Prowler

## Introduction

* Prowler is an Open-Source security tool to perform AWS, Azure and Google Cloud security best practices assessments, audits, incident response, continuous monitoring, hardening and forensics readiness.
* It contains hundreds of controls covering CIS, NIST 800, NIST CSF, CISA, RBI, FedRAMP, PCI-DSS, GDPR, HIPAA, FFIEC, SOC2, GXP, AWS Well-Architected Framework Security Pillar, AWS Foundational Technical Review (FTR), ENS (Spanish National Security Scheme) and your custom security frameworks.

## Use Case

* A large enterprise organization recently migrated its infrastructure to AWS cloud to take advantage of its scalability, flexibility, and cost-effectiveness.
* However, with the complexity of AWS services and configurations, the organization is concerned about the security implications and wants to ensure that its AWS environment adheres to best security practices and compliance standards.
* The security team decides to use Prowler to conduct comprehensive security assessments and identify any potential security gaps or misconfigurations in their AWS accounts.

## Who Can Use Prowler

**DevOps Engineers**: DevOps engineers responsible for deploying and managing AWS infrastructure can use Prowler as part of their continuous security monitoring and DevSecOps practices.

**SRE Teams**: SRE teams responsible for ensuring the security of AWS environments can use Prowler to perform regular security assessments, identify security risks, and prioritize remediation efforts.

## Setup Guide

### Installation

* Prowler is available as a project in [PyPI](https://pypi.org/project/prowler/), thus can be installed using pip with Python >= 3.9

#### Requirement

* Python >= 3.9
* Python pip >= 3.9
* AWS Credentials
  + Since Prowler uses **AWS Credentials** under the hood, you can follow any authentication method as described here.
  + Make sure you have properly configured your **AWS-CLI** with a valid Access Key and Region or declare AWS variables properly using **aws configure** or **export Access key** and **Secret Access key**
  + Those credentials must be associated to a user or role with proper permissions to do all checks. To make sure, add the following AWS managed policies to the user or role being used:
    - **arn:aws:iam::aws:policy/SecurityAudit**
    - **arn:aws:iam::aws:policy/job-function/ViewOnlyAccess**
  + Moreover, some read-only additional permissions are needed for several checks, make sure you attach also the custom policy [**prowler-additions-policy.json**](https://github.com/prowler-cloud/prowler/blob/master/permissions/prowler-additions-policy.json) to the role you are using.
  + If you want Prowler to send findings to AWS Security Hub, make sure you also attach the custom policy [**prowler-security-hub.json**](https://github.com/prowler-cloud/prowler/blob/master/permissions/prowler-security-hub.json).

#### Commands

**pip install prowler**

**prowler –v**

## Prowler container versions

* We can be able to setup and run prowler as docker container.
* The available versions of Prowler are the following:
  + latest: in sync with master branch (bear in mind that it is not a stable version)
  + <x.y.z> (release): you can find the releases here; those are stable releases.
  + stable: this tag always points to the latest release.
* The container images are available here:
  + [DockerHub](https://hub.docker.com/r/toniblyx/prowler/tags)
  + [AWS Public ECR](https://gallery.ecr.aws/prowler-cloud/prowler)

## High level architecture

We can run Prowler from our workstation, an EC2 instance, Fargate or any other container, Codebuild, CloudShell, Cloud9 and many more.

## AWS Configuration

* To run Prowler against an AWS account, we need to specify the provider **aws:**

