



JJ Tech

AWS Security Hub

Manage and improve your security posture

AWS Security Hub provides a consolidated view of your security status in AWS. Automate security checks, manage security findings, and identify the highest priority security issues across your AWS environment.

- Run automated security checks across your AWS environment
- Prioritize and remediate security issues
- Consolidate security findings from AWS and partner products in a standard format across all of your accounts
- Provides you with a comprehensive view of your security state in AWS and helps you check your environment against security industry standards and best practices
- Collects security data from across AWS accounts, services and supported third party partner products and helps you analyse security trends and identify the highest priority security issues

Benefits and features

Consolidated view of security issues

AWS Security Hub collects and consolidates findings from AWS security services enabled in your environment, such as intrusion detection findings from Amazon GuardDuty, vulnerability scans from Amazon Inspector, and S3 bucket policy findings from Amazon Macie. AWS Security Hub also consolidates findings from integrated AWS Partner Network (APN) security solutions. All findings are stored for at least 90 days within AWS Security Hub.

Automated, continuous security checks

Automate continuous, account and resource-level configuration and security checks using industry standards and best practices. For example, AWS Security Hub automates the Center for Internet Security (CIS) AWS Foundations Benchmark, a set of security configuration best practices for AWS. If any of your accounts or resources

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720



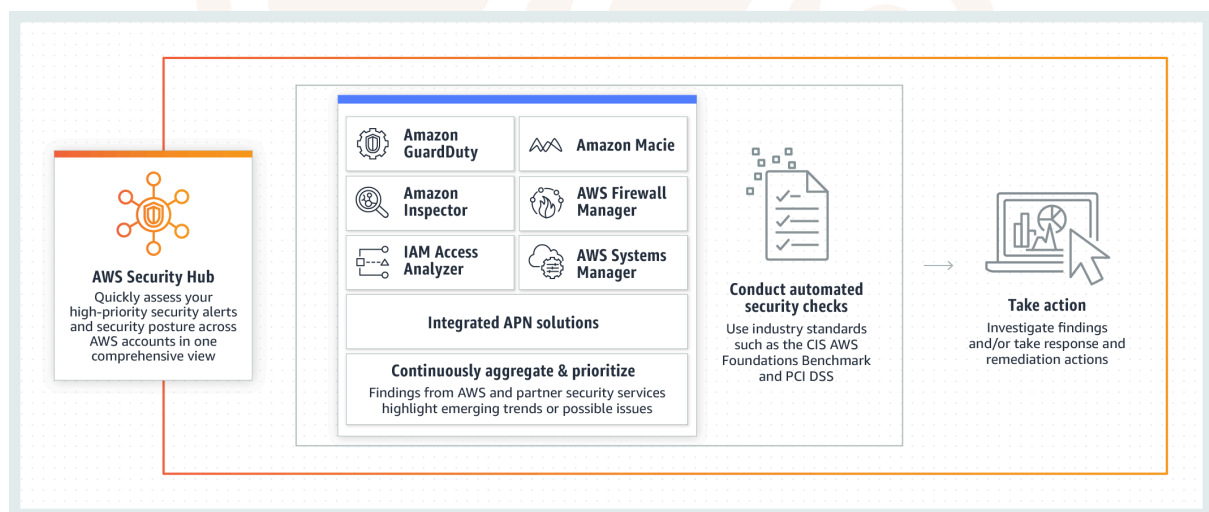
deviate from a best practice, AWS Security Hub flags the problem and recommends remediation steps.

Custom response and remediation actions

AWS Security Hub integrates with Amazon CloudWatch events, enabling you to create custom response and remediation workflows. You can easily send findings to SIEMs, chat tools, ticketing systems, Security Orchestration Automation and Response tools, and on-call management platforms. You can also use AWS System Manager Automation documents, AWS Step Functions, and AWS Lambda functions to build automated remediation workflows that can be initiated from Security Hub.

Multi-account support

With a few clicks in the AWS Security Hub console, you can connect multiple AWS accounts and consolidate findings across those accounts. By designating an administrator security account, you can enable your security team to see consolidated findings for all accounts, while individual account owners see only findings associated with their account.



