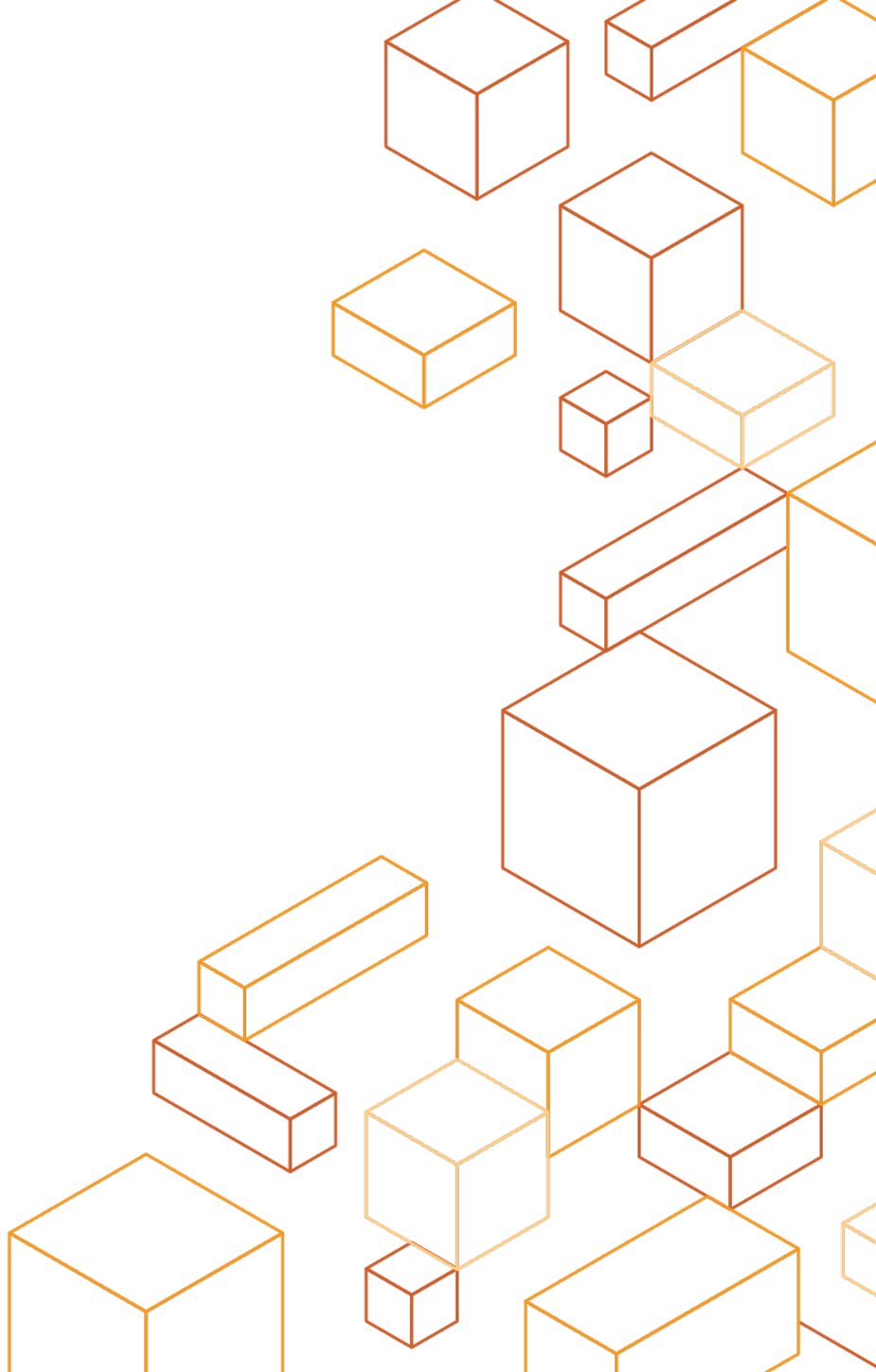
aws professional services

Logging & Monitoring



Agenda

- Log Sources
- Processing Logs
- Alerting
- Auditing

Goals

- Understand what logs are available
- Logging best practices
- Learn ways to extract value from multiple data sources
- Discover new services to enhance security awareness