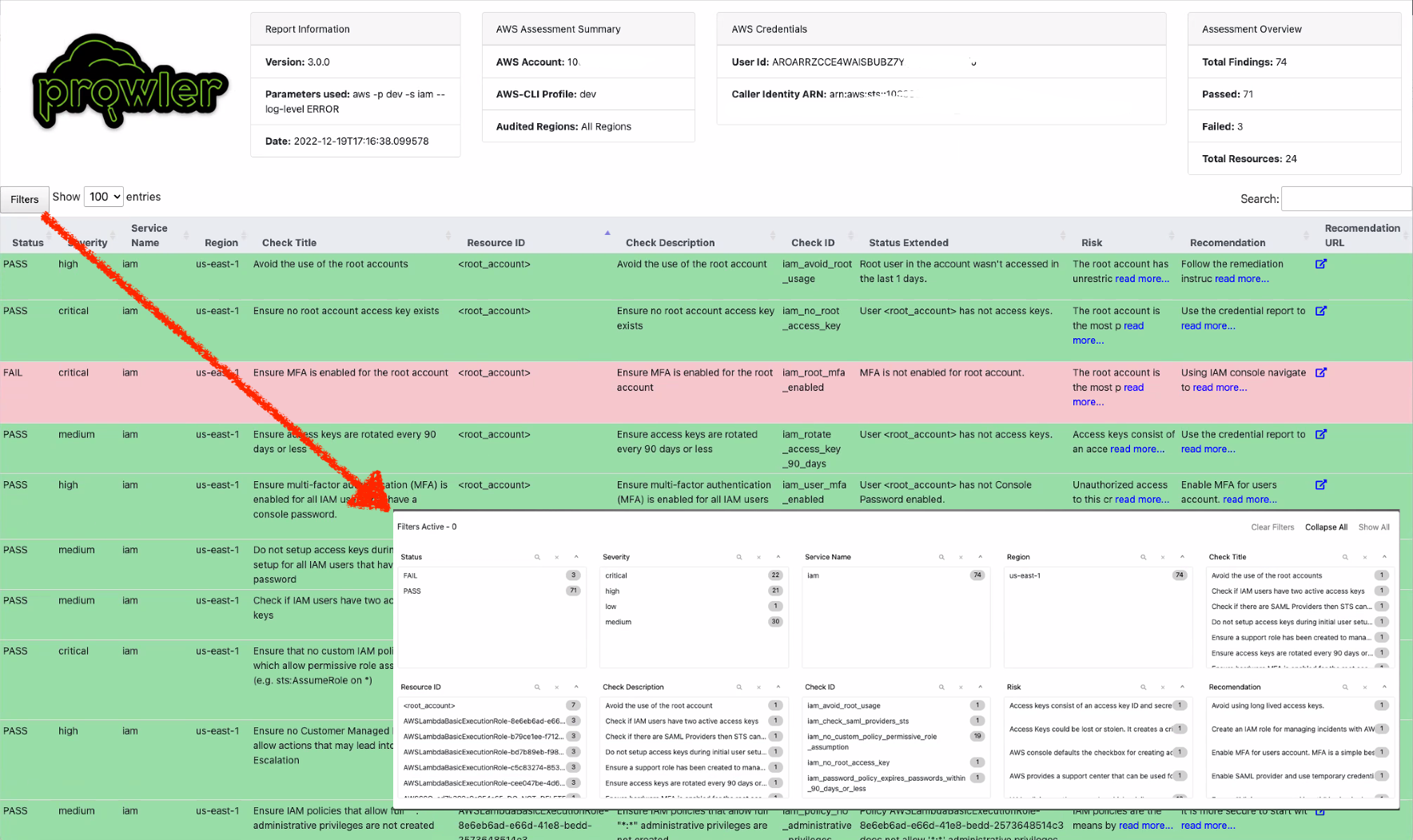
**prowler aws**

### Basic commands

* By default, Prowler will generate a CSV, JSON and HTML reports, however you can generate a JSON-ASFF (used by AWS Security Hub) report with -M or --output-modes:

**prowler aws -M csv json json-asff html**

* The html report will be in the output directory as the other files, and it will look like:



* We can use **-l/--list-checks** and **--list-services** to list all available checks or services within the aws provider:

**prowler aws --list-checks**

**prowler aws --list-services**

* For executing specific checks or services you can use options **-c/checks or -s/services**:

**prowler aws --services s3 ec2**

* Also, checks and services can be excluded with options **-e/--excluded-checks or --excluded-services**:

**prowler aws --excluded-checks s3\_bucket\_public\_access**

* Use a custom AWS profile with **-p/--profile** and ignore unused services in the AWS account with **--ignore-unused-services** and/or AWS regions which you want to audit with **-f/--filter-region**:

**prowler aws --profile <profile\_name> --ignore-unused-services -f us-east-1**

Note: By default, prowler will scan all AWS services and regions.

* Prowler allows you to scan only the resources that contain specific tags. This can be done with the flag **--resource-tags** followed by the tags **Key=Value** separated by space:

**prowler aws --resource-tags Environment=development –f us-east-1**

### Compliance

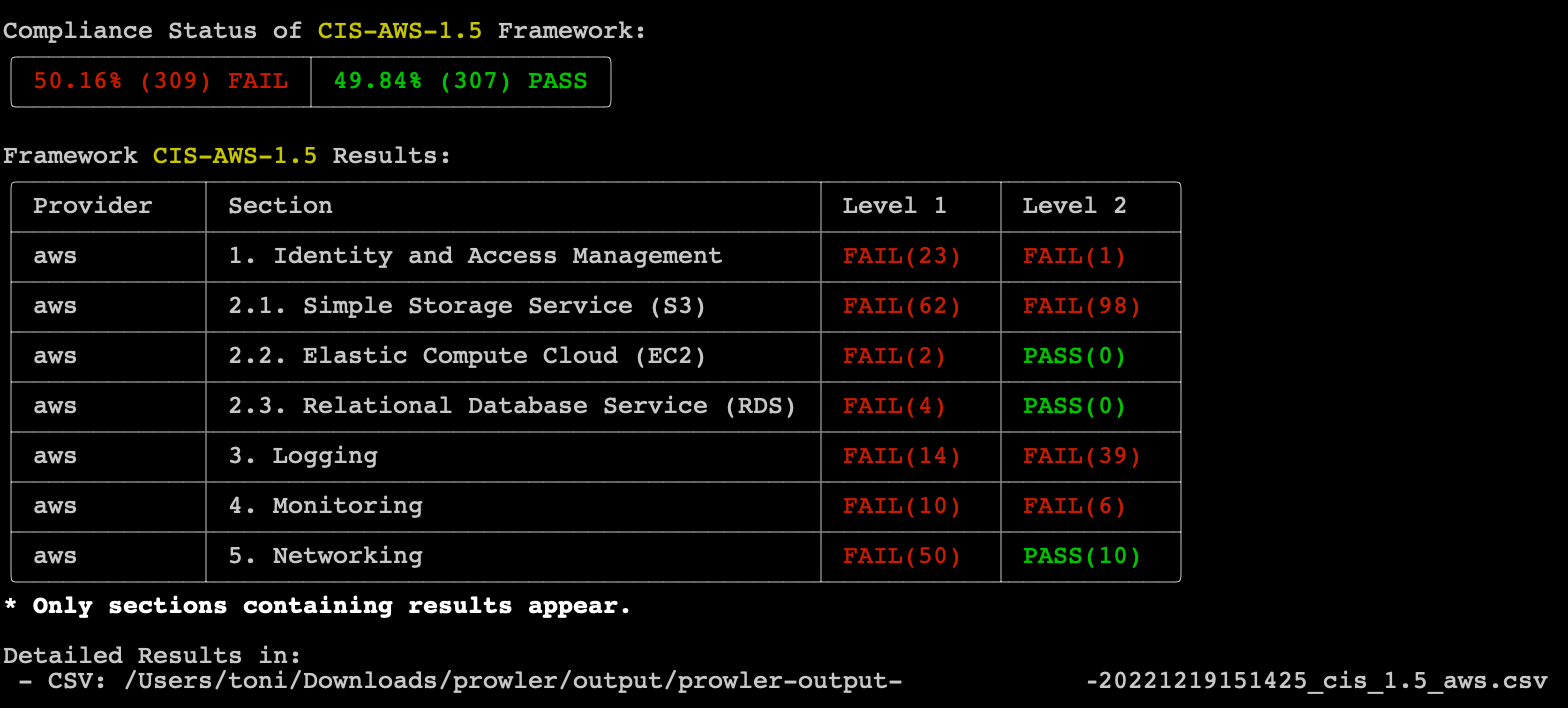
* We can execute checks based on requirements defined in compliance frameworks.
* To list Available Compliance Frameworks, we can use option **--list-compliance**:

**prowler aws --list-compliance**

* Prowler can be executed to analyze our environment based on a specific compliance framework, to do it, you can use option –**compliance:**

**prowler aws --compliance < compliance\_framework > -f us-east-1**

* Standard results will be shown and additionally the framework information as the sample below for CIS AWS 1.5. For details a CSV file has been generated as well.



### Send report to AWS S3 Bucket

* To save your report in an S3 bucket, use **-B/--output-bucket an**d custom folder and/or filename, use **-o/--output-directory** and/or **-F/--output-filename**.