+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720

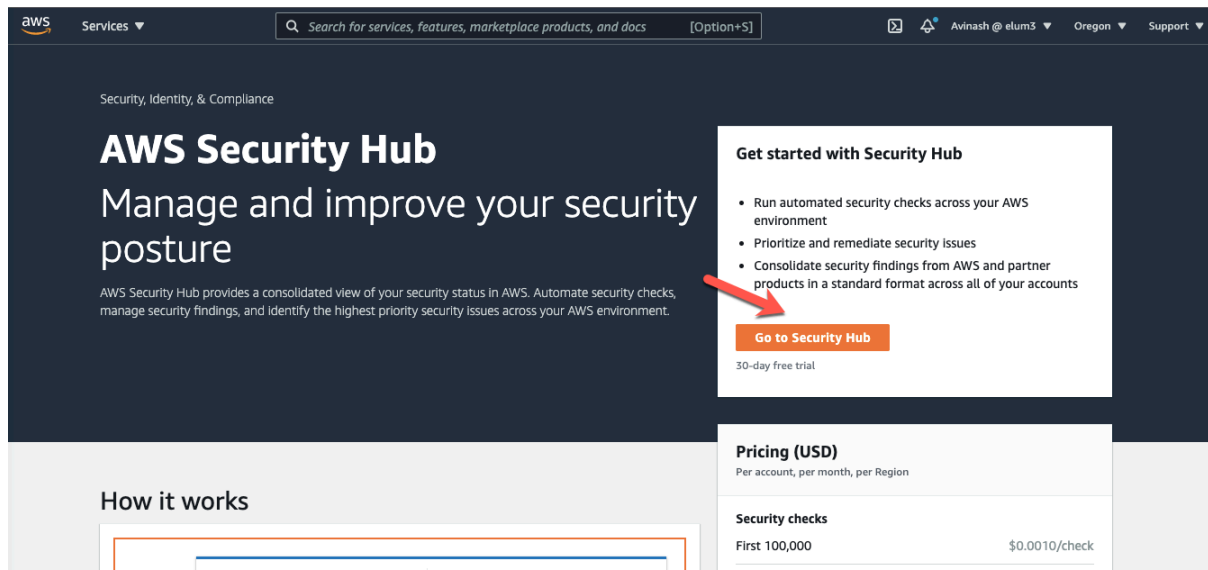




JJ Tech

Demo

- Navigate to AWS Security hub in AWS Console



- Security Hub requires the following 6 services to be enabled. Since Security hub get data from these services
- If any of the services are not enabled it will show us to enable them in the below screen
- You can enable/disable those services anytime
- In my account Security Hub suggests enabling AWS Config and It shows a download button of a Cloud Formation template. If we deploy that template it enables AWS Config.
- You can delegate access to the Administrator account as well if you have multiple accounts. You can ignore that option if you have only one account to monitor

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Enable AWS Security Hub

Enable AWS Config



Before you can enable Security Hub standards and controls, you must first enable resource recording in AWS Config. You must enable resource recording for all of the accounts and in all of the Regions where you plan to enable Security Hub standards and controls. If you do not first enable resource recording, you might experience problems when you enable Security Hub standards and controls. AWS Config bills separately for resource recording. For details, see the [AWS Config pricing page](#).

You can enable resource recording manually from the [AWS Config console](#), or you can choose Download to download and then deploy an AWS CloudFormation template as a StackSet. See our [documentation](#) for more details.

[Download](#)

Security standards

Enabling AWS Security Hub grants it permissions to conduct security checks. [Service Linked Roles \(SLRs\)](#) with the following services are used to conduct security checks: Amazon CloudWatch, Amazon SNS, AWS Config, and AWS CloudTrail.

- 
- ☒ Enable AWS Foundational Security Best Practices v1.0.0
 - ☒ Enable CIS AWS Foundations Benchmark v1.2.0
 - ☒ Enable PCI DSS v3.2.1
- 

AWS Integrations

Enabling Security Hub grants it permissions to import findings from AWS services that you have enabled.

[Learn more](#) 

[Cancel](#)[Enable Security Hub](#)

Delegated Administrator [Info](#)

Delegate permission to manage Security Hub for this organization.

Delegated administrator account ID

464599248654 

Security Hub will be enabled on this account and will be assigned a service-linked role that is required to administer Security Hub for your organization. [Learn more](#)

[Delegate](#)

+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





JJ Tech

Note :

After you enable Security Hub, it can take up to 2 hours to see the results from security checks for the newly enabled standards. Until then, the controls have a status of "No data".

The screenshot shows the AWS Security Hub console. On the left is a navigation menu with sections like Summary, Controls, Security standards, Insights, Findings, Integrations, Management, and Settings. The main area displays 'All controls (415)' with a search bar and a table of controls. The table has columns for ID, Title, Control Status, Severity, and Failed checks. Three controls are visible, all with a 'No Data' status, which is highlighted by an orange box. The controls are related to ELB configurations.

