SIGConnect 365

Keeping you connected to the world of Higher Education

Achieving Continuous Cybersecurity Compliance in AWS

PRESENTED BY:

Gabriel Tocci

Housekeeping

All participants are automatically muted by webinar administrators.

Please use the Q&A section to submit questions.

Webinar will be recorded for future use.

▶ **Strata Information Group**

Meet the Presenter

Gabriel Tocci

Sr. Cloud Architect / Sr. Consultant

Senior cloud architect with deep expertise in Amazon Web Services (AWS), Oracle Cloud (OCI), Kubernetes (K8s), Infrastructure as Code (IaC), and various HigherEd enterprise systems.

Been working in Higher Education for two decades finding new ways to leverage these technologies so colleges and universities can focus on their mission of improving student success/outcomes.

An AWS user since 2012 and running production Enterprise systems in AWS since 2016.

AGENDA

01 AWS Security Services Summary

02 AWS Security Hub

03 Finding Data

04 Security Hub Events

05 AWS Audit Manager

06 Getting Started

07 Alternative Solutions (OpenSource & SaaS)

01

AWS SECURITY SERVICES

AWS Security Portfolio

Identity and Access Management

- IAM
- SSO
- Organizations

Infrastructure Protection

- Shield
- WAF
- Network Firewall
- Firewall Manager

Data Protection

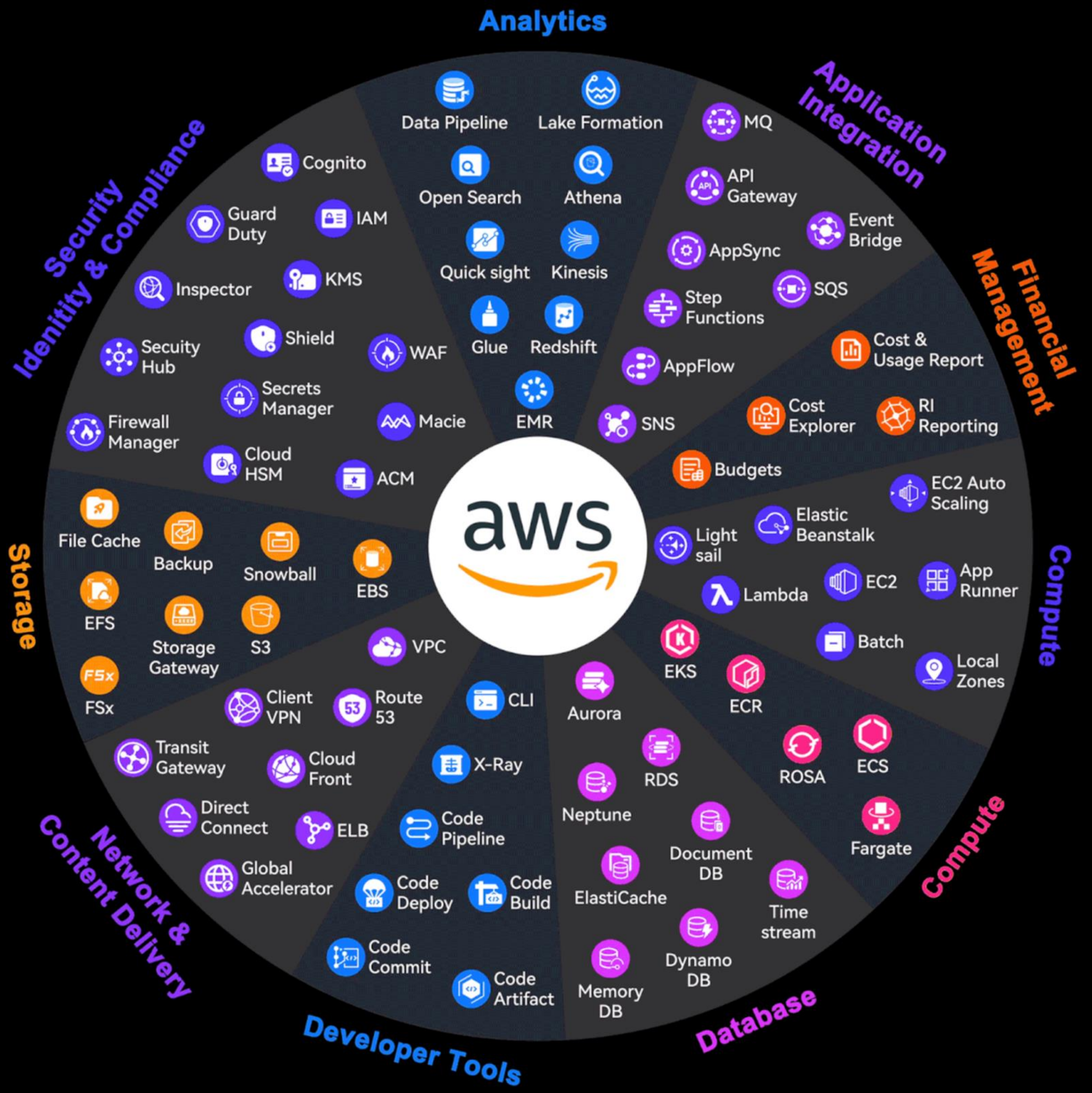
- Key Management Services
- Cloud HSM
- Macie
- Secrets Manager
- Certificates Manager

Detection & Response

- Guard Duty
- Inspector
- Detective
- Security Hub

Governance & Compliance

- Systems Manager
- Config
- Artifact
- Audit Manager



aws

Analytics

Data Pipeline
Lake Formation
Open Search
Athena
Quick sight
Kinesis
Glue
Redshift
EMR

Application Integration

MQ
API Gateway
Event Bridge
AppSync
SQS
Step Functions
AppFlow
SNS

Financial Management

Cost & Usage Report
Cost Explorer
RI Reporting
Budgets

Compute

EC2 Auto Scaling
Elastic Beanstalk
Light sail
EC2
App Runner
Lambda
Batch
Local Zones

Compute

EKS
ECR
ROSA
ECS
Fargate

Database

Aurora
RDS
Neptune
Document DB
ElastiCache
Time stream
Dynamo DB
Memory DB

Developer Tools

CLI
X-Ray
Code Pipeline
Code Deploy
Code Build
Code Commit
Code Artifact

Network & Content Delivery

VPC
Client VPN
Route 53
Transit Gateway
Cloud Front
Direct Connect
ELB
Global Accelerator

Storage

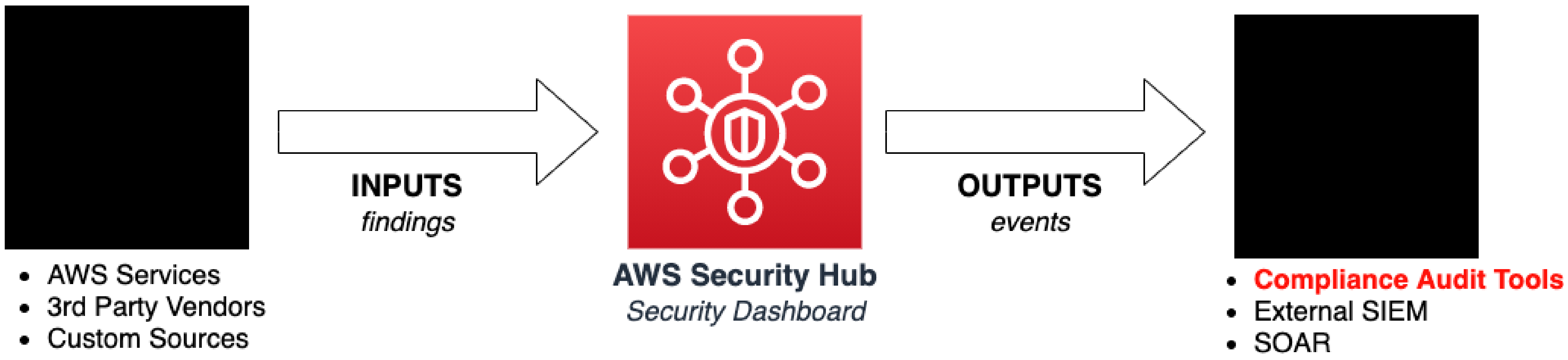
File Cache
Backup
Snowball
EBS
EFS
Storage Gateway
S3
FSx

Security Identity & Compliance

Cognito
Guard Duty
IAM
Inspector
KMS
Secuity Hub
Shield
WAF
Secrets Manager
Firewall Manager
Macie
Cloud HSM
ACM

02

AWS SECURITY HUB



[redacted]

- AWS Services
- 3rd Party Vendors
- Custom Sources

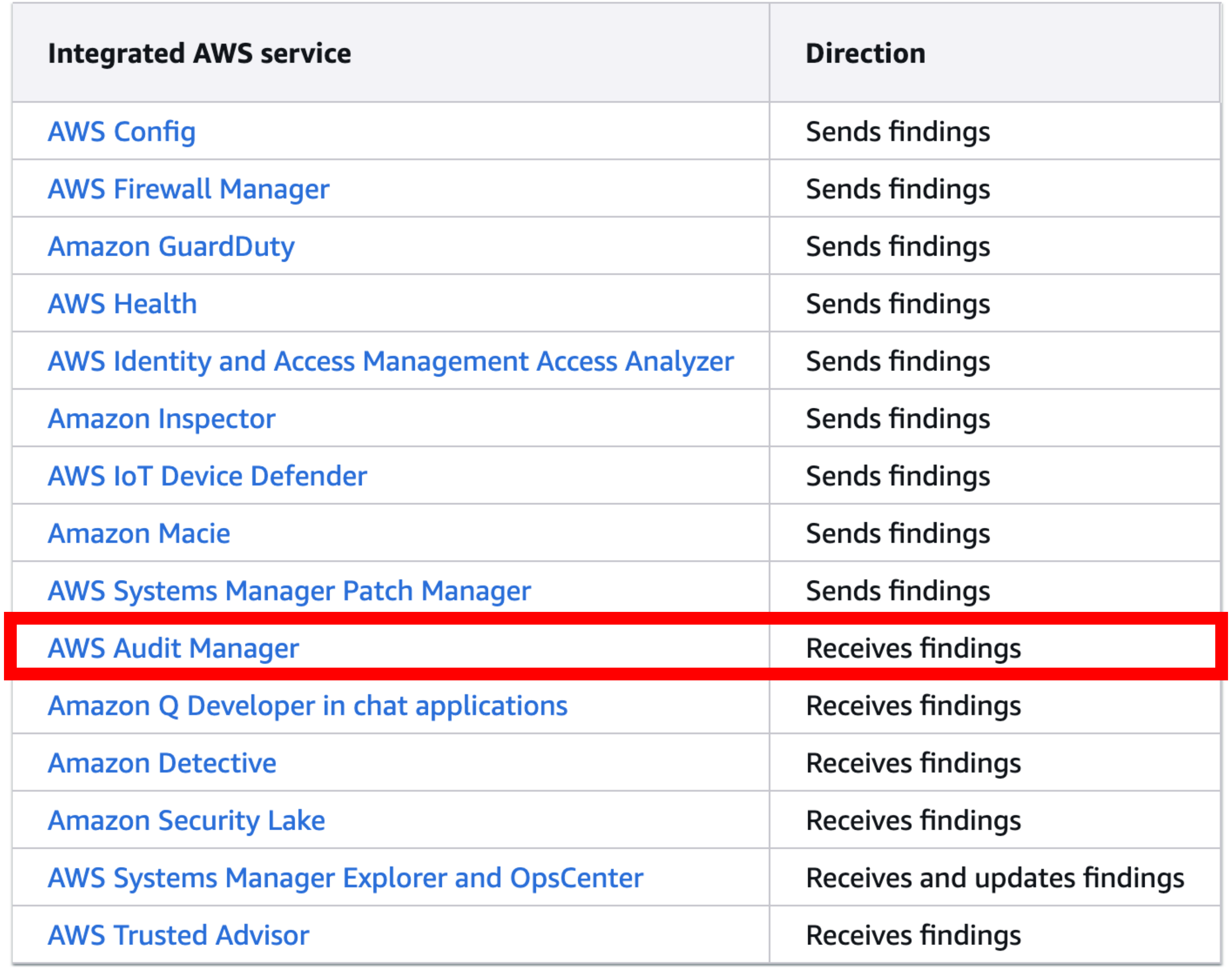
INPUTS
findings

AWS Security Hub
Security Dashboard

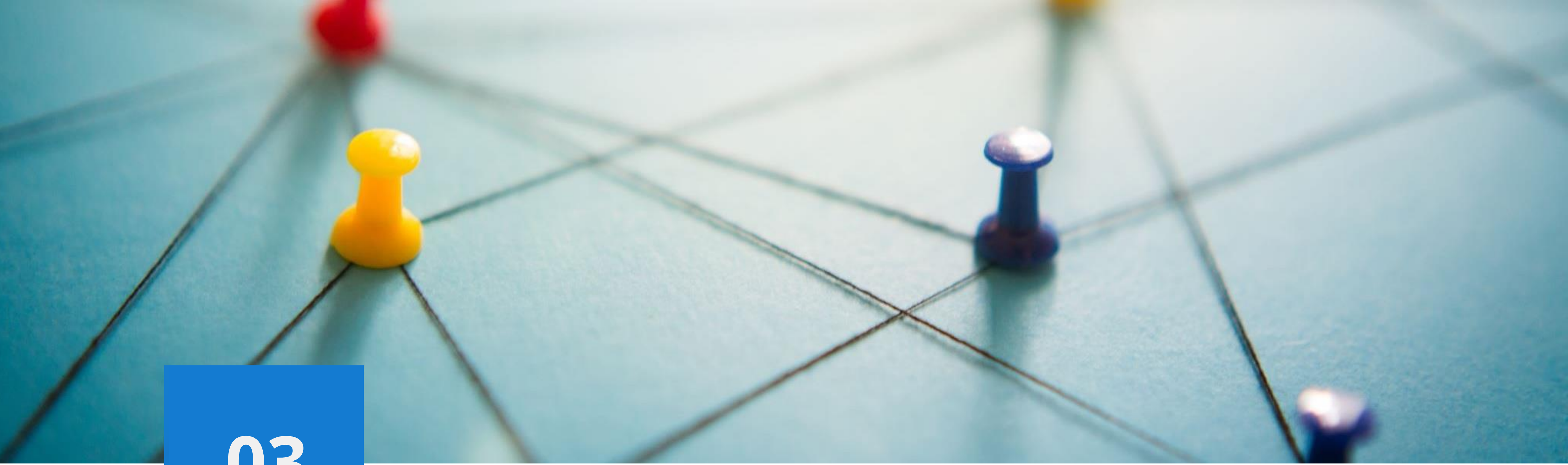
OUTPUTS
events

[redacted]