Outcomes

- Decision on which AWS logs to enable and collect (CloudTrail, Service Logs)
- Decision on which OS & Application logs to enable and collect
- Decision on where to store logs (S3/CloudWatch)
- Decisions on encryption of log files
- Decision on whether to enable AWS Config
- Decision on whether to enable GuardDuty
- Decision on who is responsible for and how alerting will take place

Different Log Categories

AWS Infrastructure logs

- AWS CloudTrail
- Amazon VPC Flow Logs

AWS service logs

- Amazon S3
- AWS Elastic Load Balancing
- Amazon CloudFront
- AWS Lambda
- AWS Elastic Beanstalk
- …

Host based logs

- Messages
- Security
- NGINX/Apache/IIS
- Windows Event Logs
- Windows Performance Counters
- …

Native AWS Logging

Category	Service	Data	Method
Compute	ELB	Access logs	Written to S3
Storage/Content	S3	Object access	Written to S3
Storage/Content	CloudFront	Access logs, cookies	Written to S3
Storage/Content	Glacier	Retrieval jobs only	SNS
Management	OpsWorks	Chef logs	Console (download)
Management	Data Pipeline	Errors only	Written to S3
Management	CloudHSM	Appliance login, trust links	Syslog
App Services	SES	Bounces, complaints	SNS
App Services	SNS	Messages sent	SNS
App Services	EMR	Infer changes from Hadoop logs	Written to S3
Networking	VPC	Flow Logs	Console/CloudWatch Logs

