Security Hub Walkthrough

In this section, you will follow a guided demonstration of the features of Security Hub. You can use this demonstration to learn about Security Hub's capabilities.

Steps

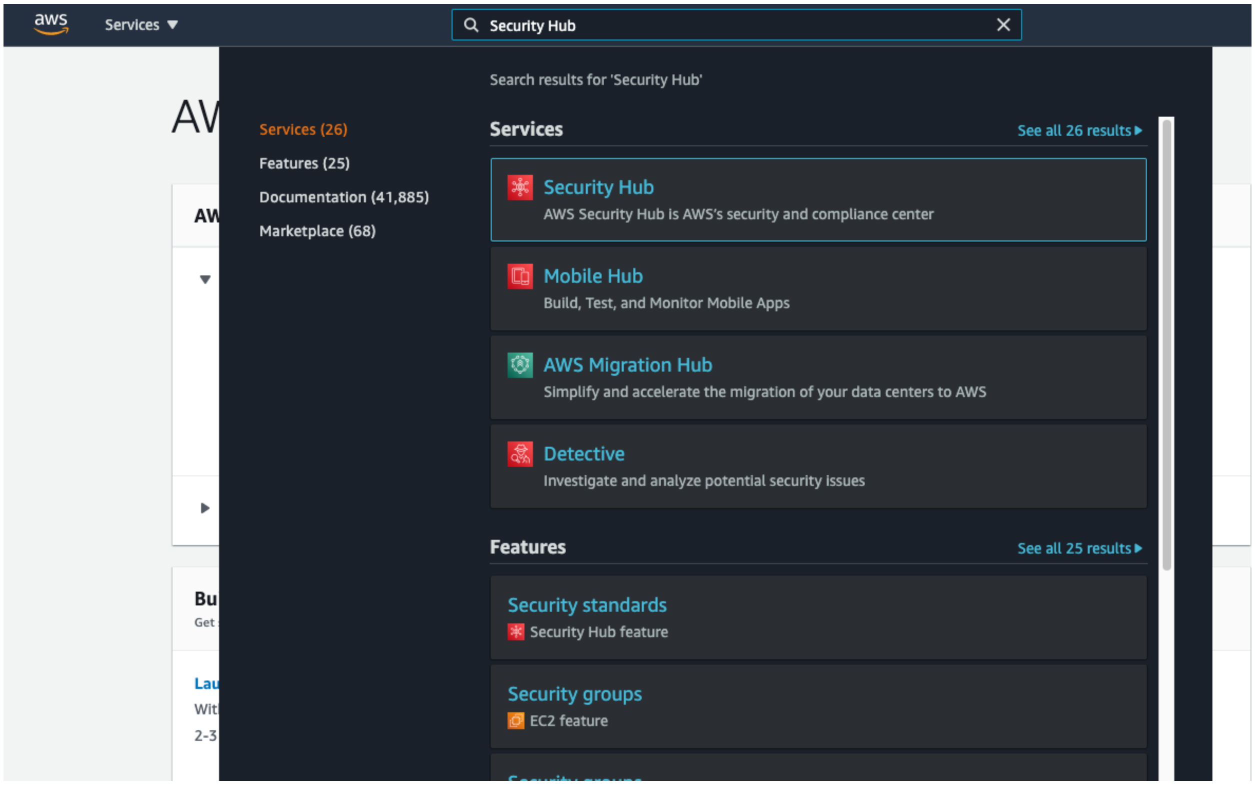
- Summary Page
- Integrations
- Insights
- Findings
- Explore Security Standards
- Understand Usage Summary

Security Hub Summary Page

The Security Hub Summary page gives you an overview of security and compliance status of your AWS account(s).

Some of the data in your account may differ from the screenshots and some may be blank.

1. From the **AWS Console** click **Services** in the top left corner
2. Type **Security Hub** in the services search bar.
3. Select **Security Hub** from the list.



Search results for 'Security Hub'

Services

Security Hub
AWS Security Hub is AWS's security and compliance center

Mobile Hub
Build, Test, and Monitor Mobile Apps

AWS Migration Hub
Simplify and accelerate the migration of your data centers to AWS

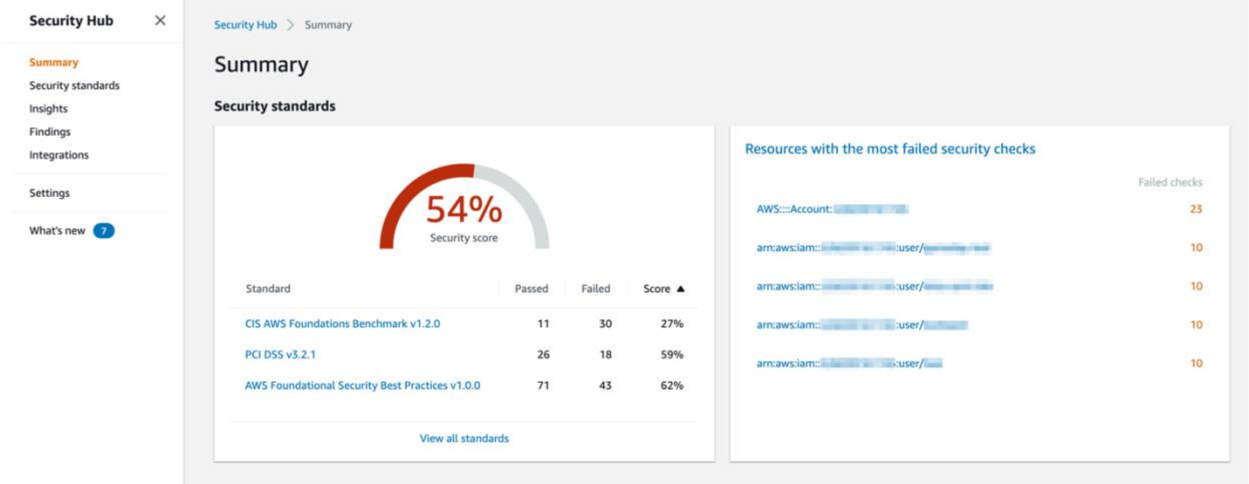
Detective
Investigate and analyze potential security issues

Features

Security standards
Security Hub feature

Security groups
EC2 feature

4. Click **Summary** on the left-hand navigation.



Summary

Security standards

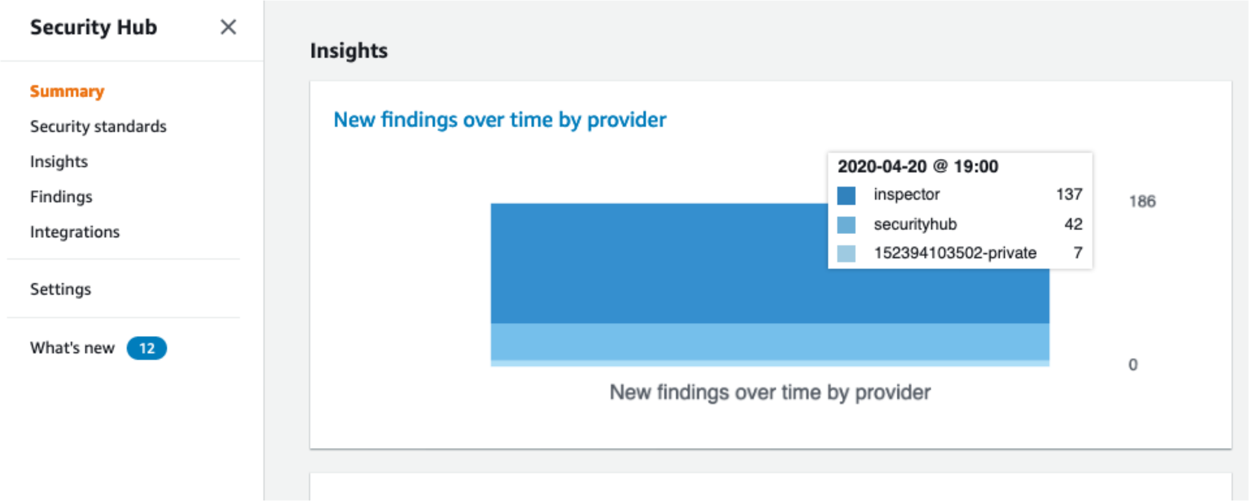
Standard	Passed	Failed	Score ▲
CIS AWS Foundations Benchmark v1.2.0	11	30	27%
PCI DSS v3.2.1	26	18	59%
AWS Foundational Security Best Practices v1.0.0	71	43	62%

Resources with the most failed security checks

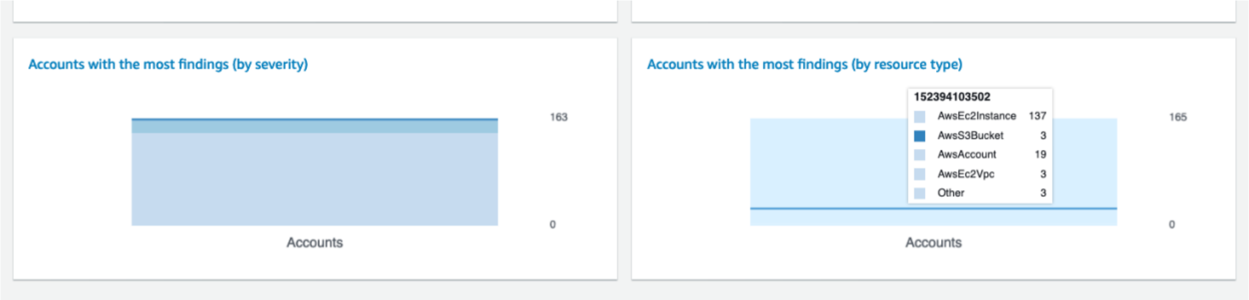
	Failed checks
AWS:::Account:[redacted]	23
arn:aws:iam::[redacted]:user/[redacted]	10
arn:aws:iam::[redacted]:user/[redacted]	10
arn:aws:iam::[redacted]:user/[redacted]	10
arn:aws:iam::[redacted]:user/[redacted]	10

5. Observe the Passed and Failed status of the **CIS AWS Foundations**. Even though the standard has recently been enabled, partial results for this security standard have already been collected.

6. Scroll down to the graphs under **Insights** (Your graphs may be different). Move your mouse over **New findings over time by provider** and observe the multiple sources of findings that Security Hub is already collecting. (There will be more throughout this workshop)



7. Scroll down further under **Insights**. Move your mouse over **Accounts with the most findings (by resource type)** and observe the sorted list of AWS resources that have findings to investigated.

