Codebuild and Security Hub in Lunar

Morten Zdrenka Christensen

LUNAR®

Who?

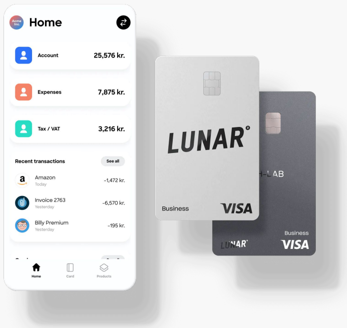
Morten Z. Christensen

Lunar
Security Engineer 2021-

InCommondities
Software Engineer 2020-2021

Danske Bank
Student / FTE 2017-2020

LUNAR®



15,000

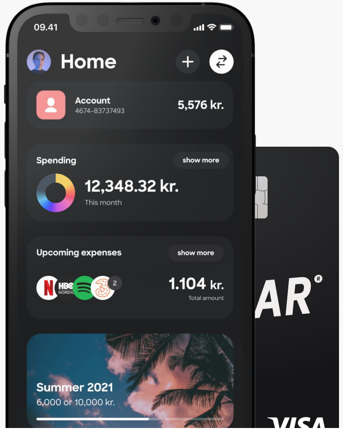
Total number of Business Customers

Company founded in 2015

700

Employees

European Banking License issued in Denmark



500,000

Customers in total

€345m

Total amount raised

Series D ✓

Recently closed our Series D of €210m

We have offices in these locations

LUNAR TECH AT A GLANCE

More than

40

deployments to production per day

151 FTE's

+80 hires within 12m

25

squads

1000

containers in prod

Multi-cloud

3

AWS, Azure, GCP

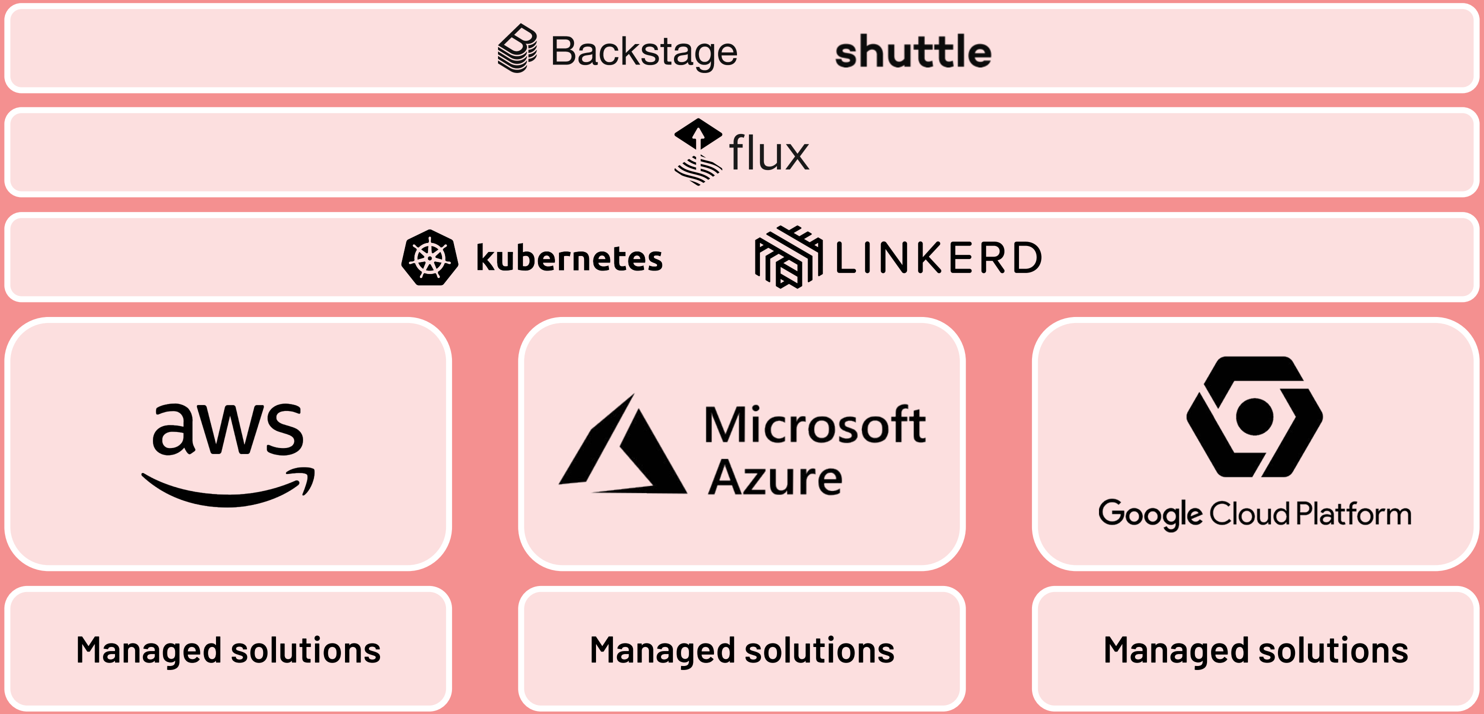
450

µServices

100

releases per day

THE PLATFORM (simplified)