- **Compliance Audit Tools**
- External SIEM
- SOAR

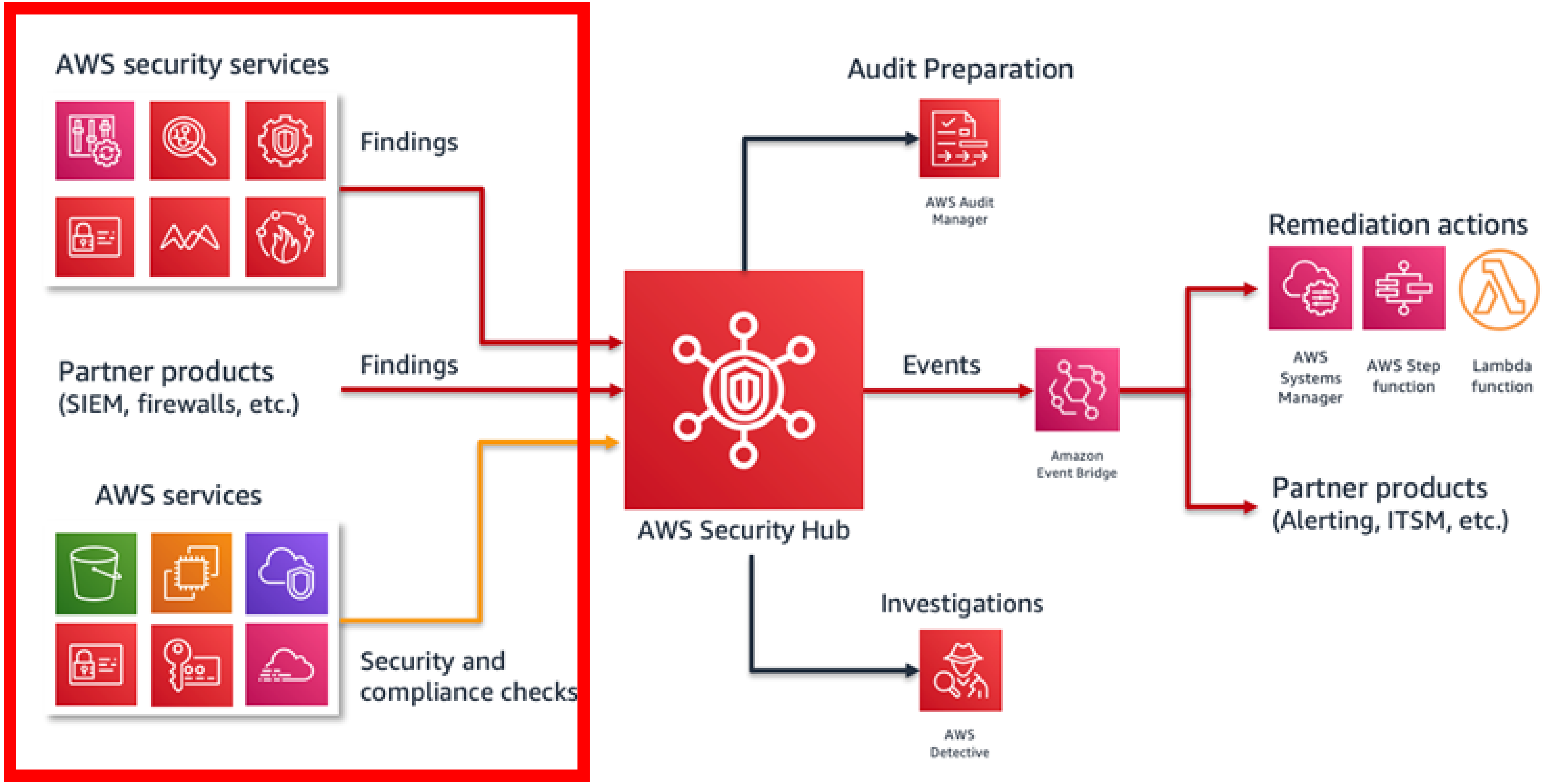


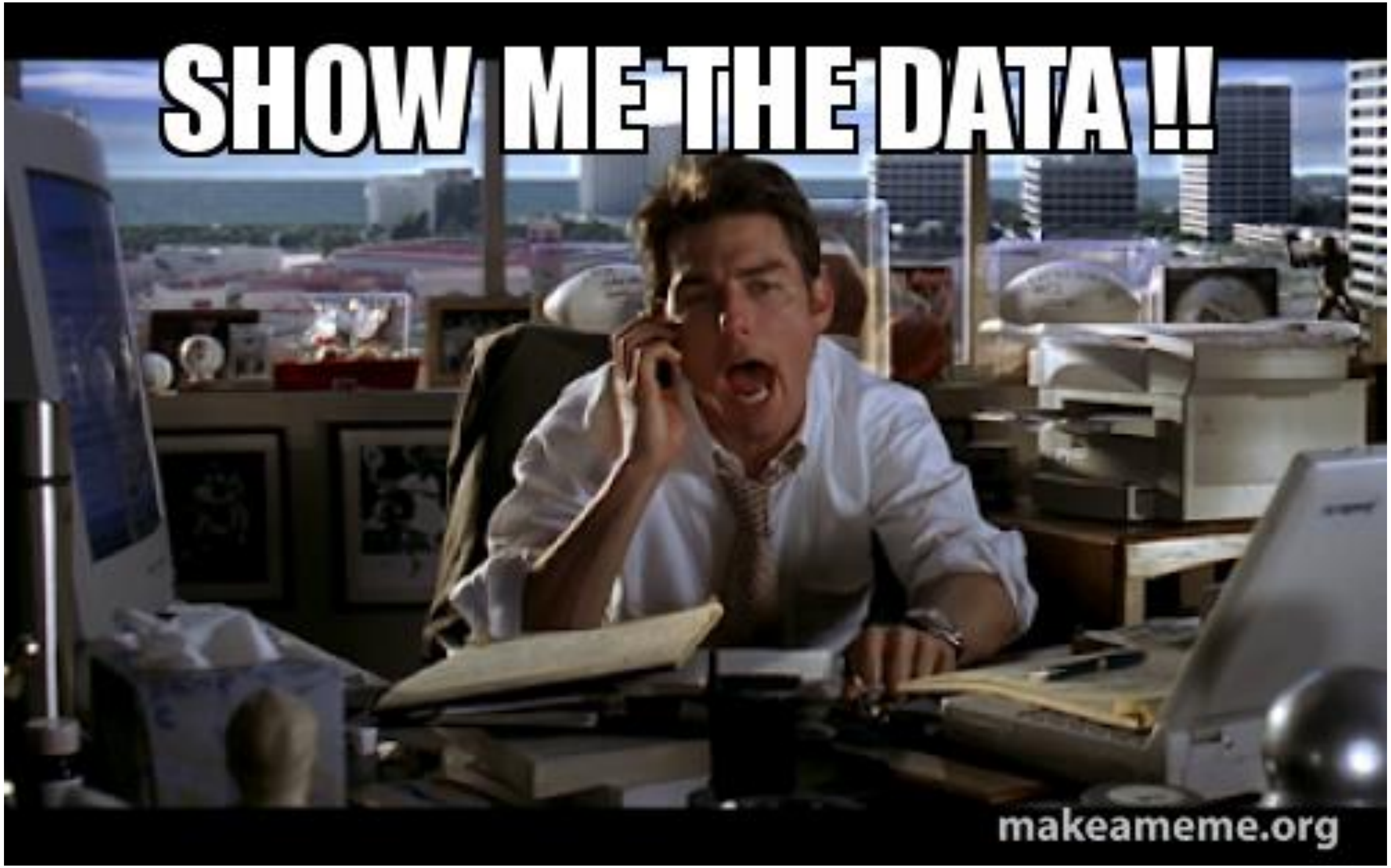
Integrated AWS service	Direction
AWS Config	Sends findings
AWS Firewall Manager	Sends findings
Amazon GuardDuty	Sends findings
AWS Health	Sends findings
AWS Identity and Access Management Access Analyzer	Sends findings
Amazon Inspector	Sends findings
AWS IoT Device Defender	Sends findings
Amazon Macie	Sends findings
AWS Systems Manager Patch Manager	Sends findings
AWS Audit Manager	Receives findings
Amazon Q Developer in chat applications	Receives findings
Amazon Detective	Receives findings
Amazon Security Lake	Receives findings
AWS Systems Manager Explorer and OpsCenter	Receives and updates findings
AWS Trusted Advisor	Receives findings



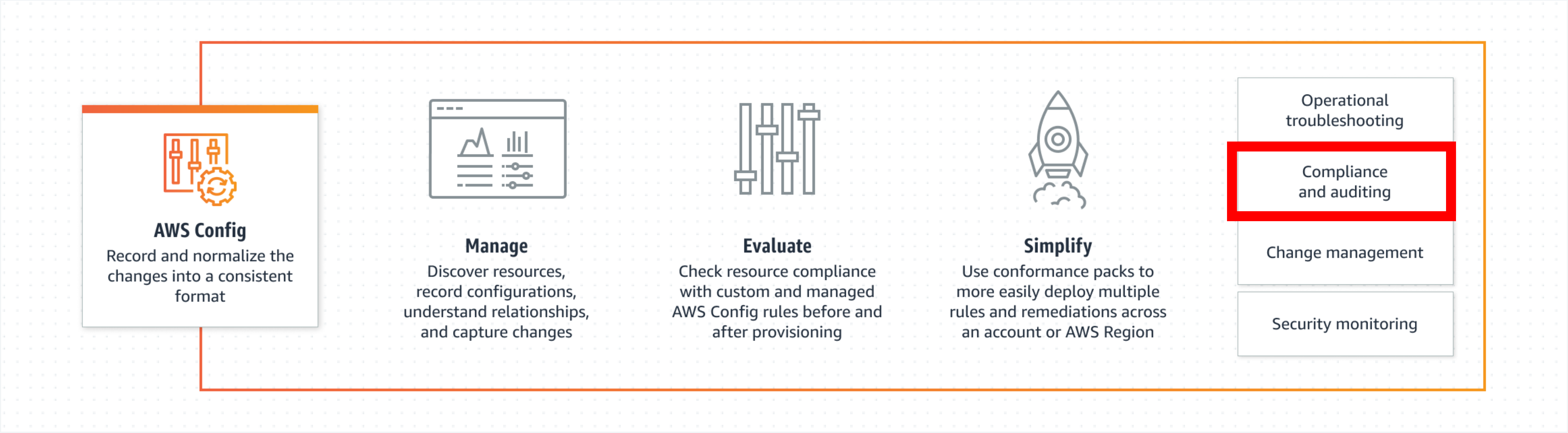
03

SECURITY FINDINGS


AWS security services
Findings
Partner products
(SIEM, firewalls, etc.)
Findings
AWS services
Security and
compliance checks
Audit Preparation
AWS Audit
Manager
AWS Security Hub
Events
Amazon
Event Bridge
Remediation actions
AWS
Systems
Manager
AWS Step
function
Lambda
function
Partner products
(Alerting, ITSM, etc.)
Investigations
AWS
Detective


SHOW ME THE DATA !!
makeameme.org

AWS Config



AWS Config
Record and normalize the changes into a consistent format

Manage
Discover resources, record configurations, understand relationships, and capture changes

Evaluate
Check resource compliance with custom and managed AWS Config rules before and after provisioning

Simplify
Use conformance packs to more easily deploy multiple rules and remediations across an account or AWS Region

Operational troubleshooting

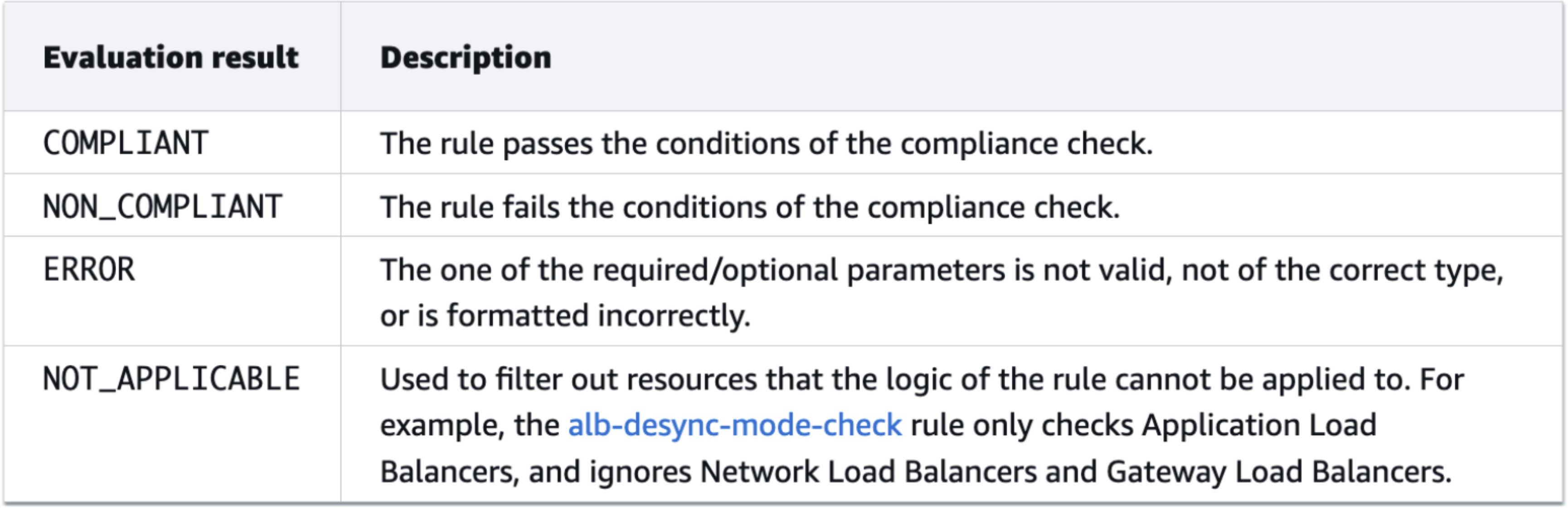
Compliance and auditing

Change management

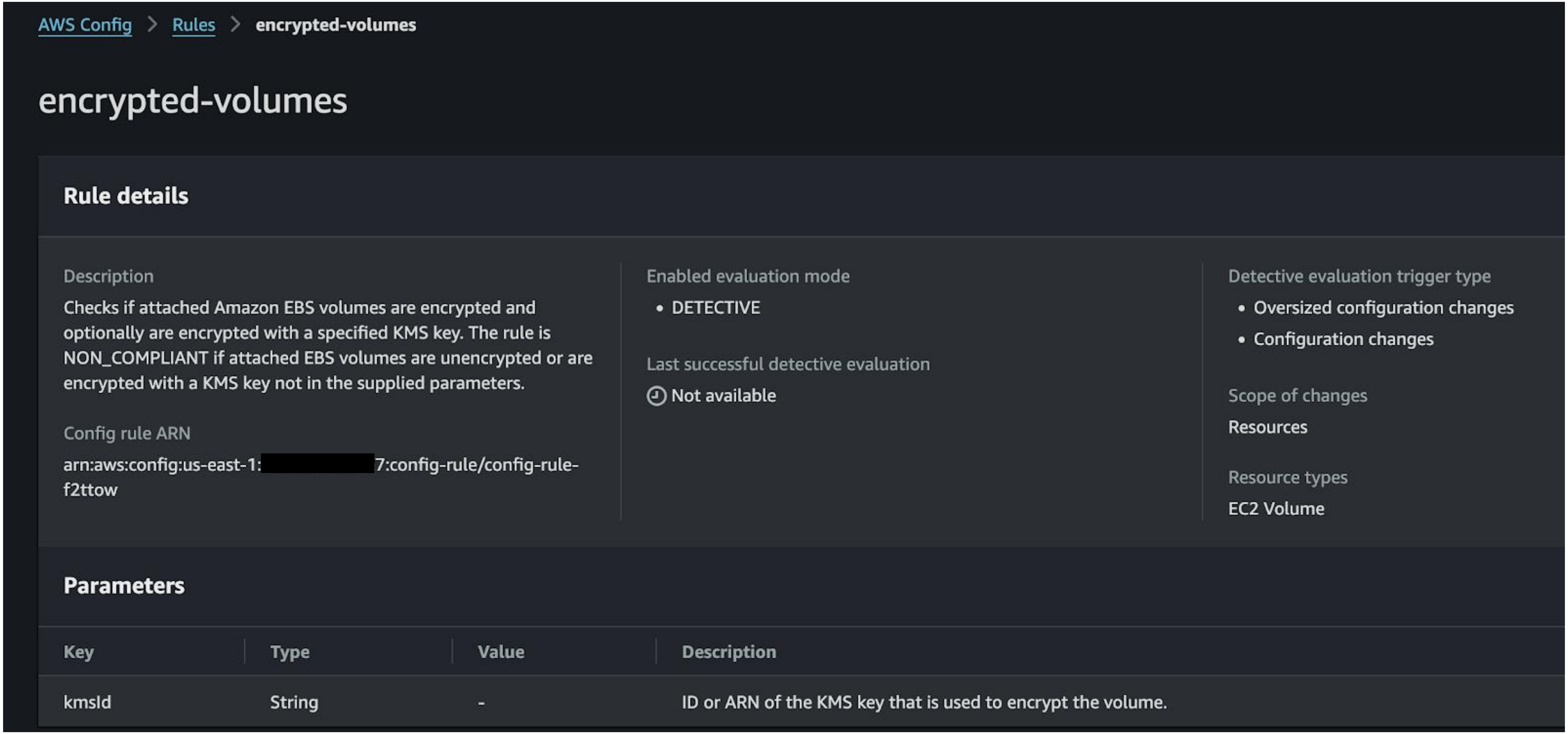
Security monitoring

AWS Config

- Findings are AWS Resource Configuration Setting Values
- Scans 300+ AWS Resource Types for Configuration Settings
- Four Possible Evaluation Results for AWS Config Rules



Evaluation result	Description
COMPLIANT	The rule passes the conditions of the compliance check.
NON_COMPLIANT	The rule fails the conditions of the compliance check.
ERROR	The one of the required/optional parameters is not valid, not of the correct type, or is formatted incorrectly.
NOT_APPLICABLE	Used to filter out resources that the logic of the rule cannot be applied to. For example, the alb-desync-mode-check rule only checks Application Load Balancers, and ignores Network Load Balancers and Gateway Load Balancers.



encrypted-volumes

Rule details

Description

Checks if attached Amazon EBS volumes are encrypted and optionally are encrypted with a specified KMS key. The rule is NON_COMPLIANT if attached EBS volumes are unencrypted or are encrypted with a KMS key not in the supplied parameters.

Config rule ARN

arn:aws:config:us-east-1:[redacted]7:config-rule/config-rule-f2ttow

Enabled evaluation mode

- DETECTIVE

Last successful detective evaluation

Not available

Detective evaluation trigger type

- Oversized configuration changes
- Configuration changes

Scope of changes

Resources

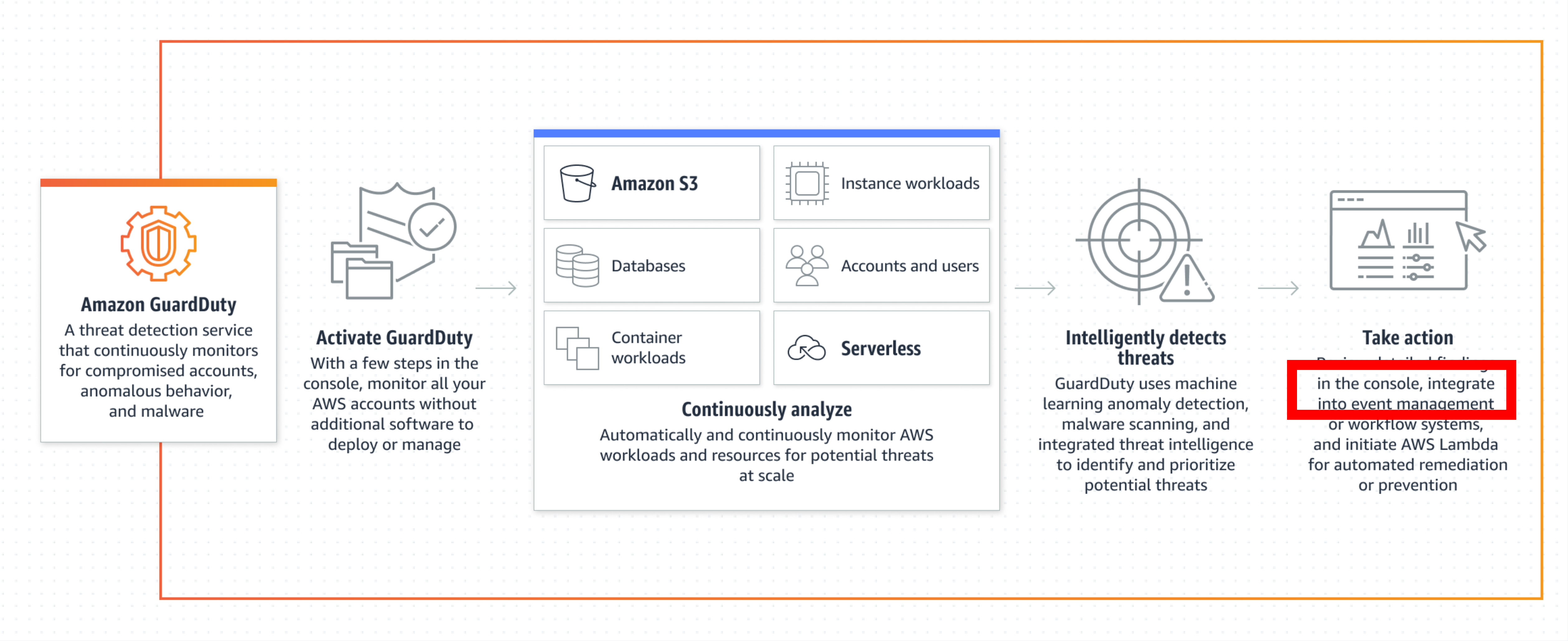
Resource types

EC2 Volume

Parameters

Key	Type	Value	Description
kmsId	String	-	ID or ARN of the KMS key that is used to encrypt the volume.