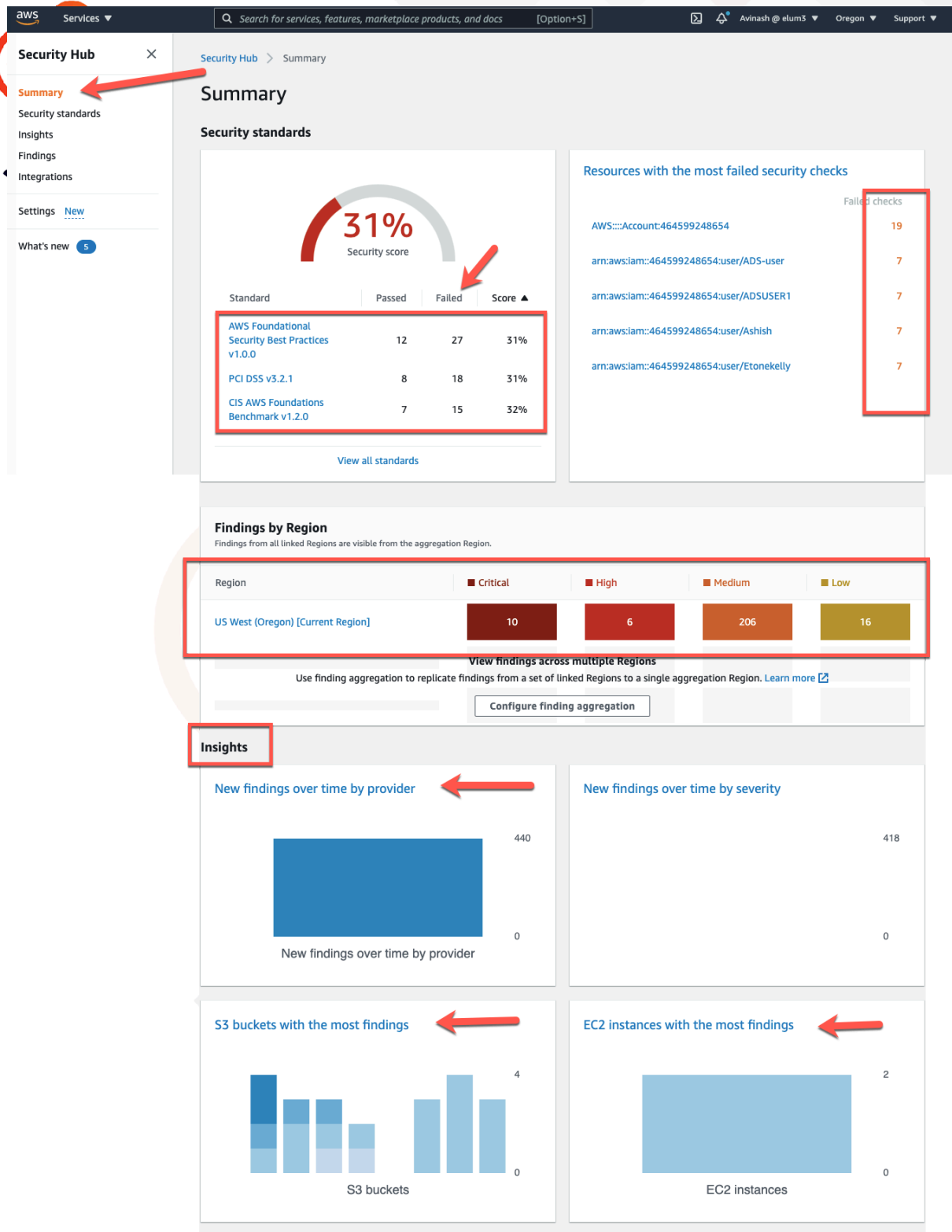
ID	Title	Control Status	Severity	Failed checks
ELB.13	Application, Network and Gateway Load Balancers should span multiple Availability Zones	No Data	Medium	0 of 0
ELB.14	Classic Load Balancer should be configured with defensive or strictest desync mitigation mode	No Data	Medium	0 of 0
ELB.16	Application Load Balancers should be associated with an AWS WAF web ACL	No Data	Medium	0 of 0