Backstage shuttle

flux

kubernetes LINKERD

aws

Microsoft Azure

Google Cloud Platform

Managed solutions

Managed solutions

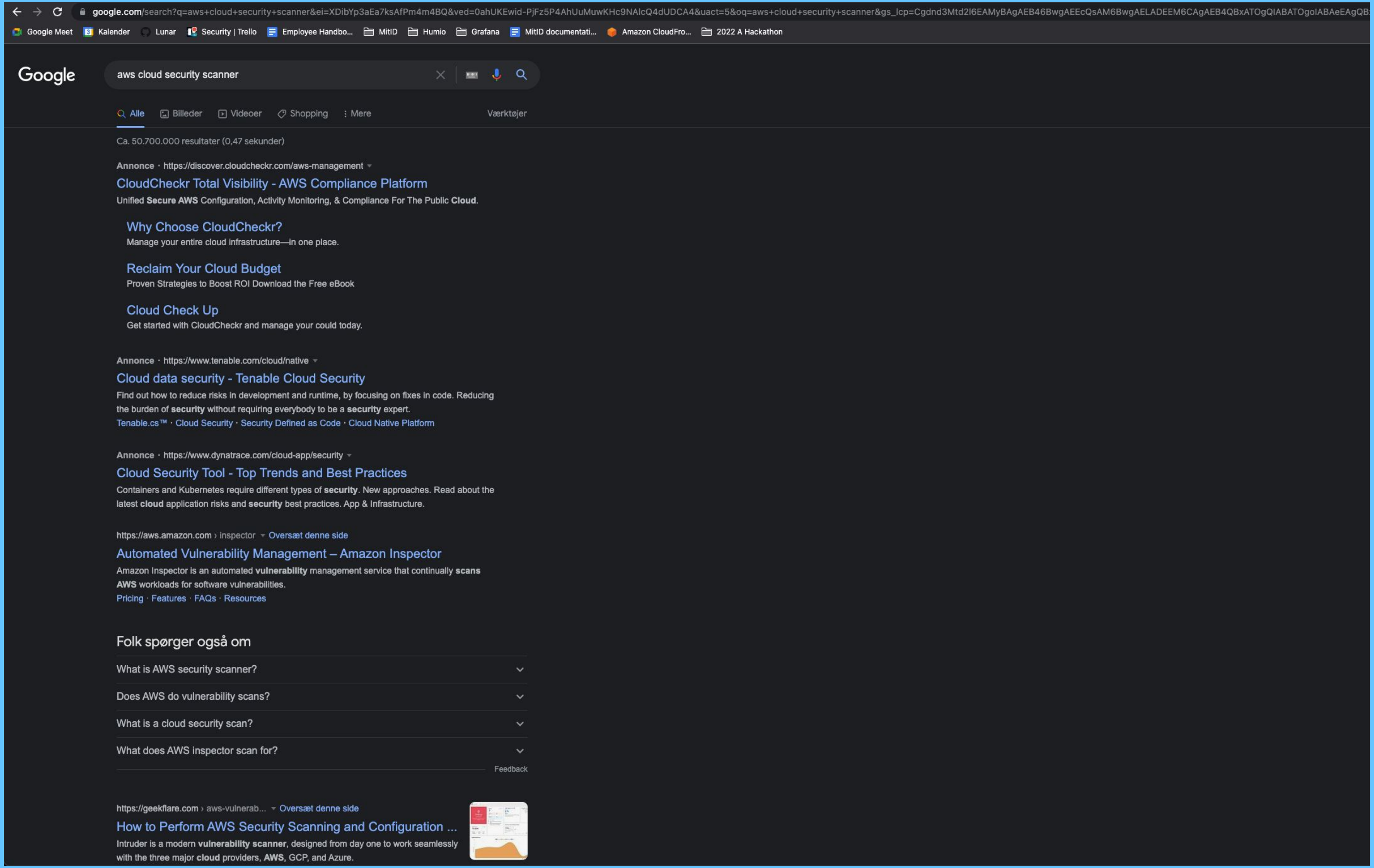
Managed solutions

Keeping an overview is hard

Concerns about what I **don't** know is usually what keeps me up at night.

Questions such as:

- What is our inventory like?
- Has everything been setup according to best practices?
- Has any configuration been changed on purpose or by accident?



google.com/search?q=aws+cloud+security+scanner&ei=XDibYp3aEa7ksAfPm4m4BQ&ved=0ahUKEwid-PjFz5P4AhUuMuwKHc9NAlcQ4dUDCA4&uact=5&oq=aws+cloud+security+scanner&gs_lcp=Cgdnd3Mtd2l6EAMyBAgAEB46BwgAEEcQsAM6BwgAELADEEM6CAgAEB4QBxATOgQIABATOgoIABAeEAgQB
Google Meet
Kalender
Lunar
Security | Trello
Employee Handbo...
MitID
Humio
Grafana
MitID documentati...
Amazon CloudFro...
2022 A Hackathon
Google
aws cloud security scanner
Alle
Billeder
Videoer
Shopping
Mere
Værktøjer

Ca. 50.700.000 resultater (0,47 sekunder)

Annonce · https://discover.cloudcheckr.com/aws-management

CloudCheckr Total Visibility - AWS Compliance Platform

Unified **Secure AWS** Configuration, Activity Monitoring, & Compliance For The Public **Cloud**.

Why Choose CloudCheckr?

Manage your entire cloud infrastructure—in one place.

Reclaim Your Cloud Budget

Proven Strategies to Boost ROI Download the Free eBook

Cloud Check Up

Get started with CloudCheckr and manage your could today.

Annonce · https://www.tenable.com/cloud/native

Cloud data security - Tenable Cloud Security

Find out how to reduce risks in development and runtime, by focusing on fixes in code. Reducing the burden of **security** without requiring everybody to be a **security** expert.

Tenable.cs™ · Cloud Security · Security Defined as Code · Cloud Native Platform

Annonce · https://www.dynatrace.com/cloud-app/security

Cloud Security Tool - Top Trends and Best Practices

Containers and Kubernetes require different types of **security**. New approaches. Read about the latest **cloud** application risks and **security** best practices. App & Infrastructure.

https://aws.amazon.com › inspector Oversæt denne side

Automated Vulnerability Management – Amazon Inspector

Amazon Inspector is an automated **vulnerability** management service that continually **scans** **AWS** workloads for software vulnerabilities.

Pricing · Features · FAQs · Resources

Folk spørger også om

What is AWS security scanner?

Does AWS do vulnerability scans?

What is a cloud security scan?

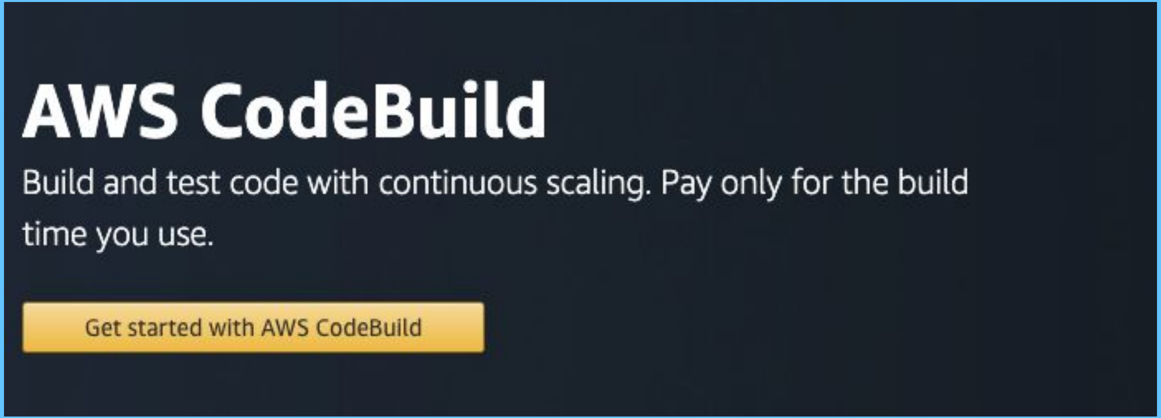
What does AWS inspector scan for?

https://geekflare.com › aws-vulnerab... Oversæt denne side

How to Perform AWS Security Scanning and Configuration ...

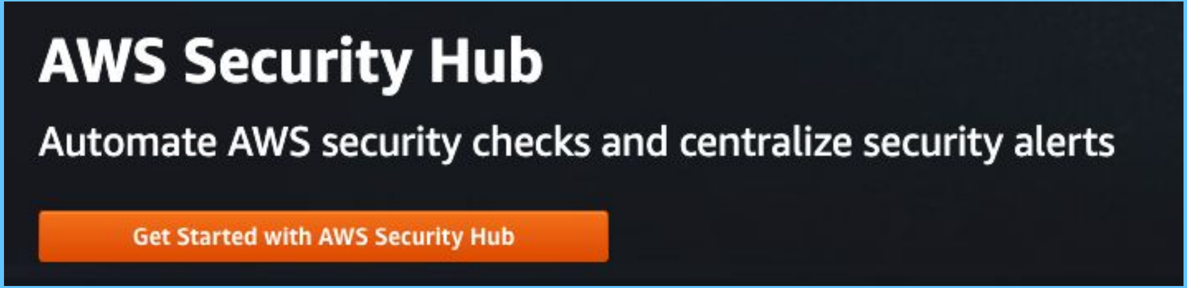
Intruder is a modern **vulnerability scanner**, designed from day one to work seamlessly with the three major **cloud** providers, **AWS**, GCP, and Azure.

Codebuild & Security Hub



AWS CodeBuild

Build and test code with continuous scaling. Pay only for the build time you use.