**prowler aws \**

**-B <Bucket\_Name> \**

**--output-directory prowler-outputs \**

**--output-filename dev-env-report \**

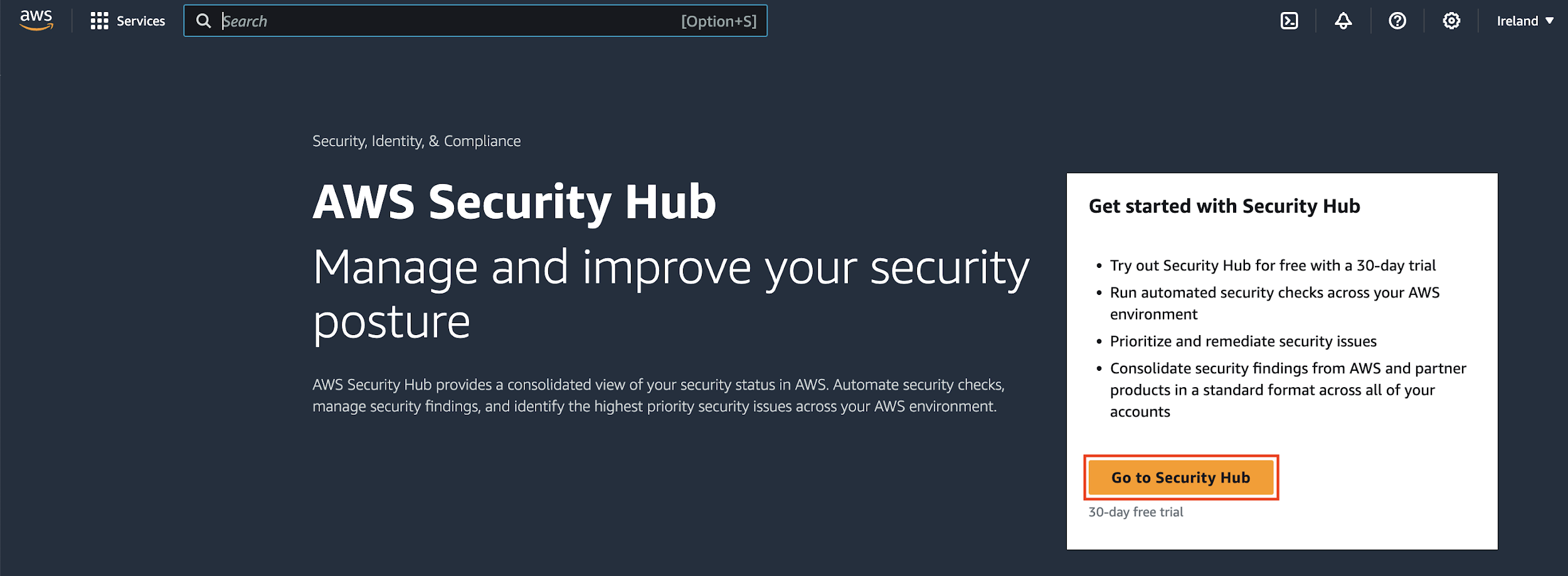
**-f us-east-1**

### AWS Security Hub Integration

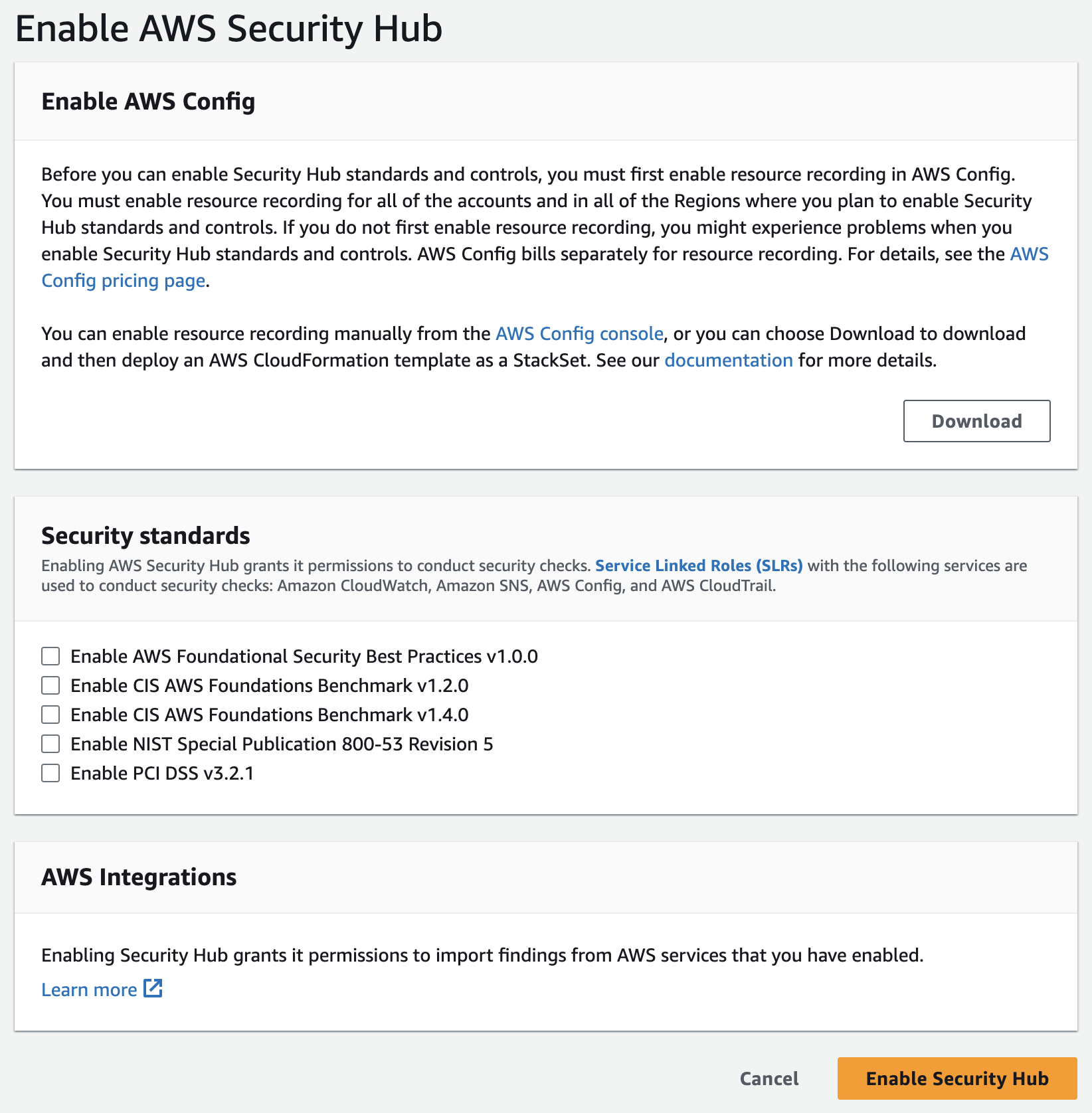
* Prowler supports natively and as official integration sending findings to **AWS Security Hub**.
* This integration allows **Prowler** to import its findings to **AWS Security Hub**.
* Before sending findings, you will need to enable **AWS Security Hub** and the **Prowler** integration.