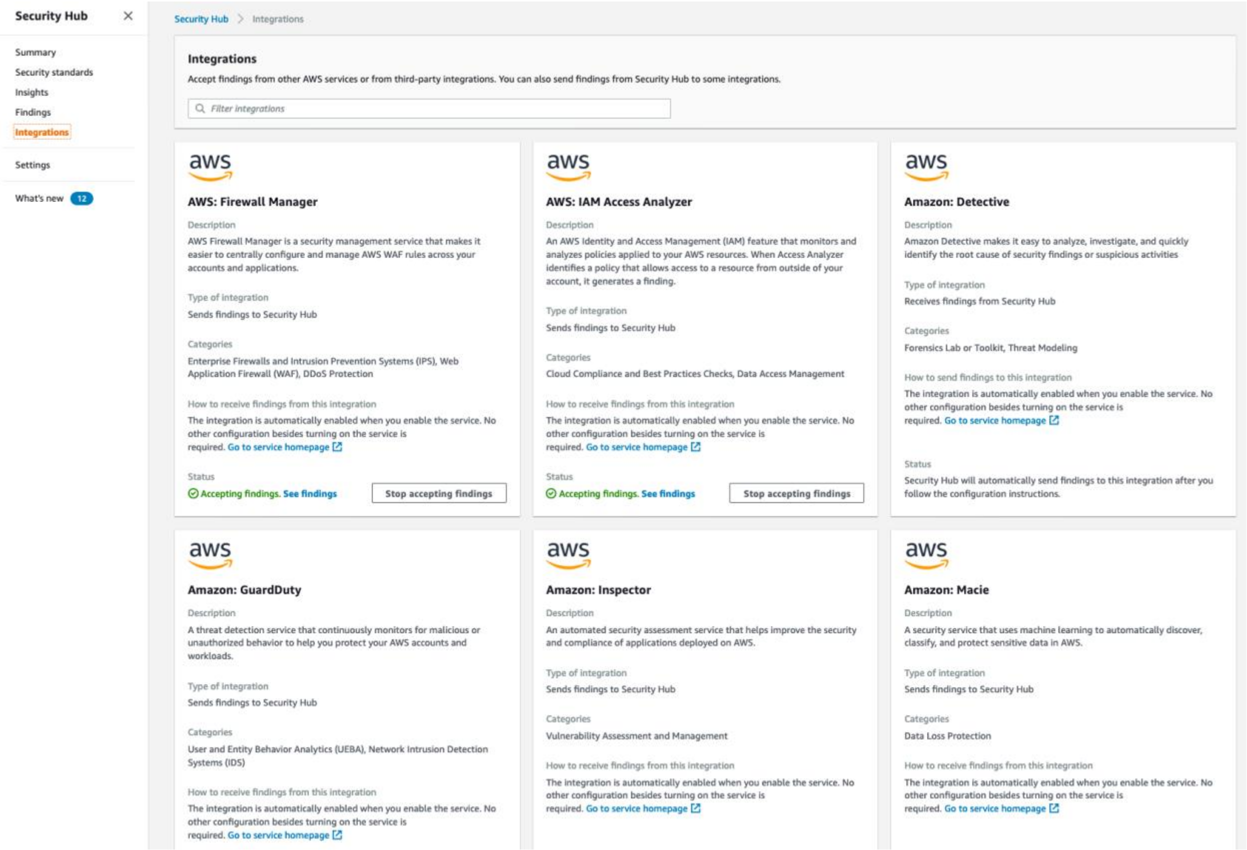


Integrations

In this section, we will walk through the Security Hub side of enabling a partner integration. Security Hub provides the ability to integrate security findings from AWS services and third-party products. For AWS services, Security Hub automatically enables the integration, and you can optionally disable each integration. For third-party products Security Hub gives you the ability to selectively enable the integrations and provides a link to the configuration instructions related to the third-party product.

Security Hub detects and consolidates only those security findings from the supported AWS and partner product integrations that are generated after Security Hub is enabled in your AWS accounts. It doesn't retroactively detect and consolidate security findings that were generated before you enabled Security Hub.

1. Click on **Integrations** from the left-hand navigation pane.



Integrations

Accept findings from other AWS services or from third-party integrations. You can also send findings from Security Hub to some integrations.

AWS: Firewall Manager

Description

AWS Firewall Manager is a security management service that makes it easier to centrally configure and manage AWS WAF rules across your accounts and applications.

Type of integration

Sends findings to Security Hub

Categories

Enterprise Firewalls and Intrusion Prevention Systems (IPS), Web Application Firewall (WAF), DDoS Protection

How to receive findings from this integration

The integration is automatically enabled when you enable the service. No other configuration besides turning on the service is required. Go to service homepage

Status

Accepting findings. See findings

AWS: IAM Access Analyzer

Description

An AWS Identity and Access Management (IAM) feature that monitors and analyzes policies applied to your AWS resources. When Access Analyzer identifies a policy that allows access to a resource from outside of your account, it generates a finding.

Type of integration

Sends findings to Security Hub

Categories

Cloud Compliance and Best Practices Checks, Data Access Management

How to receive findings from this integration

The integration is automatically enabled when you enable the service. No other configuration besides turning on the service is required. Go to service homepage

Status

Accepting findings. See findings

Amazon: Detective

Description

Amazon Detective makes it easy to analyze, investigate, and quickly identify the root cause of security findings or suspicious activities

Type of integration

Receives findings from Security Hub

Categories

Forensics Lab or Toolkit, Threat Modeling

How to send findings to this integration

The integration is automatically enabled when you enable the service. No other configuration besides turning on the service is required. Go to service homepage

Status

Security Hub will automatically send findings to this integration after you follow the configuration instructions.

Amazon: GuardDuty

Description

A threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads.

Type of integration

Sends findings to Security Hub

Categories

User and Entity Behavior Analytics (UEBA), Network Intrusion Detection Systems (IDS)

How to receive findings from this integration

The integration is automatically enabled when you enable the service. No other configuration besides turning on the service is required. Go to service homepage

Amazon: Inspector

Description

An automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

Type of integration

Sends findings to Security Hub

Categories

Vulnerability Assessment and Management

How to receive findings from this integration

The integration is automatically enabled when you enable the service. No other configuration besides turning on the service is required. Go to service homepage

Amazon: Macie

Description

A security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS.

Type of integration

Sends findings to Security Hub

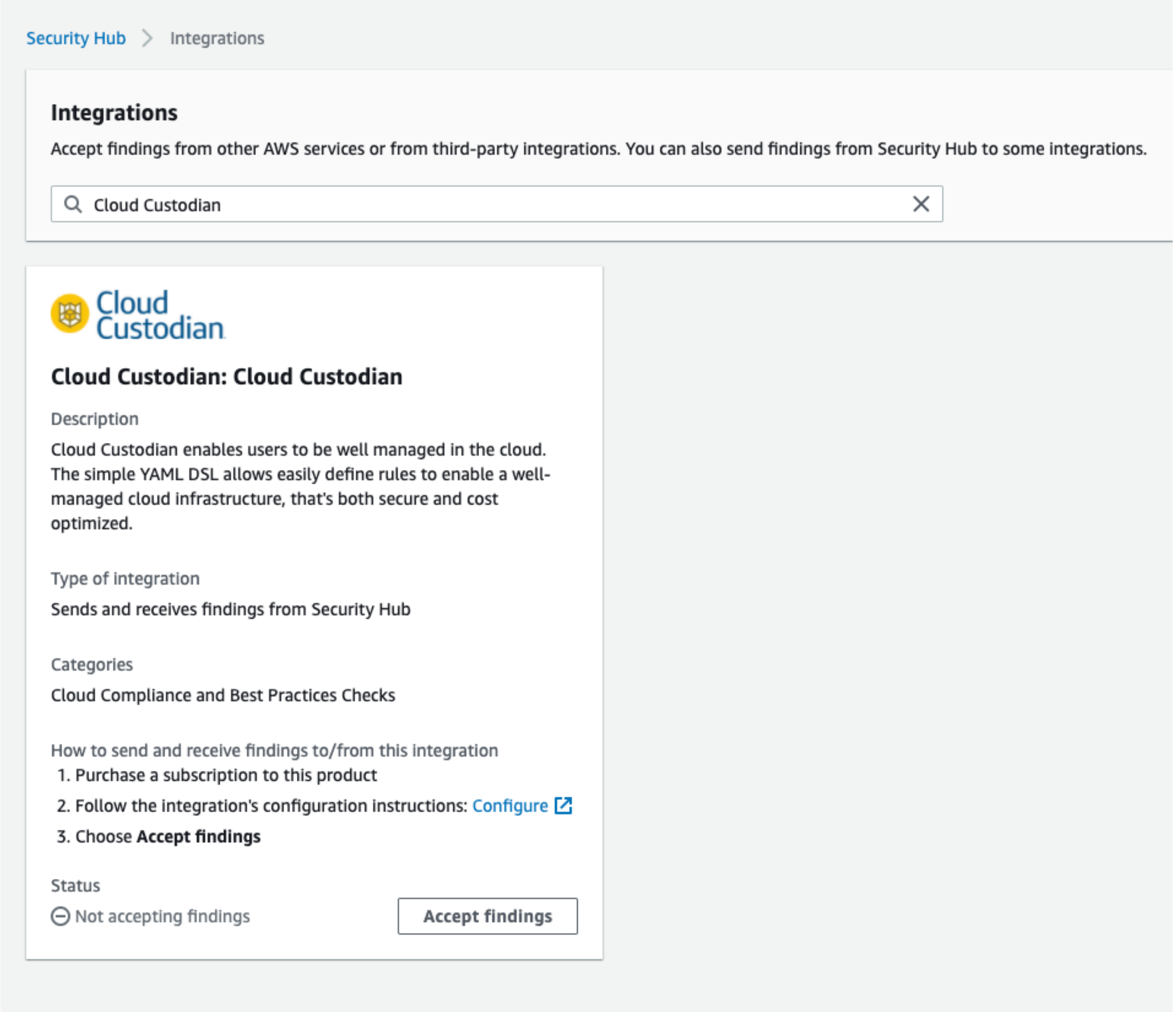
Categories

Data Loss Protection

How to receive findings from this integration

The integration is automatically enabled when you enable the service. No other configuration besides turning on the service is required. Go to service homepage

2. Scroll through the list of available integrations. Note that integrations for AWS services are automatically enabled. Return to the top and **search** for **Cloud Custodian**.



Security Hub > Integrations

Integrations

Accept findings from other AWS services or from third-party integrations. You can also send findings from Security Hub to some integrations.

Cloud Custodian

Cloud Custodian: Cloud Custodian

Description

Cloud Custodian enables users to be well managed in the cloud. The simple YAML DSL allows easily define rules to enable a well-managed cloud infrastructure, that's both secure and cost optimized.