AWS Security Hub

Automate AWS security checks and centralize security alerts

AWS Codebuild

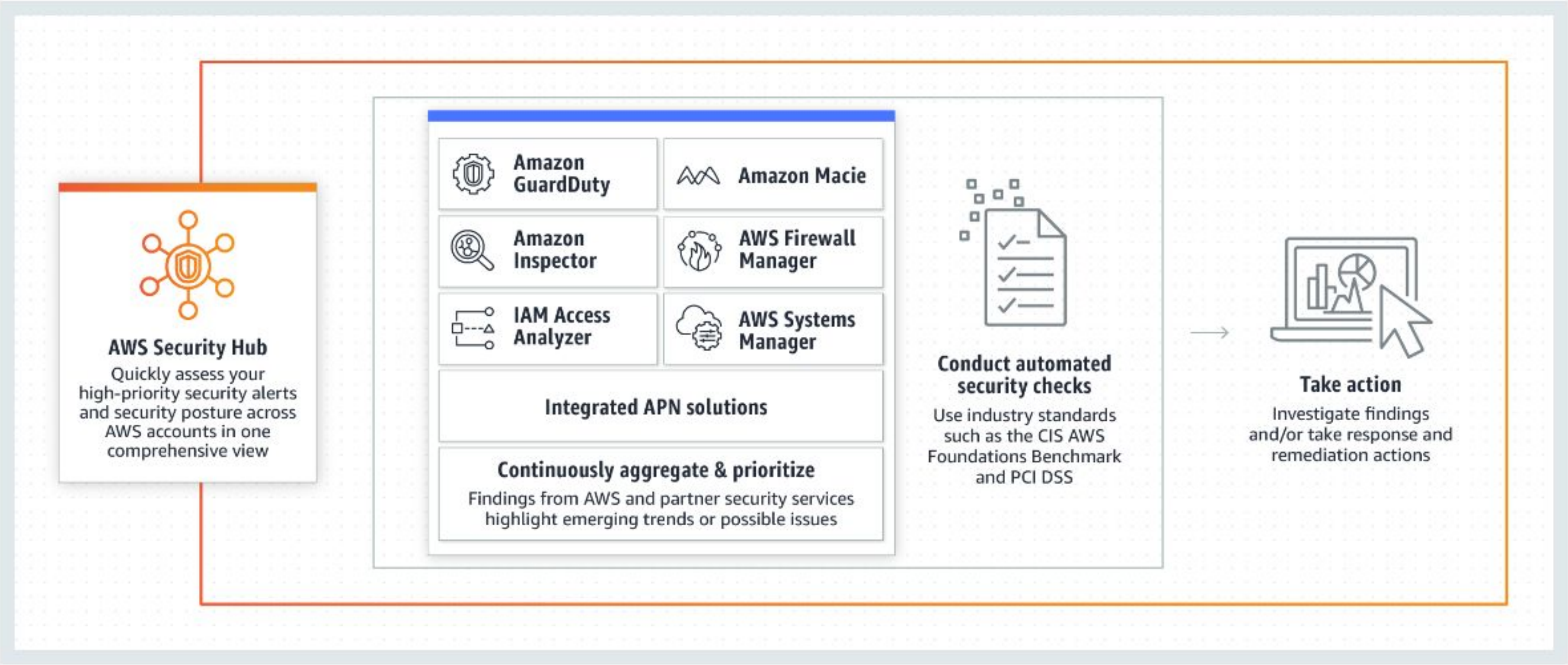
How it works: CI/CD in AWS

- Pipeline: RCE as a service
- Send logs to S3/cloudwatch
- Artifacts in S3 buckets
- IAM roles
- Trigger Lambdas, send events

AWS Security Hub

How it works

- Automatically run security checks on your AWS account
- Keep track of security results from various other AWS products
- Aggregate across many regions and accounts



AWS Security Hub

Quickly assess your high-priority security alerts and security posture across AWS accounts in one comprehensive view

Amazon GuardDuty

Amazon Macie

Amazon Inspector

AWS Firewall Manager

IAM Access Analyzer

AWS Systems Manager

Integrated APN solutions

Continuously aggregate & prioritize

Findings from AWS and partner security services highlight emerging trends or possible issues

Conduct automated security checks

Use industry standards such as the CIS AWS Foundations Benchmark and PCI DSS

Take action

Investigate findings and/or take response and remediation actions

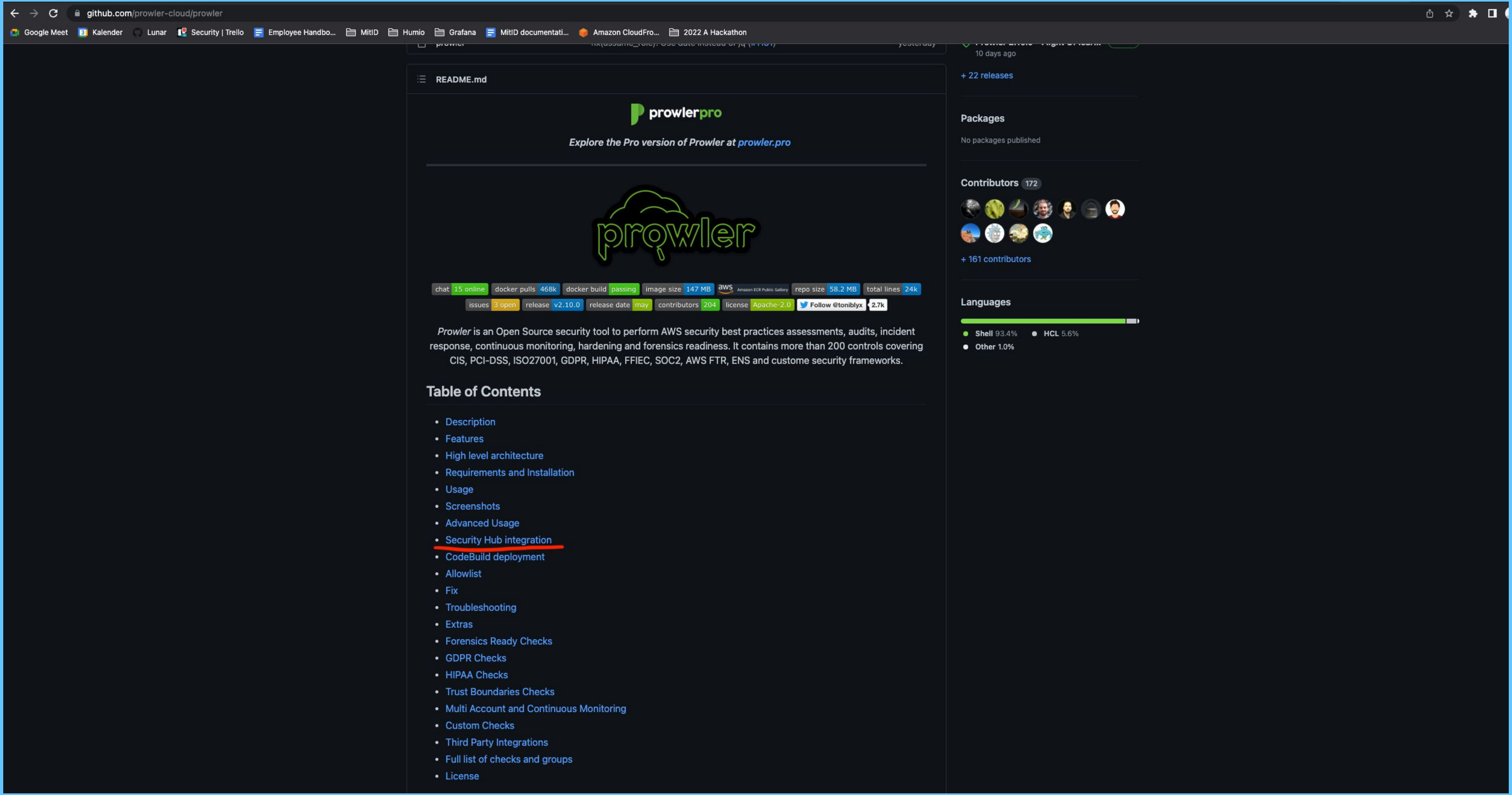
The whole is greater than the sum of the parts

How it works

- Codebuild executes "some scanner"
- Scanning results are processed to ASFF
- Send result to AWS Security Hub

Last piece missing...