#### Using the AWS Management Console

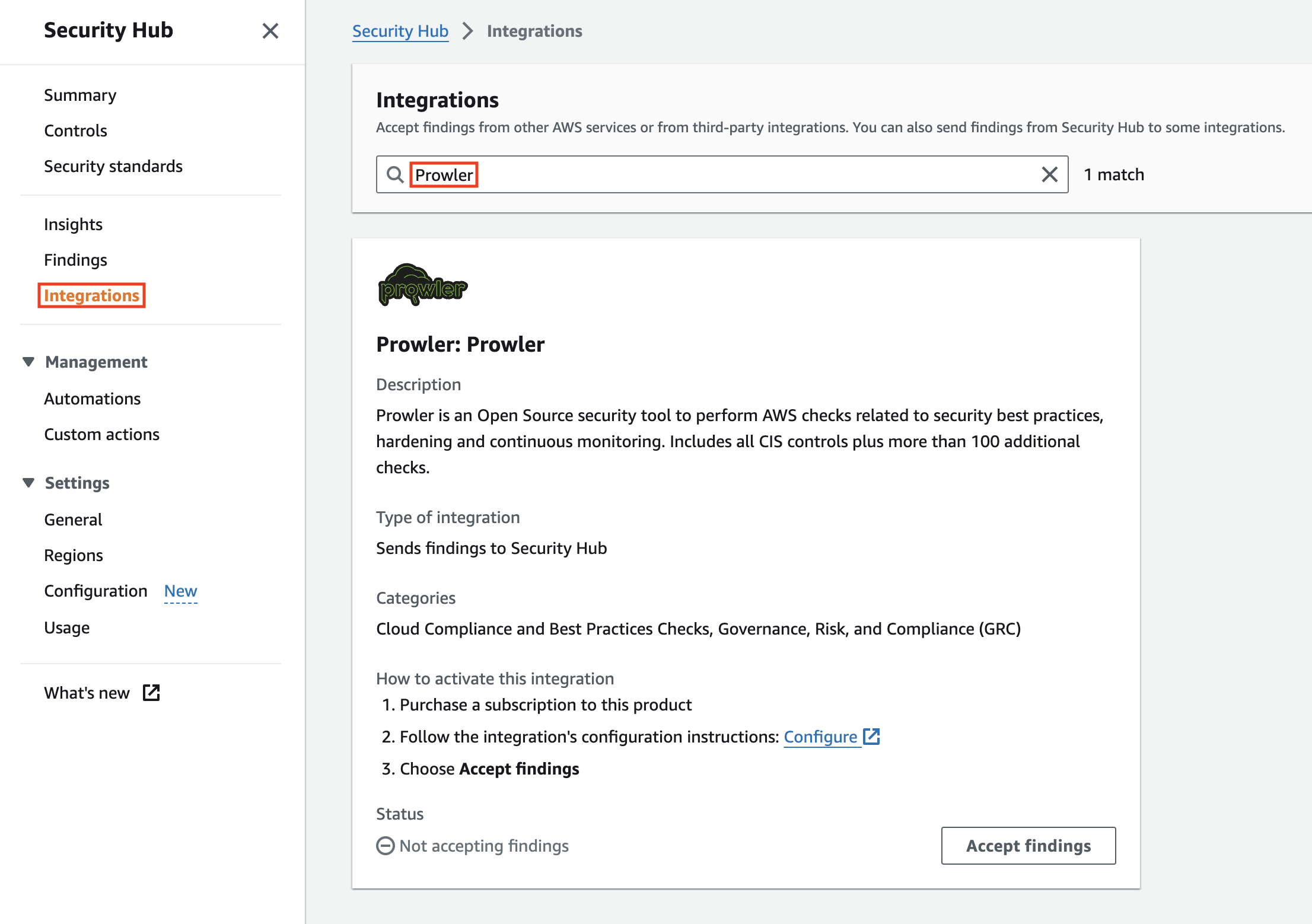
* Open the **AWS Security Hub** console at https://console.aws.amazon.com/securityhub/.
* When you open the Security Hub console for the first time make sure that you are in the **region** you want to enable, then choose **Go to Security Hub**.



