

Custom Insights and Custom Findings

A key feature of Security Hub is the ability to create security findings that are above and beyond the native integrations that Security Hub has with AWS services or 3rd party providers. This custom findings feature gives customers the flexibility to build their security checks against their AWS environment and import them into Security Hub.

In the environment for this workshop, multiple sources are sending custom findings into Security Hub:

- The open-source Cloud Custodian project running on an EC2 instance.
- A Config Rule checking for non-compliant AMIs.
- A Lambda function looking for non-compliant secrets.

This module will guide you on how to either view or fully integrate these findings sources into Security Hub.

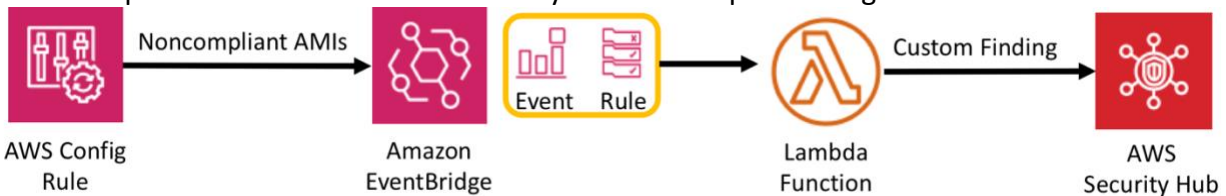
Steps

1. Create Custom Findings with AWS Config
2. Create Custom Insight for Custom Findings

Create Custom Findings with AWS Config

In this section we will cover how you can create your own findings in Security Hub. The foundation for this section will be using AWS Config Rules to identify compliance violations and then posting those violations into Security Hub.

This is a representation of the architecture you will be implementing:



For this part of the workshop a Config rule has already been defined. The specific Config rule being used is **approved-amis-by-id**. This rule looks for EC2 instances backed by AMIs that are not in the rule's list of approved AMIs. Any EC2 instances that are not using an AMI that is in the approved list will be reported by the rule as noncompliant.

Create EventBridge Rule

This section creates the rule which will catch messages sent from Config rules about noncompliant resources and route them to a target.

1. Navigate to the **Amazon EventBridge** Console.
2. Click on **Create rule** on the right side.

Application Integration

Amazon EventBridge

Build event-driven applications at scale

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.

Create a new rule

Create a rule. Choose an AWS service, SaaS app or custom app as event source, define event pattern, and attach an AWS service or SaaS apps via API Destination as target(s).

[Create rule](#) [View rules](#)

Pricing

There is no up-front commitment or minimum fee. You simply pay for what you use and will be charged at the end of the month for your usage. Pricing varies by region.


[Cost calculator](#)

Getting started

[Introduction to Amazon EventBridge](#)

[Amazon EventBridge Blog](#)

How it works



3. 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

unapproved-amis-rule

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

Description - optional

Rule to capture events for unapproved amis

All Config Rule output is sent as events to the AWS default event bus. The define pattern section allows you to identify filters to take a specific action when matched events appear.

4. Under **Define pattern**, select **Event pattern**.
5. Select **Pre-defined pattern by service**.
6. In the drop down for **Service Provider**, select **AWS**.
7. In the drop down for **Service Name**, select or type and select or search for **Config**.
8. For the **Event Type**, choose **Config Rules Compliance Change**.
9. Chose the **Specific rule name(s)** radio button and enter **approved-amis-by-id** in the text box.

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

Config ▼

Event type

The type of events as the source of the matching pattern

Config Rules Compliance Change ▼

☒ **Any message type**
☐ Specific message type(s)

☐ Any rule name
☒ **Specific rule name(s)**

approved-amis-by-id

Rem
ove

Add

☒ **Any resource type**
☐ Specific resource type(s)

☒ **Any resource ID**
☐ Specific resource ID(s)

Event pattern

Edit

```
{
  "source": [
    "aws.config"
  ],
  "detail-type": [
    "Config Rules Compliance Change"
  ],
  "detail": {
    "configRuleName": [
      "approved-amis-by-id"
    ]
  }
}
```

10. Scroll to bottom of page. Under Select targets, ensure **Lambda function** is populated in the top drop down and then select **ec2-non-compliant-ami-sechub** 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)

Remove

Lambda function

▼

Function

ec2-non-compliant-ami-sechub

▼

► Configure version/alias

► Configure input

Add target

Tags - optional

| Key | Value | |
|--|--|------------|
| <input type="text" value="Enter key"/> | <input type="text" value="Enter value"/> | Remove tag |
| Add tag | | |

Cancel

Create

Note: **ec2-non-compliant-ami-sechub** is a custom Lambda function created during the setup of this workshop. Feel free to look at the function to learn more about how it integrates with Security Hub.