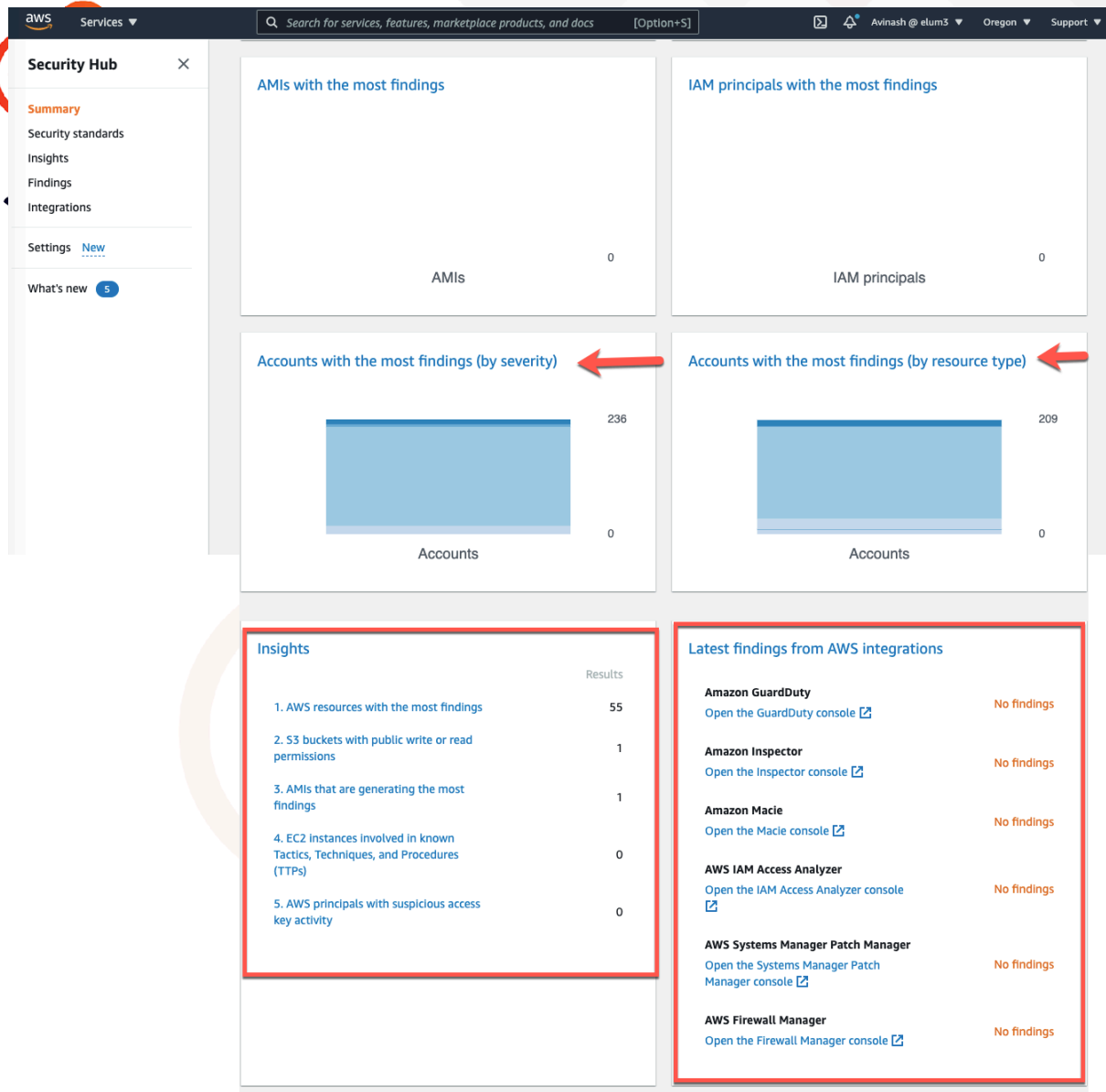
- The main security hub page gives us the summary of all the resources if any security vulnerabilities are detected
- You can click on each section to view more details