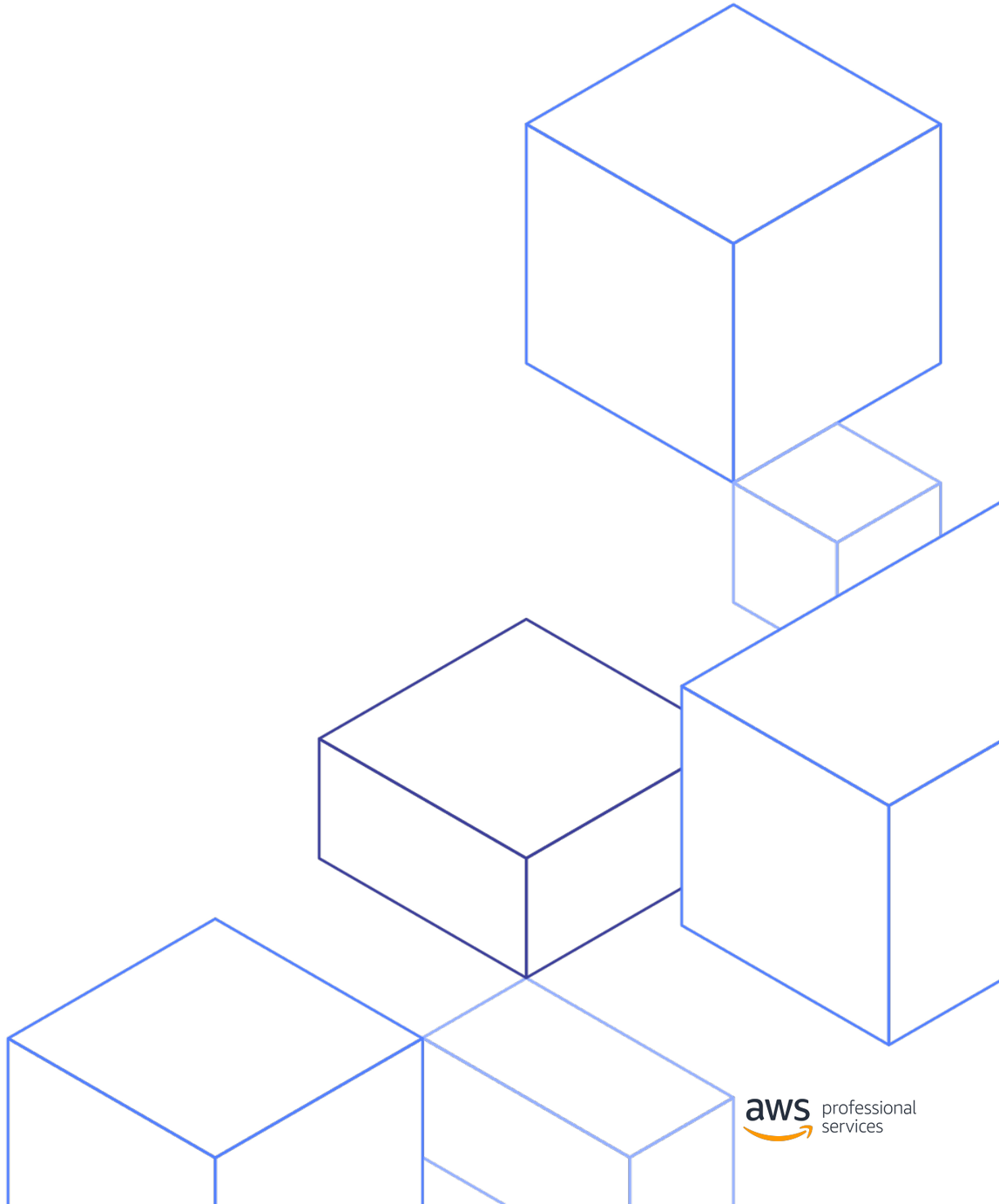
Ubiquitous Logging and Monitoring

Amazon CloudWatch Logs lets you **grab everything** and **monitor activity**

- Managed service to collect and keep your logs
- CloudWatch Logs Agent for Linux and Windows instances
- Integration with **Metrics** and **Alarms**
- Export data to S3 for analytics
- Stream to Amazon OpenSearch Service or AWS Lambda

AWS CloudTrail

Logging & Monitoring

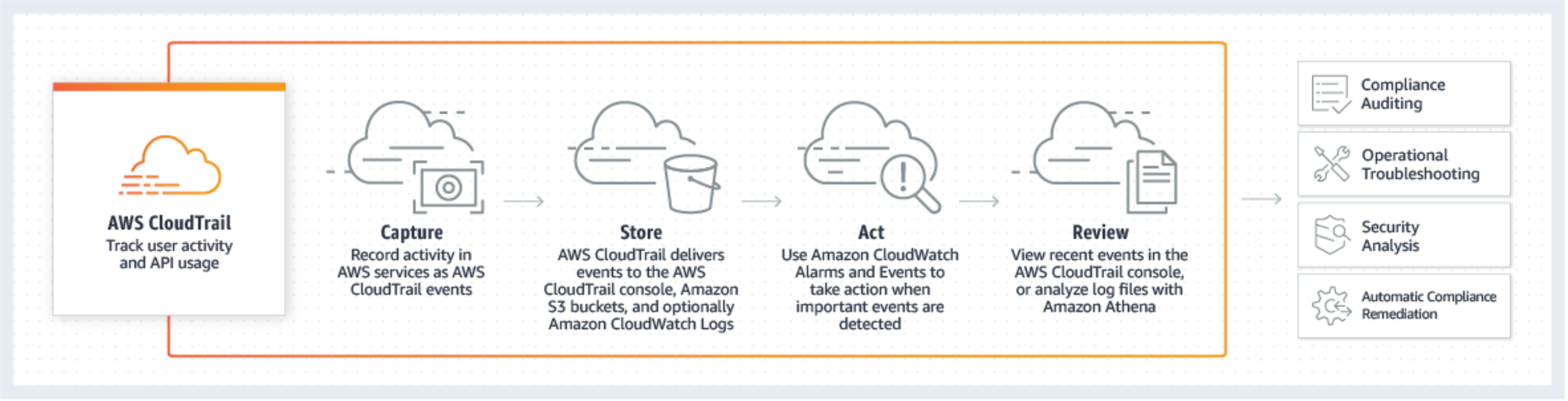


aws professional services

AWS CloudTrail

What is it?