10. Click **Create**.

Create a rule to track approved AMIs

This section will run the Config rule to generate information on noncompliant resources and send them to Security Hub.

1. Navigate to the **AWS Config** dashboard
2. From the Config Dashboard click **Rules** on the left menu.

Note: Make sure to not choose Rules from the Aggregated view menu. This requires Config Aggregator and this feature is not used in this workshop.

3. In the Rules page there will be a rule named **approved-amis-by-id**. Click on the rule name to go to the detail page for that rule.

In the rule detail screen you will see the rule configured with a list of approved AMIs. There will resources showing as noncompliant. Now that the EventBridge is in place you want to see the noncompliant instances show in Security Hub as a finding.

The screenshot displays the AWS Config console for the rule 'approved-amis-by-id'. The breadcrumb navigation at the top reads 'AWS Config > Rules > approved-amis-by-id'. The rule name 'approved-amis-by-id' is shown at the top left, with an 'Actions' dropdown menu to its right. Below this, the 'Rule details' section is expanded, showing the description 'Config Rule to check for approved AMIs in the account', the Config rule ARN 'arn:aws:configus-west-2:2:config-rule/config-rule-ricrhv', the trigger type 'Oversized configuration changes' and 'Configuration changes', the scope of changes 'All changes', and the last successful evaluation 'August 9, 2021 9:31 PM'. The 'Parameters' section is also expanded, showing a table with one parameter: 'amids' (CSV type) with the value 'ami-03191f18e2403e784,ami-083ac7c7ecf9bb9b0,ami-080387efdab3c4ce3' and a description 'Specify AMI IDs (comma separated list of up to 10)'. Below the parameters, the 'Resources in scope' section is expanded, showing a dropdown menu set to 'Noncompliant'. A table lists the resources in scope, with one resource shown: 'I-0a01c57c4f741b0a2' (EC2 Instance) with a status of 'Noncompliant'. The table has columns for ID, Type, Status, Annotation, and Compliance. The 'Status' column shows a red triangle icon and the text 'Noncompliant'.

| Key | Type | Value | Description |
|-------|------|---|---|
| amids | CSV | ami-03191f18e2403e784,ami-083ac7c7ecf9bb9b0,ami-080387efdab3c4ce3 | Specify AMI IDs (comma separated list of up to 10). |

| ID | Type | Status | Annotation | Compliance |
|---------------------|--------------|--------|------------|--------------|
| I-0a01c57c4f741b0a2 | EC2 Instance | - | - | Noncompliant |

4. In the **Actions** drop down on the top left, choose **Delete results**. Enter **Delete** in the the confirmation box.
5. Click on the refresh button in the **Resources in scope** section. The noncompliant resource section should now be empty.
6. In the **Actions** drop down choose **Re-evaluate**. You will get a message that the Config rule is being reevaluated.
7. To track progress of the rule re-evaluation you can either refresh the entire page in your browser or use the refresh button in the **Resources in scope** section of the page.

It may take a couple minutes and refreshes before the noncompliant resource re-appears in the **Resources in scope** section.