Our scanner of choice



Explore the Pro version of Prowler at prowler.pro

Prowler is an Open Source security tool to perform AWS security best practices assessments, audits, incident response, continuous monitoring, hardening and forensics readiness. It contains more than 200 controls covering CIS, PCI-DSS, ISO27001, GDPR, HIPAA, FFIEC, SOC2, AWS FTR, ENS and custome security frameworks.

Table of Contents

- Description
- Features
- High level architecture
- Requirements and Installation
- Usage
- Screenshots
- Advanced Usage
- Security Hub integration
- CodeBuild deployment
- Allowlist
- Fix
- Troubleshooting
- Extras
- Forensics Ready Checks
- GDPR Checks
- HIPAA Checks
- Trust Boundaries Checks
- Multi Account and Continuous Monitoring
- Custom Checks
- Third Party Integrations
- Full list of checks and groups
- License

Packages

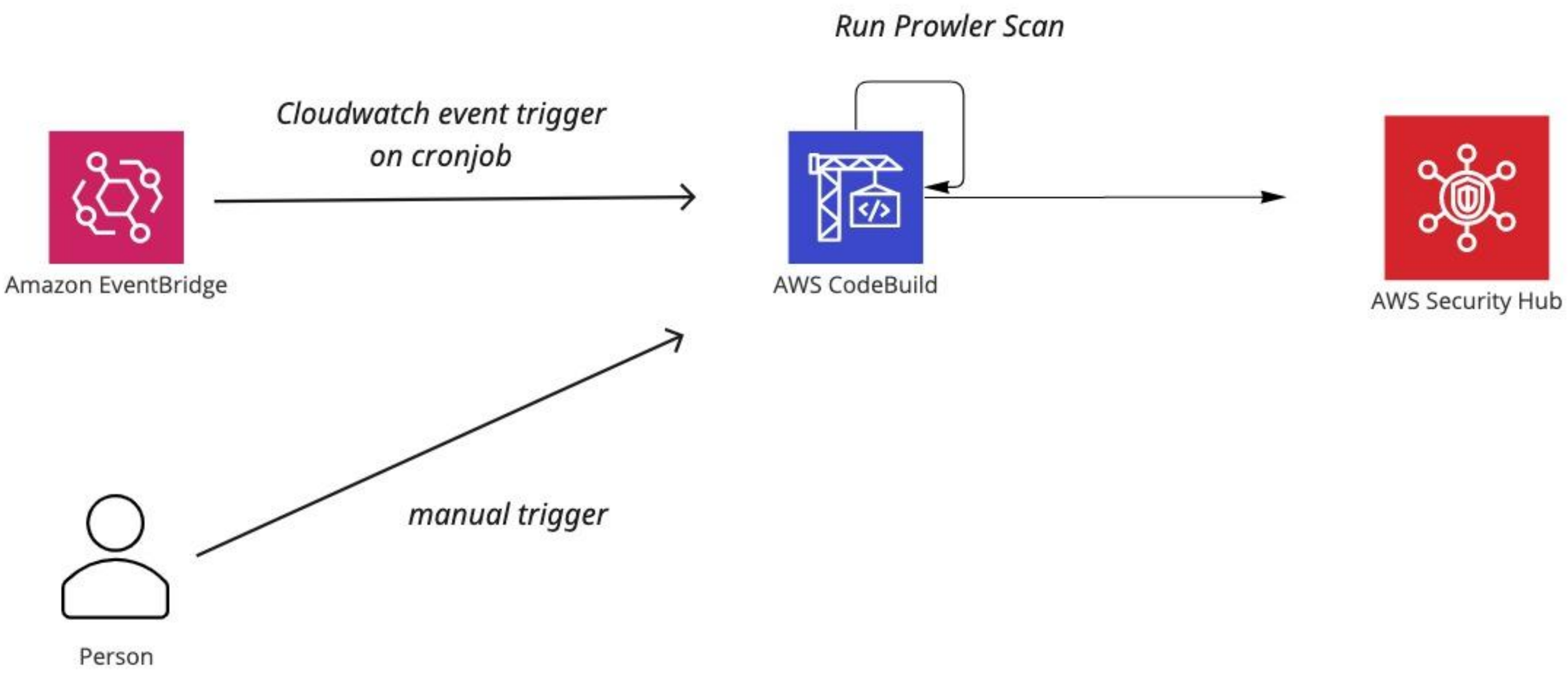
No packages published

Contributors 172

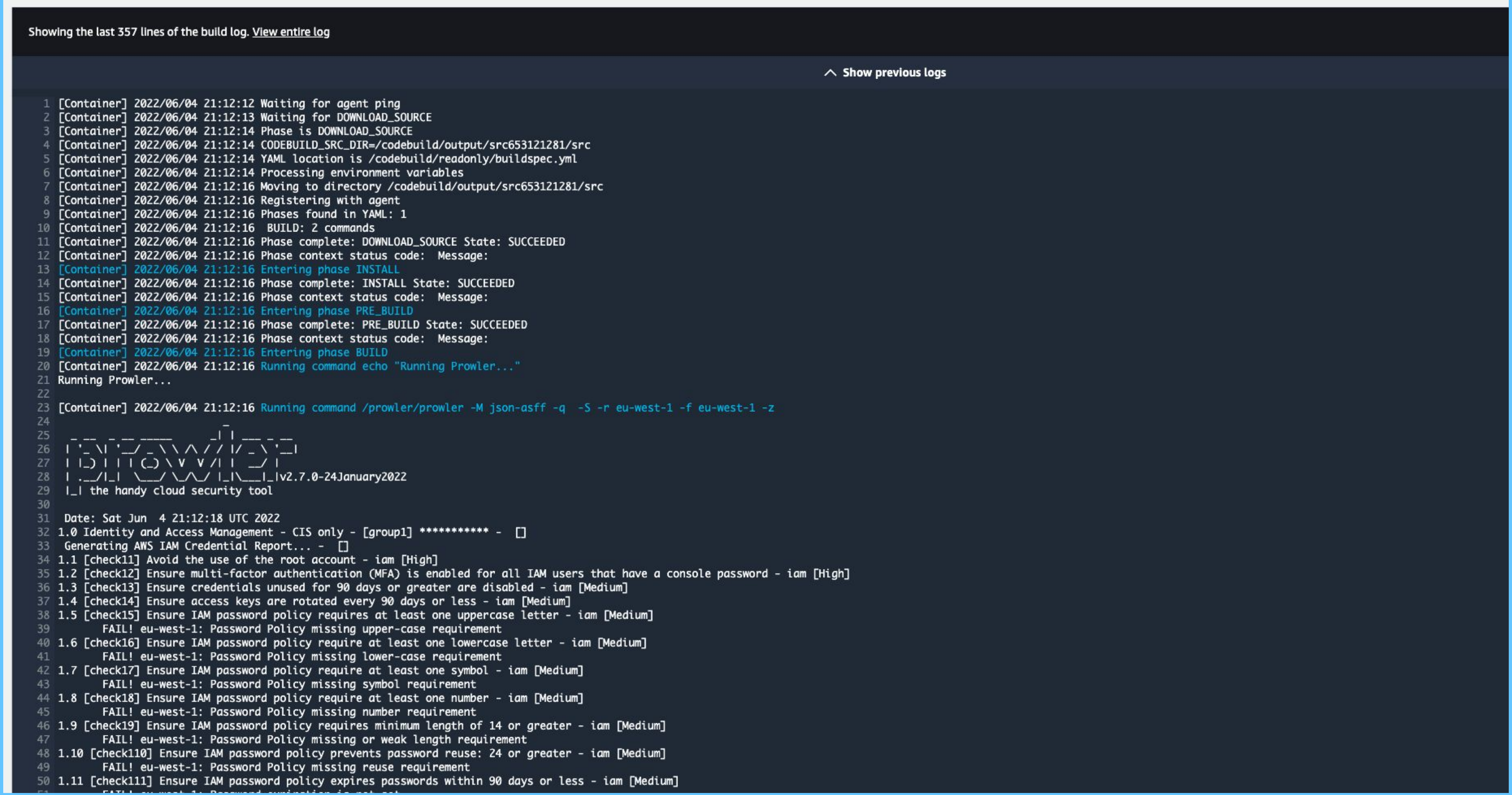
+ 161 contributors

Languages

- Shell 93.4%
- HCL 5.6%
- Other 1.0%


Run Prowler Scan
Cloudwatch event trigger
on cronjob
Amazon EventBridge
AWS CodeBuild
AWS Security Hub
manual trigger
Person