Guard Duty



Amazon GuardDuty
A threat detection service that continuously monitors for compromised accounts, anomalous behavior, and malware

Activate GuardDuty
With a few steps in the console, monitor all your AWS accounts without additional software to deploy or manage

Continuously analyze
Automatically and continuously monitor AWS workloads and resources for potential threats at scale

Intelligently detects threats
GuardDuty uses machine learning anomaly detection, malware scanning, and integrated threat intelligence to identify and prioritize potential threats

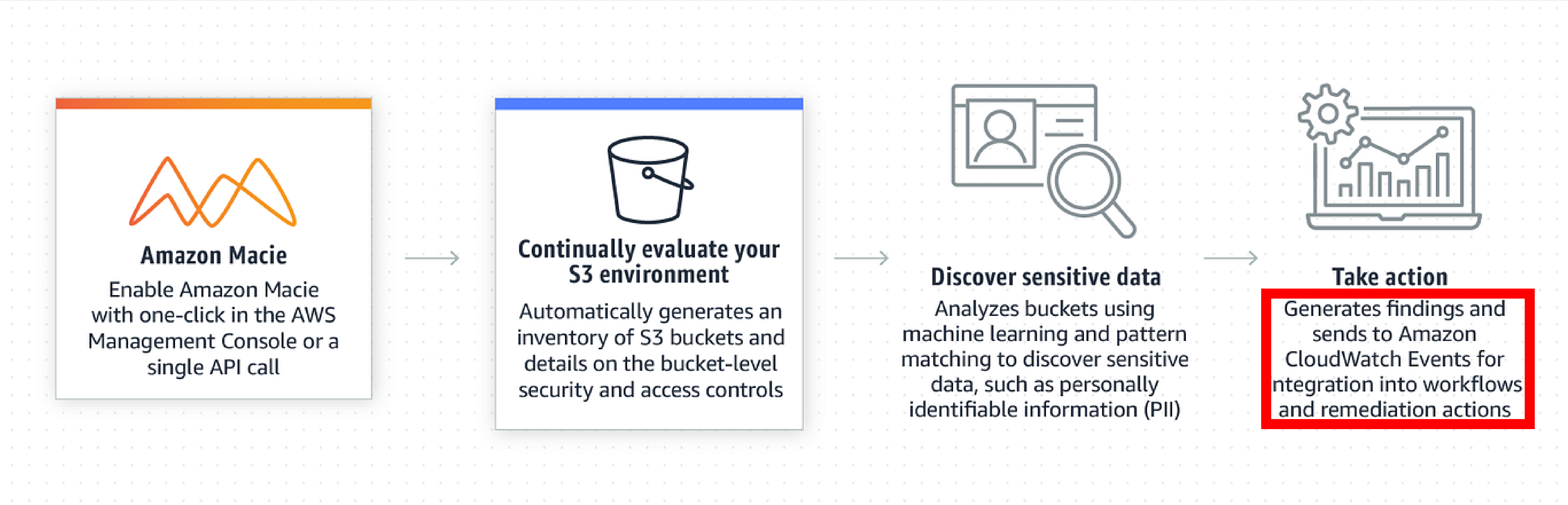
Take action
Review detailed findings in the console, integrate into event management or workflow systems, and initiate AWS Lambda for automated remediation or prevention

Guard Duty

- Findings are (potentially) Malicious Activity In
  - VPC Flow Logs
  - DNS Logs
  - CloudTrail Events
  - S3 Data Access
  - Kubernetes Clusters Audit Logs
  - RDS Database Login Activity

- Types of Findings
  - Anomalies in behavior (AWS and Network)
  - Launching New Instances
  - Changing Network Rules
  - Service/Data Access Patterns
- Types of Attacks
  - Bitcoin Mining
  - Command & Control
  - Anonymous Connections

Amazon Macie



Amazon Macie

Enable Amazon Macie with one-click in the AWS Management Console or a single API call

Continually evaluate your S3 environment

Automatically generates an inventory of S3 buckets and details on the bucket-level security and access controls

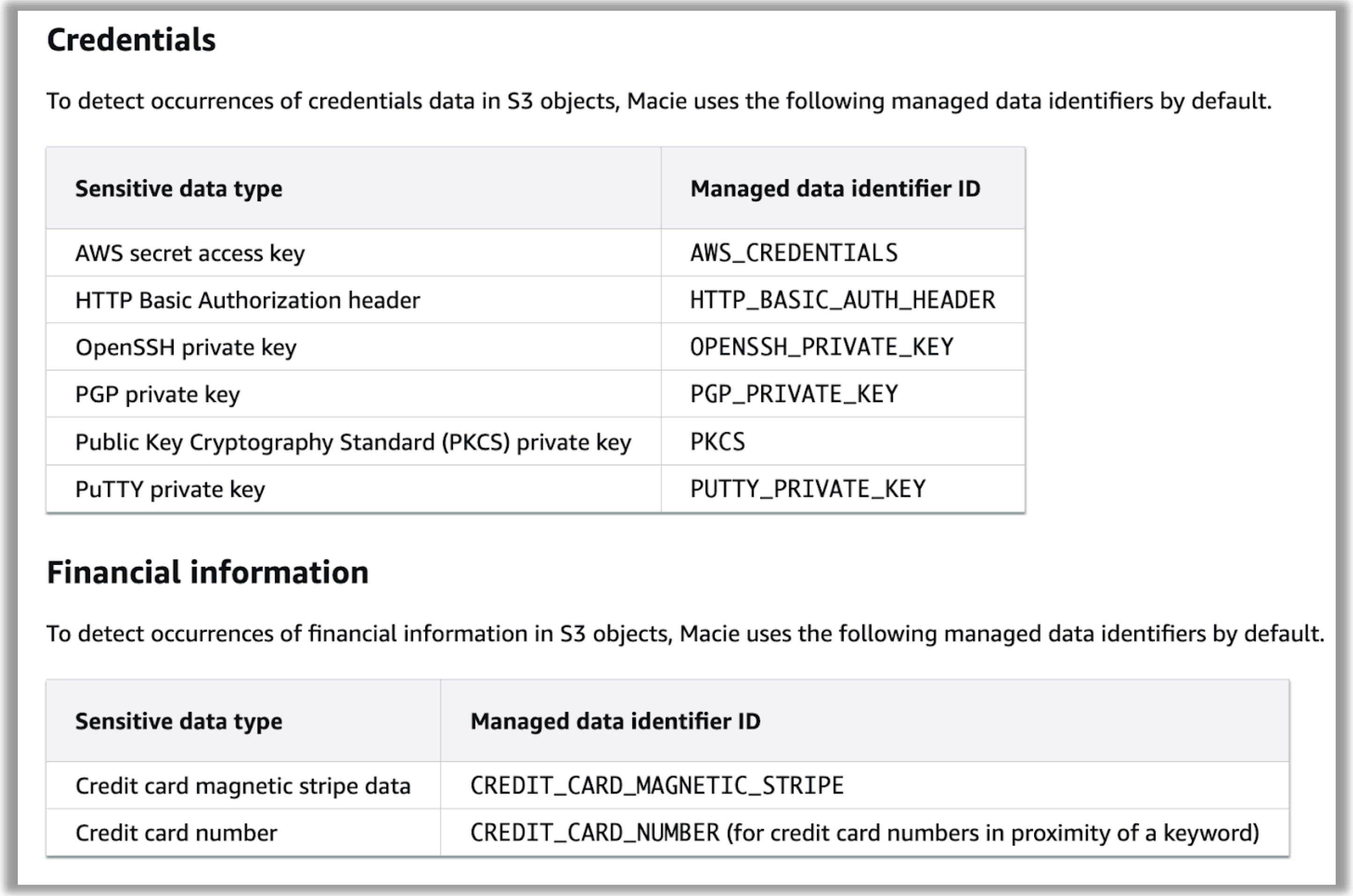
Discover sensitive data

Analyzes buckets using machine learning and pattern matching to discover sensitive data, such as personally identifiable information (PII)

Take action

Generates findings and sends to Amazon CloudWatch Events for ntegration into workflows and remediation actions

Amazon Macie



Credentials

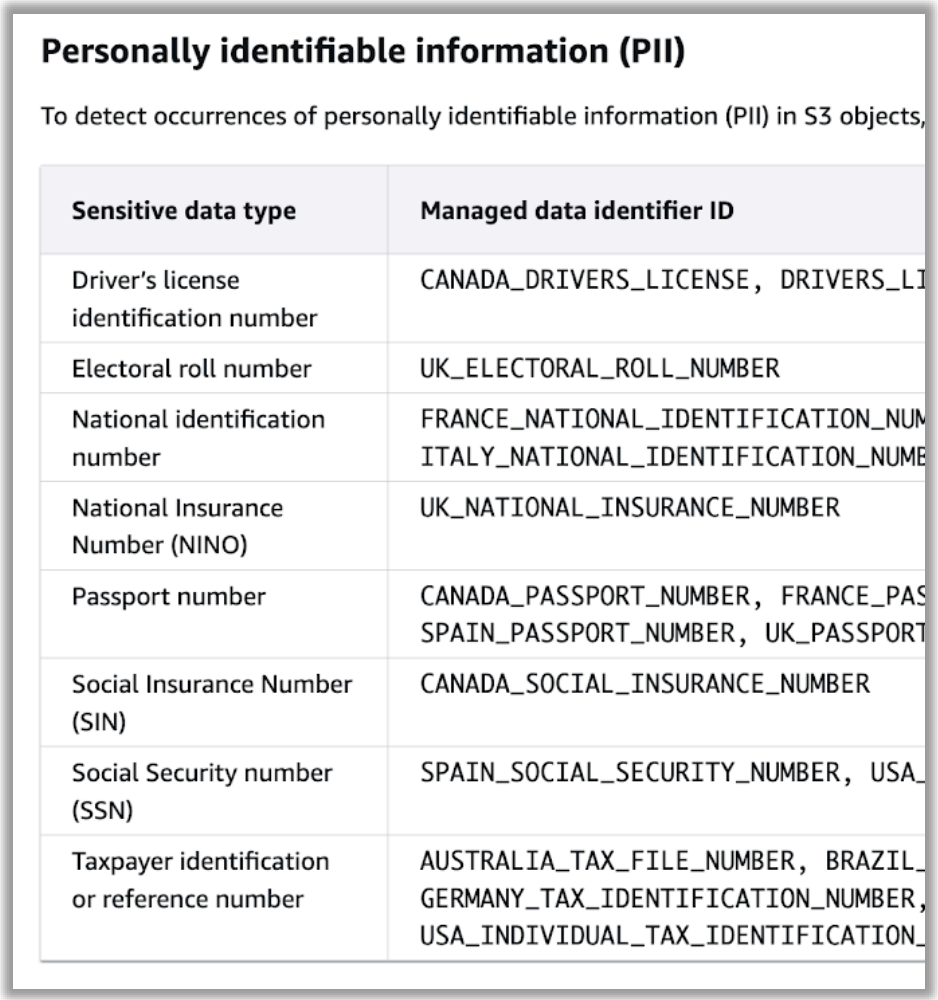
To detect occurrences of credentials data in S3 objects, Macie uses the following managed data identifiers by default.

Sensitive data type	Managed data identifier ID
AWS secret access key	AWS_CREDENTIALS
HTTP Basic Authorization header	HTTP_BASIC_AUTH_HEADER
OpenSSH private key	OPENSSH_PRIVATE_KEY
PGP private key	PGP_PRIVATE_KEY
Public Key Cryptography Standard (PKCS) private key	PKCS
PuTTY private key	PUTTY_PRIVATE_KEY

Financial information

To detect occurrences of financial information in S3 objects, Macie uses the following managed data identifiers by default.

Sensitive data type	Managed data identifier ID
Credit card magnetic stripe data	CREDIT_CARD_MAGNETIC_STRIPE
Credit card number	CREDIT_CARD_NUMBER (for credit card numbers in proximity of a keyword)

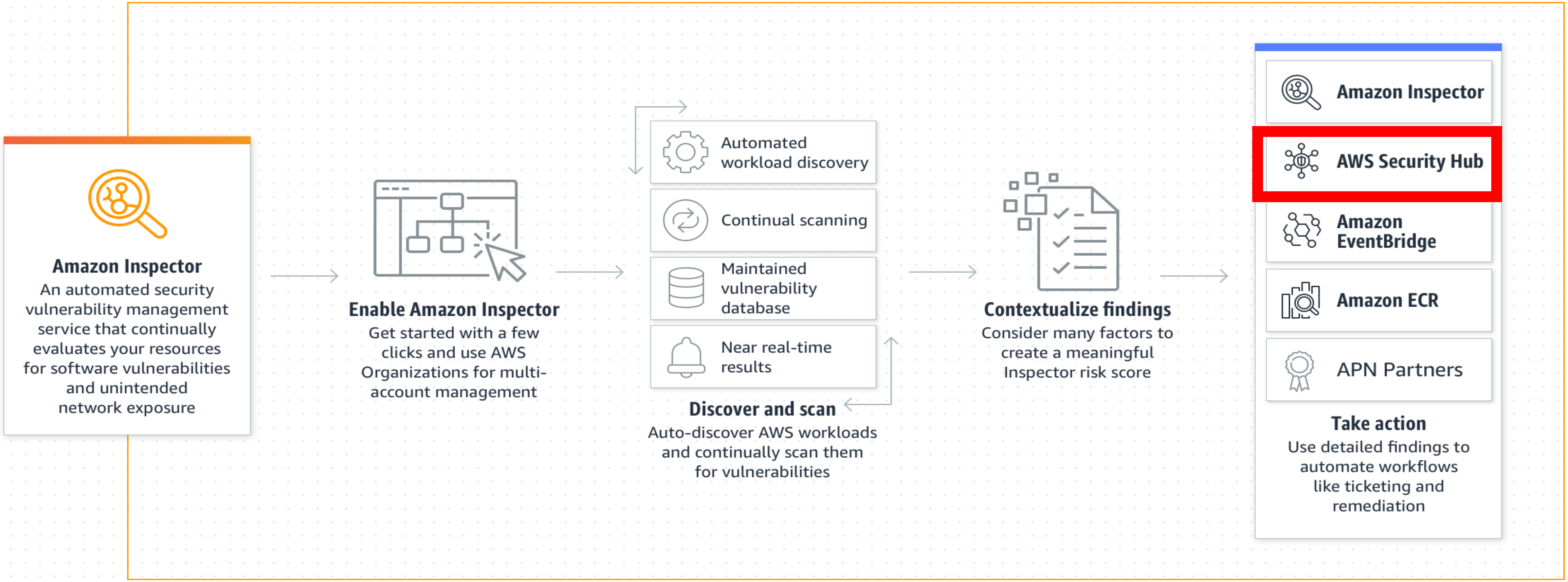


Personally identifiable information (PII)

To detect occurrences of personally identifiable information (PII) in S3 objects,

Sensitive data type	Managed data identifier ID
Driver's license identification number	CANADA_DRIVERS_LICENSE, DRIVERS_LI
Electoral roll number	UK_ELECTORAL_ROLL_NUMBER
National identification number	FRANCE_NATIONAL_IDENTIFICATION_NUM ITALY_NATIONAL_IDENTIFICATION_NUMB
National Insurance Number (NINO)	UK_NATIONAL_INSURANCE_NUMBER
Passport number	CANADA_PASSPORT_NUMBER, FRANCE_PAS SPAIN_PASSPORT_NUMBER, UK_PASSPORT
Social Insurance Number (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
Social Security number (SSN)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_
Taxpayer identification or reference number	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_ GERMANY_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_

Amazon Inspector



Amazon Inspector
An automated security vulnerability management service that continually evaluates your resources for software vulnerabilities and unintended network exposure

Enable Amazon Inspector
Get started with a few clicks and use AWS Organizations for multi-account management

Automated workload discovery

Continual scanning

Maintained vulnerability database

Near real-time results

Discover and scan
Auto-discover AWS workloads and continually scan them for vulnerabilities

Contextualize findings
Consider many factors to create a meaningful Inspector risk score

