Click the title of any finding in this filtered list where the target is the type **AwsEc2Instance**.

6.23 Expand **Resources** section of the finding.

6.24 Click the blue link for this EC2 instance, under the heading **Resource ID**.

6.25 Click the instance record, and then click the **Security** tab and record the name of the current **security group**.



Instances (1/1) Info

Instance ID: i-045fafe13973b8eb0

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm Status	Availability zone	Public IPv4 DNS	Public IPv4 ...
☑	Cloud Custod...	i-045fafe13973b8eb0	Running	t2.micro	2/2 checks ...	No alarms	us-west-1b	ec2-13-56-183-69.us-...	13.56.183.69

Instance: i-045fafe13973b8eb0 (Cloud Custodian-test-CloudCustodianTemplate-9MR363U7SA9K)

▼ Security details

IAM Role
test-CloudCustodianTempla-CloudCustodianInstanceRo-1PPM9J04OP7E8

Owner ID
500700464584

Launch time
Thu Oct 22 2020 14:48:06 GMT-0500 (Central Daylight Time)

Security groups
sg-05d6978c451b67707 (test-CloudCustodianTemplate-9MR363U7SA9K-CloudCustodianSG-YWI3H3YE7RTR)

▼ Inbound rules

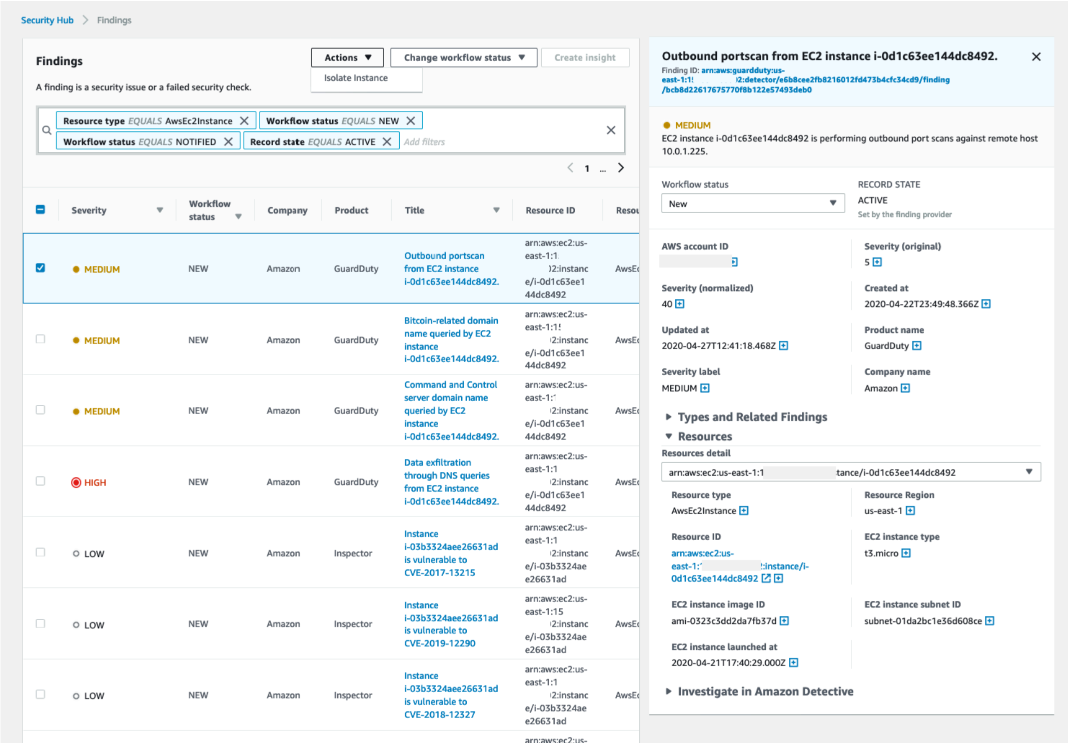
Port range	Protocol	Source	Security groups
22	TCP	0.0.0.0/0	test-CloudCustodianTemplate-9MR363U7SA9K-CloudCustodianSG-YWI3H3YE7RTR

▼ Outbound rules

Port range	Protocol	Destination	Security groups
All	All	0.0.0.0/0	test-CloudCustodianTemplate-9MR363U7SA9K-CloudCustodianSG-YWI3H3YE7RTR

6.26 Go back to the Security Hub tab in your browser and click in the check box in the far left of this same finding.

6.27 In the **Actions** drop down choose the name of your custom action to Isolate EC2 Instances.



Findings

A finding is a security issue or a failed security check.