Type of integration

Sends and receives findings from Security Hub

Categories

Cloud Compliance and Best Practices Checks

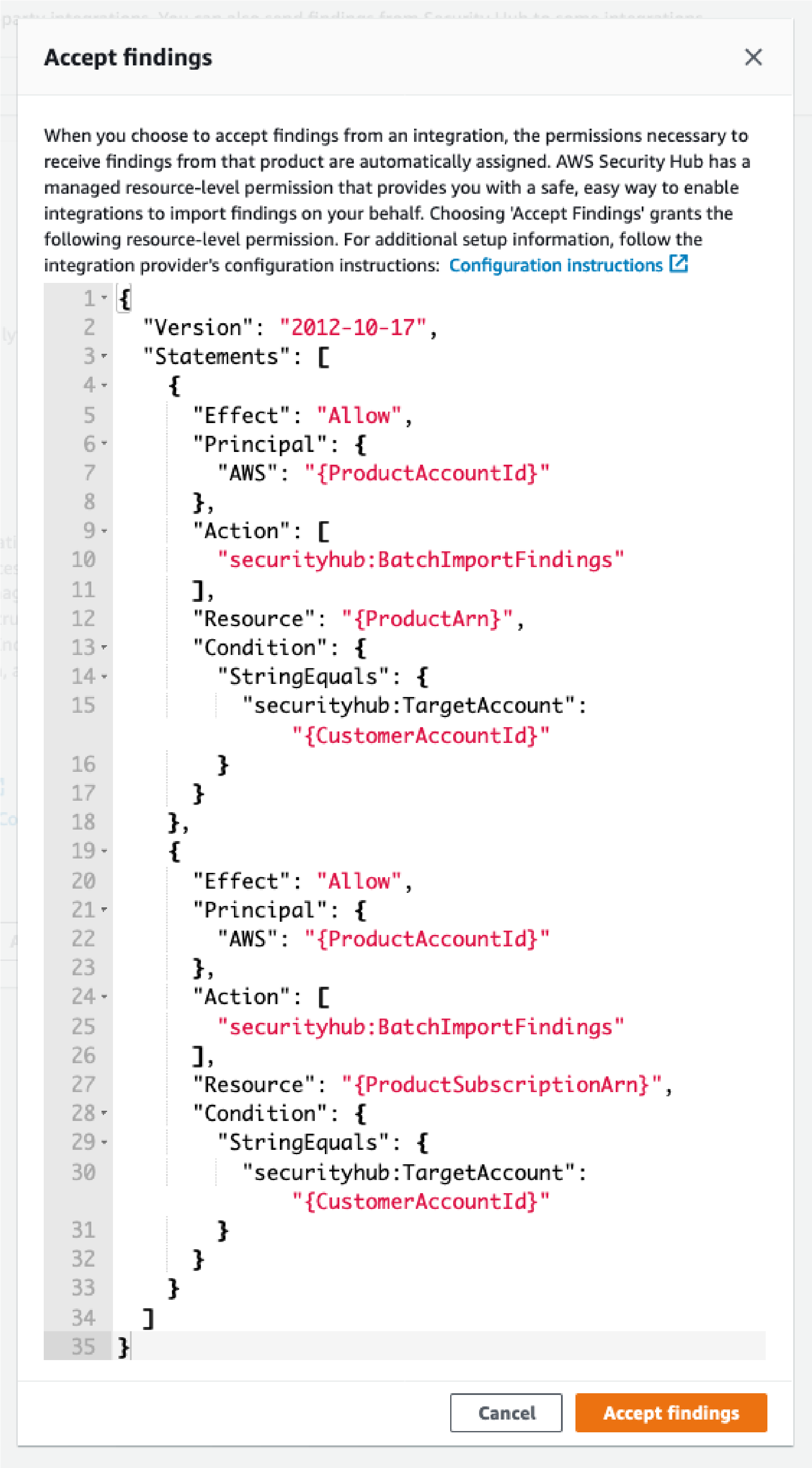
How to send and receive findings to/from this integration

1. Purchase a subscription to this product
2. Follow the integration's configuration instructions: Configure
3. Choose **Accept findings**

Status

Not accepting findings

3. Click **Accept Findings**. Review the permissions required for the integration.



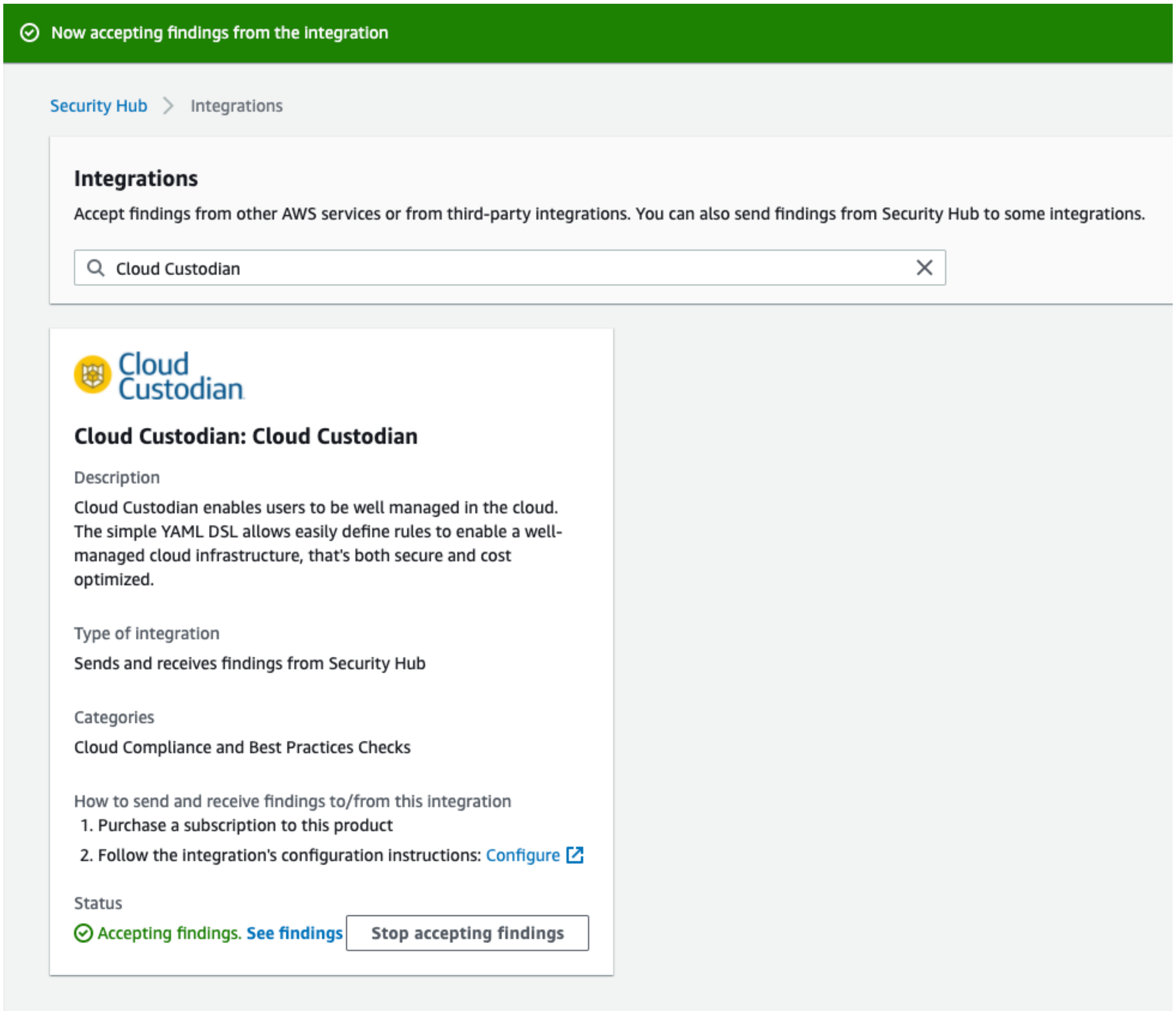
Accept findings

When you choose to accept findings from an integration, the permissions necessary to receive findings from that product are automatically assigned. AWS Security Hub has a managed resource-level permission that provides you with a safe, easy way to enable integrations to import findings on your behalf. Choosing 'Accept Findings' grants the following resource-level permission. For additional setup information, follow the integration provider's configuration instructions: Configuration instructions

```
{
  "Version": "2012-10-17",
  "Statements": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "{ProductAccountId}"
      },
      "Action": [
        "securityhub:BatchImportFindings"
      ],
      "Resource": "{ProductArn}",
      "Condition": {
        "StringEquals": {
          "securityhub:TargetAccount":
              "{CustomerAccountId}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "{ProductAccountId}"
      },
      "Action": [
        "securityhub:BatchImportFindings"
      ],
      "Resource": "{ProductSubscriptionArn}",
      "Condition": {
        "StringEquals": {
          "securityhub:TargetAccount":
              "{CustomerAccountId}"
        }
      }
    }
  ]
}
```

4. Click **Accept findings**.

This will put in place a service policy allowing the partner solution to send finding information into this account. For the purposes of this workshop a Cloud Custodian instance is already set up to automatically send findings to the integration you just enabled. To use other partner integrations in your account, you would still need to complete the Configure step in the partner solution so findings that are created by the partner solution are sent to Security Hub.



Now accepting findings from the integration

Security Hub > Integrations

Integrations

Accept findings from other AWS services or from third-party integrations. You can also send findings from Security Hub to some integrations.

Cloud Custodian

Cloud Custodian

Cloud Custodian: Cloud Custodian

Description

Cloud Custodian enables users to be well managed in the cloud. The simple YAML DSL allows easily define rules to enable a well-managed cloud infrastructure, that's both secure and cost optimized.