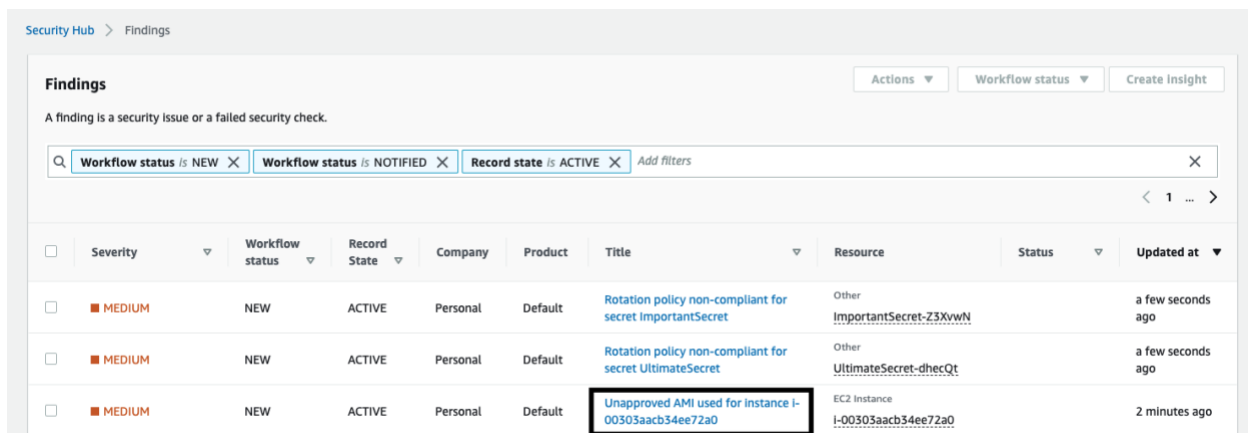
An instance should now be showing as noncompliant in the **Resources in scope** section. This re-run of the Config rule will trigger the EventBridge rule that is looking for noncompliant resources, resulting in the finding showing in Security Hub.

NOTE: Clearing results and re-evaluating the Config rule is being done to help force sending findings into Security Hub for this workshop. Under normal circumstances you will not need manually run the Config rule in order to get findings to show in Security Hub. Once you have the Config and EventBridge rules configured, new noncompliant resources will automatically flow into Security Hub as a Config rule finds noncompliant resources.

View the noncompliant AMI finding in Security Hub

1. Navigate to the **Security Hub** dashboard.
2. Click on the **Findings** option in the left-hand navigate menu.
3. You should see a finding towards the top of the findings list with a **Company** of **Personal** and a **Title** about an unapproved AMI for an instance. This finding is the result of your compliance rule and its integration with EventBridge. Click on the **Title** link for the finding to view more details for your finding.

NOTE: If the finding is not showing towards the top you can filter for the finding. Click in the filter bar and choose a filter of "Title", choose a filter match type of "starts with" and enter "Unapproved AMI" as the filter value.



| | Severity | Workflow status | Record State | Company | Product | Title | Resource | Status | Updated at |
|--------------------------|----------|-----------------|--------------|----------|---------|--|----------------------------------|--------|-------------------|
| <input type="checkbox"/> | MEDIUM | NEW | ACTIVE | Personal | Default | Rotation policy non-compliant for secret ImportantSecret | Other ImportantSecret-Z3XvwN | | a few seconds ago |
| <input type="checkbox"/> | MEDIUM | NEW | ACTIVE | Personal | Default | Rotation policy non-compliant for secret UltimateSecret | Other UltimateSecret-dhecQt | | a few seconds ago |
| <input type="checkbox"/> | MEDIUM | NEW | ACTIVE | Personal | Default | Unapproved AMI used for instance i-00303aacb34ee72a0 | EC2 Instance i-00303aacb34ee72a0 | | 2 minutes ago |

You now have a setup in place that helps demonstrate how you can send custom findings into Security Hub using AWS data sources and EventBridge rules.

NOTE: Your environment also includes a Lambda function named "find-secrets-without-rotation" that checks for secrets that have a rotation time that is beyond the max day's parameter on the function. When secrets are found with a rotation time beyond what is defined in the function a finding is created in Security Hub. Take some time to explore the Lambda function to see how you can directly send custom findings into Security Hub.

Create Custom Insights for Custom Findings

This section will walk you through how to create a custom insight to give you more visibility about the sources that are sending findings into Security Hub for custom findings.

When a custom finding is sent into Security Hub it will have a company of **Personal** and a product of **Default**.

Security Hub provides the ability to create insights that filter on more attributes than you can see from the initial findings console. You can filter on additional attributes that are passed in as part of a finding that enable you to get more granular in how you filter findings.

For this lab the custom findings have been built to utilize the Generator ID field in the AWS Security Finding Format (ASFF) to help in identifying sources of findings.

1. Navigate to the **Security Hub** dashboard.
2. Choose **Insights** from the left hand navigation.
3. Click **Create insight**.
4. Click in the filter field at the top to add additional filters. Choose a filter field of **Company name**, a filter match type of **is**, and a value of **Personal**.

Create insight

To create an insight, add any relevant filters and choose how your findings are grouped by using the 'Group by' filter (required).