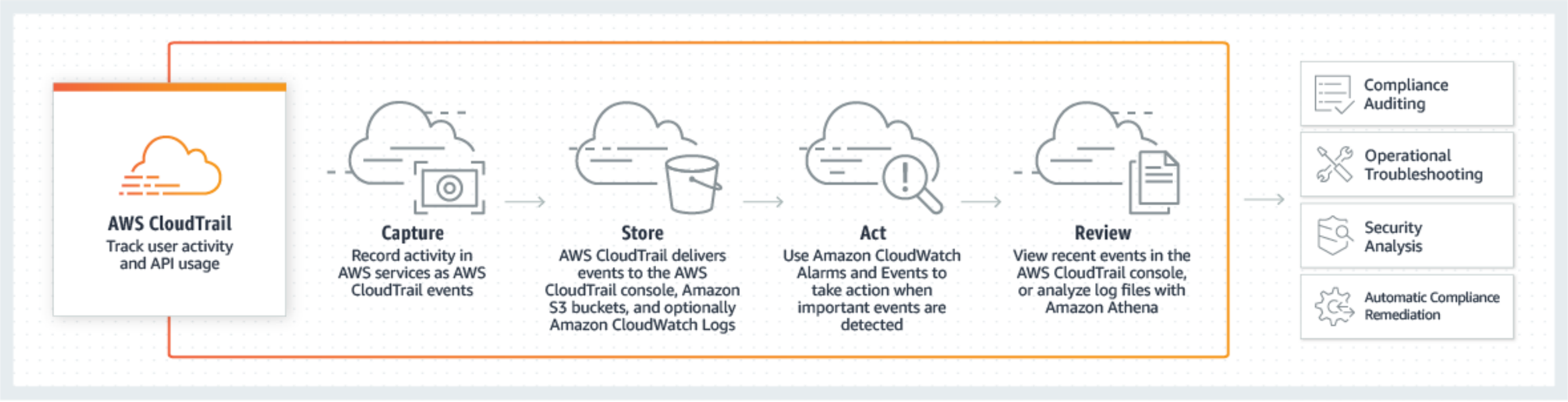
- A service that enables governance, compliance, and operational and risk auditing of your AWS account
- With CloudTrail, you can capture and log events related to API calls and account activity events across your AWS infrastructure and resources



AWS CloudTrail

What can you do?

- Simplify your compliance audits by automatically recording and storing activity logs for your AWS account
- Increase visibility into your user and resource activity
- Discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in your AWS account