Type of integration

Sends and receives findings from Security Hub

Categories

Cloud Compliance and Best Practices Checks

How to send and receive findings to/from this integration

1. Purchase a subscription to this product
2. Follow the integration's configuration instructions: Configure

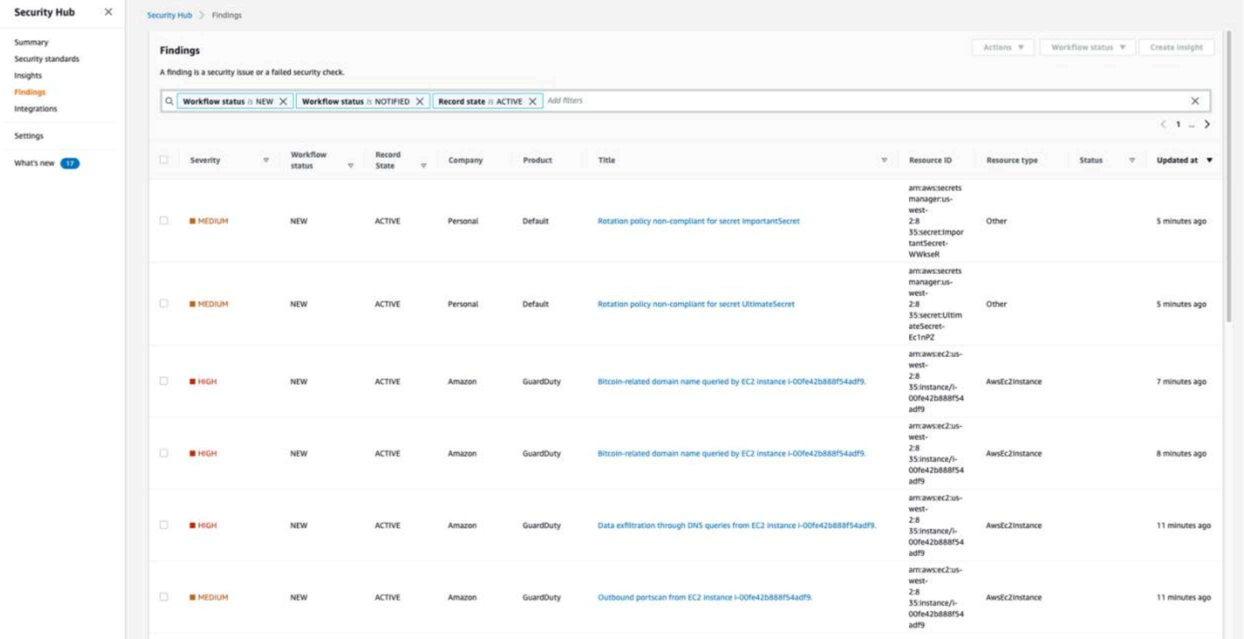
Status

Accepting findings. See findings

Findings

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. For more information about the findings format, see AWS Security Finding Format.

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



Findings

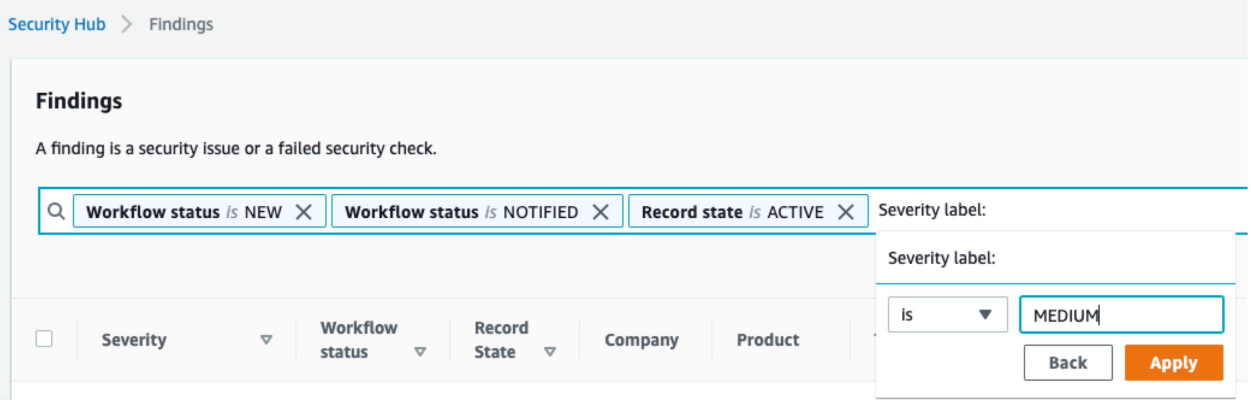
A finding is a security issue or a failed security check.

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-2:8 35:secret:ImportantSecret-WWkseR	Other		5 minutes ago
□	MEDIUM	NEW	ACTIVE	Personal	Default	Rotation policy non-compliant for secret UltimateSecret	arn:aws:secretsmanager:us-west-2:8 35: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-2:8 35: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-2:8 35: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-2:8 35:instance/i-00fe42b888f54adf9	AwsEc2Instance		11 minutes ago
□	MEDIUM	NEW	ACTIVE	Amazon	GuardDuty	Outbound portscan from EC2 instance i-00fe42b888f54adf9.	arn:aws:ec2:us-west-2:8 35:instance/i-00fe42b888f54adf9	AwsEc2Instance		11 minutes ago

2. In its default view the Findings tab can have a lot of information for you to consume. To narrow the overall list of findings down enter some search criteria.

   Click in the Search bar and select a filter field of **Severity label**, a filter match type of **is** and a search value **MEDIUM** (Search value must be all capitalized).



Findings

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

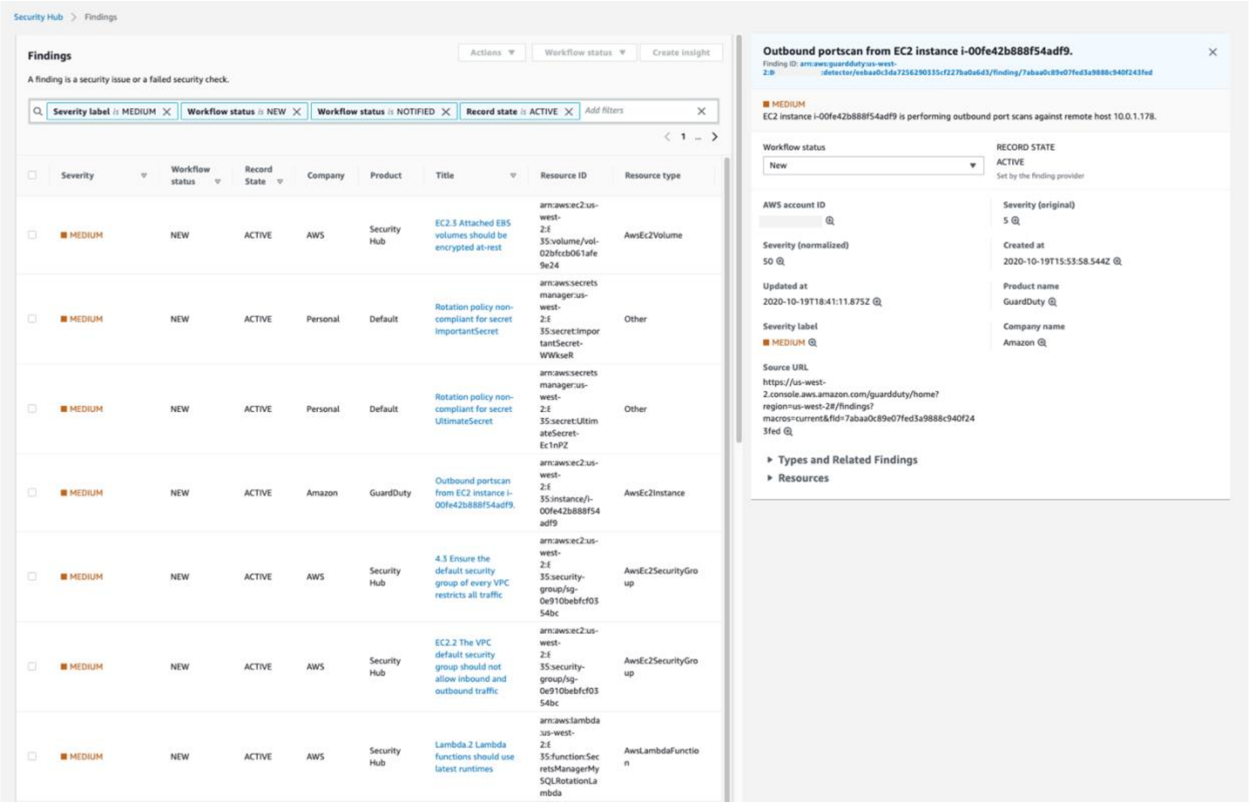
Workflow status *is* NEW ✕ | Workflow status *is* NOTIFIED ✕ | Record state *is* ACTIVE ✕ | Severity label:

Severity label:

is ▼ | MEDIUM

□	Severity	Workflow status	Record State	Company	Product

3. Click **Apply**.
4. Select a **Title** of any finding to see more information in the finding details pane.



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 ✕

< 1 ... >

□	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:£[redacted]35:volume/vol-02bfccb061afe9e24	AwsEc2Volume
□	■ MEDIUM	NEW	ACTIVE	Personal	Default	Rotation policy non-compliant for secret ImportantSecret	arn:aws:secretsmanager:us-west-2:£[redacted]35:secret:ImportantSecret-WWkseR	Other
□	■ MEDIUM	NEW	ACTIVE	Personal	Default	Rotation policy non-compliant for secret UltimateSecret	arn:aws:secretsmanager:us-west-2:£[redacted]35:secret:UltimateSecret-Ec1nPZ	Other
□	■ MEDIUM	NEW	ACTIVE	Amazon	GuardDuty	Outbound portscan from EC2 instance i-00fe42b888f54adf9.	arn:aws:ec2:us-west-2:£[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:£[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:£[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:£[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