Amazon Inspector

AWS Security Hub

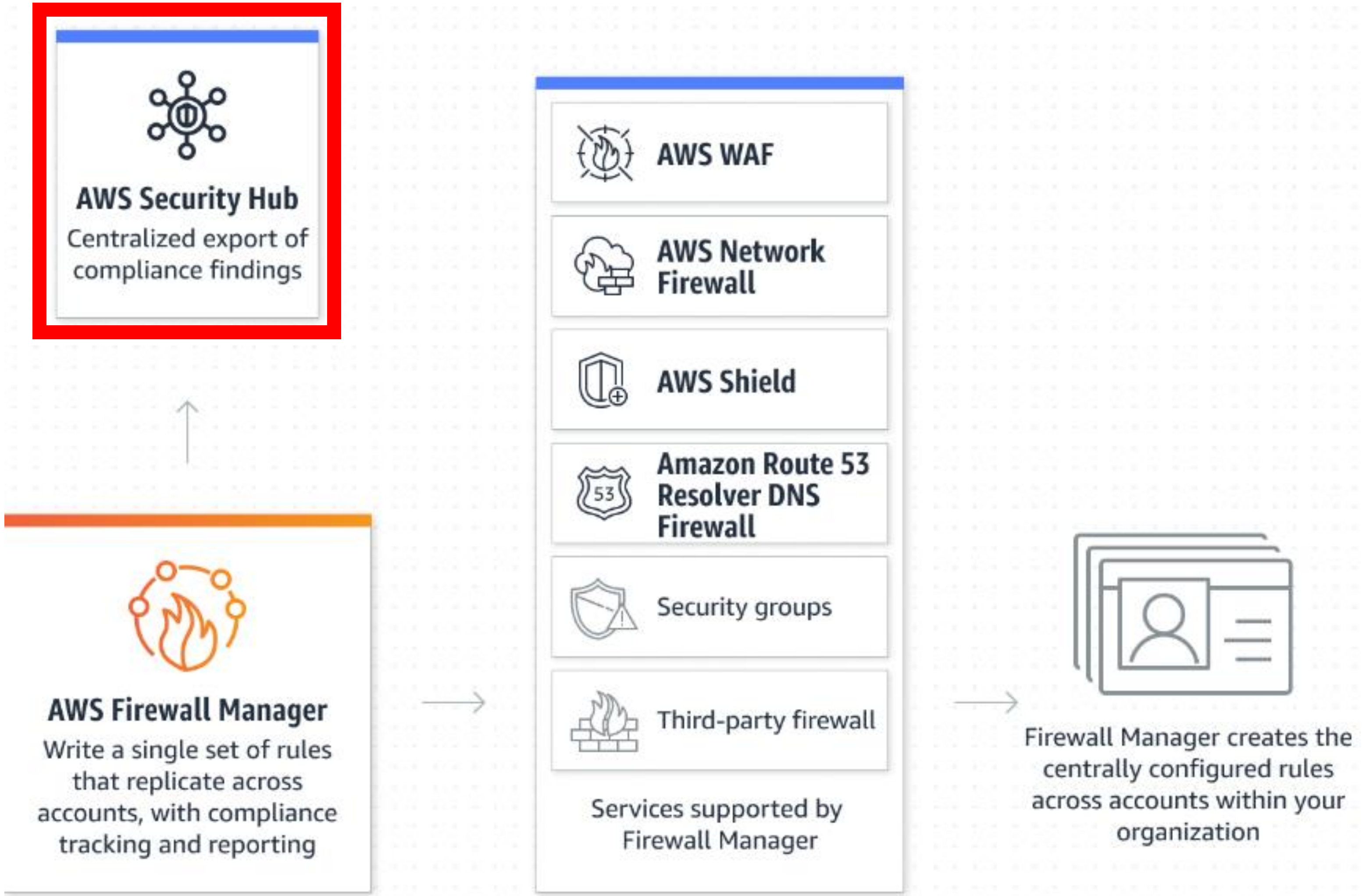
Amazon EventBridge

Amazon ECR

APN Partners

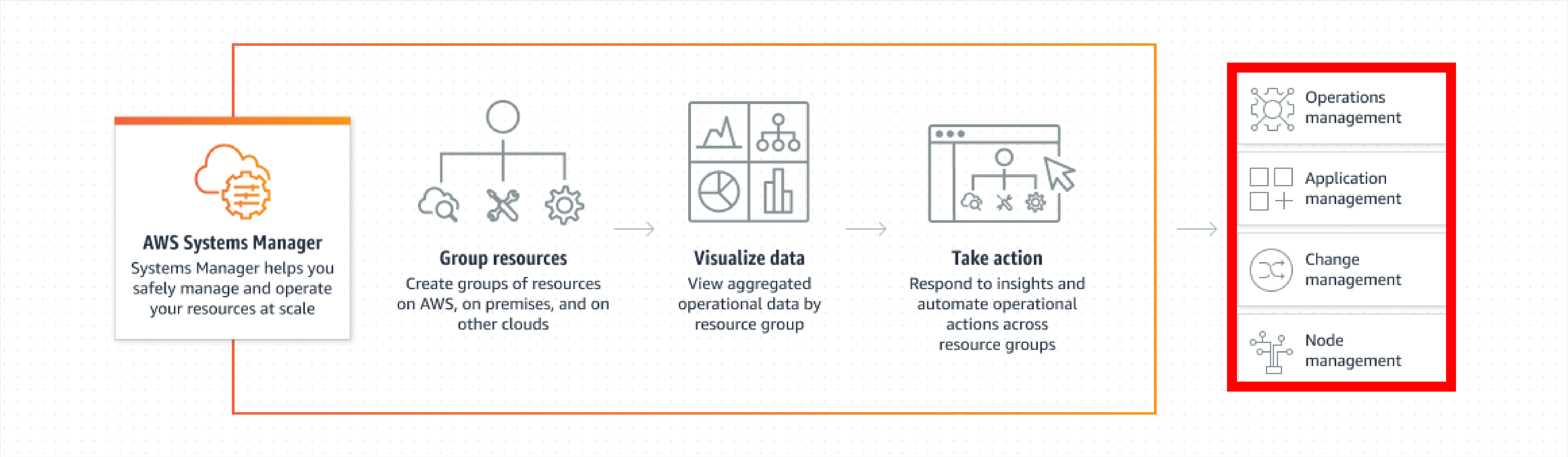
Take action
Use detailed findings to automate workflows like ticketing and remediation

AWS Firewall Manager



AWS Security Hub
Centralized export of compliance findings
AWS Firewall Manager
Write a single set of rules that replicate across accounts, with compliance tracking and reporting
AWS WAF
AWS Network Firewall
AWS Shield
Amazon Route 53 Resolver DNS Firewall
Security groups
Third-party firewall
Services supported by Firewall Manager
Firewall Manager creates the centrally configured rules across accounts within your organization

AWS Systems Manager



AWS Systems Manager
Systems Manager helps you safely manage and operate your resources at scale

Group resources
Create groups of resources on AWS, on premises, and on other clouds

Visualize data
View aggregated operational data by resource group

Take action
Respond to insights and automate operational actions across resource groups

Operations management

Application management

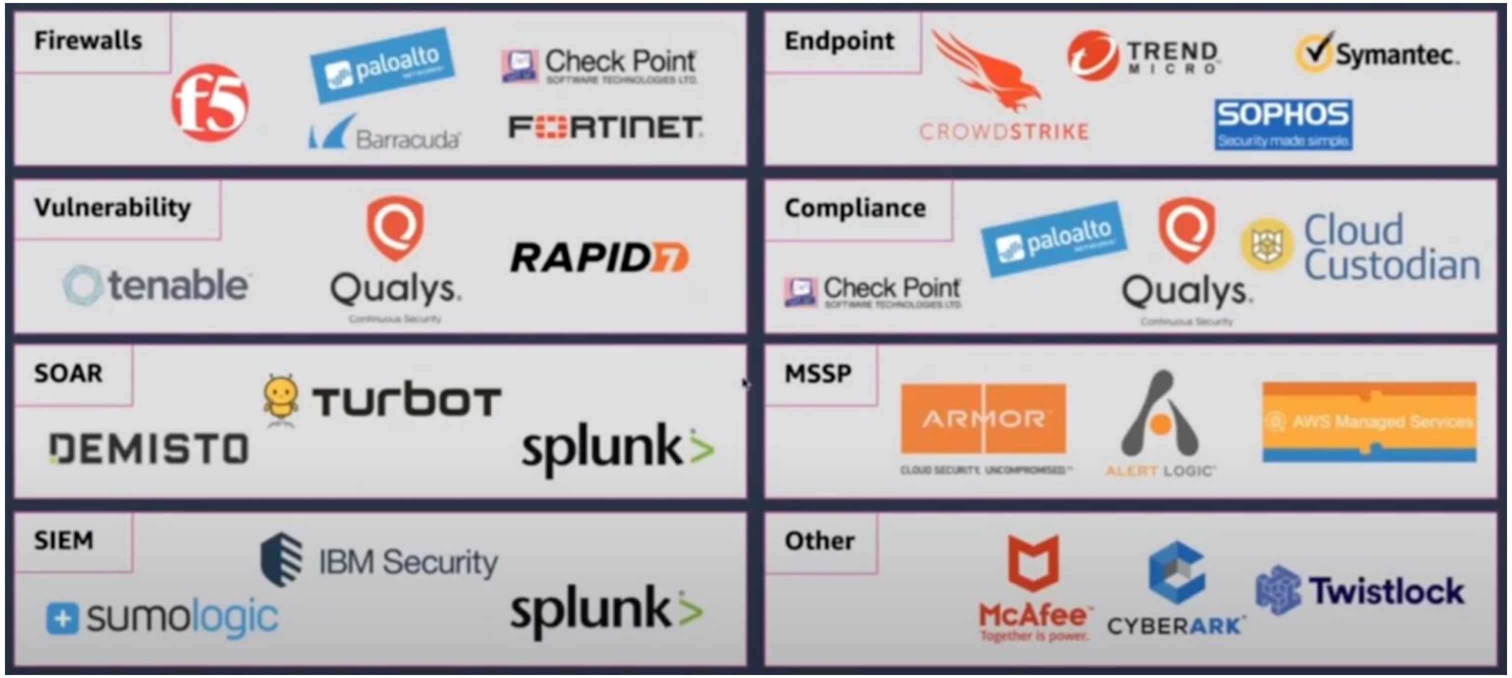
Change management

Node management

IAM Access Analyzer

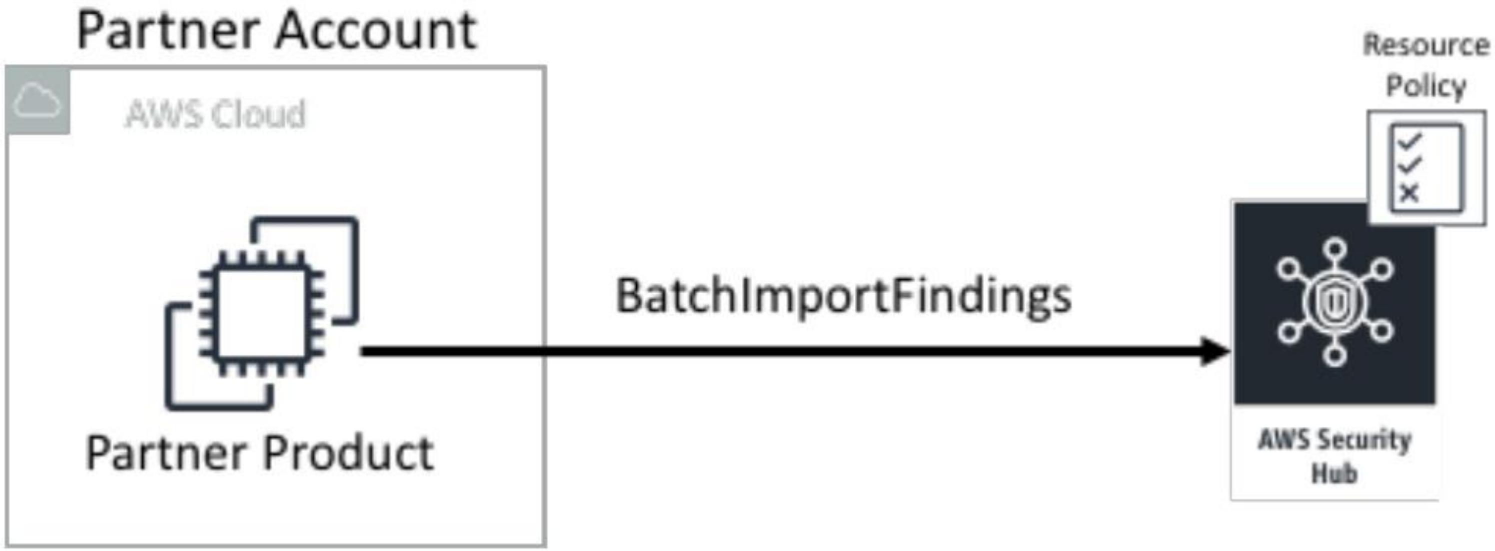
- Findings include
  - Unused
    - Roles
    - Access keys
    - Passwords
  - IAM Policy Review

Custom and Third-Party Sources



Category	Vendors
Firewalls	f5 paloalto Check Point Barracuda FORTINET
Vulnerability	tenable Qualys. RAPID7
SOAR	turbot DEMISTO splunk>
SIEM	IBM Security sumologic splunk>
Endpoint	CROWDSTRIKE TREND MICRO Symantec. SOPHOS
Compliance	Check Point paloalto Qualys. Cloud Custodian
MSSP	ARMOR ALERT LOGIC AWS Managed Services
Other	McAfee CYBERARK Twistlock

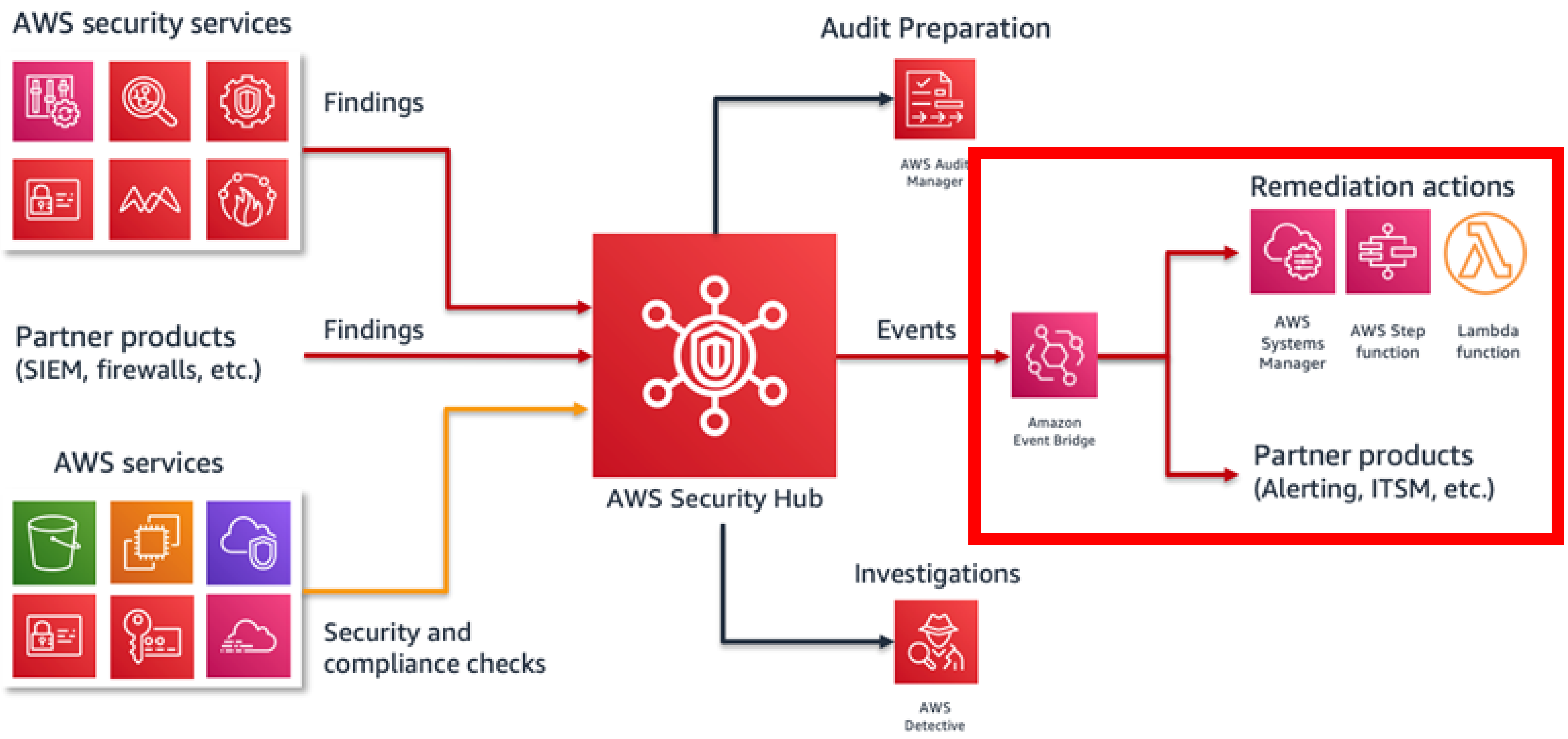
AWS Security Finding Format (ASFF / JSON)



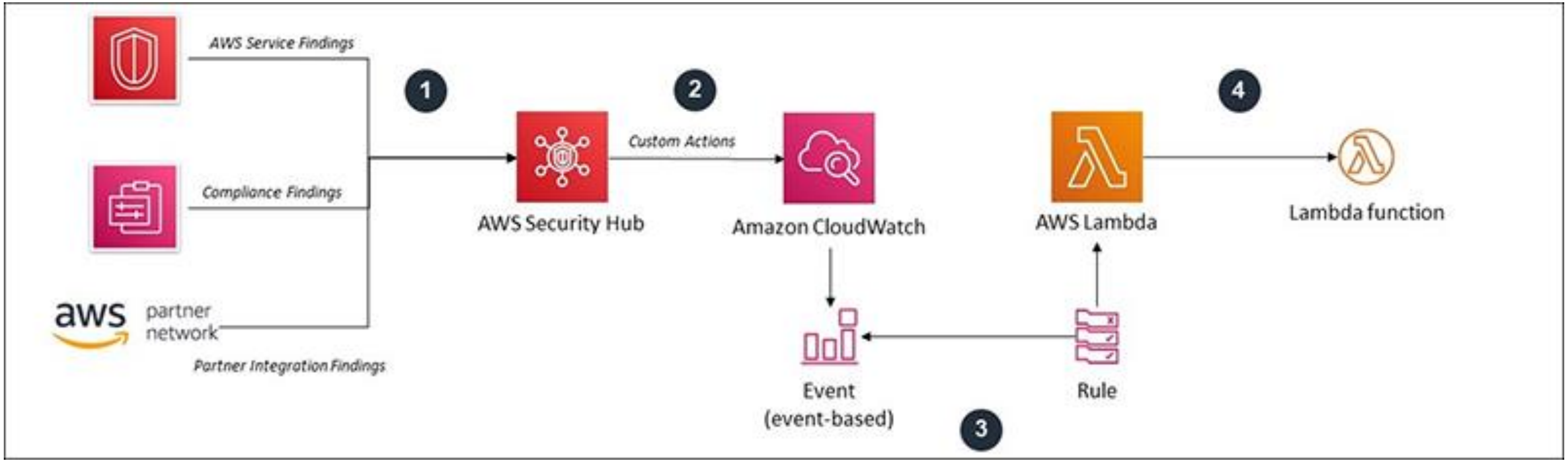
Ref: https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-findings-format.html