The result

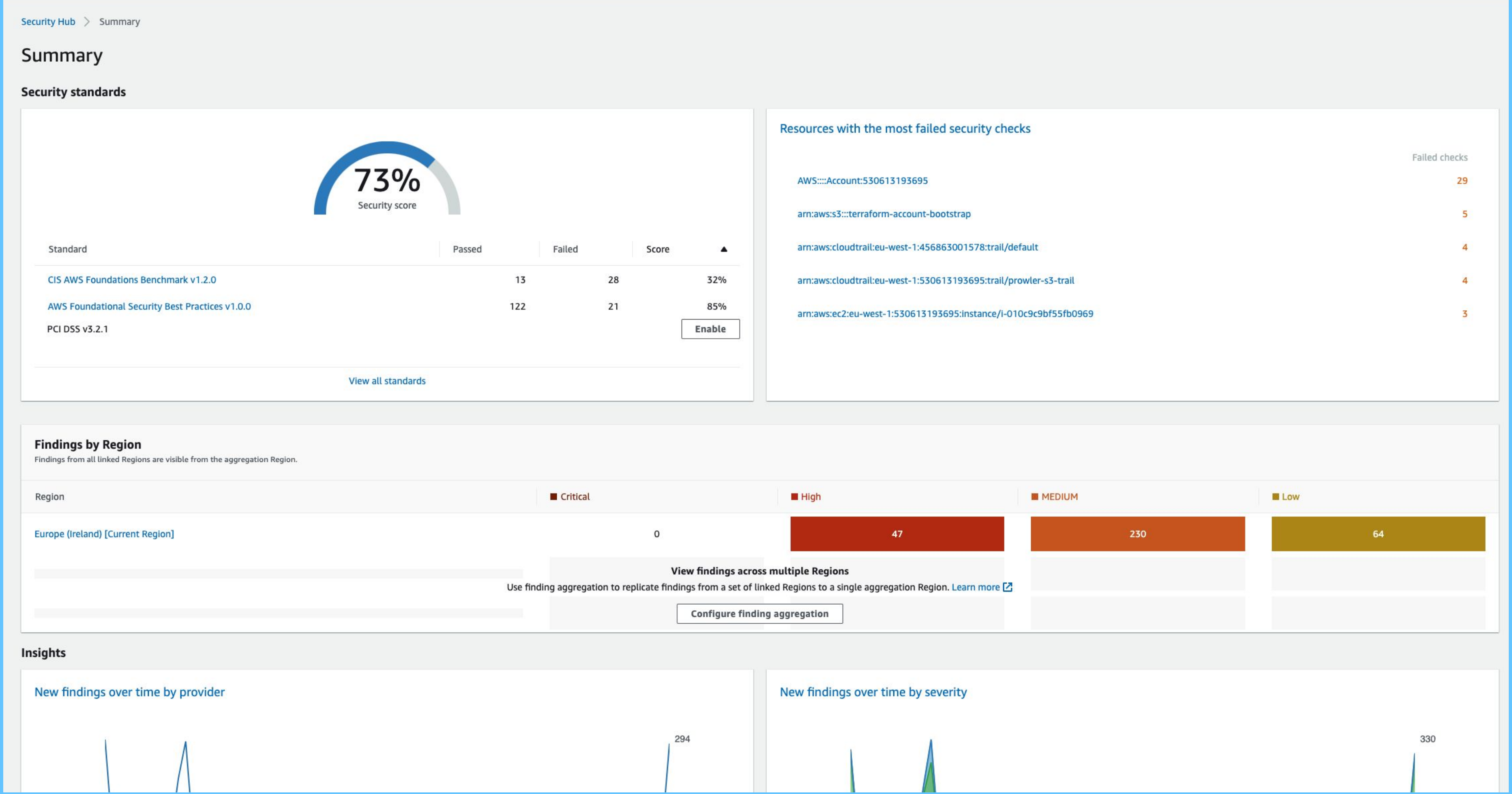


Showing the last 357 lines of the build log. View entire log

```
[Container] 2022/06/04 21:12:12 Waiting for agent ping
[Container] 2022/06/04 21:12:13 Waiting for DOWNLOAD_SOURCE
[Container] 2022/06/04 21:12:14 Phase is DOWNLOAD_SOURCE
[Container] 2022/06/04 21:12:14 CODEBUILD_SRC_DIR=/codebuild/output/src653121281/src
[Container] 2022/06/04 21:12:14 YAML location is /codebuild/readonly/buildspec.yml
[Container] 2022/06/04 21:12:14 Processing environment variables
[Container] 2022/06/04 21:12:16 Moving to directory /codebuild/output/src653121281/src
[Container] 2022/06/04 21:12:16 Registering with agent
[Container] 2022/06/04 21:12:16 Phases found in YAML: 1
[Container] 2022/06/04 21:12:16  BUILD: 2 commands
[Container] 2022/06/04 21:12:16 Phase complete: DOWNLOAD_SOURCE State: SUCCEEDED
[Container] 2022/06/04 21:12:16 Phase context status code:  Message:
[Container] 2022/06/04 21:12:16 Entering phase INSTALL
[Container] 2022/06/04 21:12:16 Phase complete: INSTALL State: SUCCEEDED
[Container] 2022/06/04 21:12:16 Phase context status code:  Message:
[Container] 2022/06/04 21:12:16 Entering phase PRE_BUILD
[Container] 2022/06/04 21:12:16 Phase complete: PRE_BUILD State: SUCCEEDED
[Container] 2022/06/04 21:12:16 Phase context status code:  Message:
[Container] 2022/06/04 21:12:16 Entering phase BUILD
[Container] 2022/06/04 21:12:16 Running command echo "Running Prowler..."
Running Prowler...

[Container] 2022/06/04 21:12:16 Running command /prowler/prowler -M json-asff -q  -S -r eu-west-1 -f eu-west-1 -z
                          _
  _ __  _ __ _____      _| | ___ _ __
 | '_ \| '__/ _ \ \ /\ / / |/ _ \ '__|
 | |_) | | | (_) \ V  V /| |  __/ |
 | .__/|_|  \___/ \_/\_/ |_|\___|_|v2.7.0-24January2022
 |_| the handy cloud security tool

 Date: Sat Jun  4 21:12:18 UTC 2022
1.0 Identity and Access Management - CIS only - [group1] *********** -  □
 Generating AWS IAM Credential Report... -  □
1.1 [check11] Avoid the use of the root account - iam [High]
1.2 [check12] Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password - iam [High]
1.3 [check13] Ensure credentials unused for 90 days or greater are disabled - iam [Medium]
1.4 [check14] Ensure access keys are rotated every 90 days or less - iam [Medium]
1.5 [check15] Ensure IAM password policy requires at least one uppercase letter - iam [Medium]
       FAIL! eu-west-1: Password Policy missing upper-case requirement
1.6 [check16] Ensure IAM password policy require at least one lowercase letter - iam [Medium]
       FAIL! eu-west-1: Password Policy missing lower-case requirement
1.7 [check17] Ensure IAM password policy require at least one symbol - iam [Medium]
       FAIL! eu-west-1: Password Policy missing symbol requirement
1.8 [check18] Ensure IAM password policy require at least one number - iam [Medium]
       FAIL! eu-west-1: Password Policy missing number requirement
1.9 [check19] Ensure IAM password policy requires minimum length of 14 or greater - iam [Medium]
       FAIL! eu-west-1: Password Policy missing or weak length requirement
1.10 [check110] Ensure IAM password policy prevents password reuse: 24 or greater - iam [Medium]
       FAIL! eu-west-1: Password Policy missing reuse requirement
1.11 [check111] Ensure IAM password policy expires passwords within 90 days or less - iam [Medium]
       FAIL! eu-west-1: Password expiration is not set
```