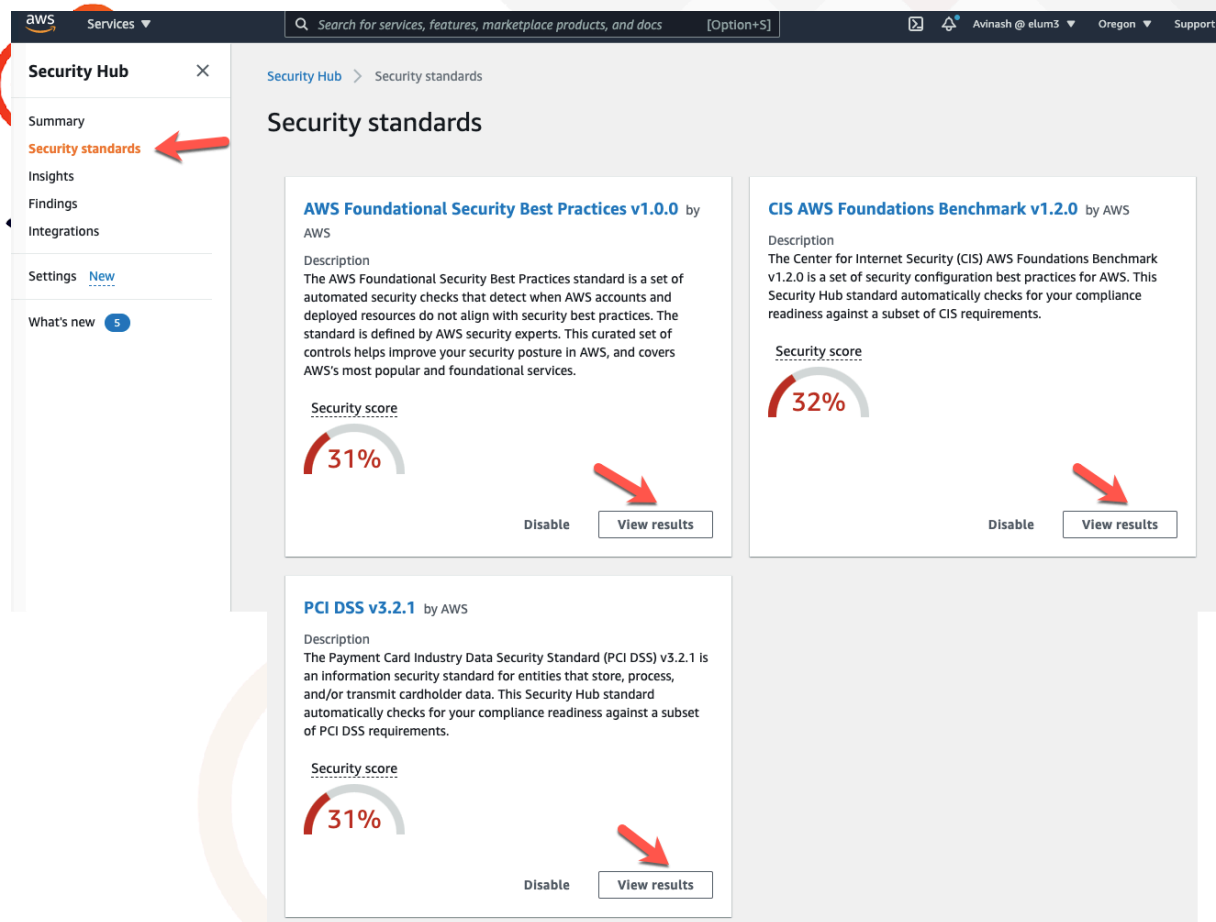
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720









- We have checked 3 security standards while we enable Security Hub
- You can view results on each Security Standards
- You can Enable/Disable them
- In the below picture you can see the results from “AWS Foundational Security best Practices v1.0.0”
- You can see 27 failed compliances
- You can view remediation instructions on each and every failed compliance

+1 (410) 8887049
 contact@jjtechinc.co
 www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720





14103 Hammermil Field Dr Bowie MD 20720

Security Hub > Security standards > AWS Foundational Security Best Practices v1.0.0 > IAM.4

IAM root user access key should not exist

[IAM.4] This AWS control checks whether the root user access key is available. [Remediation instructions](#)

Control status
Security Hub calculates the control status every 24 hours.

Compliance Status: Failed Severity: Critical

All checks	Failed	Unknown	Passed	Suppressed
1	1	0	0	0

All checks (1) Workflow status Download < 1 >

<input type="checkbox"/>	Compliance Status	Workflow	Account	Resource	Investigate	Updated	Finding json
<input type="checkbox"/>	Failed	NEW	464599248654	Account 464599248654	⋮	27 minutes ago	

Security Hub > Insights

Insights (32) Create insight

An insight is a saved filter that shows related findings.