04

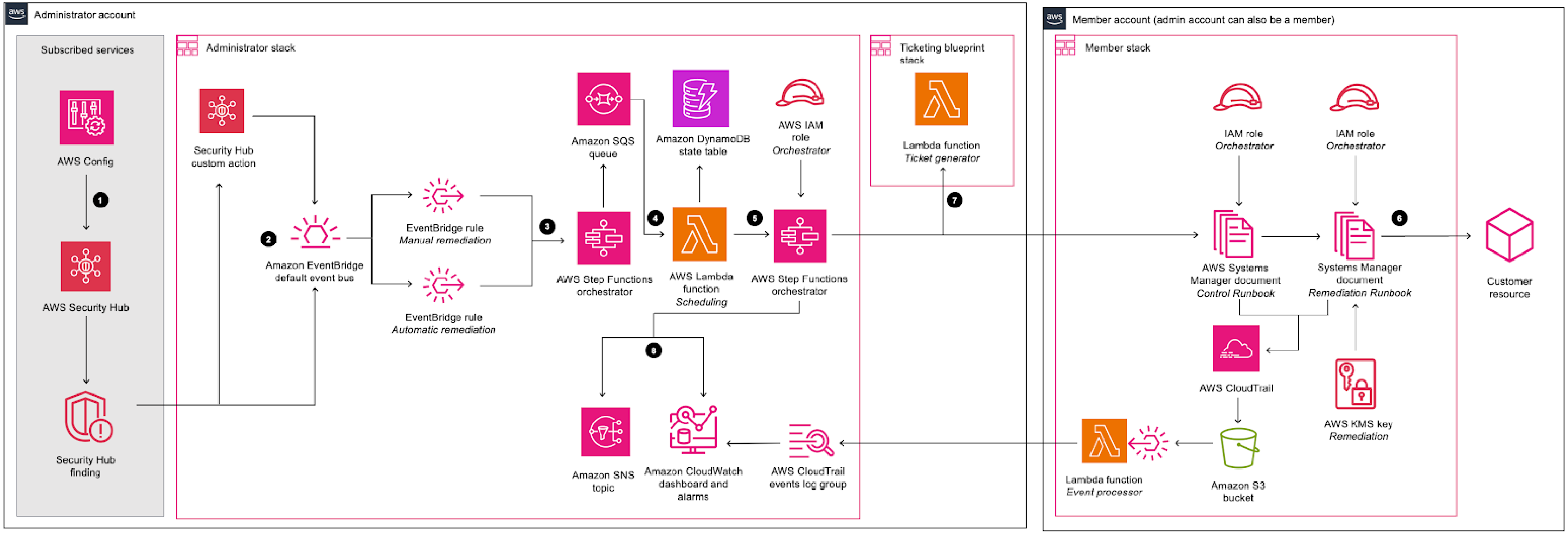
SECURITY HUB EVENTS


AWS security services
Findings
Partner products
(SIEM, firewalls, etc.)
Findings
AWS services
Security and
compliance checks
AWS Security Hub
Audit Preparation
AWS Audit
Manager
Events
Amazon
Event Bridge
Remediation actions
AWS
Systems
Manager
AWS Step
function
Lambda
function
Partner products
(Alerting, ITSM, etc.)
Investigations
AWS
Detective

Response and Remediation - 2020



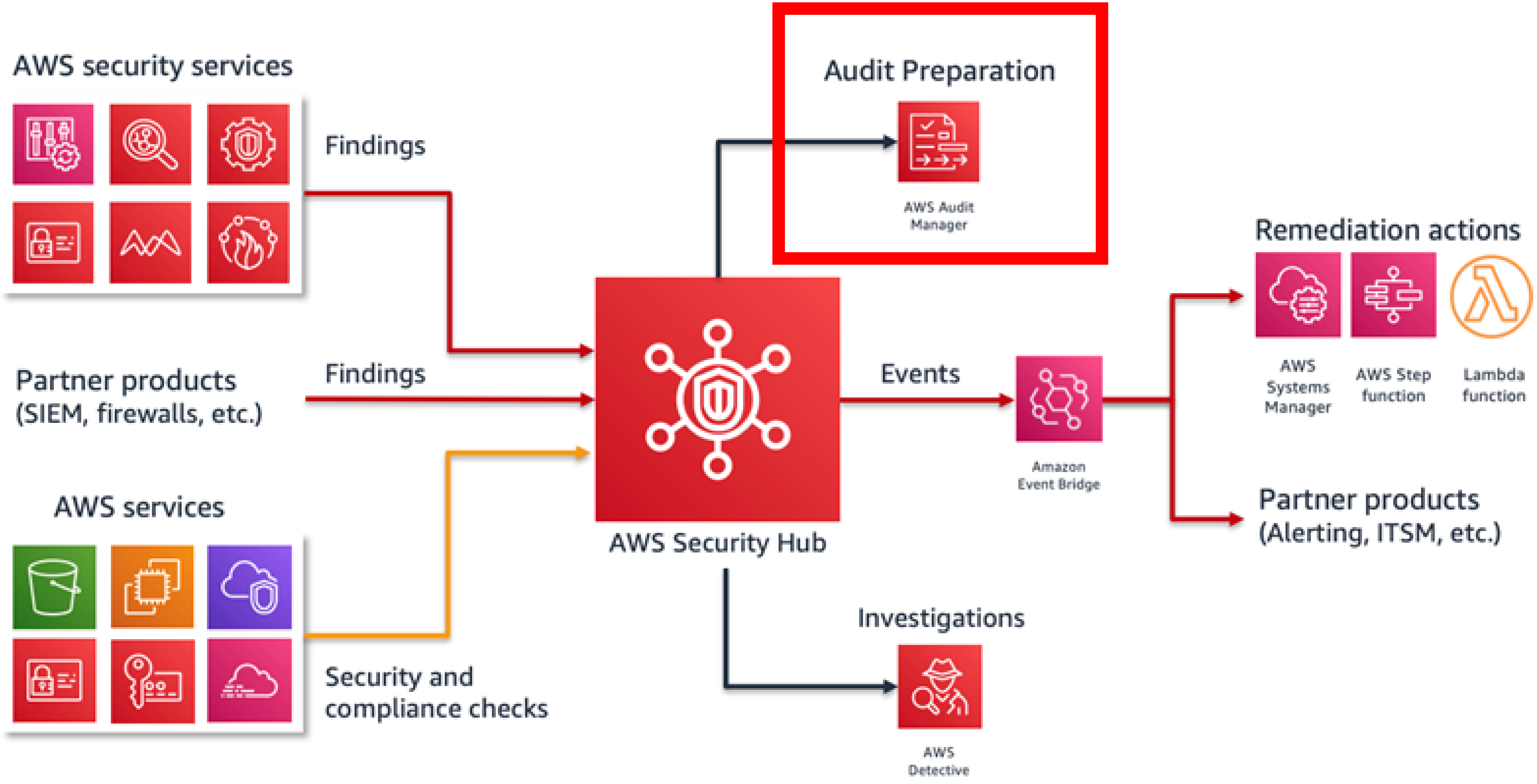
Response and Remediation - 2025



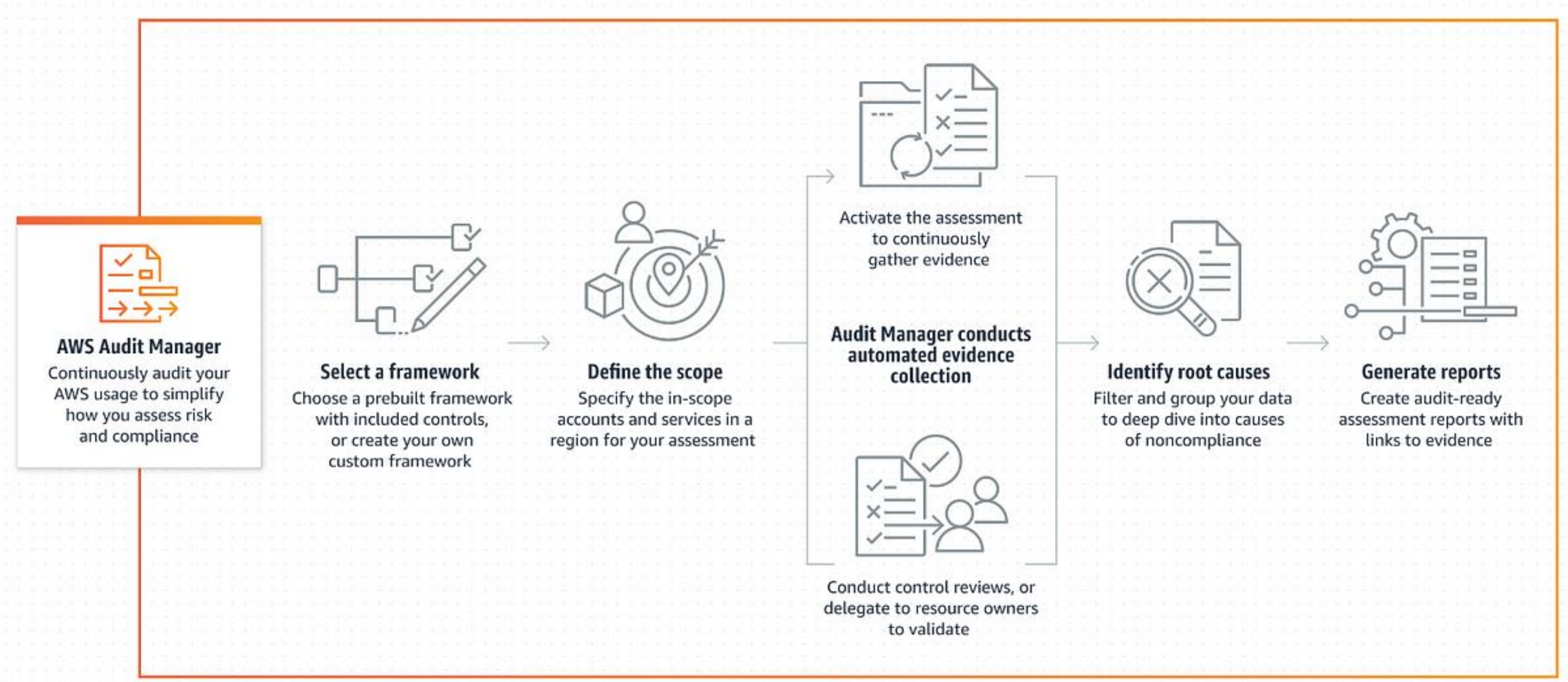
Ref: https://aws.amazon.com/solutions/implementations/automated-security-response-on-aws/#

05

AWS AUDIT MANAGER


AWS security services
Findings
Partner products
(SIEM, firewalls, etc.)
Findings
AWS services
Security and
compliance checks
Audit Preparation
AWS Audit
Manager
AWS Security Hub
Events
Amazon
Event Bridge
Remediation actions
AWS
Systems
Manager
AWS Step
function
Lambda
function
Partner products
(Alerting, ITSM, etc.)
Investigations
AWS
Detective

AWS Audit Manager



AWS Audit Manager

Continuously audit your AWS usage to simplify how you assess risk and compliance

Select a framework

Choose a prebuilt framework with included controls, or create your own custom framework

Define the scope

Specify the in-scope accounts and services in a region for your assessment

Activate the assessment to continuously gather evidence

Audit Manager conducts automated evidence collection

Conduct control reviews, or delegate to resource owners to validate

Identify root causes

Filter and group your data to deep dive into causes of noncompliance

Generate reports

Create audit-ready assessment reports with links to evidence

Security Frameworks in Audit Manager

ACSC Essential Eight

ACSC ISM 02 March 2023

AWS Audit Manager Sample Framework

AWS Control Tower Guardrails

AWS Generative AI Best Practices Framework v2

AWS License Manager

AWS Foundational Security Best Practices

AWS Operational Best Practices

AWS Well Architected Framework WAF v10

CCCS Medium Cloud Control

CIS AWS Benchmark v1.2.0

CIS AWS Benchmark v1.3.0

CIS AWS Benchmark v1.4.0

CIS Controls v7.1, IG1

CIS Critical Security Controls version 8.0, IG1

FedRAMP Security Baseline Controls r4

GDPR 2016

Gramm-Leach-Bliley Act

Title 21 CFR Part 11

EU GMP Annex 11, v1

HIPAA Security Rule: Feb 2003

HIPAA Omnibus Final Rule

ISO/IEC 27001:2013 Annex A

NIST SP 800-53 Rev 5

NIST Cybersecurity Framework v1.1

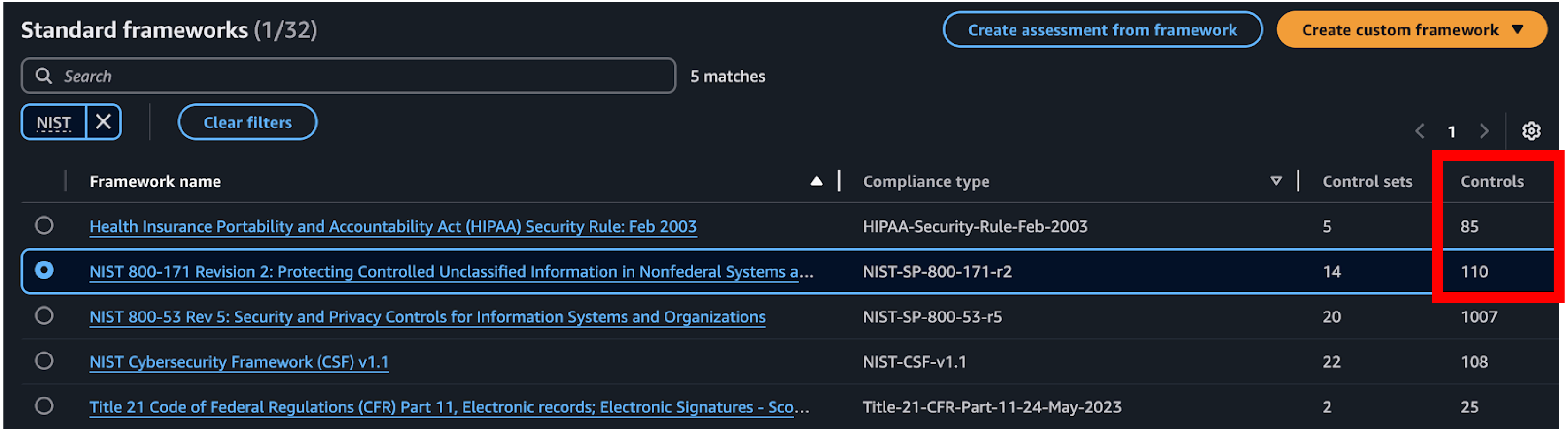
NIST SP 800-171 Rev 2

PCI DSS V3.2.1

PCI DSS V4.0

SSAE-18 SOC 2

Common Security Frameworks

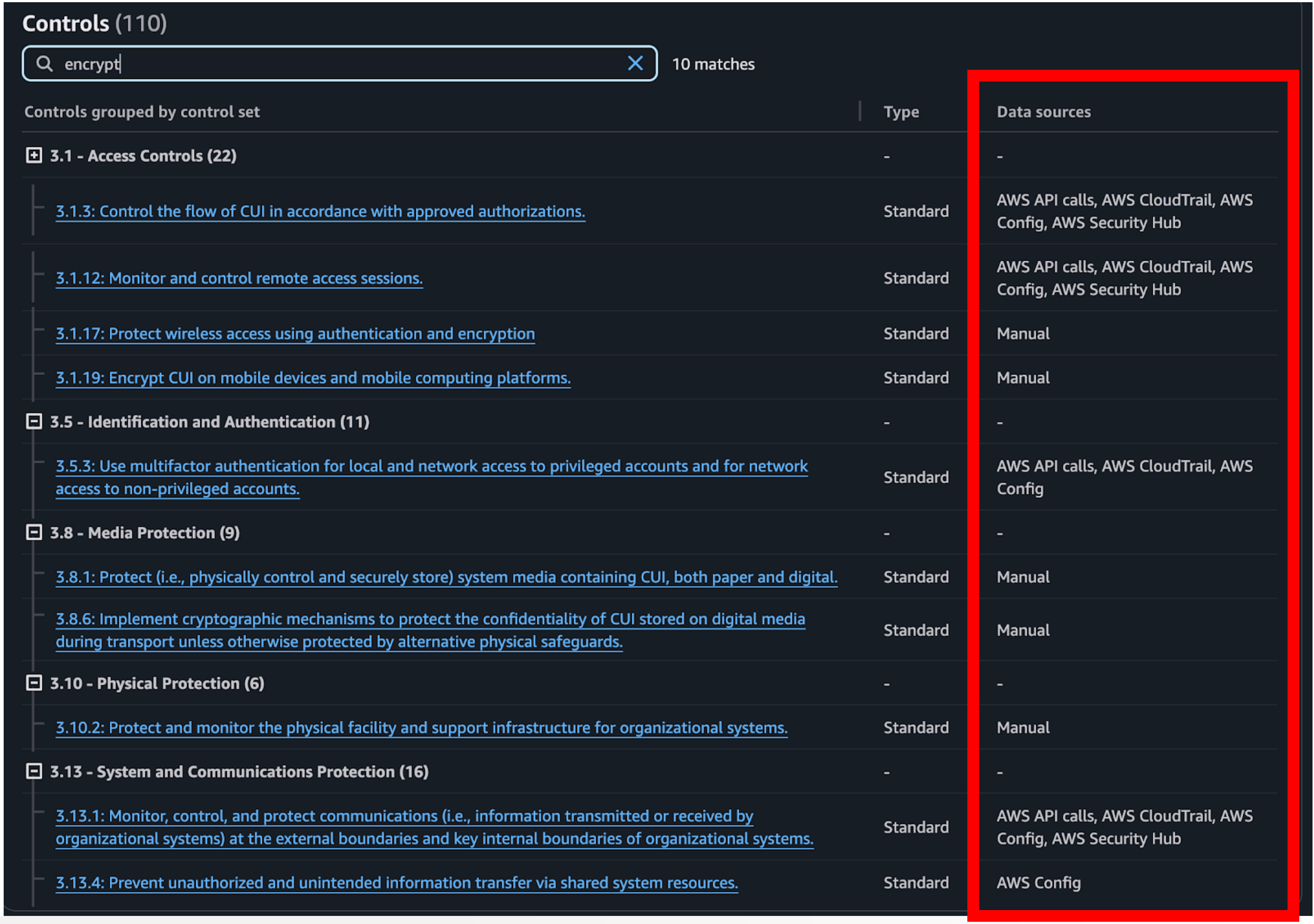


Standard frameworks (1/32)