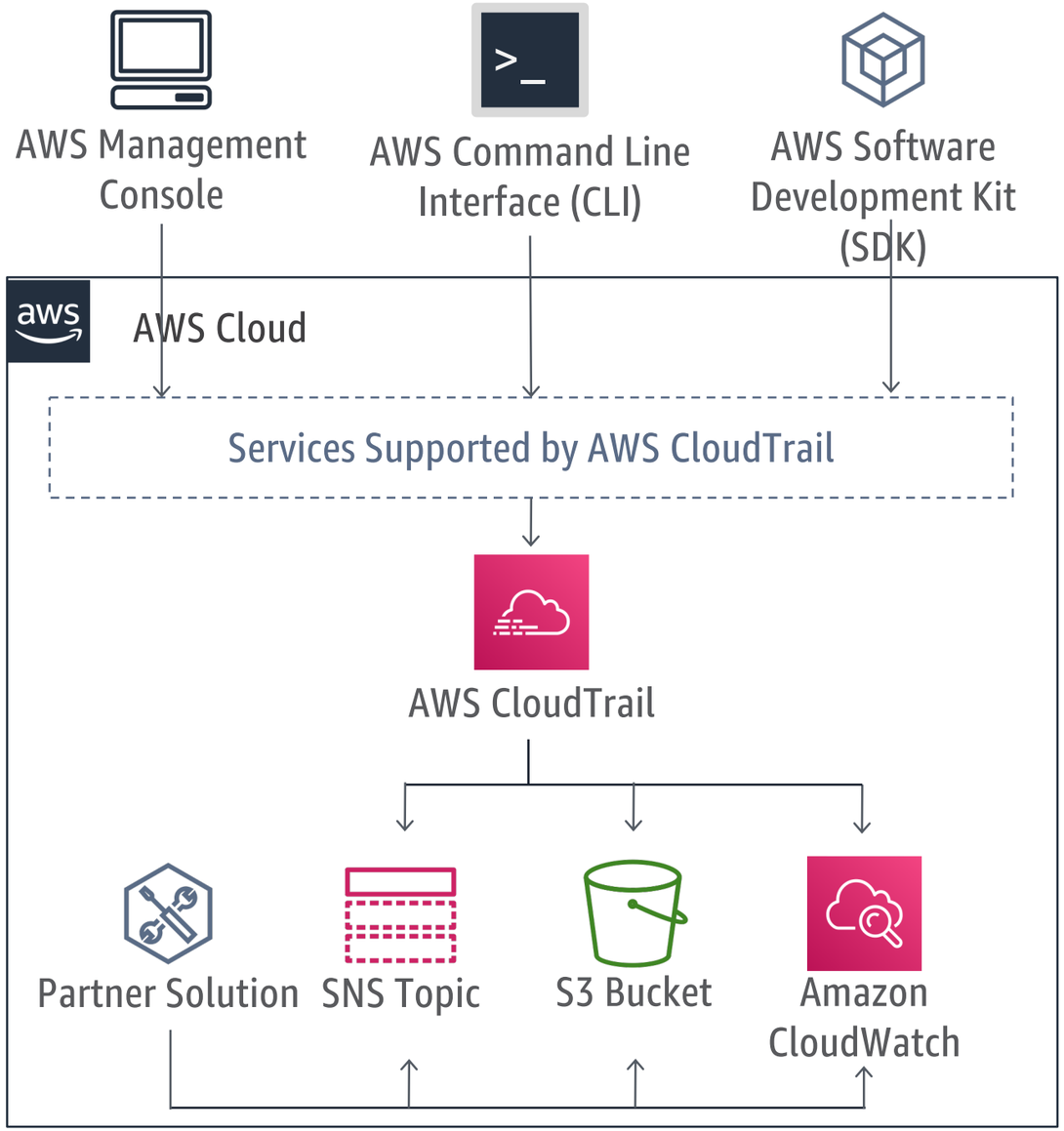


AWS CloudTrail - Common Use Cases

- **Compliance Aid**: AWS CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards by providing a history of API calls in your AWS account
- **Security Analysis**: You can perform security analysis and detect user behavior patterns by ingesting AWS CloudTrail API call history into your log management and analytics solutions such as CloudWatch Logs, CloudWatch Events, Athena, OpenSearch, or other 3rd party solution
- **Data Exfiltration**: You can detect data exfiltration by collecting activity data on S3 objects through object-level API events recorded in CloudTrail. After the activity data is collected, you can use other AWS services, such as Amazon CloudWatch Events and AWS Lambda, to trigger response procedures
- **Operational Issue Troubleshooting:** You can troubleshoot operational issues by leveraging the AWS API call history produced by AWS CloudTrail. For example, you can quickly identify the most recent changes made to resources in your environment, including creation, modification, and deletion of AWS resources (e.g., Amazon EC2 instances, Amazon VPC security groups, and Amazon EBS volumes)

AWS CloudTrail

- CloudTrail records API calls in your account and delivers a log file to your S3 bucket.
- Typically, delivers an event within 15 minutes of the API call.
- Log files are delivered approximately every 5 minutes.
- Multiple partners offer integrated solutions to analyze log files.



AWS CloudTrail - Security-Relevant Logs

- **Who** made the API call?
- **When** was the API call made?
- **What** was the API call?
- **Where** was the API call made from?
- **Which** resources were acted upon in the API call?