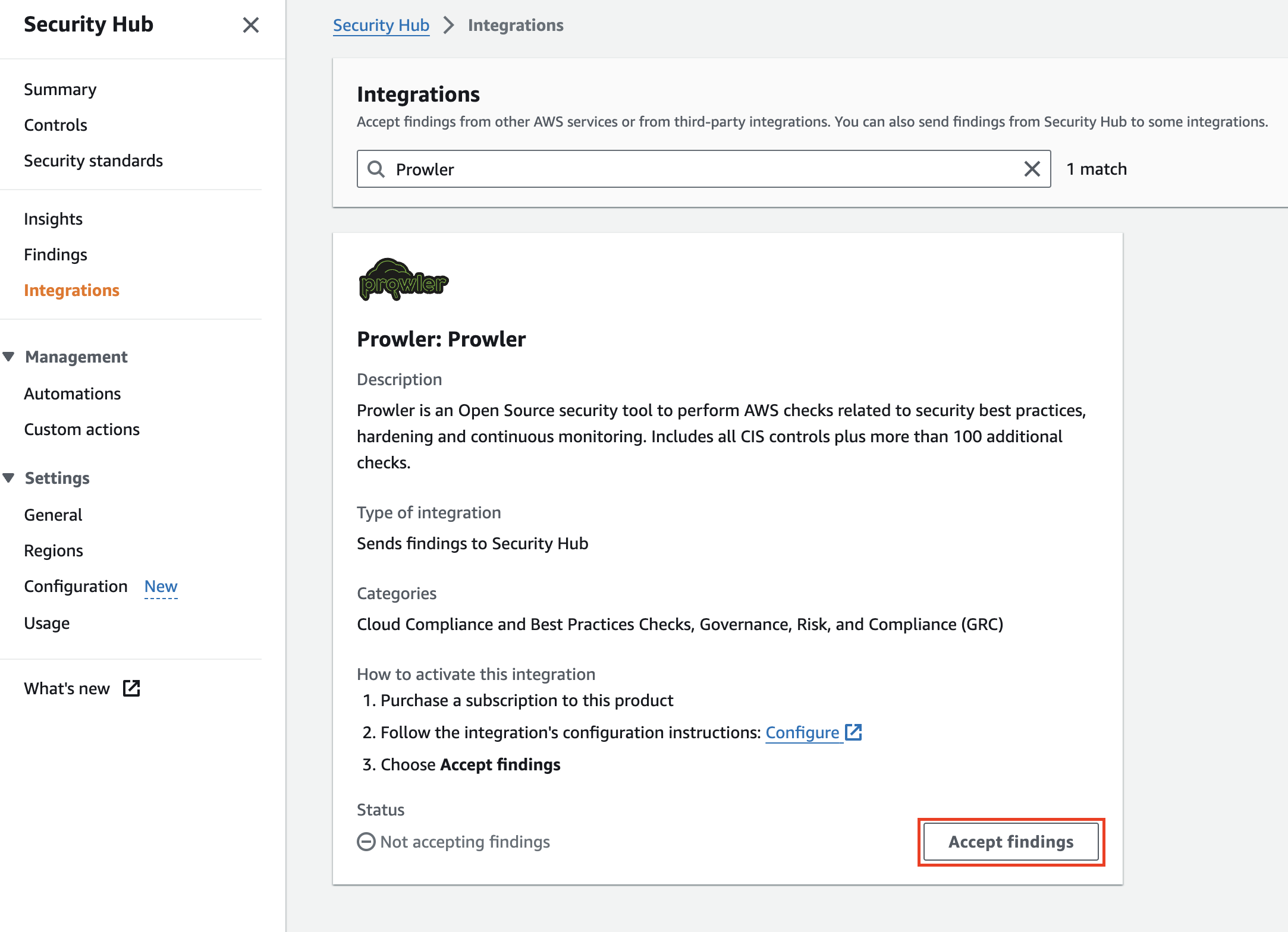
* On the next page, the Security standards section lists the security standards that Security Hub supports. Select the check box for a standard to enable it and **clear the check box to disable it**.
* Choose **Enable Security Hub**.