Actions Workflow status Create insight

Workflow status is NEW Workflow status is NOTIFIED Record state is ACTIVE Company name: X

Company name: is Personal Back Apply

| | Severity | Workflow status | Record State | Company | Product | Title | Source type | Status |
|--------------------------|----------|-----------------|--------------|----------|---------|--|--|--------|
| <input type="checkbox"/> | MEDIUM | NEW | ACTIVE | Personal | Default | Rotation policy non-compliant for secret ImportantSecret | arn:aws:secretsmanager:us-west-1:54:secret:ImportantSecret | Other |

5. Now add one more filter. Choose a filter field of **Product name**, a filter match type of **is**, and a value of **Default**.

6. Choose a Grouping of **Group by**:. In the list of options choose **Generator ID**.

Create insight

To create an insight, add any relevant filters and choose how your findings are grouped by using the 'Group by' filter (required).

Actions Workflow status Create insight

Product name is Default X Company name is Personal X Workflow status is NEW X Workflow status is NOTIFIED X Record state is ACTIVE X X

Group by:

Group by:

- ☐ AWS account ID
- ☐ Company name
- ☐ Status
- ☒ Generator ID
- ☐ Malware name
- ☐ Process name

Back Apply

| Record State | Company | Product | Title | Resource ID | Resource type | Status |
|--------------|----------|---------|--|--|---------------|--------|
| ACTIVE | Personal | Default | Rotation policy non-compliant for secret ImportantSecret | arn:aws:secretsmanager:us-west-1:54secret:importantSecret-c3BsaG | Other | |
| ACTIVE | Personal | Default | Rotation policy non-compliant for secret UltimateSecret | arn:aws:secretsmanager:us-west-1:54secret:UltimateSecret-ZpbqJk | Other | |

7. Click on **Create insight** to save your custom insight.
8. Give your insight a name that is meaningful to you and click **Create insight**.

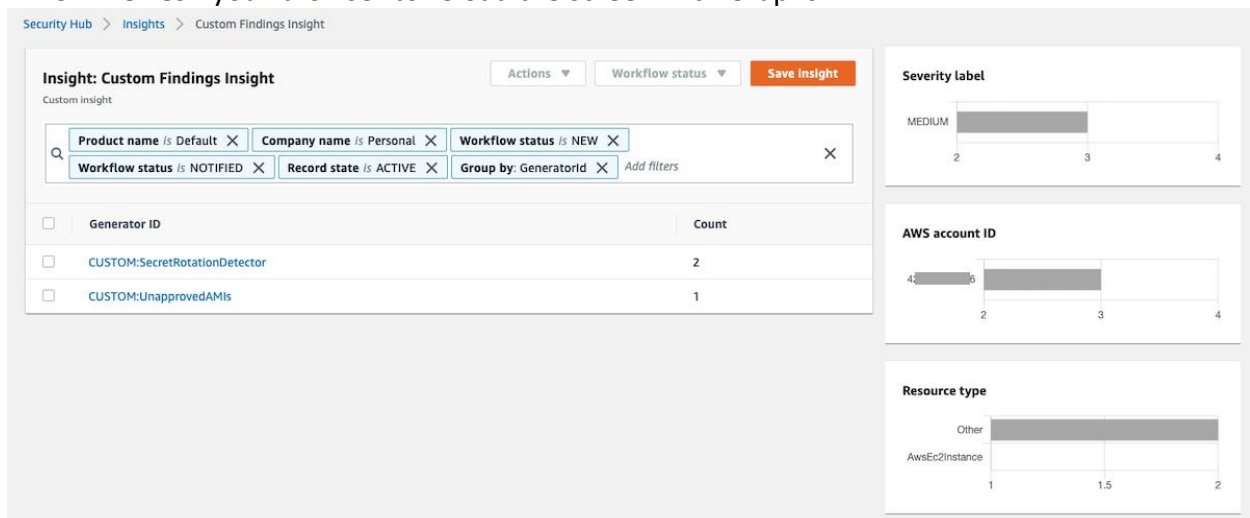
Create insight

Insight name

Custom Findings Insight

Cancel Create insight

9. **Refresh** your browser to reload the screen with Graphs.



You now have a custom insight that allows you to get more visibility around custom findings that are coming into Security Hub, allowing you more visibility into what your security findings are related to, what the source of the findings are, and where you should prioritize your remediation efforts.

For the findings in this custom insight, you can click on the resource ID links to drill into the specific findings related to those resources.