Security Hub > Summary

Summary

Security standards

73%
Security score

Standard	Passed	Failed	Score ▲
CIS AWS Foundations Benchmark v1.2.0	13	28	32%
AWS Foundational Security Best Practices v1.0.0	122	21	85%
PCI DSS v3.2.1			Enable

View all standards

Resources with the most failed security checks

	Failed checks
AWS::::Account:530613193695	29
arn:aws:s3:::terraform-account-bootstrap	5
arn:aws:cloudtrail:eu-west-1:456863001578:trail/default	4
arn:aws:cloudtrail:eu-west-1:530613193695:trail/prowler-s3-trail	4
arn:aws:ec2:eu-west-1:530613193695:instance/i-010c9c9bf55fb0969	3

Findings by Region

Findings from all linked Regions are visible from the aggregation Region.

Region	■ Critical	■ High	■ MEDIUM	■ Low
Europe (Ireland) [Current Region]	0	47	230	64

View findings across multiple Regions

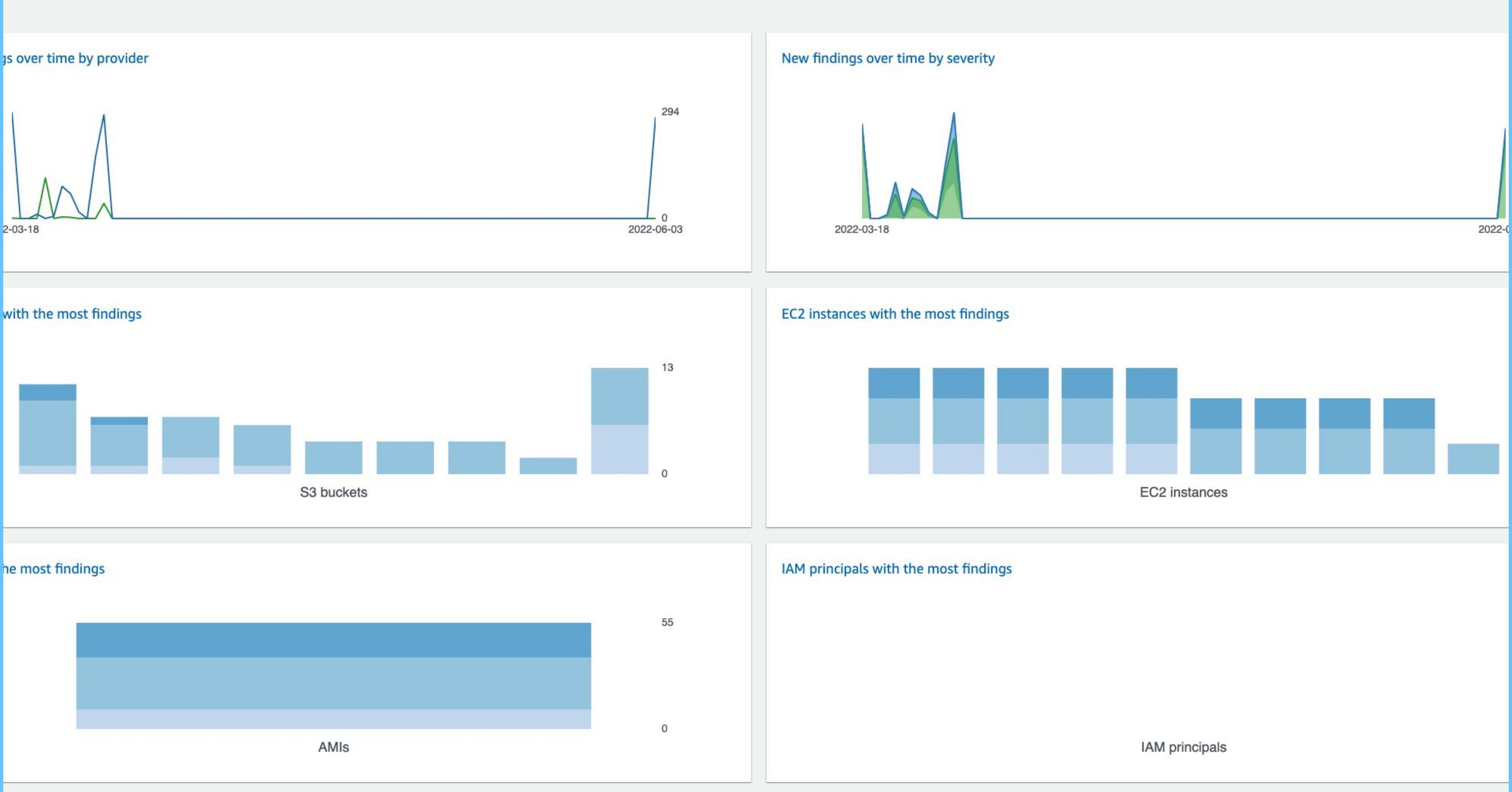
Use finding aggregation to replicate findings from a set of linked Regions to a single aggregation Region. Learn more