5 matches

	Framework name	Compliance type	Control sets	Controls
○	Health Insurance Portability and Accountability Act (HIPAA) Security Rule: Feb 2003	HIPAA-Security-Rule-Feb-2003	5	85
●	NIST 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems a...	NIST-SP-800-171-r2	14	110
○	NIST 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations	NIST-SP-800-53-r5	20	1007
○	NIST Cybersecurity Framework (CSF) v1.1	NIST-CSF-v1.1	22	108
○	Title 21 Code of Federal Regulations (CFR) Part 11, Electronic records; Electronic Signatures - Sco...	Title-21-CFR-Part-11-24-May-2023	2	25

NIST 800-171



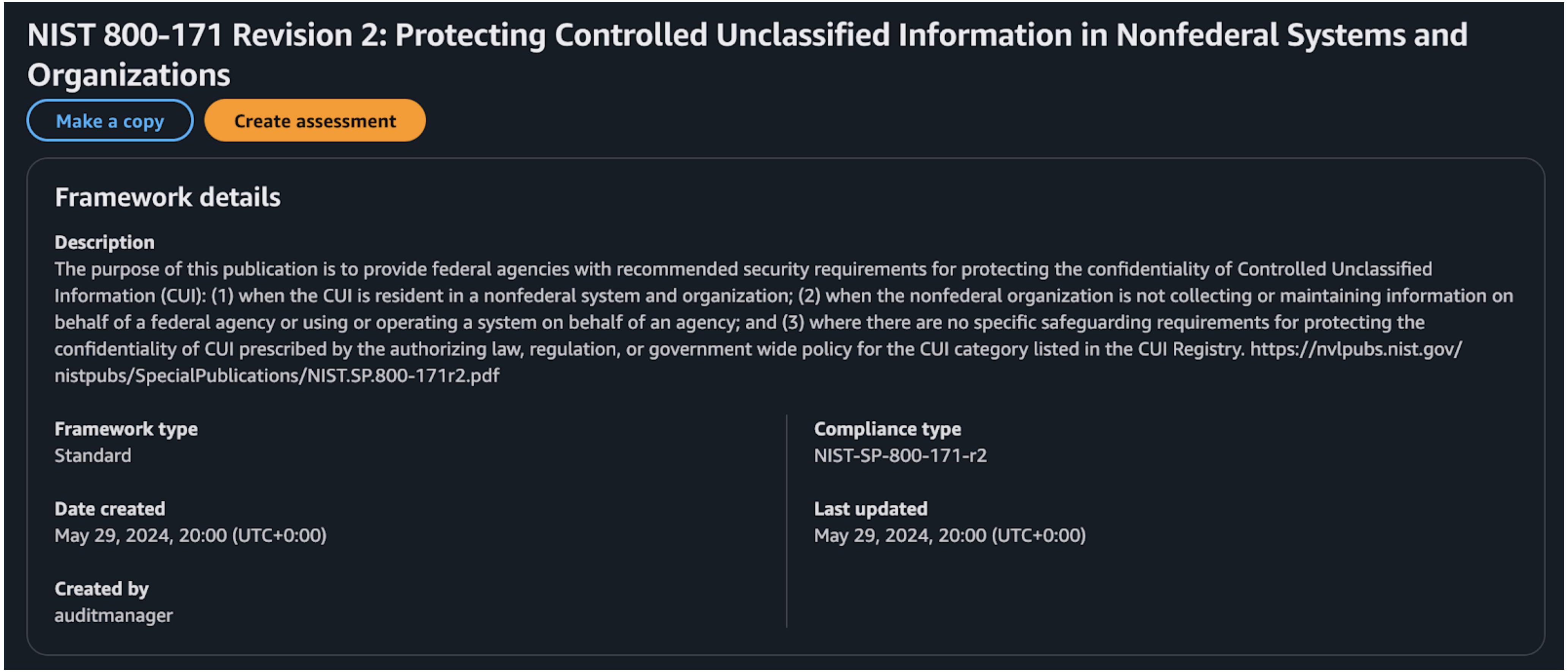
Controls (110)

encrypt

10 matches

Controls grouped by control set	Type	Data sources
⊞ **3.1 - Access Controls (22)**	-	-
3.1.3: Control the flow of CUI in accordance with approved authorizations.	Standard	AWS API calls, AWS CloudTrail, AWS Config, AWS Security Hub
3.1.12: Monitor and control remote access sessions.	Standard	AWS API calls, AWS CloudTrail, AWS Config, AWS Security Hub
3.1.17: Protect wireless access using authentication and encryption	Standard	Manual
3.1.19: Encrypt CUI on mobile devices and mobile computing platforms.	Standard	Manual
⊟ **3.5 - Identification and Authentication (11)**	-	-
3.5.3: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Standard	AWS API calls, AWS CloudTrail, AWS Config
⊟ **3.8 - Media Protection (9)**	-	-
3.8.1: Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	Standard	Manual
3.8.6: Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Standard	Manual
⊟ **3.10 - Physical Protection (6)**	-	-
3.10.2: Protect and monitor the physical facility and support infrastructure for organizational systems.	Standard	Manual
⊟ **3.13 - System and Communications Protection (16)**	-	-
3.13.1: Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	Standard	AWS API calls, AWS CloudTrail, AWS Config, AWS Security Hub
3.13.4: Prevent unauthorized and unintended information transfer via shared system resources.	Standard	AWS Config

NIST 800-171



NIST 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Framework details

Description
The purpose of this publication is to provide federal agencies with recommended security requirements for protecting the confidentiality of Controlled Unclassified Information (CUI): (1) when the CUI is resident in a nonfederal system and organization; (2) when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government wide policy for the CUI category listed in the CUI Registry. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

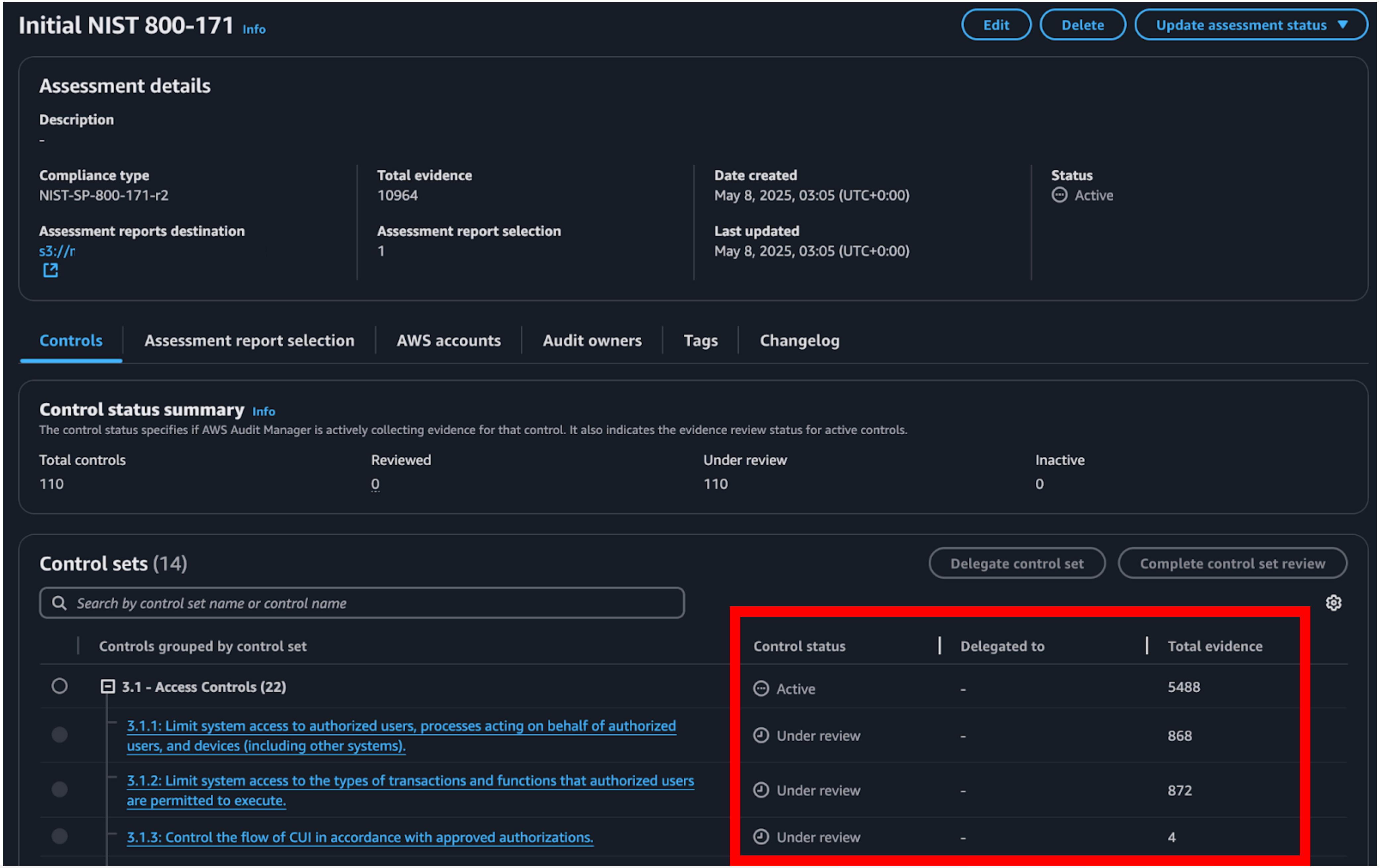
Framework type
Standard

Date created
May 29, 2024, 20:00 (UTC+0:00)

Created by
auditmanager

Compliance type
NIST-SP-800-171-r2

Last updated
May 29, 2024, 20:00 (UTC+0:00)



Initial NIST 800-171 Info

Assessment details

Description
-

Compliance type
NIST-SP-800-171-r2

Assessment reports destination
s3://r

Total evidence
10964

Assessment report selection
1

Date created
May 8, 2025, 03:05 (UTC+0:00)

Last updated
May 8, 2025, 03:05 (UTC+0:00)

Status
Active

Control status summary Info

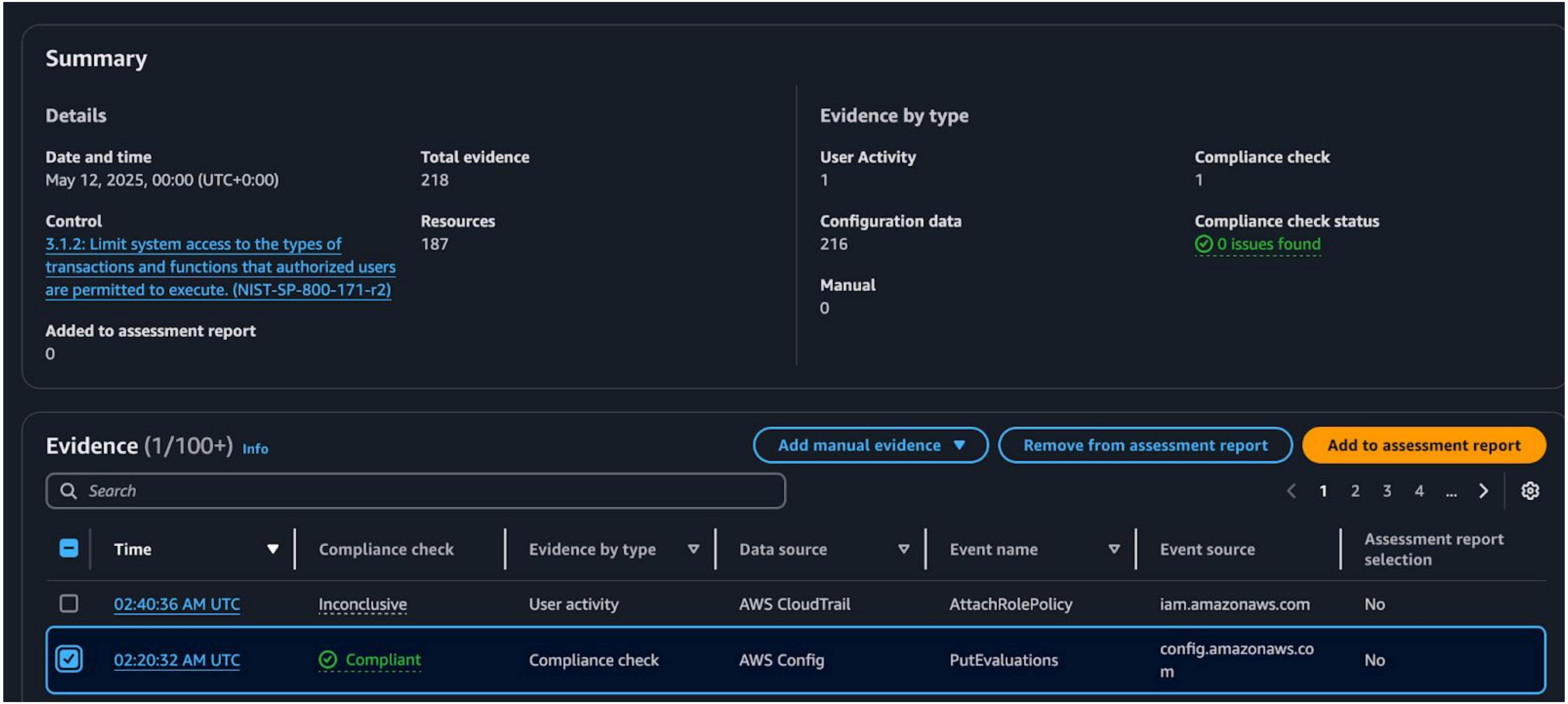
The control status specifies if AWS Audit Manager is actively collecting evidence for that control. It also indicates the evidence review status for active controls.

Total controls	Reviewed	Under review	Inactive
110	0	110	0

Control sets (14)

Delegate control set
Complete control set review
Search by control set name or control name

	Controls grouped by control set	Control status	Delegated to	Total evidence
○	⊟ 3.1 - Access Controls (22)	Active	-	5488
●	3.1.1: Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Under review	-	868
●	3.1.2: Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Under review	-	872
●	3.1.3: Control the flow of CUI in accordance with approved authorizations.	Under review	-	4



Summary

Details

Date and time
May 12, 2025, 00:00 (UTC+0:00)

Total evidence
218

Control
3.1.2: Limit system access to the types of transactions and functions that authorized users are permitted to execute. (NIST-SP-800-171-r2)

Resources
187

Added to assessment report
0

Evidence by type

User Activity
1

Compliance check
1

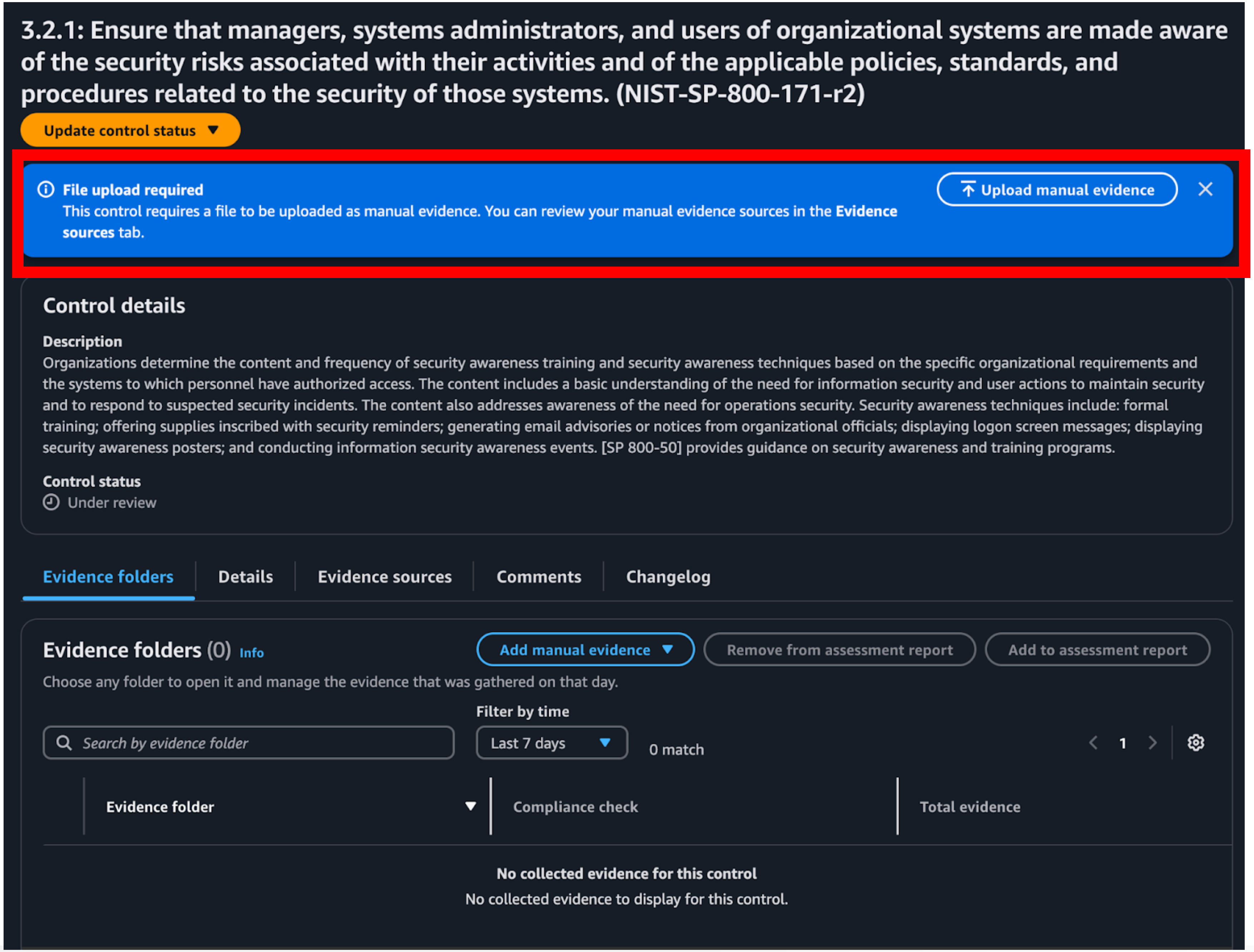
Configuration data
216

Compliance check status
✓ 0 issues found

Manual
0

Evidence (1/100+) Info

▣	Time ▼	Compliance check	Evidence by type ▽	Data source ▽	Event name ▽	Event source	Assessment report selection
□	02:40:36 AM UTC	Inconclusive	User activity	AWS CloudTrail	AttachRolePolicy	iam.amazonaws.com	No
☑	02:20:32 AM UTC	✓ Compliant	Compliance check	AWS Config	PutEvaluations	config.amazonaws.com	No



3.2.1: Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. (NIST-SP-800-171-r2)

File upload required
This control requires a file to be uploaded as manual evidence. You can review your manual evidence sources in the **Evidence sources** tab.