* Once **AWS Security Hub** is enabled you will need to **enable Prowler as partner integration** to allow **Prowler** to send findings to your **AWS Security Hub**.
* Open the **AWS Security Hub** console at https://console.aws.amazon.com/securityhub/.
* Select the **Integrations** tab in the right-side menu bar.



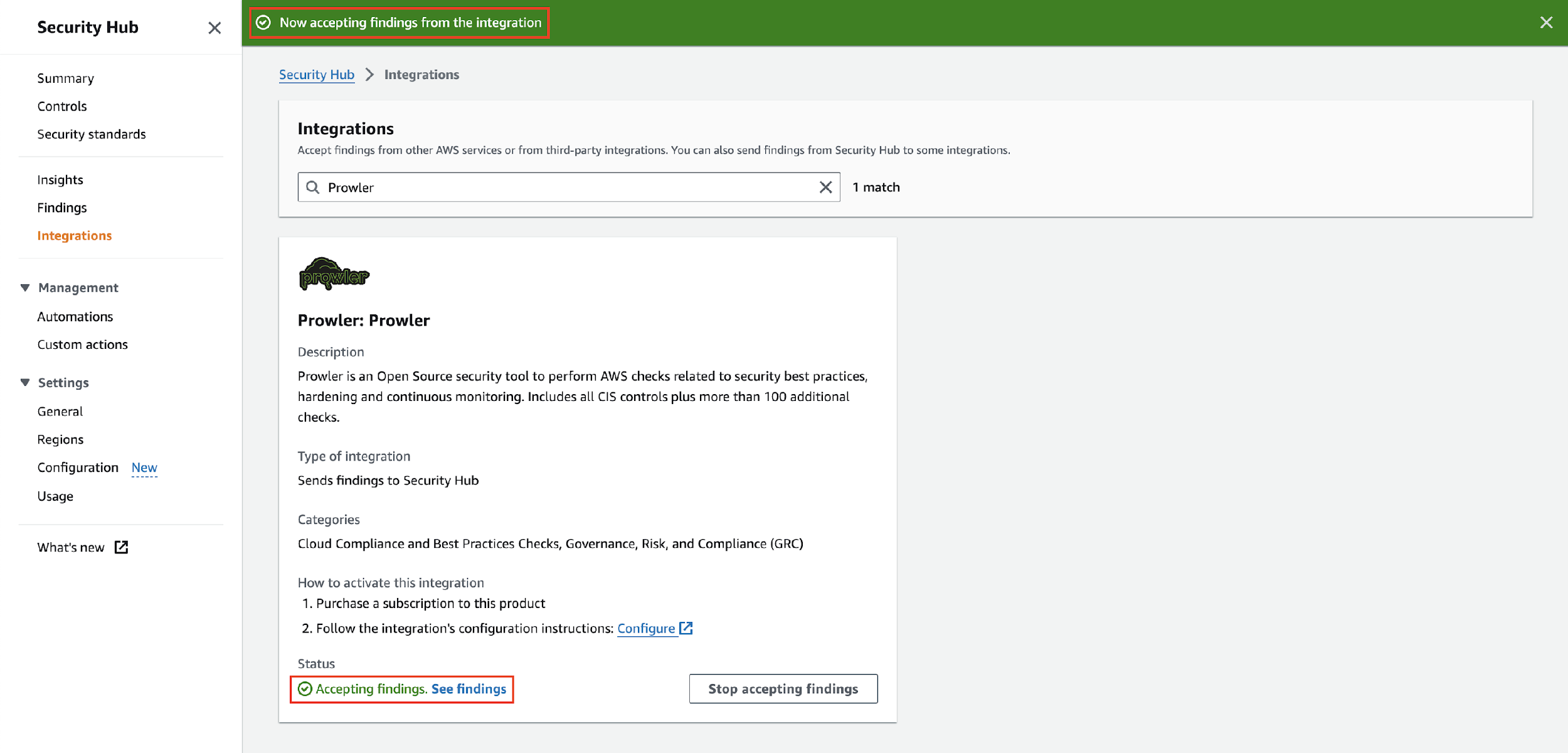
* Search for Prowler in the text search box and the Prowler integration will appear.
* Once there, click on **Accept Findings** to allow AWS Security Hub to receive findings from Prowler.