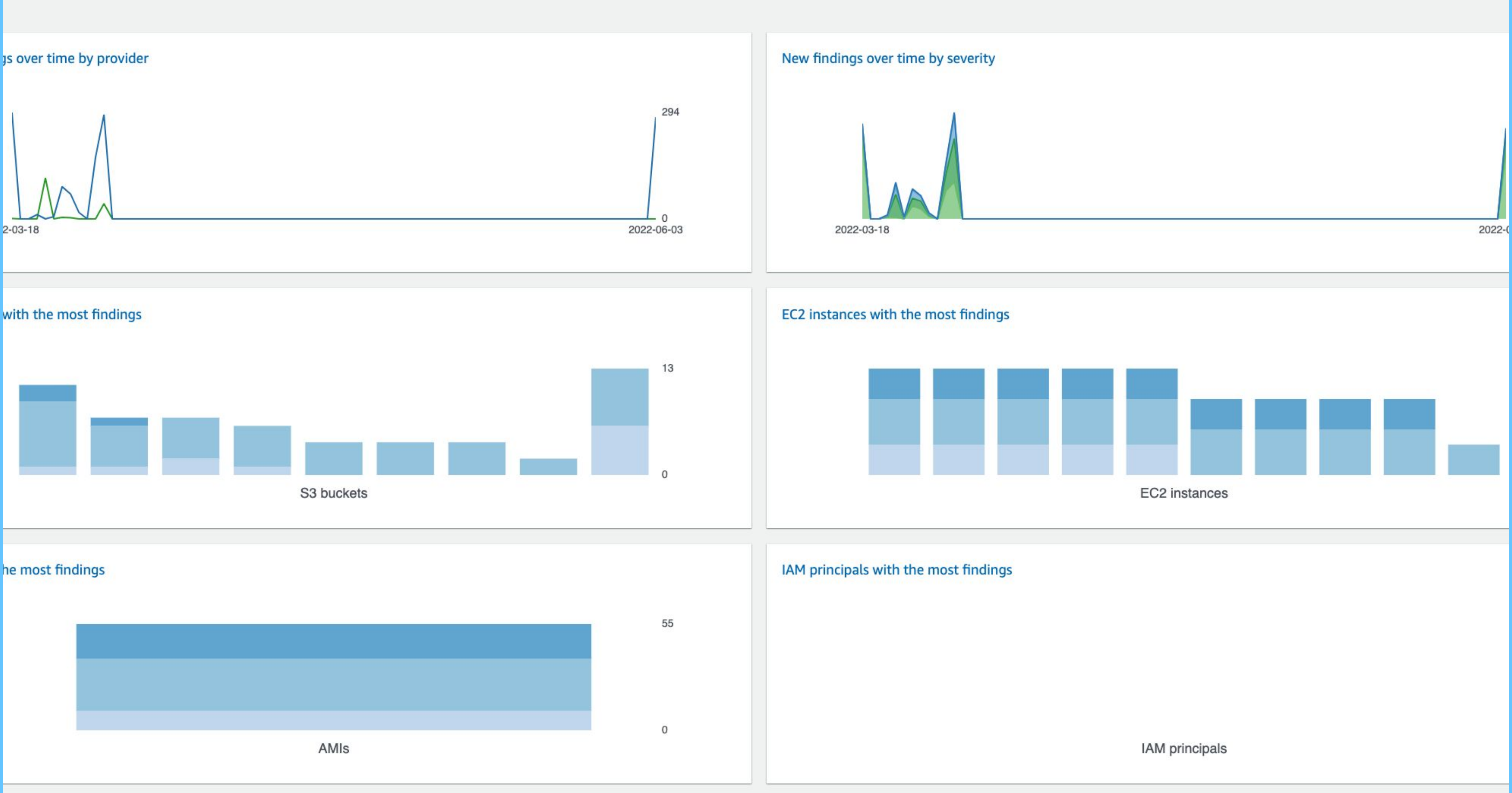
Configure finding aggregation

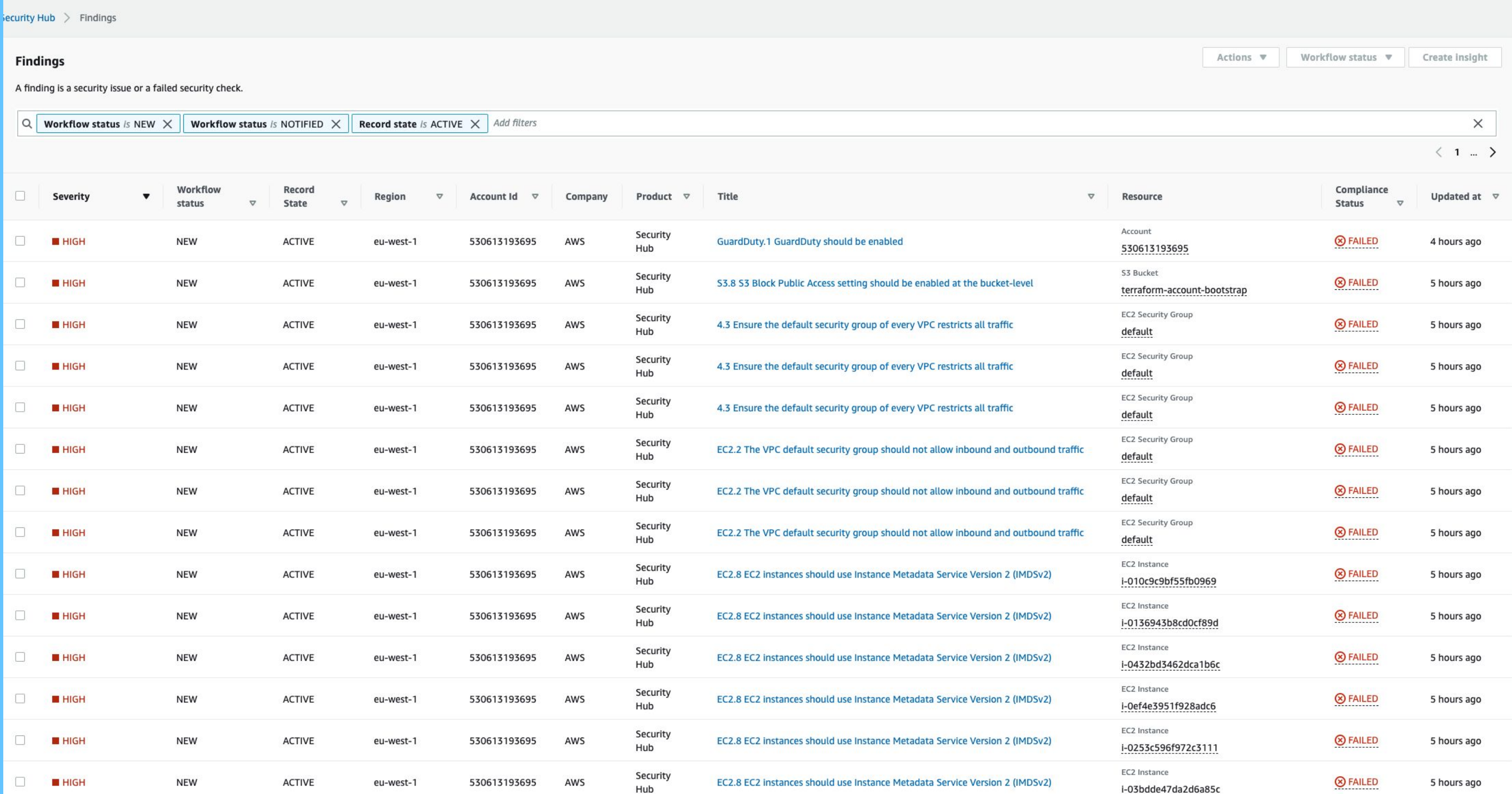
Insights

New findings over time by provider

New findings over time by severity


gs over time by provider
294
0
2-03-18
2022-06-03
New findings over time by severity
2022-03-18
2022-0
with the most findings
13
0
S3 buckets
EC2 instances with the most findings
EC2 instances
he most findings
55
0
AMIs
IAM principals with the most findings
IAM principals


gs over time by provider
294
0
2-03-18
2022-06-03
New findings over time by severity
2022-03-18
2022-0
with the most findings
13
0
S3 buckets
EC2 instances with the most findings
EC2 instances
he most findings
55
0
AMIs
IAM principals with the most findings
IAM principals