Control details

Description
Organizations determine the content and frequency of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques include: formal training; offering supplies inscribed with security reminders; generating email advisories or notices from organizational officials; displaying logon screen messages; displaying security awareness posters; and conducting information security awareness events. [SP 800-50] provides guidance on security awareness and training programs.

Control status
Under review

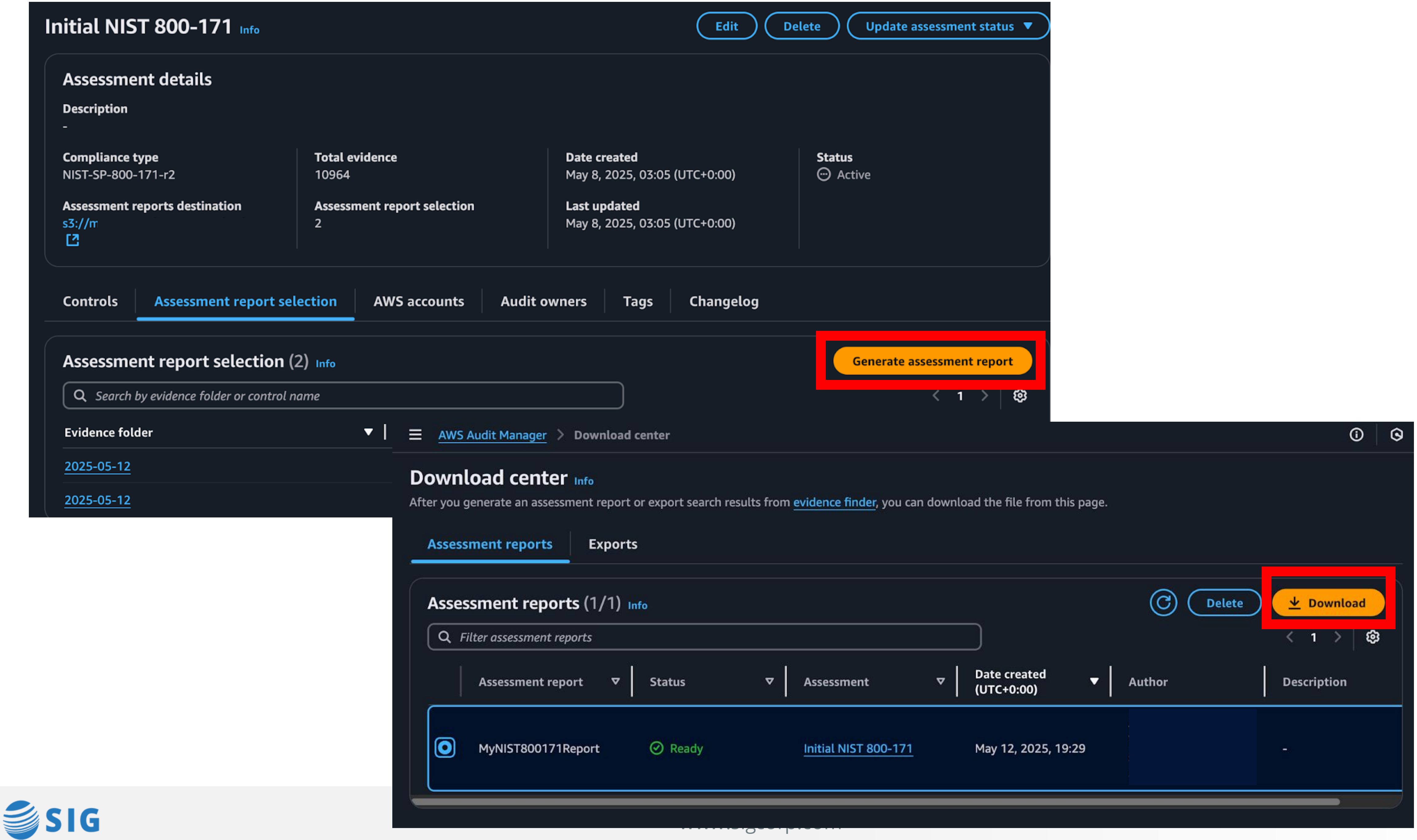
Evidence folders (0) Info

Choose any folder to open it and manage the evidence that was gathered on that day.

Filter by time: Last 7 days

Evidence folder	Compliance check	Total evidence

No collected evidence for this control
No collected evidence to display for this control.



Edit
Delete
Update assessment status ▼

Initial NIST 800-171 Info

Assessment details

Description
-

Compliance type NIST-SP-800-171-r2	**Total evidence** 10964	**Date created** May 8, 2025, 03:05 (UTC+0:00)	**Status** Active
Assessment reports destination s3://m	**Assessment report selection** 2	**Last updated** May 8, 2025, 03:05 (UTC+0:00)	

Controls
Assessment report selection
AWS accounts
Audit owners
Tags
Changelog

Assessment report selection (2) Info

Generate assessment report
Search by evidence folder or control name
1

Evidence folder
2025-05-12
2025-05-12

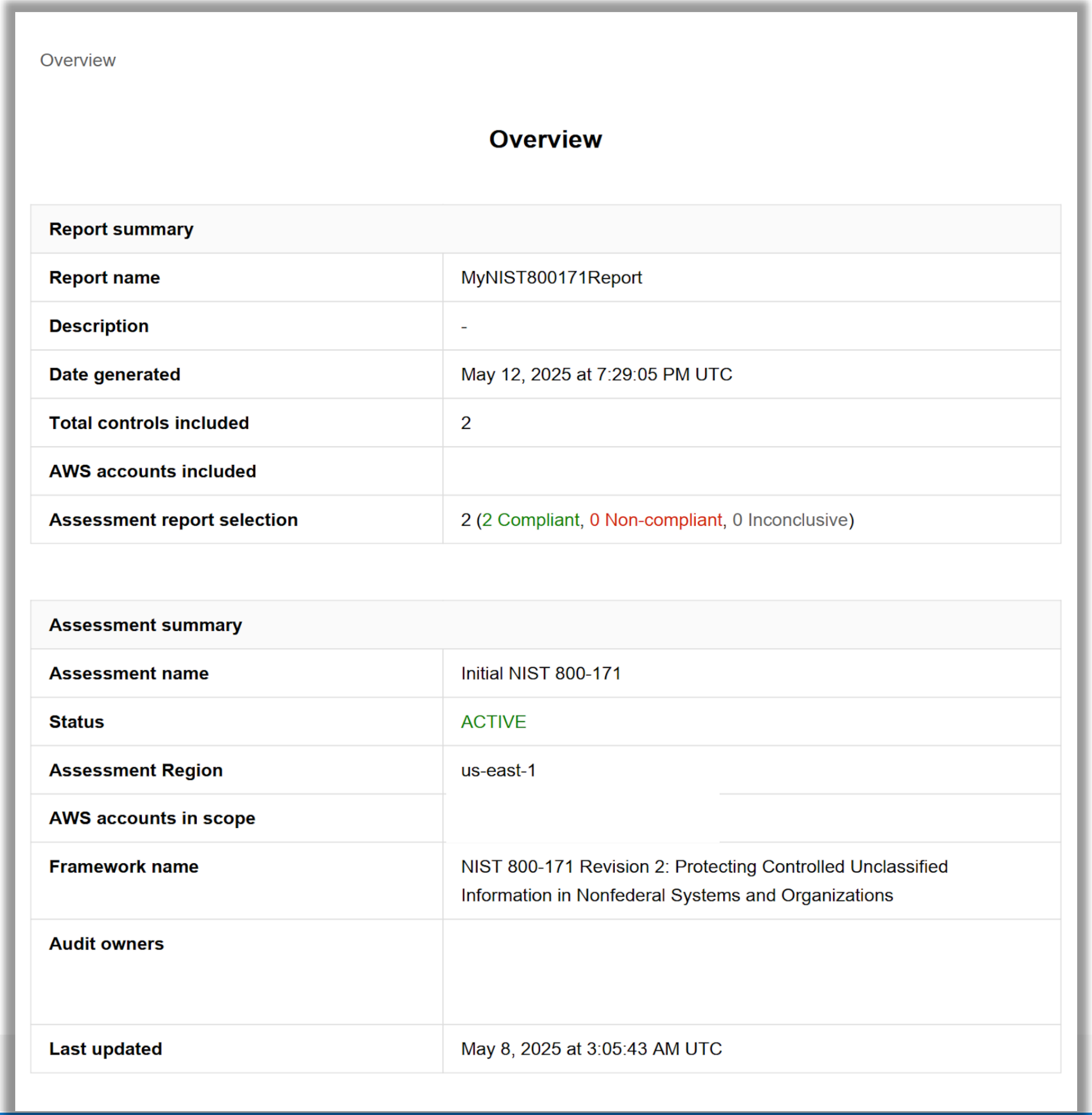
AWS Audit Manager > Download center

Download center Info

After you generate an assessment report or export search results from evidence finder, you can download the file from this page.

Assessment reports (1/1) Info

	Assessment report	Status	Assessment	Date created (UTC+0:00)	Author	Description
●	MyNIST800171Report	✓ Ready	Initial NIST 800-171	May 12, 2025, 19:29	[redacted]	-

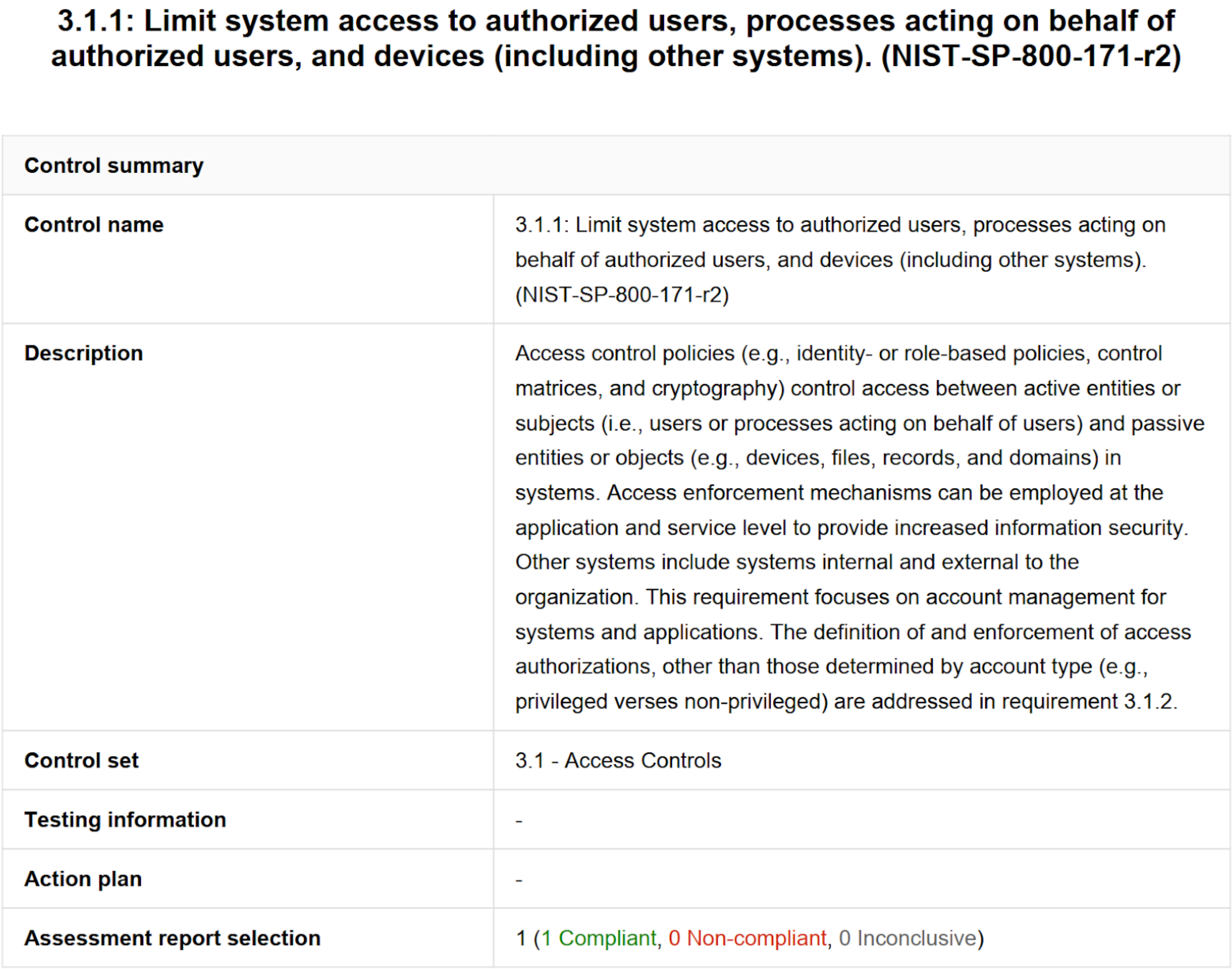


Overview

Overview

Report summary	
Report name	MyNIST800171Report
Description	-
Date generated	May 12, 2025 at 7:29:05 PM UTC
Total controls included	2
AWS accounts included	
Assessment report selection	2 (2 Compliant, 0 Non-compliant, 0 Inconclusive)

Assessment summary	
Assessment name	Initial NIST 800-171
Status	ACTIVE
Assessment Region	us-east-1
AWS accounts in scope	
Framework name	NIST 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
Audit owners	
Last updated	May 8, 2025 at 3:05:43 AM UTC



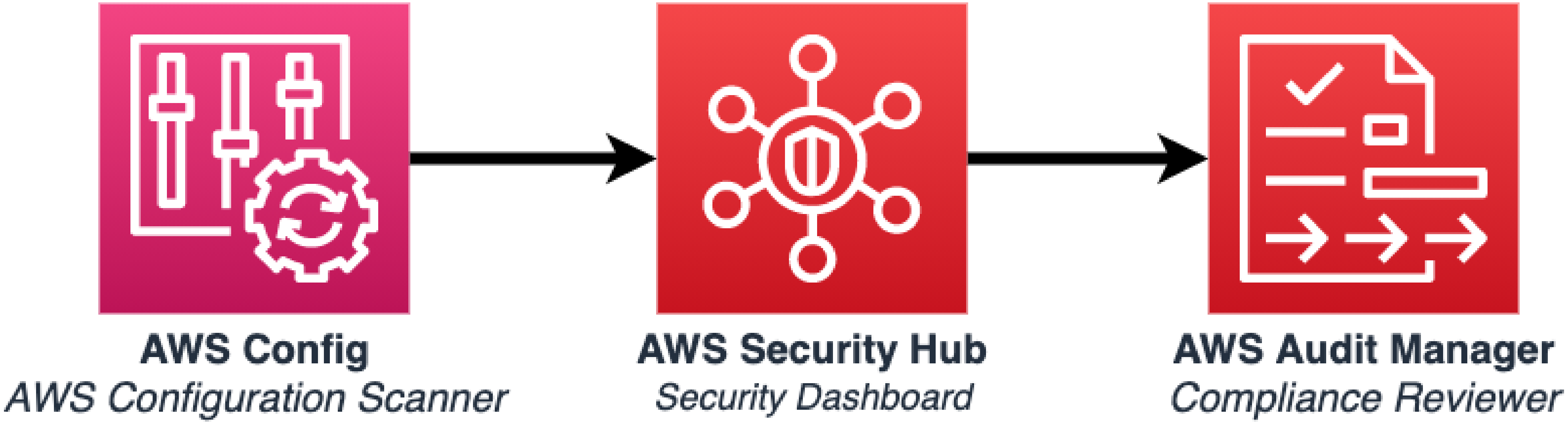
3.1.1: Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). (NIST-SP-800-171-r2)