All insights < 1 2 >

1. AWS resources with the most findings

Security Hub managed insight

100+ current

90-day finding trend

2. S3 buckets with public write or read permissions

Security Hub managed insight

1 current

90-day finding trend

3. AMIs that are generating the most findings

Security Hub managed insight

2 current

90-day finding trend

4. EC2 instances involved in known Tactics, Techniques, and Procedures (TTPs)

Security Hub managed insight

0 current

90-day finding trend

5. AWS principals with suspicious access key activity

Security Hub managed insight

0 current

90-day finding trend

6. AWS resources instances that don't meet security standards / best practices

Security Hub managed insight

0 current

90-day finding trend

- We can see findings based on resources in insights
- For example we select “S3 buckets with public write or read permissions”

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Security Hub > Insights > 2. S3 buckets with public write or read permissions

Insight: 2. S3 buckets with public write or read permissions
Security Hub managed insight

Actions Workflow status Create Insight

Type starts with Effects/Data Exposure/ Workflow status is NEW
Resource type is AwsS3Bucket Workflow status is NOTIFIED
Resource type is AWS::S3::Bucket Record state is ACTIVE
Group by: ResourceId Add filters

Resource ID	Count
arn:aws:s3::jjtech-demo-test	2

Severity label
CRITICAL 1 2 3

AWS account ID
464599248654 1 2 3

Resource type
AwsS3Bucket

- There is a security finding with the bucket name “jjtech-demo-test”

Insight: 2. S3 buckets with public write or read permissions
Security Hub managed insight

This list shows a subset of findings in this insight.

Type starts with Effects/Data Exposure/ Resource ID is arn:aws:s3::jjtech-demo-test Workflow status is NEW Resource type is AwsS3Bucket
Workflow status is NOTIFIED Resource type is AWS::S3::Bucket Record state is ACTIVE Add filters

Severity	Workflow status	Record State	Region	Company	Product	Title	Resource	Compliance Status	Updated at
CRITICAL	NEW	ACTIVE	us-west-2	AWS	Security Hub	PCL53.2 S3 buckets should prohibit public read access	S3 Bucket arn:aws:s3::jjtech-demo-test	FAILED	2 hours ago
CRITICAL	NEW	ACTIVE	us-west-2	AWS	Security Hub	S3.2 S3 buckets should prohibit public read access	S3 Bucket arn:aws:s3::jjtech-demo-test	FAILED	2 hours ago

JJ Tech

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720



Security Hub > Insights > 2. S3 buckets with public write or read permissions

Insight: 2. S3 buckets with public write or read permissions

Security Hub managed insight

This list shows a subset of findings in this insight.

Actions Workflow status Create insight

Type starts with Effects/Data Exposure/ Resource type is AwsS3Bucket

Resource type is AWS::S3::Bucket Resource ID is arn:aws:s3::jjtech-demo-test

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

Add filters

Severity	Workflow status	Record State	Region	Company	Product
CRITICAL	NEW	ACTIVE	us-west-2	AWS	Security Hub
CRITICAL	NEW	ACTIVE	us-west-2	AWS	Security Hub

S3.2 S3 buckets should prohibit public read access

Finding ID: arn:aws:securityhub:us-west-2:464599248654:subscription/aws-foundational-security-best-practices/v/1.0.0/S3.2/finding/7563f41f-d010-4430-96c5-34f56f09e7c5

CRITICAL

This AWS control checks whether your S3 buckets allow public read access by evaluating the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).

Rule(s)

Workflow status: New RECORD STATE: ACTIVE

Set by the finding provider

AWS account ID: 464599248654 Severity (original): 90

Compliance status: **FAILED**

Updated at: 2021-11-03T13:40:26.968Z

Severity label: **CRITICAL**

Created at: 2021-11-03T13:40:26.968Z

Product name: Security Hub

Company name: AWS

Types and Related Findings

Resources

Remediation

For directions on how to fix this issue, consult the AWS Security Hub Foundational Security Best Practices documentation.

- You can find remediations on each insights.
- There are two critical findings on the bucket named "jjtech-demo-test"
 - One PCI and the other is standard
 - Issue : The bucket is public

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Account snapshot

Last updated: Nov 2, 2021 by Storage Lens. Metrics are generated every 24 hours. [Learn more](#)

Total storage	Object count	Avg. object size
99.6 GB	1.4 M	76.0 KB

You can enable advanced metrics in the "default-account-dashboard" configuration.