* A new modal will appear to **confirm** that you are **enabling the Prowler integration**.



* Right after clicking on **Accept Findings**, we will see that the integration is enabled in **AWS Security Hub**.

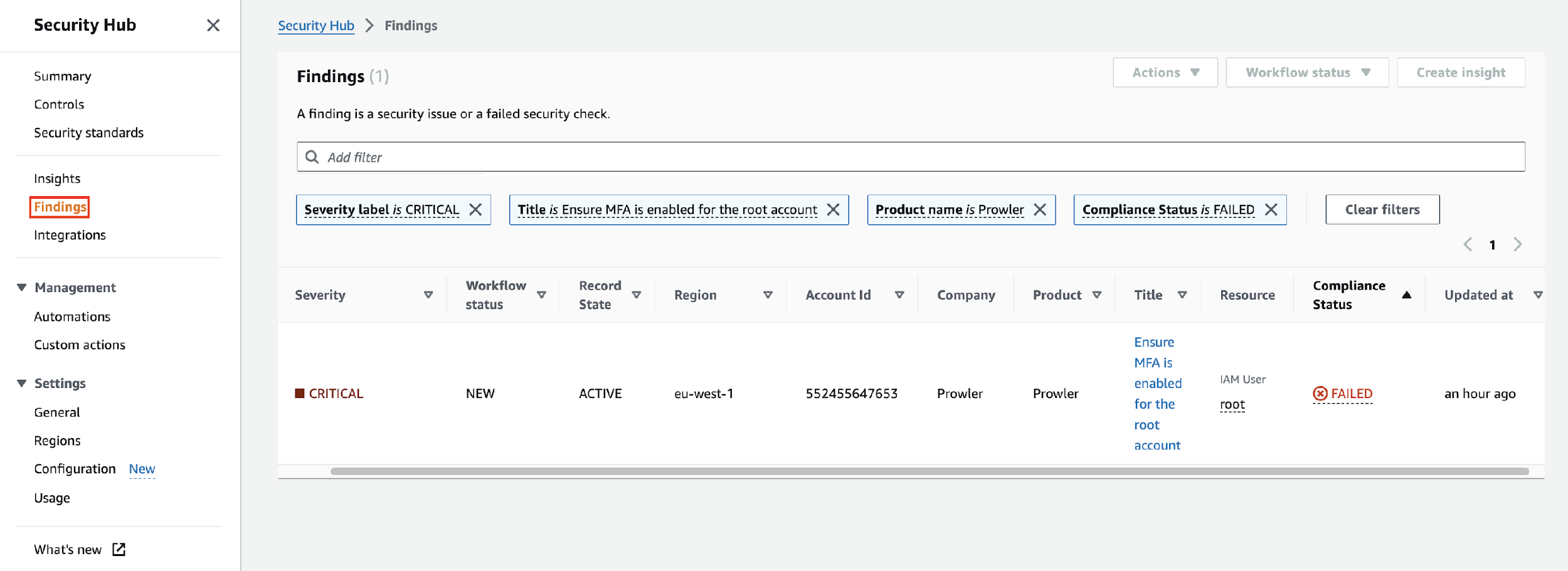


#### Send Findings

* Once it is enabled, it is as simple as running the command below to run checks for a specific region:

**prowler aws --security-hub -f us-east-1**

* Once the AWS Security Hub has been configured in your next scan you will receive the Prowler findings in the AWS regions configured.
* To review those findings in AWS Security Hub, go to the **AWS Security Hu**b console and select the **Findings** tab in the right-side menu bar.



#### Send only failed findings to Security Hub

* When using the AWS Security Hub integration you can send only the **FAIL** findings generated by Prowler.
* Therefore, the AWS Security Hub usage costs eventually would be lower.
* To follow that recommendation, you could add the **-q/--quiet** flag to the Prowler command

**prowler --security-hub –quiet -f us-east-1**

* We can use, instead of the **-q/--quiet** argument, the **--send-sh-only-fails** argument to save all the findings in the **Prowler outputs** but just to send **FAIL** findings to **AWS Security Hub**:

**prowler --security-hub --send-sh-only-fails -f us-east-1**