AWS CloudTrail - Security-Relevant Logs

- Who
- When
- What
- Where
- Which

aws professional services

AWS CloudTrail - Configuration

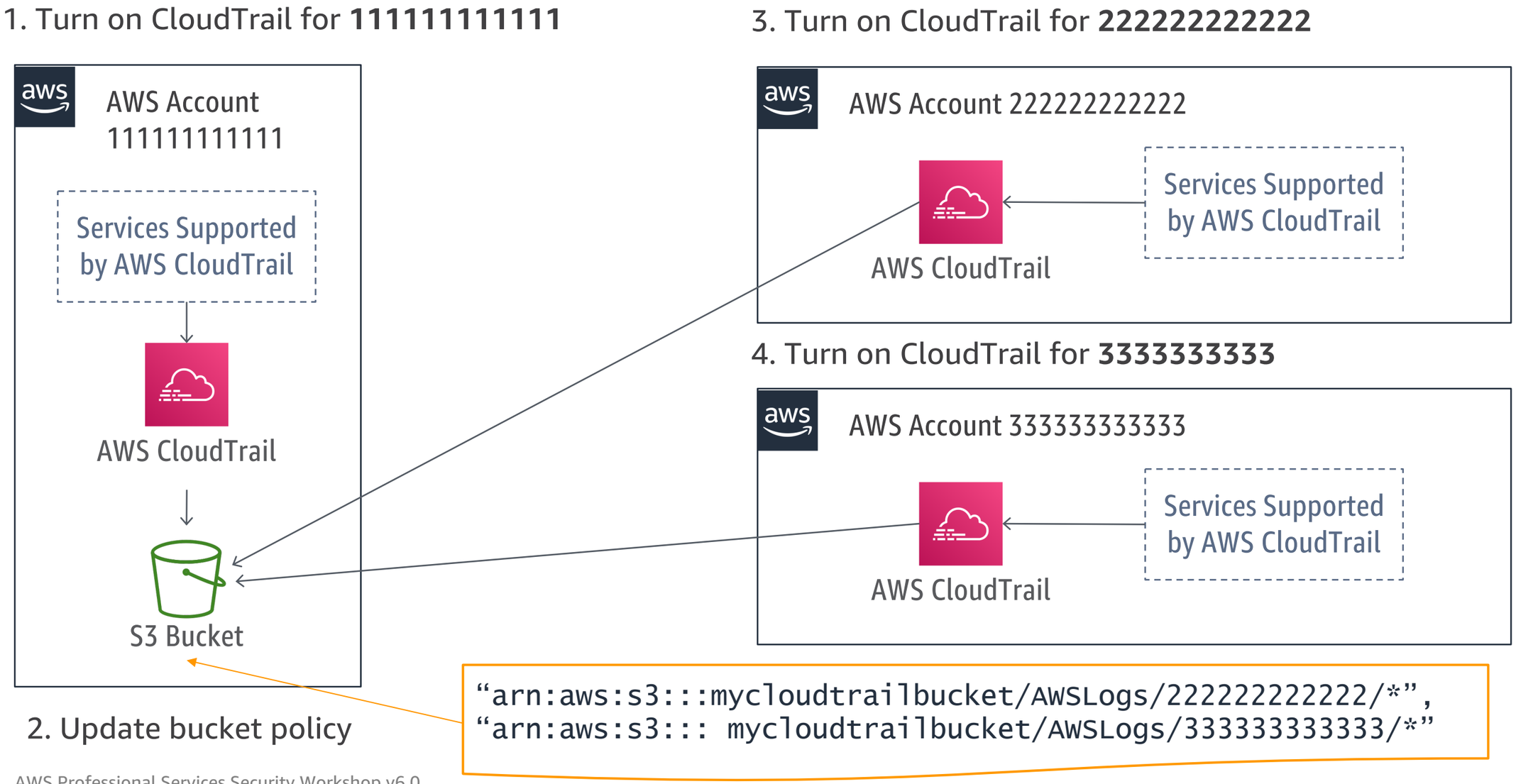
- You can create two types of “trails”:
  - A trail that applies to all regions
  - A trail that applies to one region

- When you create a trail that applies to all regions, CloudTrail creates the same trail in each region, records the log files in each region, and delivers the log files to the single S3 bucket