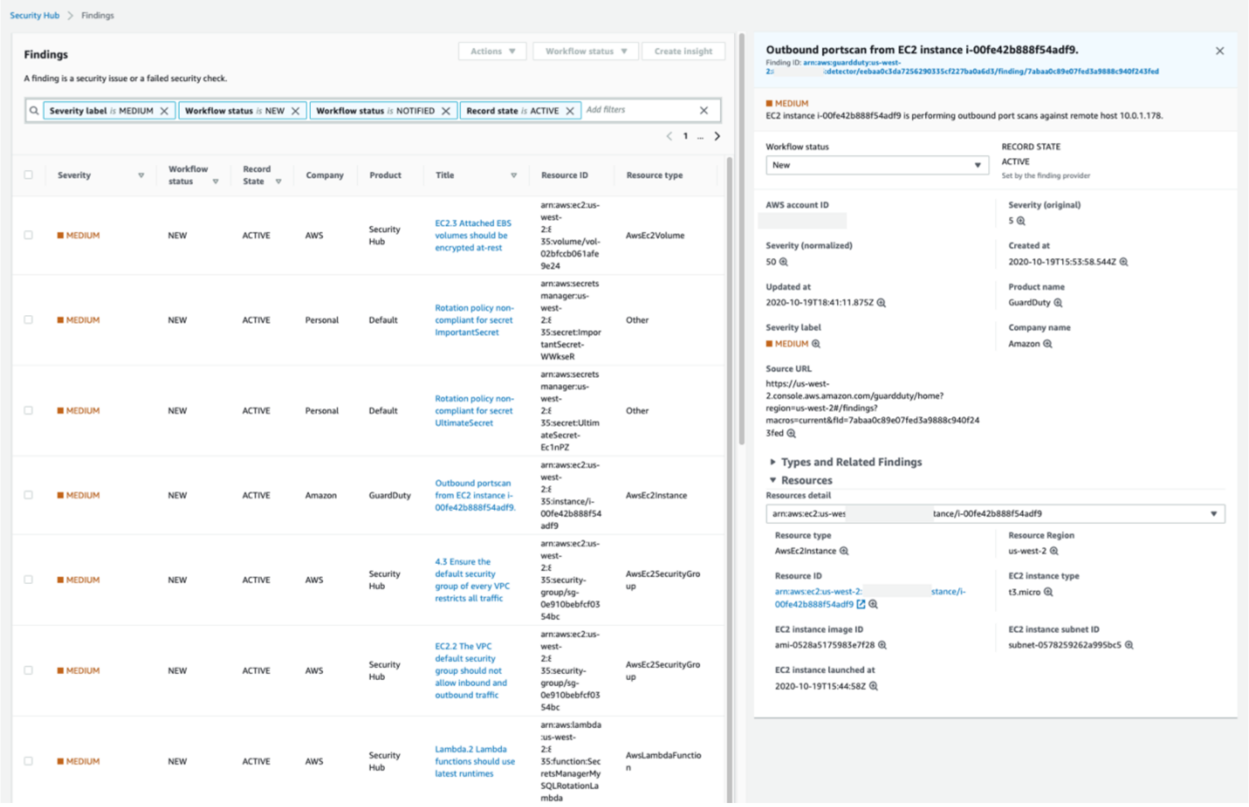
Severity label
■ MEDIUM

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

5. In the finding details pane click the arrow next to **Resources** on bottom right.



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 ✕

< 1 ... >

□	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:£[redacted]35:volume/vol-02bfccb061afe9e24	AwsEc2Volume
□	■ MEDIUM	NEW	ACTIVE	Personal	Default	Rotation policy non-compliant for secret ImportantSecret	arn:aws:secretsmanager:us-west-2:£[redacted]35:secret:ImportantSecret-WWkseR	Other
□	■ MEDIUM	NEW	ACTIVE	Personal	Default	Rotation policy non-compliant for secret UltimateSecret	arn:aws:secretsmanager:us-west-2:£[redacted]35:secret:UltimateSecret-Ec1nPZ	Other
□	■ MEDIUM	NEW	ACTIVE	Amazon	GuardDuty	Outbound portscan from EC2 instance i-00fe42b888f54adf9.	arn:aws:ec2:us-west-2:£[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:£[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:£[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:£[redacted]35:function:SecretsManagerMySQLRotationLambda	AwsLambdaFunction

Outbound portscan from EC2 instance i-00fe42b888f54adf9. ✕

Finding ID: arn:aws:guardduty:us-west-2:[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

Resources detail
arn:aws:ec2:us-wes[redacted]tance/i-00fe42b888f54adf9 ▼

Resource type
AwsEc2Instance

Resource Region
us-west-2

Resource ID
arn:aws:ec2:us-west-2:[redacted]stance/i-00fe42b888f54adf9

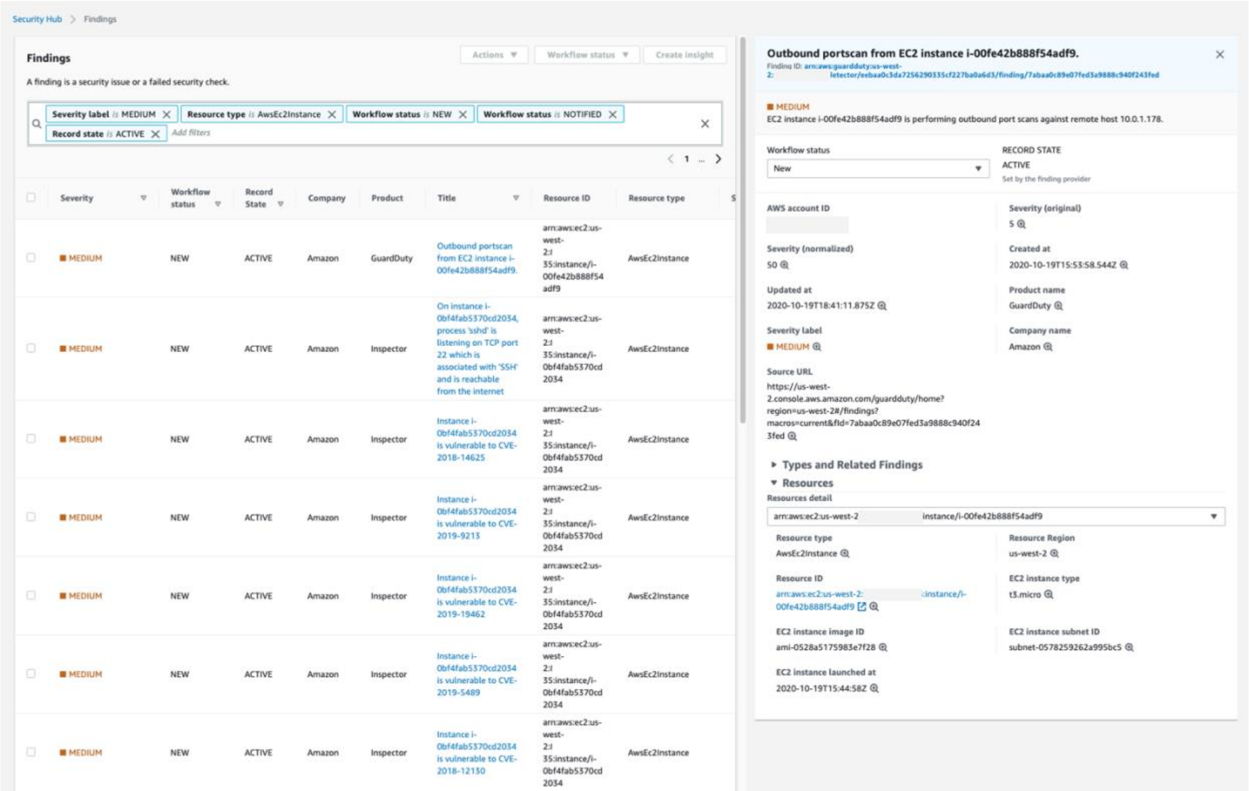
EC2 instance type
t3.micro

EC2 instance image ID
ami-0528a5175983e7f28

EC2 instance subnet ID
subnet-0578259262a995bc5

EC2 instance launched at
2020-10-19T15:44:58Z

6. Click the [+] to the right of this findings **Resource Type** (e.g. AWSEc2Instance). This will add the resource as a filter to the search.



Security Hub > Findings

Findings

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

Severity label *is* MEDIUM ✕ | Resource type *is* AwsEc2Instance ✕ | Workflow status *is* NEW ✕ | Workflow status *is* NOTIFIED ✕ | Record state *is* ACTIVE ✕ | *Add filters*

< 1 ... >

□	Severity	Workflow status	Record State	Company	Product	Title	Resource ID	Resource type
□	■ MEDIUM	NEW	ACTIVE	Amazon	GuardDuty	Outbound portscan from EC2 instance i-00fe42b888f54adf9.	arn:aws:ec2:us-west-2:I 35:instance/i-00fe42b888f54adf9	AwsEc2Instance
□	■ MEDIUM	NEW	ACTIVE	Amazon	Inspector	On instance i-0bf4fab5370cd2034, process 'sshd' is listening on TCP port 22 which is associated with 'SSH' and is reachable from the internet	arn:aws:ec2:us-west-2:I 35:instance/i-0bf4fab5370cd2034	AwsEc2Instance
□	■ MEDIUM	NEW	ACTIVE	Amazon	Inspector	Instance i-0bf4fab5370cd2034 is vulnerable to CVE-2018-14625	arn:aws:ec2:us-west-2:I 35:instance/i-0bf4fab5370cd2034	AwsEc2Instance
□	■ MEDIUM	NEW	ACTIVE	Amazon	Inspector	Instance i-0bf4fab5370cd2034 is vulnerable to CVE-2019-9213	arn:aws:ec2:us-west-2:I 35:instance/i-0bf4fab5370cd2034	AwsEc2Instance
□	■ MEDIUM	NEW	ACTIVE	Amazon	Inspector	Instance i-0bf4fab5370cd2034 is vulnerable to CVE-2019-19462	arn:aws:ec2:us-west-2:I 35:instance/i-0bf4fab5370cd2034	AwsEc2Instance
□	■ MEDIUM	NEW	ACTIVE	Amazon	Inspector	Instance i-0bf4fab5370cd2034 is vulnerable to CVE-2019-5489	arn:aws:ec2:us-west-2:I 35:instance/i-0bf4fab5370cd2034	AwsEc2Instance
□	■ MEDIUM	NEW	ACTIVE	Amazon	Inspector	Instance i-0bf4fab5370cd2034 is vulnerable to CVE-2018-12130	arn:aws:ec2:us-west-2:I 35:instance/i-0bf4fab5370cd2034	AwsEc2Instance

Outbound portscan from EC2 instance i-00fe42b888f54adf9. ✕

Finding ID: arn:aws:guardduty:us-west-2:[redacted]letector/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

Resources detail: arn:aws:ec2:us-west-2[redacted]instance/i-00fe42b888f54adf9 ▼

Resource type: AwsEc2Instance

Resource Region: us-west-2

Resource ID: arn:aws:ec2:us-west-2:[redacted]:instance/i-00fe42b888f54adf9

EC2 instance type: t3.micro

EC2 instance image ID: ami-0528a5175983e7f28

EC2 instance subnet ID: subnet-0578259262a995bc5

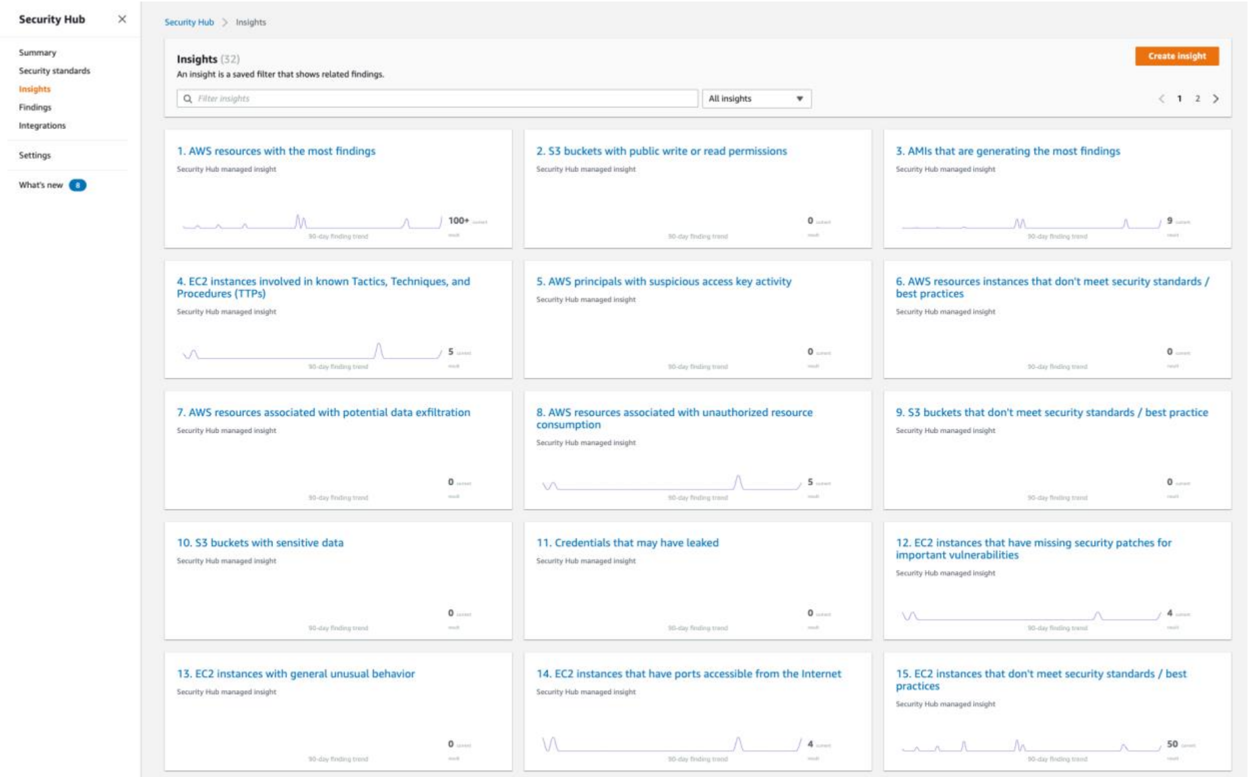
EC2 instance launched at: 2020-10-19T15:44:58Z