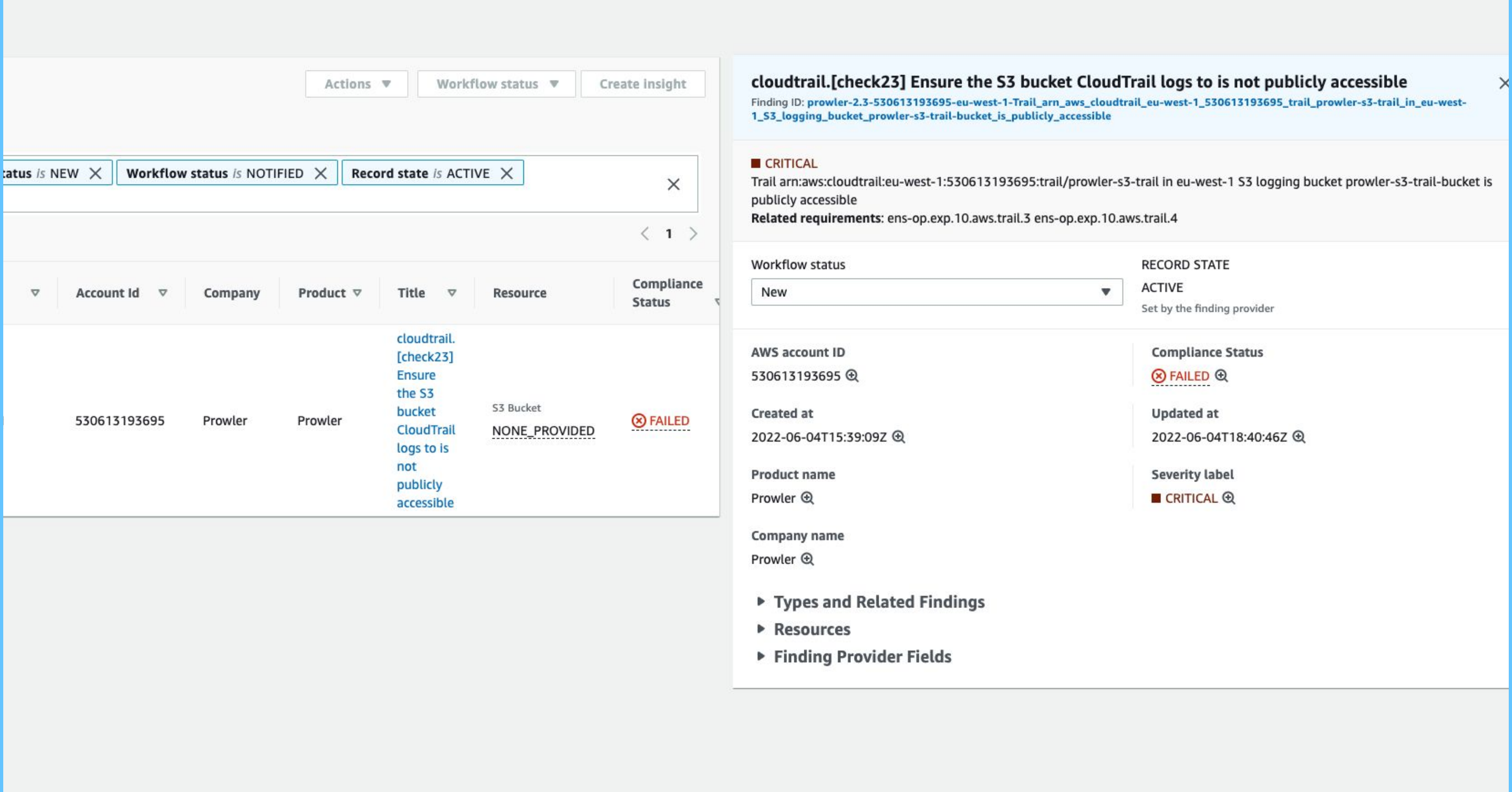


Findings

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	Region	Account Id	Company	Product	Title	Resource	Compliance Status	Updated at
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	GuardDuty.1 GuardDuty should be enabled	Account 530613193695	⊗ FAILED	4 hours ago
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	S3.8 S3 Block Public Access setting should be enabled at the bucket-level	S3 Bucket terraform-account-bootstrap	⊗ FAILED	5 hours ago
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	4.3 Ensure the default security group of every VPC restricts all traffic	EC2 Security Group default	⊗ FAILED	5 hours ago
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	4.3 Ensure the default security group of every VPC restricts all traffic	EC2 Security Group default	⊗ FAILED	5 hours ago
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	4.3 Ensure the default security group of every VPC restricts all traffic	EC2 Security Group default	⊗ FAILED	5 hours ago
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	EC2.2 The VPC default security group should not allow inbound and outbound traffic	EC2 Security Group default	⊗ FAILED	5 hours ago
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	EC2.2 The VPC default security group should not allow inbound and outbound traffic	EC2 Security Group default	⊗ FAILED	5 hours ago
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	EC2.2 The VPC default security group should not allow inbound and outbound traffic	EC2 Security Group default	⊗ FAILED	5 hours ago
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	EC2.8 EC2 instances should use Instance Metadata Service Version 2 (IMDSv2)	EC2 Instance i-010c9c9bf55fb0969	⊗ FAILED	5 hours ago
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	EC2.8 EC2 instances should use Instance Metadata Service Version 2 (IMDSv2)	EC2 Instance i-0136943b8cd0cf89d	⊗ FAILED	5 hours ago
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	EC2.8 EC2 instances should use Instance Metadata Service Version 2 (IMDSv2)	EC2 Instance i-0432bd3462dca1b6c	⊗ FAILED	5 hours ago
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	EC2.8 EC2 instances should use Instance Metadata Service Version 2 (IMDSv2)	EC2 Instance i-0ef4e3951f928adc6	⊗ FAILED	5 hours ago
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	EC2.8 EC2 instances should use Instance Metadata Service Version 2 (IMDSv2)	EC2 Instance i-0253c596f972c3111	⊗ FAILED	5 hours ago
□	HIGH	NEW	ACTIVE	eu-west-1	530613193695	AWS	Security Hub	EC2.8 EC2 instances should use Instance Metadata Service Version 2 (IMDSv2)	EC2 Instance i-03bdde47da2d6a85c	⊗ FAILED	5 hours ago



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

	Account Id	Company	Product	Title	Resource	Compliance Status
	530613193695	Prowler	Prowler	cloudtrail.[check23] Ensure the S3 bucket CloudTrail logs to is not publicly accessible	S3 Bucket NONE_PROVIDED	⊗ FAILED

cloudtrail.[check23] Ensure the S3 bucket CloudTrail logs to is not publicly accessible

Finding ID: prowler-2.3-530613193695-eu-west-1-Trail_arn_aws_cloudtrail_eu-west-1_530613193695_trail_prowler-s3-trail_in_eu-west-1_S3_logging_bucket_prowler-s3-trail-bucket_is_publicly_accessible

■ CRITICAL

Trail arn:aws:cloudtrail:eu-west-1:530613193695:trail/prowler-s3-trail in eu-west-1 S3 logging bucket prowler-s3-trail-bucket is publicly accessible

Related requirements: ens-op.exp.10.aws.trail.3 ens-op.exp.10.aws.trail.4

Workflow status: New ▼

RECORD STATE: ACTIVE
Set by the finding provider

AWS account ID: 530613193695

Compliance Status: ⊗ FAILED

Created at: 2022-06-04T15:39:09Z

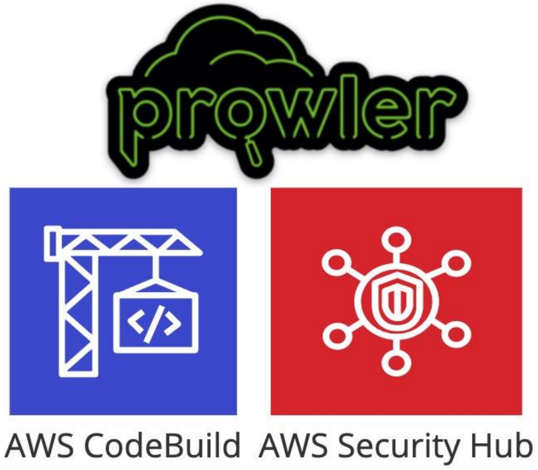
Updated at: 2022-06-04T18:40:46Z

Product name: Prowler

Severity label: ■ CRITICAL

Company name: Prowler

That was the story so far



Next steps

- Generalize the setup to run "any scanner" and send the result to SH
- Run the setup in a Security Account, assuming a role in other accounts
- Security Hubs from various accounts sent to a singular account
- Figure out the "workflow" of working with the findings.

  (this will most likely involve notifications in slack)

THAT’S ALL FOLKS

QUESTIONS?

Morten Z. Christensen

LUNAR®

LUNAR®