Buckets (93)

Buckets are containers for data stored in S3. [Learn more](#)

Search: demo 3 matches

Name	AWS Region	Access	Creation date
jjtech-demo-test	US West (Oregon) us-west-2	Public	August 29, 2020, 03:08:36 (UTC+05:30)





- Let's make the bucket private and refresh the s3 insights . So that S3 should be cleared

Amazon S3 > jjtech-demo-test

jjtech-demo-test Info


Objects | Properties | **Permissions** | Metrics | Management | Access Points

Permissions overview

Access
Only authorized users of this account

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access 

☒ On

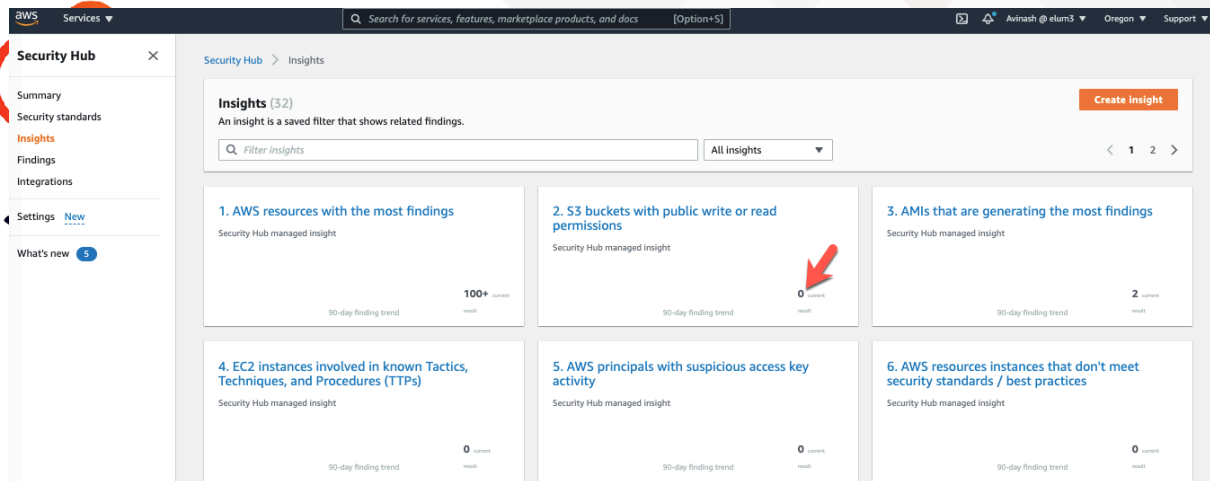
- ☒ On Block public access to buckets and objects granted through *new* access control lists (ACLs)
- ☒ On Block public access to buckets and objects granted through *any* access control lists (ACLs)
- ☒ On Block public access to buckets and objects granted through *new* public bucket or access point policies
- ☒ On Block public and cross-account access to buckets and objects through *any* public bucket or access point policies

- Once I make the bucket to private. S3 insight is resolved in Security Hub.

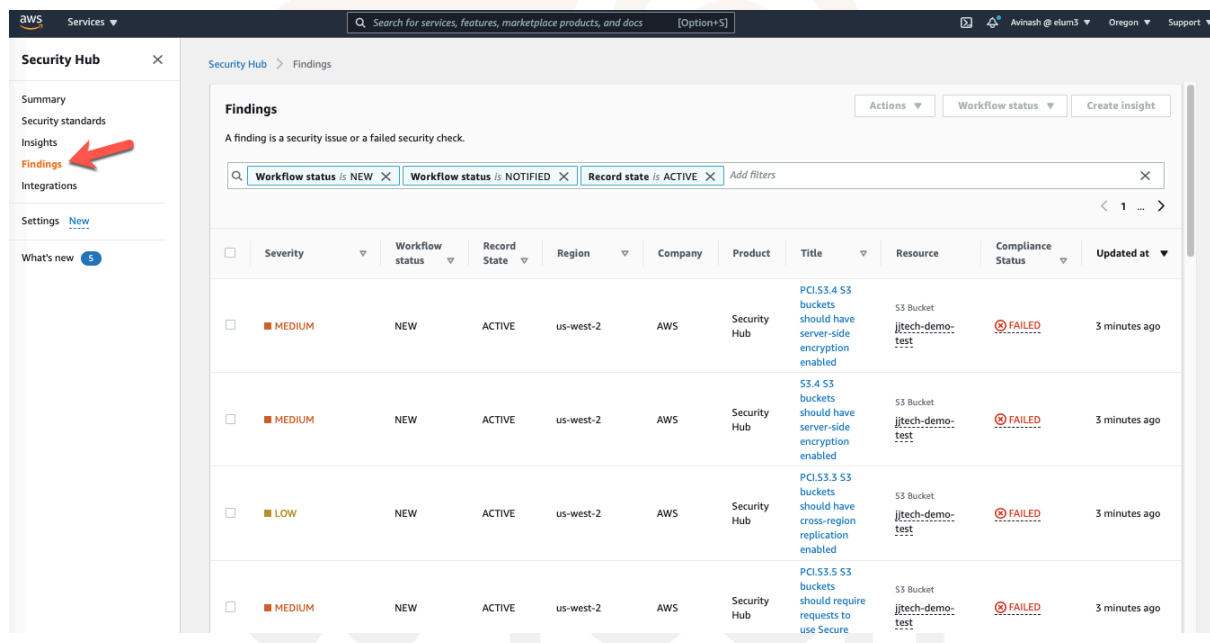
+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720