7. In the finding details pane to the right, choose the finding ID hyperlink at the top of the pane to display the complete JSON for the finding. The finding JSON can be downloaded to a file if ever needed for further investigation.

Insights

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.

1. Click on **Insights** from the left-hand navigation pane.



Security Hub

Summary
Security standards
Insights
Findings
Integrations

Settings

What's new 8

Security Hub > Insights

Insights (32)
An insight is a saved filter that shows related findings.

Filter insights | All insights ▼ | < 1 2 >

Create insight

1. AWS resources with the most findings
Security Hub managed insight
100+ current result

2. S3 buckets with public write or read permissions
Security Hub managed insight
0 current result

3. AMIs that are generating the most findings
Security Hub managed insight
9 current result

4. EC2 instances involved in known Tactics, Techniques, and Procedures (TTPs)
Security Hub managed insight
5 current result

5. AWS principals with suspicious access key activity
Security Hub managed insight
0 current result

6. AWS resources instances that don't meet security standards / best practices
Security Hub managed insight
0 current result

7. AWS resources associated with potential data exfiltration
Security Hub managed insight
0 current result

8. AWS resources associated with unauthorized resource consumption
Security Hub managed insight
5 current result

9. S3 buckets that don't meet security standards / best practice
Security Hub managed insight
0 current result

10. S3 buckets with sensitive data
Security Hub managed insight
0 current result

11. Credentials that may have leaked
Security Hub managed insight
0 current result

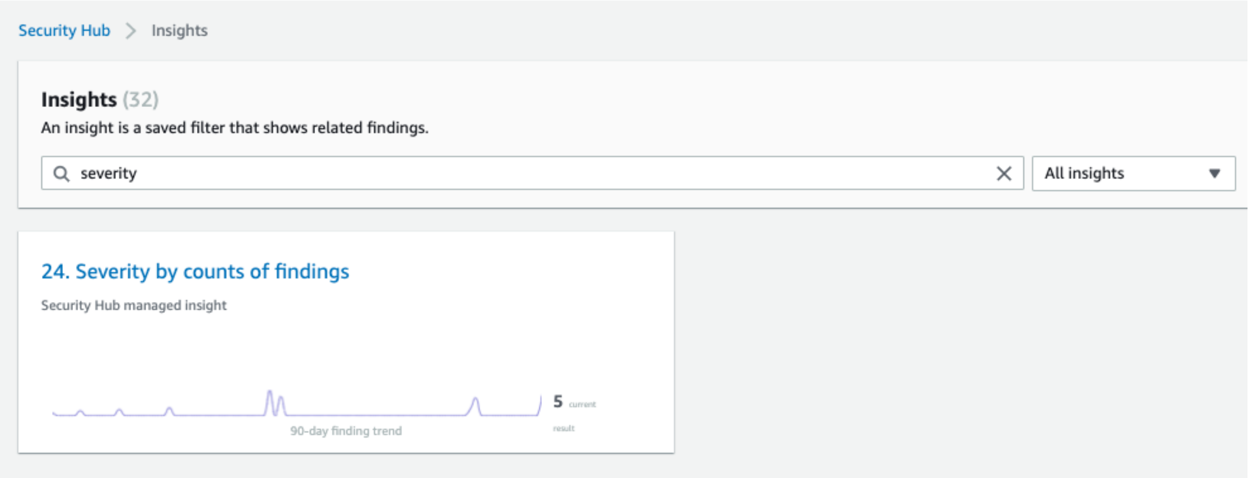
12. EC2 instances that have missing security patches for important vulnerabilities
Security Hub managed insight
4 current result

13. EC2 instances with general unusual behavior
Security Hub managed insight
0 current result

14. EC2 instances that have ports accessible from the Internet
Security Hub managed insight
4 current result

15. EC2 instances that don't meet security standards / best practices
Security Hub managed insight
50 current result

2. Filter for insight **severity**.



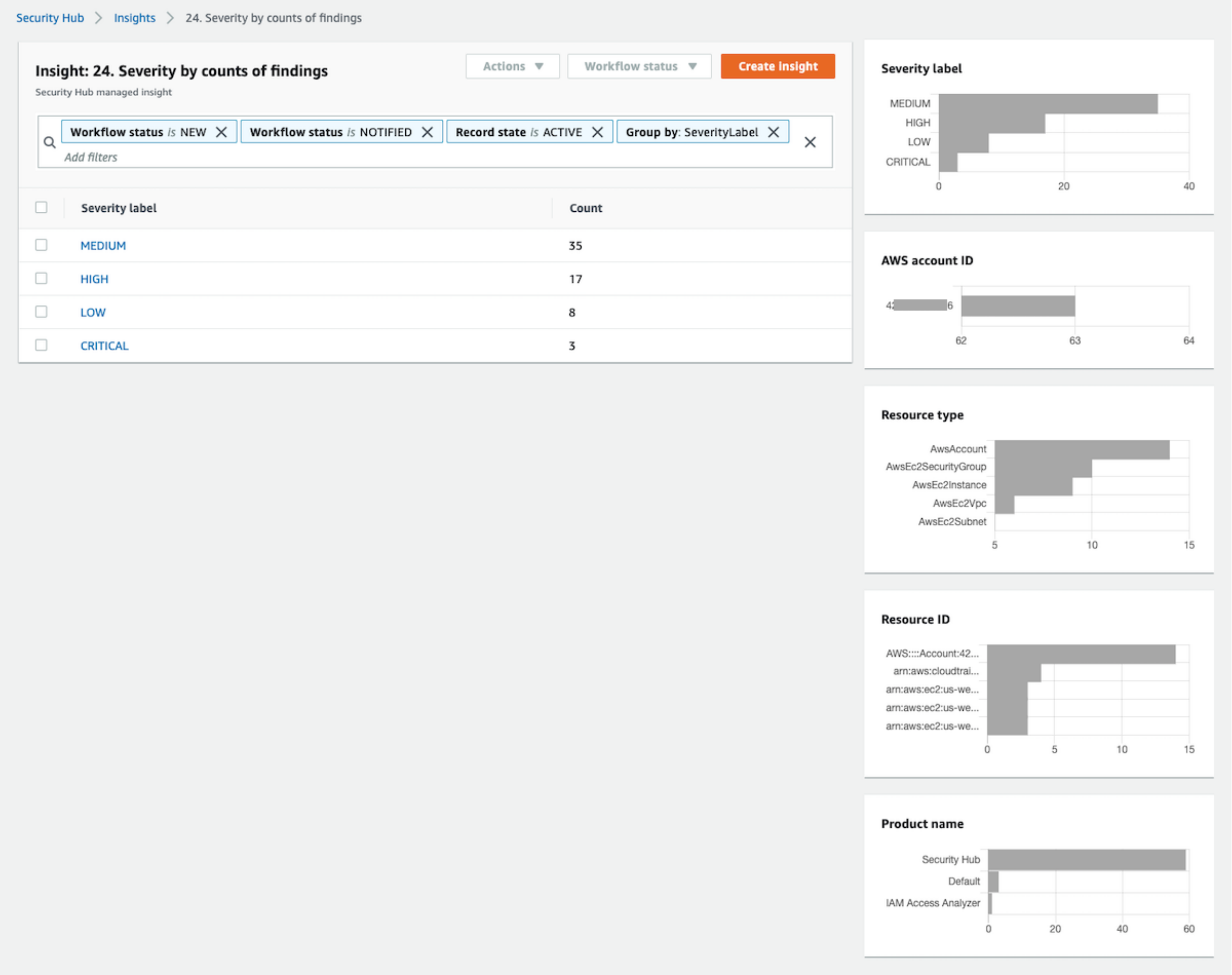
Security Hub > Insights

Insights (32)
An insight is a saved filter that shows related findings.

severity | All insights ▼

24. Severity by counts of findings
Security Hub managed insight
5 current result

3. Click on **24. Severity by counts of findings**.



Insight: 24. Severity by counts of findings

Security Hub managed insight

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

□	Severity label	Count
□	MEDIUM	35
□	HIGH	17
□	LOW	8
□	CRITICAL	3

4. Select a **Severity Label** (e.g. Critical) to see the underlying finding(s).

Security Standards

Security Hub currently supports multiple security standards:

- Center for Internet Security (CIS) AWS Foundations v1.2.0:

AWS Security Hub has satisfied the requirements of CIS Security Software Certification and is hereby awarded CIS Security Software Certification for the following CIS Benchmarks: CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.2.0, Level 1 and Level 2

- AWS Foundational Security Best Practices v1.0.0:

The AWS Foundational Security Best Practices standard is a set of controls that detect when your deployed accounts and resources deviate from security best practices. The controls include best practices from across multiple AWS services. Each control belongs to one of the following categories, which are based on the functions described in the NIST Cybersecurity Framework.

- Payment Card Industry Data Security Standard (PCI DSS) v3.2.1:

The Payment Card Industry Data Security Standard (PCI DSS) standard in Security Hub consists of a set of AWS security best practices controls. Each control applies to a specific AWS resource, and relates to one or more PCI DSS version 3.2.1 requirements. A PCI DSS requirement can be related to multiple controls. The details page for each PCI DSS control lists the specific PCI DSS requirements that are related to that control.