Resource type EQUALS AwsEc2Instance | Workflow status EQUALS NEW | Workflow status EQUALS NOTIFIED | Record state EQUALS ACTIVE

☐	Severity	Workflow status	Company	Product	Title	Resource ID	Resou
☑	● MEDIUM	NEW	Amazon	GuardDuty	Outbound portscan from EC2 instance i-0d1c63ee144dc8492.	arn:aws:ec2:us-east-1:1 [redacted] 2:instance/i-0d1c63ee144dc8492	AwsE
☐	● MEDIUM	NEW	Amazon	GuardDuty	Bitcoin-related domain name queried by EC2 instance i-0d1c63ee144dc8492.	arn:aws:ec2:us-east-1:1 [redacted] 2:instance/i-0d1c63ee144dc8492	AwsE
☐	● MEDIUM	NEW	Amazon	GuardDuty	Command and Control server domain name queried by EC2 instance i-0d1c63ee144dc8492.	arn:aws:ec2:us-east-1:1 [redacted] 2:instance/i-0d1c63ee144dc8492	AwsE
☐	◉ HIGH	NEW	Amazon	GuardDuty	Data exfiltration through DNS queries from EC2 instance i-0d1c63ee144dc8492.	arn:aws:ec2:us-east-1:1 [redacted] 2:instance/i-0d1c63ee144dc8492	AwsE
☐	○ LOW	NEW	Amazon	Inspector	Instance i-03b3324aee26631ad is vulnerable to CVE-2017-13215	arn:aws:ec2:us-east-1:1 [redacted] 2:instance/i-03b3324aee26631ad	AwsE
☐	○ LOW	NEW	Amazon	Inspector	Instance i-03b3324aee26631ad is vulnerable to CVE-2019-12290	arn:aws:ec2:us-east-1:15 [redacted] 2:instance/i-03b3324aee26631ad	AwsE
☐	○ LOW	NEW	Amazon	Inspector	Instance i-03b3324aee26631ad is vulnerable to CVE-2018-12327	arn:aws:ec2:us-east-1:1 [redacted] 2:instance/i-03b3324aee26631ad	AwsE

Outbound portscan from EC2 instance i-0d1c63ee144dc8492.

Finding ID: arn:aws:guardduty:us-east-1:1 [redacted] 2:detector/e6b8cee2fb8216012fd473b4cfc34cd9/finding/bcb8d22617675770f8b122e57493deb0

● MEDIUM
EC2 instance i-0d1c63ee144dc8492 is performing outbound port scans against remote host 10.0.1.225.

Workflow status: New

RECORD STATE: ACTIVE
Set by the finding provider

AWS account ID
[redacted]

Severity (original)
5

Severity (normalized)
40

Created at
2020-04-22T23:49:48.366Z

Updated at
2020-04-27T12:41:18.468Z

Product name
GuardDuty

Severity label
MEDIUM

Company name
Amazon

▶ Types and Related Findings

▼ Resources

Resources detail
arn:aws:ec2:us-east-1:1 [redacted] tance/i-0d1c63ee144dc8492

Resource type
AwsEc2Instance

Resource Region
us-east-1

Resource ID
arn:aws:ec2:us-east-1: [redacted] :instance/i-0d1c63ee144dc8492

EC2 instance type
t3.micro

EC2 instance image ID
ami-0323c3dd2da7fb37d

EC2 instance subnet ID
subnet-01da2bc1e36d608ce

EC2 instance launched at
2020-04-21T17:40:29.000Z

▶ Investigate in Amazon Detective

6.28 Go back to the **EC2 browser tab**. Refresh the tab. Verify that the security group on the instance has been changed to the security team security group. Review the isolate-ec2-security-group Lambda function. What changes would you make for your own custom actions?

7. Investigating a Threat

The final part of the workshop is a demo of investigating a threat using GuardDuty and Detective.
See your facilitator.

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3. With the cloud, the collection and aggregation of account and network activities is simplified, but it can be time consuming for security teams to continuously analyze event log data for potential threats. With GuardDuty, you now have an intelligent and cost-effective option for continuous threat detection in AWS. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs. With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain. By integrating with Amazon CloudWatch Events, GuardDuty alerts are actionable, easy to aggregate across multiple accounts, and straightforward to push into existing event management and workflow systems.

Learn more about Amazon GuardDuty here: https://aws.amazon.com/guardduty/.

Amazon Detective makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities. Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations.

AWS security services like Amazon GuardDuty, Amazon Macie, and AWS Security Hub as well as partner security products can be used to identify potential security issues, or findings. These services are really helpful in alerting you when something is wrong and pointing out where to go to fix it. But sometimes there might be a security finding where you need to dig a lot deeper and analyze more information to isolate the root cause and take action. Determining the root cause of security findings can be a complex process that often involves collecting and combining logs from many separate data sources, using extract, transform, and load (ETL) tools or custom scripting to organize the data, and then security analysts having to analyze the data and conduct lengthy investigations.

Amazon Detective simplifies this process by enabling your security teams to easily investigate and quickly get to the root cause of a finding. Amazon Detective can analyze trillions of events from multiple data sources such as Virtual Private Cloud (VPC) Flow Logs, AWS CloudTrail, and Amazon GuardDuty, and automatically creates a unified, interactive view of your resources, users, and the interactions between them over time. With this unified view, you can visualize all the details and context in one place to identify the underlying reasons for the findings, drill down into relevant historical activities, and quickly determine the root cause.

Learn more about Amazon Detective here: https://aws.amazon.com/detective/.