- You can see all the findings below



- You can integrate with other resources with security hub.

+1 (410) 8887049
 contact@jjtechinc.co
 www.jitechinc.co
 14103 Hammermill Field Dr Bowie MD 20720





- You can stop/start accepting findings from other AWS resources and third party tools

Security Hub ✕

Summary
Security standards
Insights
Findings
Integrations
Settings **New**
What's new 5

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.

Filter integrations

aws

AWS: Audit Manager

Description
AWS Audit Manager continuously audits your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

Type of integration
Receives findings from Security Hub

Categories
Governance, Risk, Compliance (GRC)

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
After you follow the configuration instructions, Security Hub automatically sends findings to this service.

aws

AWS: Chatbot

Description
AWS Chatbot is an interactive agent that makes it easy to monitor and interact with your AWS resources in your Slack channels and Amazon Chime chat rooms.

Type of integration
Receives findings from Security Hub

Categories
Instant messaging

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
After you follow the configuration instructions, Security Hub automatically sends findings to this service.

aws

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

Stop accepting findings

aws

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

Stop accepting findings

aws

AWS: Systems Manager OpsCenter and Explorer

Description
AWS Systems Manager OpsCenter and Explorer provide you with a central location to view, investigate, and resolve operational work items and provide you with a customizable dashboard.

Type of integration
Receives findings from and updates findings in Security Hub

Categories
IT Ticketing, Security Orchestration Automation and Response (SOAR)

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
After you follow the configuration instructions, Security Hub automatically sends findings to and receives finding updates from this service.

aws

AWS: Systems Manager Patch Manager

Description
Systems Manager Patch Manager centralized management for patching your fleet of Amazon EC2 Windows and Linux instances or your on-premises servers and virtual machines (VMs).

Type of integration
Sends findings to Security Hub

Categories
Configuration and Patch 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](#)

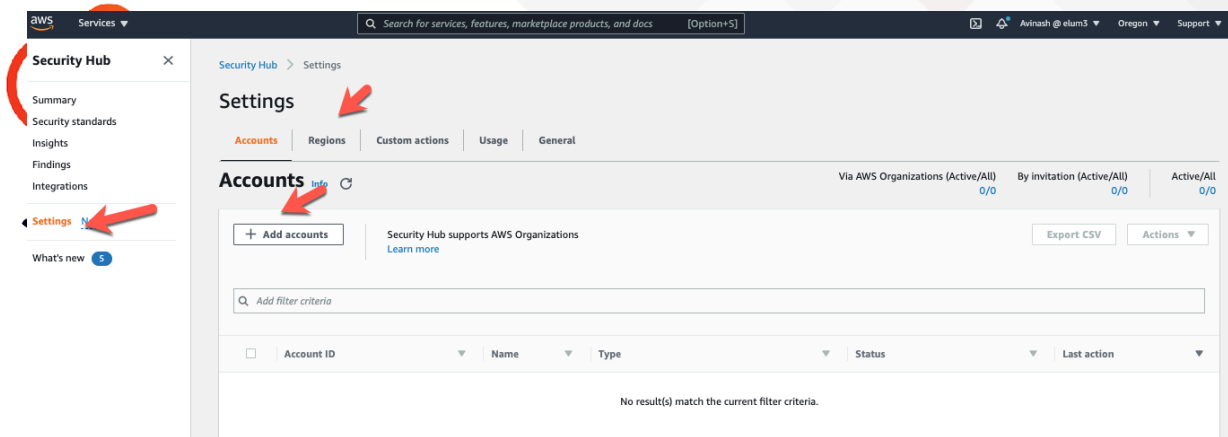
Status
Accepting findings. See findings

Stop accepting findings

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co

14103 Hammernil Field Dr Bowie MD 20720





- In the settings section
 - You can add multiple accounts
 - You can add multiple regions

JJ Tech

+1 (410) 8887049
contact@jjtechinc.co
www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720