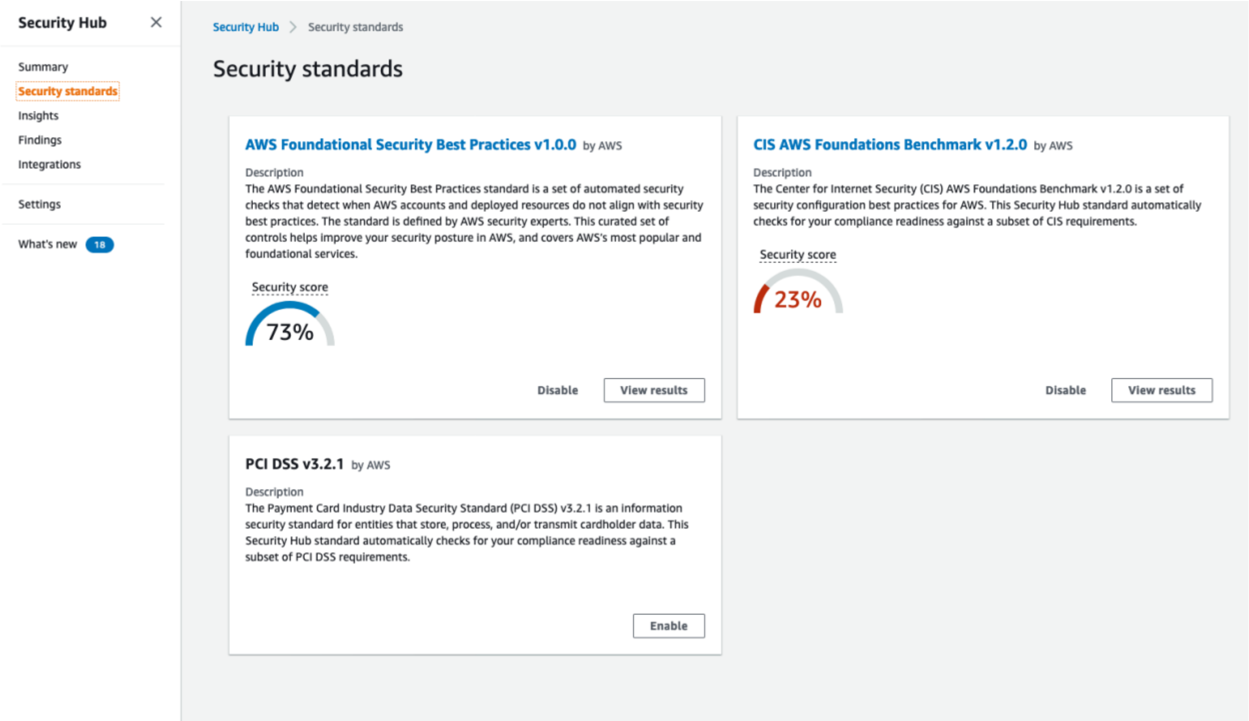
The PCI DSS Compliance Standard in Security Hub is designed to help you with your ongoing PCI DSS security activities. The controls cannot verify whether your systems are compliant with the PCI DSS standard. They can neither replace internal efforts nor guarantee that you will pass a PCI DSS assessment.

More information about each of these security standards can be found at: Available security standards in AWS Security Hub

To run the CIS AWS Foundations standard's compliance checks on your environment's resources, Security Hub either runs through the exact audit steps prescribed for the checks in Securing Amazon Web Services or uses specific AWS Config managed rules. To use the AWS Config managed rules AWS Config must be enabled in the account where you are using Security Hub. For this workshop Config has already been enabled for you.

The first round of compliance checks will be done within 2 hours of enabling Security Hub and then runs every 12 hours.

1. Click on **Security standards**.



Security standards

AWS Foundational Security Best Practices v1.0.0 by AWS

Description

The AWS Foundational Security Best Practices standard is a set of automated security checks that detect when AWS accounts and deployed resources do not align with security best practices. The standard is defined by AWS security experts. This curated set of controls helps improve your security posture in AWS, and covers AWS's most popular and foundational services.

Security score

73%

CIS AWS Foundations Benchmark v1.2.0 by AWS

Description

The Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 is a set of security configuration best practices for AWS. This Security Hub standard automatically checks for your compliance readiness against a subset of CIS requirements.

Security score

23%

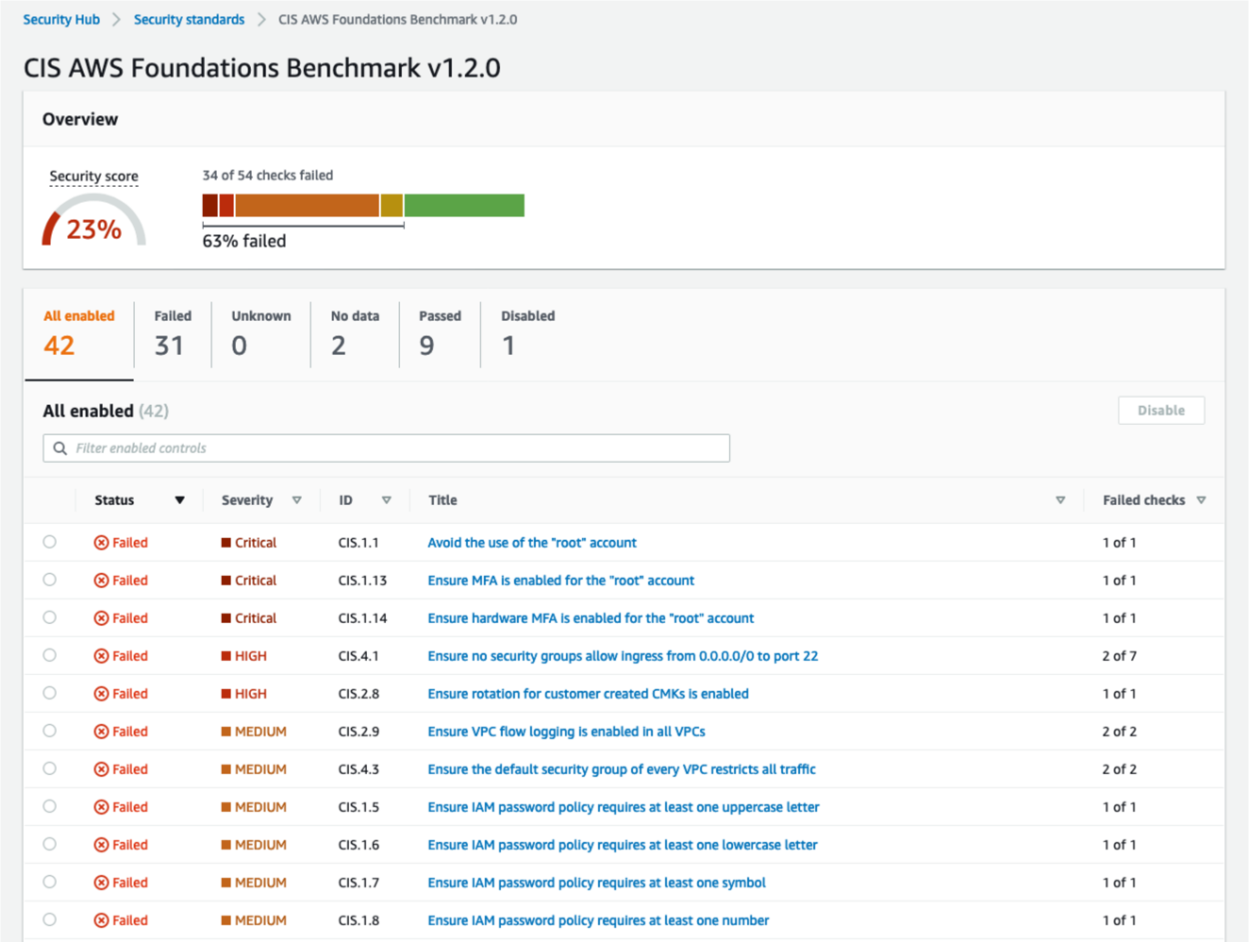
PCI DSS v3.2.1 by AWS

Description

The Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 is an information security standard for entities that store, process, and/or transmit cardholder data. This Security Hub standard automatically checks for your compliance readiness against a subset of PCI DSS requirements.

Note the Security score should be above 0% If your score shows 0% or -, disable and then re-enable the security standards.

2. 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

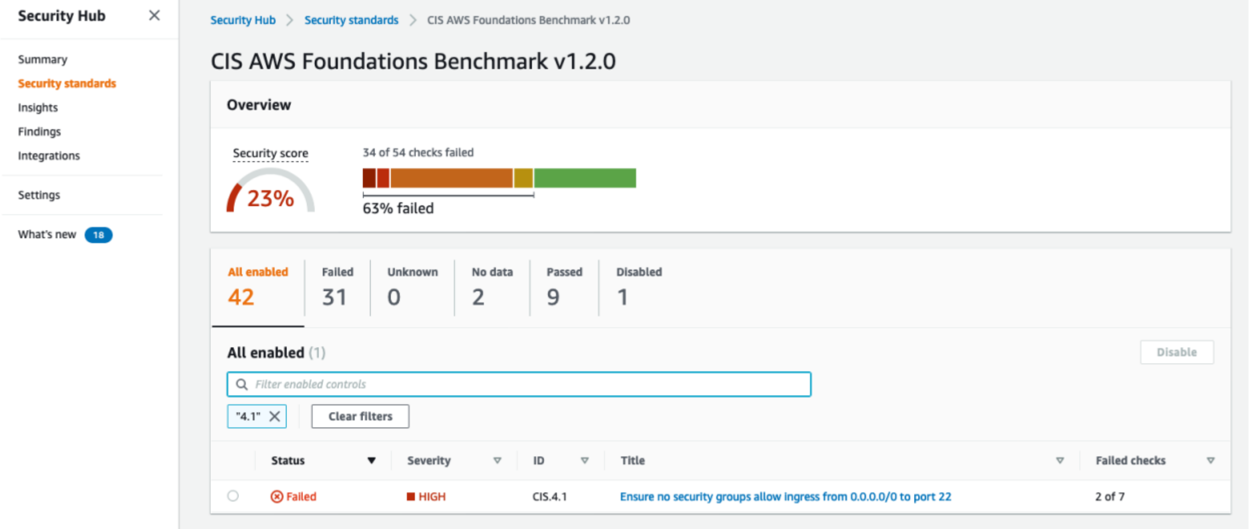
All enabled (42)

Disable

Filter enabled controls

	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

3. Filter on **4.1**.



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 (1)