Control summary	
Control name	3.1.1: Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). (NIST-SP-800-171-r2)
Description	Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2.
Control set	3.1 - Access Controls
Testing information	-
Action plan	-
Assessment report selection	1 (1 Compliant, 0 Non-compliant, 0 Inconclusive)

06

GETTING STARTED

Minimum Viable Stack

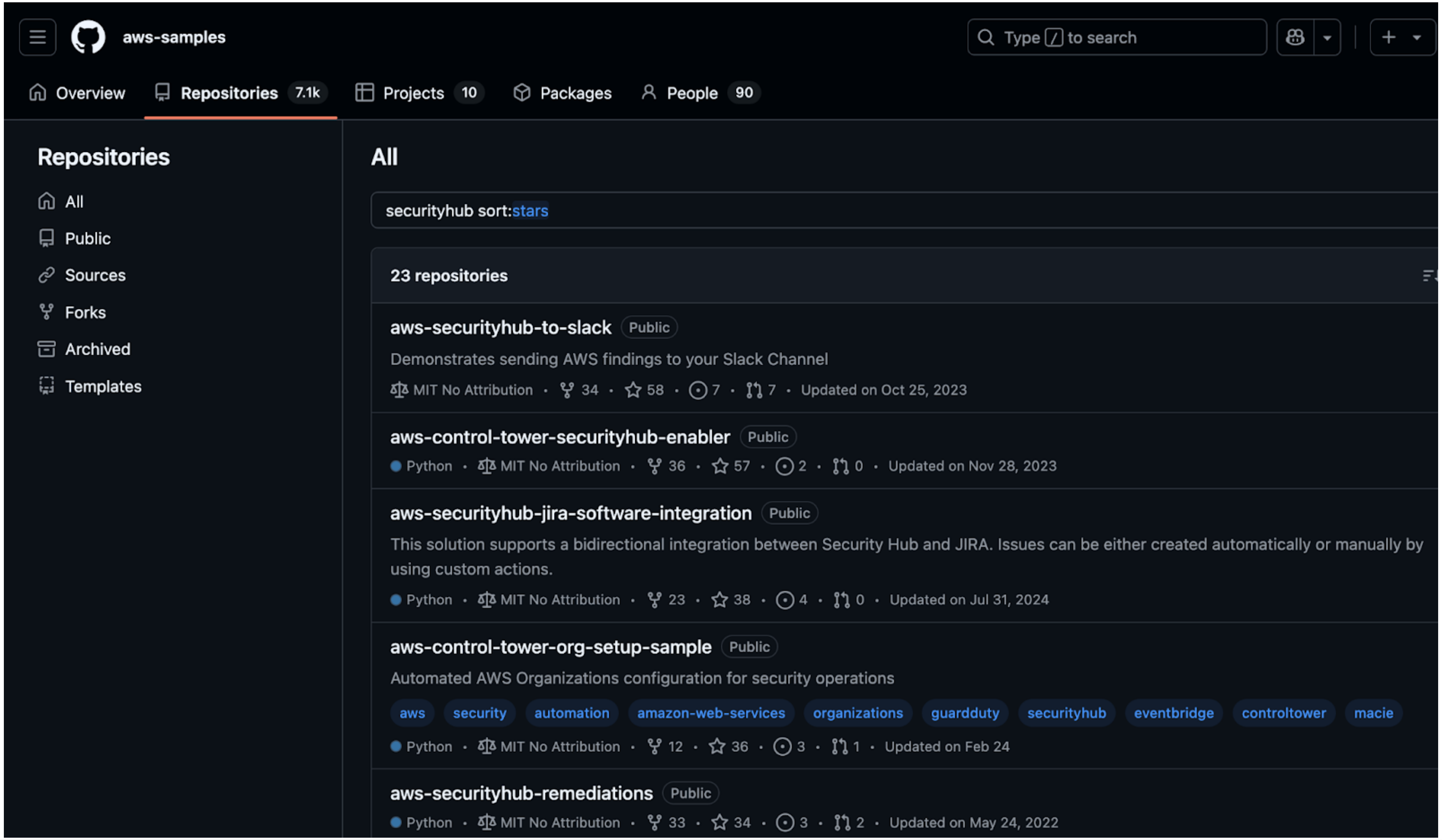


AWS Config
AWS Configuration Scanner

AWS Security Hub
Security Dashboard

AWS Audit Manager
Compliance Reviewer

Infrastructure as Code - GitHub



All

securityhub sort:stars

23 repositories

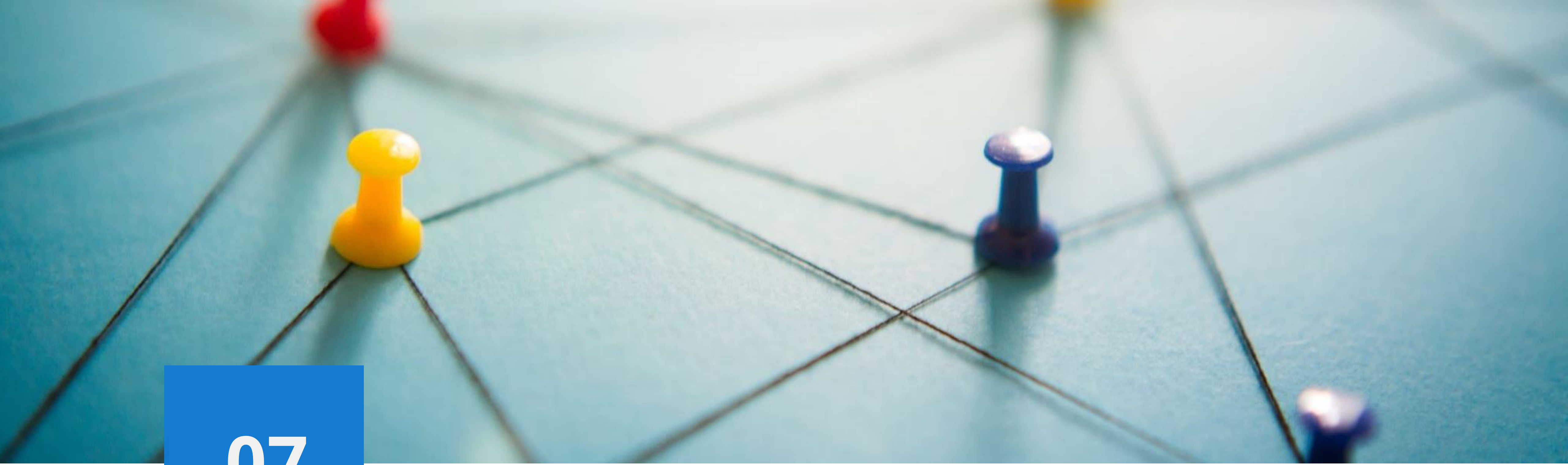
aws-securityhub-to-slack Public
Demonstrates sending AWS findings to your Slack Channel
MIT No Attribution · 34 · 58 · 7 · 7 · Updated on Oct 25, 2023

aws-control-tower-securityhub-enabler Public
Python · MIT No Attribution · 36 · 57 · 2 · 0 · Updated on Nov 28, 2023

aws-securityhub-jira-software-integration Public
This solution supports a bidirectional integration between Security Hub and JIRA. Issues can be either created automatically or manually by using custom actions.
Python · MIT No Attribution · 23 · 38 · 4 · 0 · Updated on Jul 31, 2024

aws-control-tower-org-setup-sample Public
Automated AWS Organizations configuration for security operations
aws security automation amazon-web-services organizations guardduty securityhub eventbridge controltower macie
Python · MIT No Attribution · 12 · 36 · 3 · 1 · Updated on Feb 24

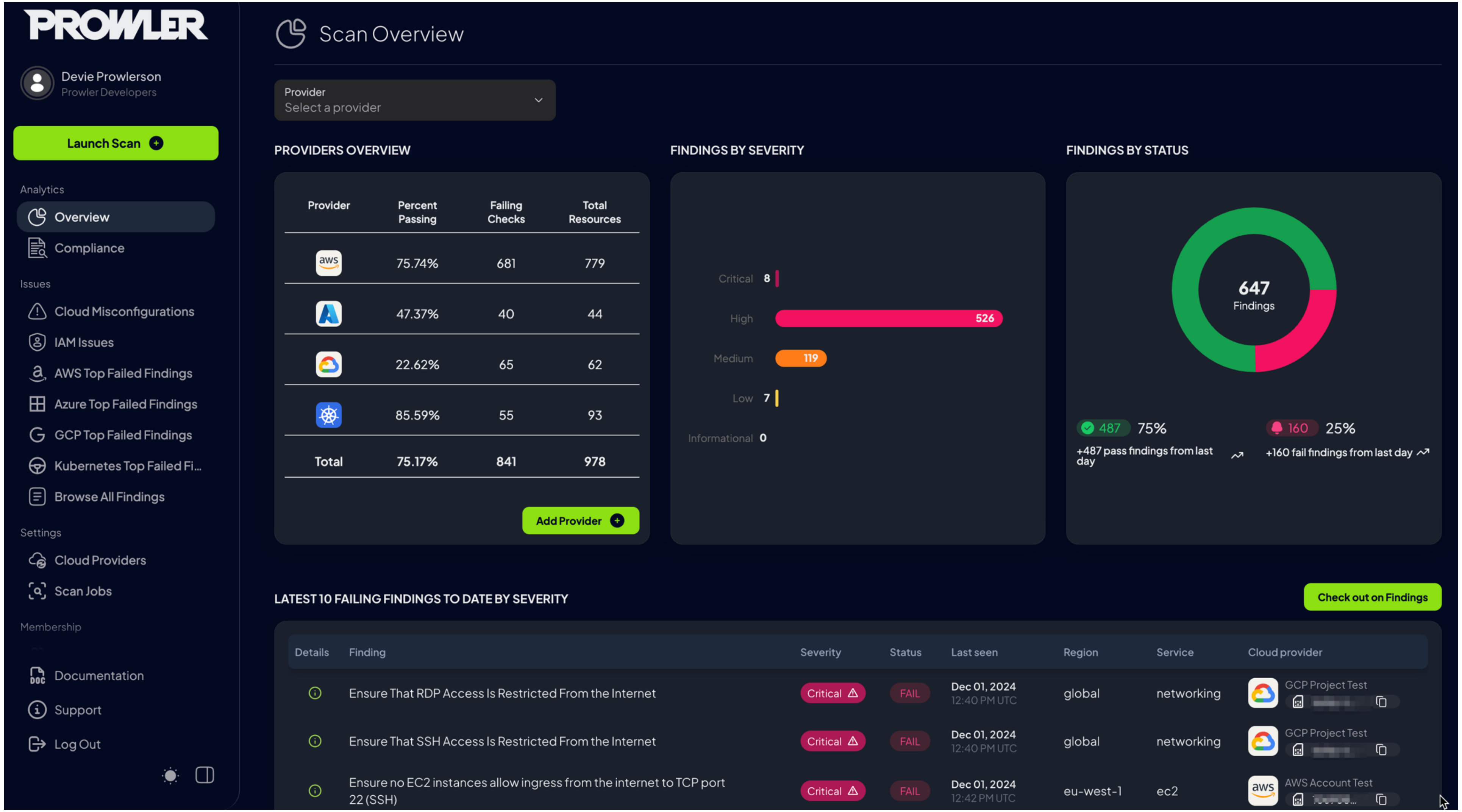
aws-securityhub-remediations Public
Python · MIT No Attribution · 33 · 34 · 3 · 2 · Updated on May 24, 2022



07

ALTERNATIVE SOLUTIONS

Open Source - Prowler



Scan Overview

Provider
Select a provider

PROVIDERS OVERVIEW

Provider	Percent Passing	Failing Checks	Total Resources
aws	75.74%	681	779
A	47.37%	40	44
	22.62%	65	62
☸	85.59%	55	93
Total	75.17%	841	978

Add Provider

FINDINGS BY SEVERITY

FINDINGS BY STATUS

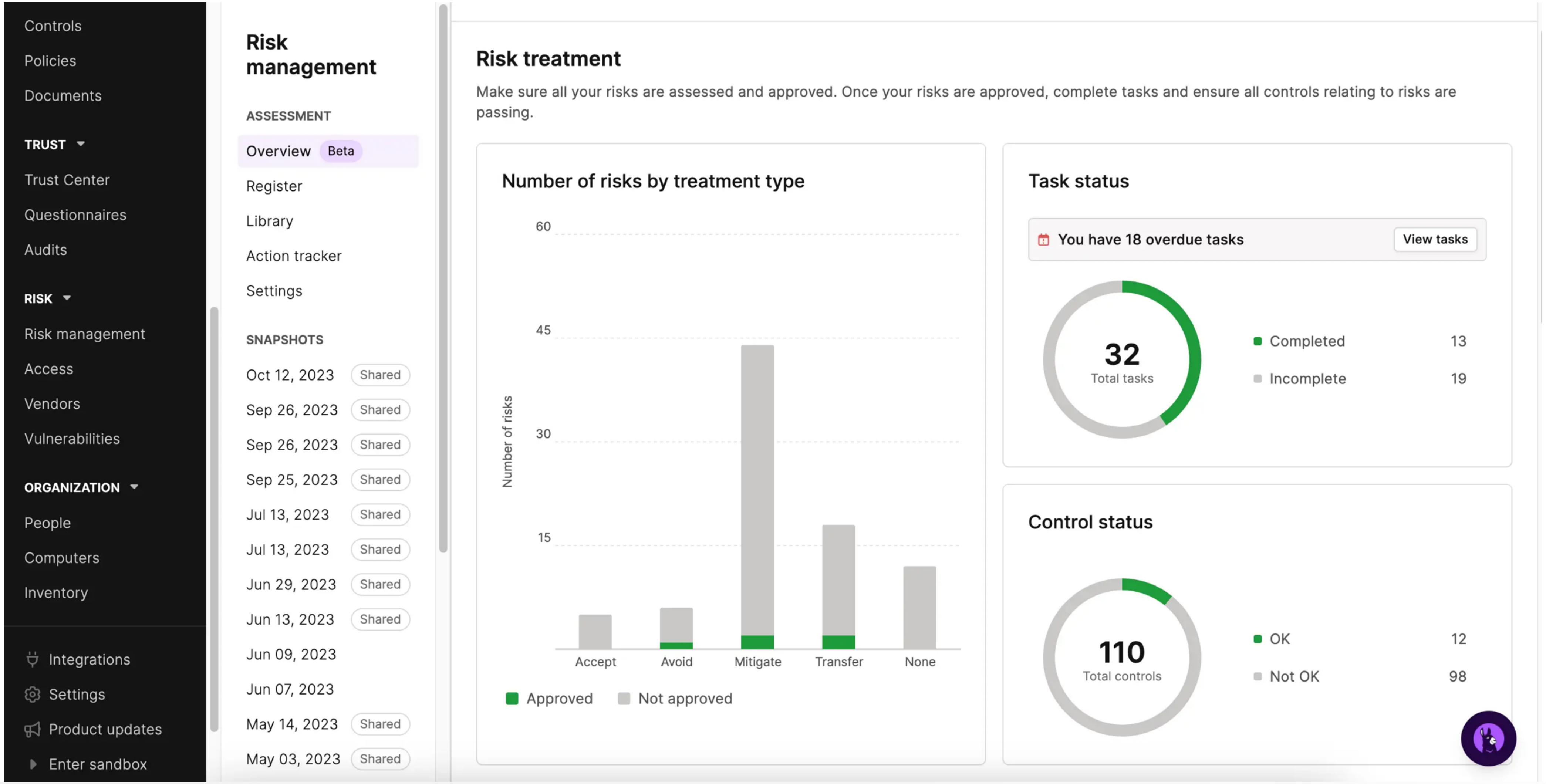
647
Findings
487 75%
+487 pass findings from last day
160 25%
+160 fail findings from last day

LATEST 10 FAILING FINDINGS TO DATE BY SEVERITY

Check out on Findings

Details	Finding	Severity	Status	Last seen	Region	Service	Cloud provider
ⓘ	Ensure That RDP Access Is Restricted From the Internet	Critical ⚠	FAIL	Dec 01, 2024 12:40 PM UTC	global	networking	GCP Project Test [redacted]
ⓘ	Ensure That SSH Access Is Restricted From the Internet	Critical ⚠	FAIL	Dec 01, 2024 12:40 PM UTC	global	networking	GCP Project Test [redacted]
ⓘ	Ensure no EC2 instances allow ingress from the internet to TCP port 22 (SSH)	Critical ⚠	FAIL	Dec 01, 2024 12:42 PM UTC	eu-west-1	ec2	aws AWS Account Test [redacted]

SaaS - Vanta



Risk management

ASSESSMENT

SNAPSHOTS

Oct 12, 2023	Shared
Sep 26, 2023	Shared
Sep 26, 2023	Shared
Sep 25, 2023	Shared
Jul 13, 2023	Shared
Jul 13, 2023	Shared
Jun 29, 2023	Shared
Jun 13, 2023	Shared
Jun 09, 2023	
Jun 07, 2023	
May 14, 2023	Shared
May 03, 2023	Shared

Risk treatment

Make sure all your risks are assessed and approved. Once your risks are approved, complete tasks and ensure all controls relating to risks are passing.

Number of risks by treatment type

Task status

You have 18 overdue tasks

32 Total tasks

🟩 Completed	13
▨ Incomplete	19

Control status

110 Total controls

🟩 OK	12
▨ Not OK	98

QUESTIONS?

WWW.SIGCORP.COM

Contact

Gabriel Tocci

Sr. Cloud Architect / Sr. Consultant

tocci@sigcorp.com

/strata-information-group

@SIGCorpLIVE

sigcorp.com