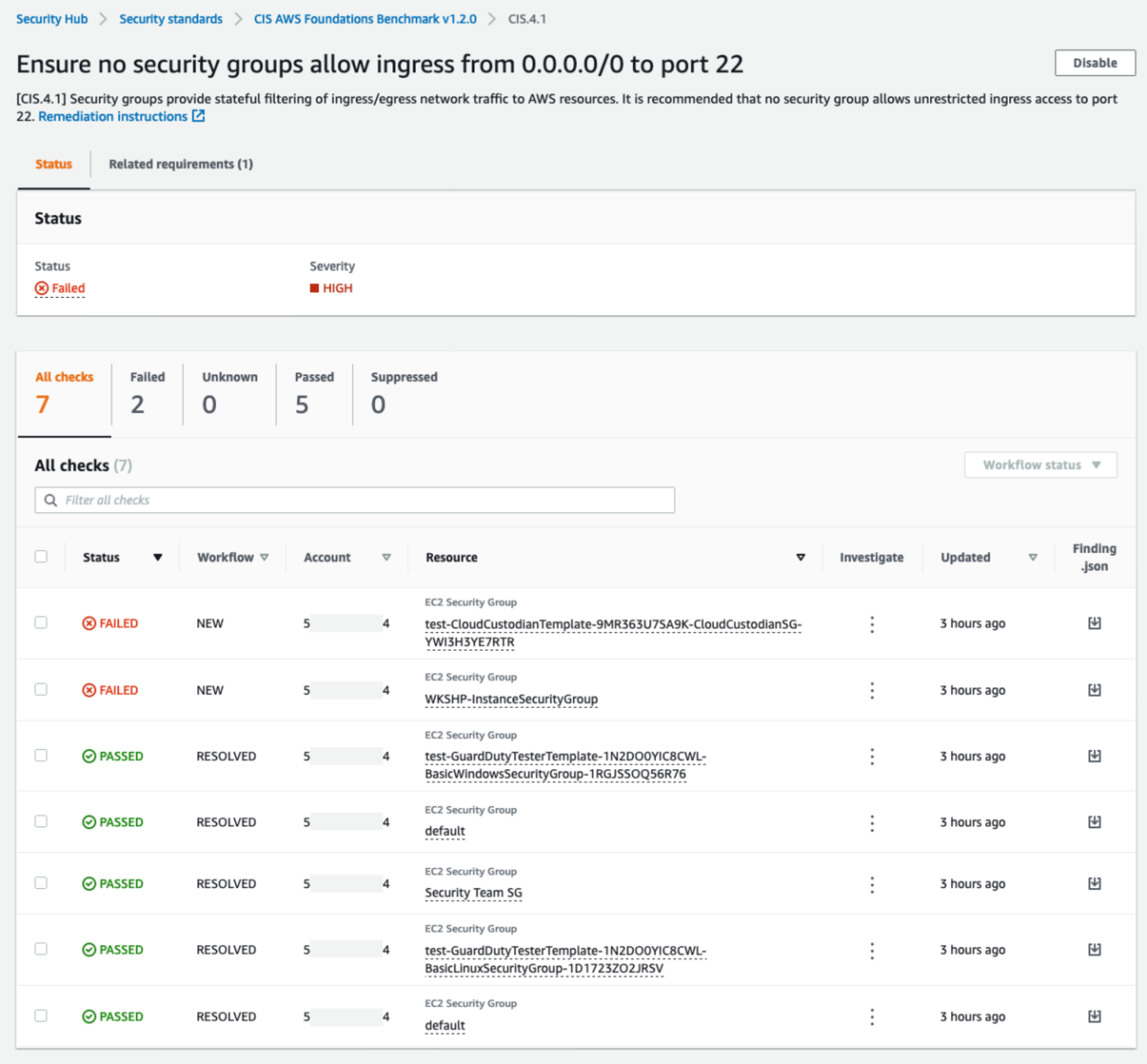
Disable

Filter enabled controls

"4.1" ✕ Clear filters

	Status	Severity	ID	Title	Failed checks
○	⊗ Failed	■ HIGH	CIS.4.1	Ensure no security groups allow ingress from 0.0.0.0/0 to port 22	2 of 7

4. Click on the Title: **Ensure no security groups allow ingress from 0.0.0.0/0**. This presents a view of all resources evaluated for this particular control and the current status of each resource as it relates to the control.



Security Hub > Security standards > CIS AWS Foundations Benchmark v1.2.0 > CIS.4.1

Ensure no security groups allow ingress from 0.0.0.0/0 to port 22

[CIS.4.1] Security groups provide stateful filtering of ingress/egress network traffic to AWS resources. It is recommended that no security group allows unrestricted ingress access to port 22. Remediation instructions

Status

Status: Failed

Severity: HIGH

All checks	Failed	Unknown	Passed	Suppressed
7	2	0	5	0

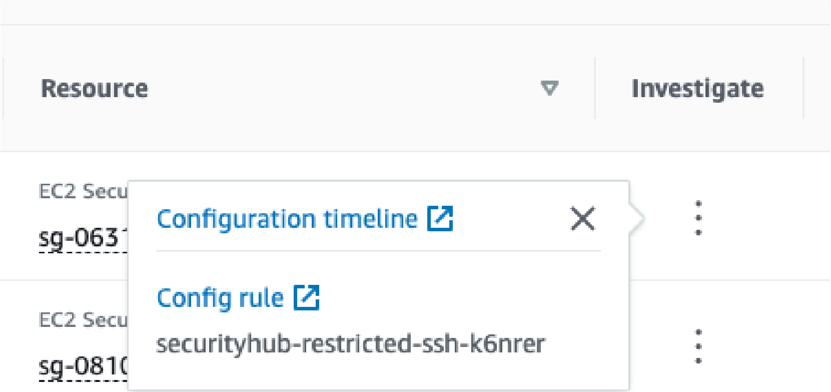
All checks (7)

□	Status	Workflow	Account	Resource	Investigate	Updated	Finding .json
□	FAILED	NEW	5[redacted]4	EC2 Security Group test-CloudCustodianTemplate-9MR363U7SA9K-CloudCustodianSG-YWI3H3YE7RTR	⋮	3 hours ago	
□	FAILED	NEW	5[redacted]4	EC2 Security Group WKSHP-InstanceSecurityGroup	⋮	3 hours ago	
□	PASSED	RESOLVED	5[redacted]4	EC2 Security Group test-GuardDutyTesterTemplate-1N2DO0YIC8CWL-BasicWindowsSecurityGroup-1RGJSSOQ56R76	⋮	3 hours ago	
□	PASSED	RESOLVED	5[redacted]4	EC2 Security Group default	⋮	3 hours ago	
□	PASSED	RESOLVED	5[redacted]4	EC2 Security Group Security Team SG	⋮	3 hours ago	
□	PASSED	RESOLVED	5[redacted]4	EC2 Security Group test-GuardDutyTesterTemplate-1N2DO0YIC8CWL-BasicLinuxSecurityGroup-1D1723ZO2JRSV	⋮	3 hours ago	
□	PASSED	RESOLVED	5[redacted]4	EC2 Security Group default	⋮	3 hours ago	

5. At the top of the page click the **Remediation instructions link**, to open guidance in a new tab.

AWS Security Hub Security Standards provide remediation instructions for each check.

6. Scroll down and you will notice there are some resources with a **FAILED** and status some with a **PASSED** status. For one of the **FAILED** resources click on the three dots in the **Investigate** column. This will display links that will take you to AWS Config to view the configuration timeline for this resource or the overall config rule that performed the evaluation on this resource. Feel free to click the links to explore more about the resource and the config rule.



Resource	Investigate
EC2 Secu sg-063	
EC2 Secu sg-081(	

Configuration timeline

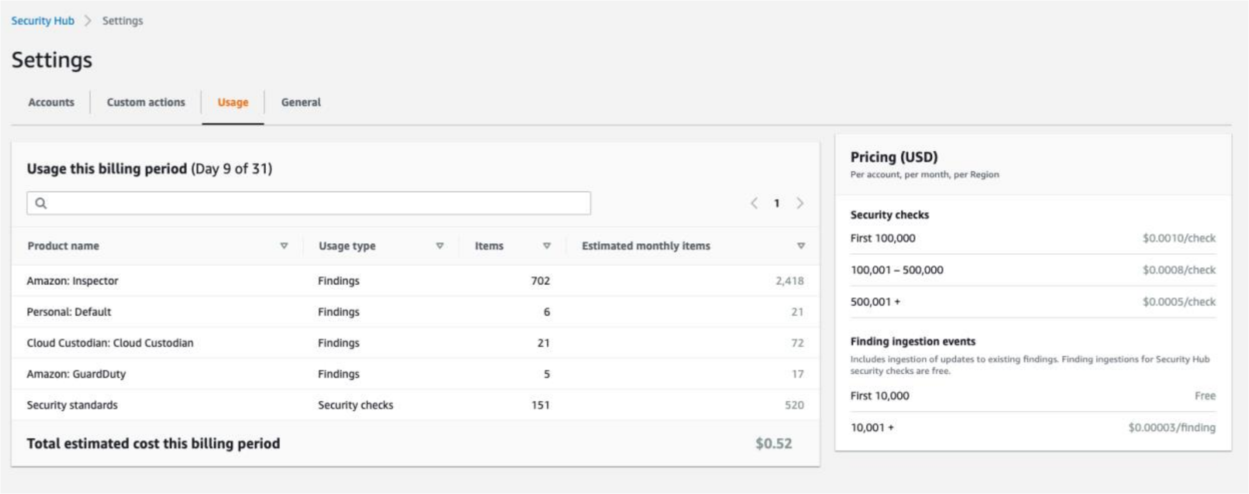
Config rule

securityhub-restricted-ssh-k6nrer

Usage Summary

Security Hub provides usage info for your AWS account, helping you to understand what your monthly billing estimate will be and which components of Security Hub are contributing to your bill. Security Hub offers a 30-day free trial for each account. During the free trial Security Hub provides an estimate of what the spend would be so you can assess your spend beyond the free trial.

1. Click **Settings** on the left-hand navigation.
2. Click the **Usage** tab in the **Settings** screen.
3. On the left-hand side of the screen your usage for the billing period is displayed. Usage is broken down by findings ingested and by security checks that have been run. At the bottom of the usage summary is the total estimated cost for the billing period. On the right-hand side is the current Security Hub pricing so that you can see how the usage in your account contributed to the estimated cost.
4.



Usage this billing period (Day 9 of 31)

Product name	Usage type	Items	Estimated monthly items
Amazon: Inspector	Findings	702	2,418
Personal: Default	Findings	6	21
Cloud Custodian: Cloud Custodian	Findings	21	72
Amazon: GuardDuty	Findings	5	17
Security standards	Security checks	151	520
Total estimated cost this billing period			$0.52

Pricing (USD)

Per account, per month, per Region

Security checks

First 100,000	$0.0010/check
100,001 – 500,000	$0.0008/check
500,001 +	$0.0005/check

Finding ingestion events

Includes ingestion of updates to existing findings. Finding ingestions for Security Hub security checks are free.

First 10,000	Free
10,001 +	$0.00003/finding

Now that you have explored Security Hub's capabilities, you can proceed to the next module.