AWS CloudTrail – Centralizing Logs

- Many-to-one centralization
    - From multiple regions into one S3 bucket (described before)
    - From multiple accounts into one account's S3 bucket

AWS CloudTrail – Centralizing Logs



aws professional services

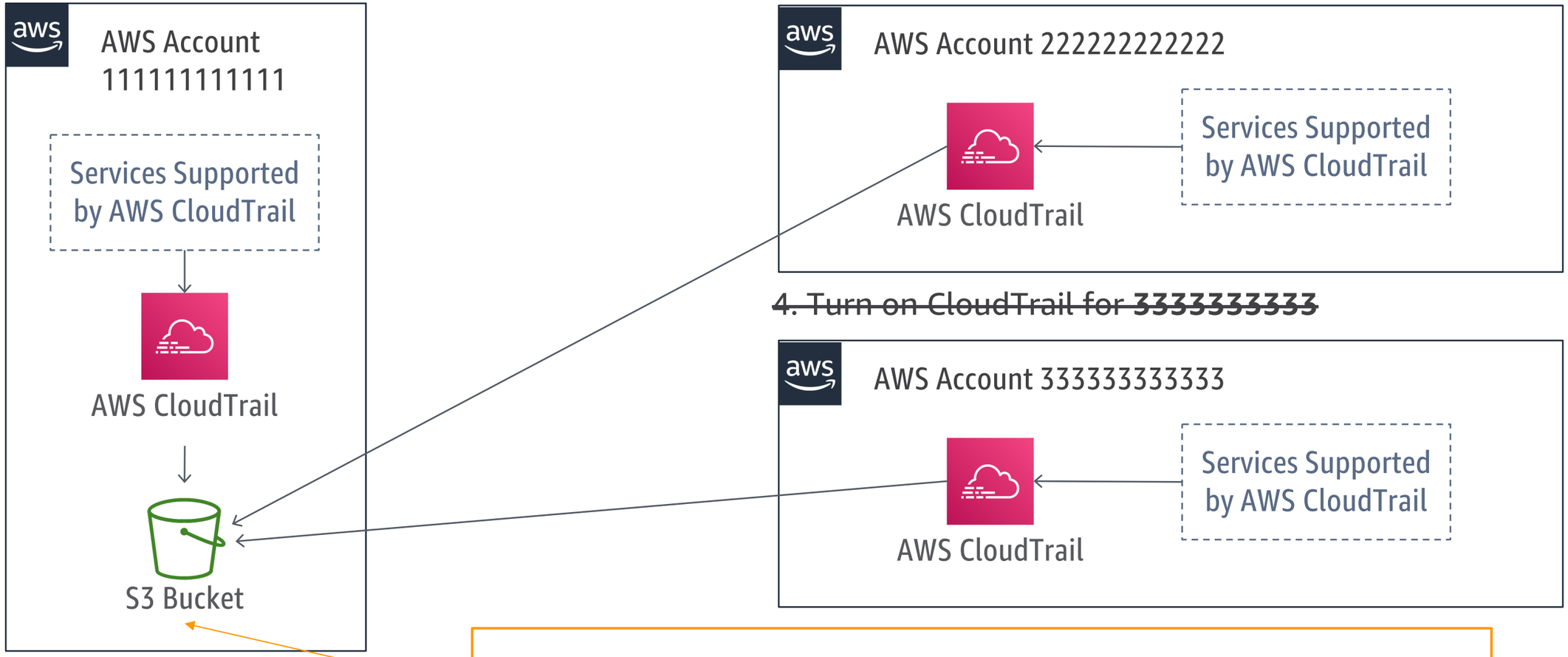
AWS CloudTrail – Centralizing Logs

- Centralization within your AWS Organization
    - Enable CloudTrail once in the Master account and have it applied to all AWS accounts
    - log prefix changes from “/AWSLogs/<accountID>/” to “/AWSLogs/<OrganizationID>/” – no more updating of the bucket policy

Watch out for multiple trails when enabling in an existing Organization!

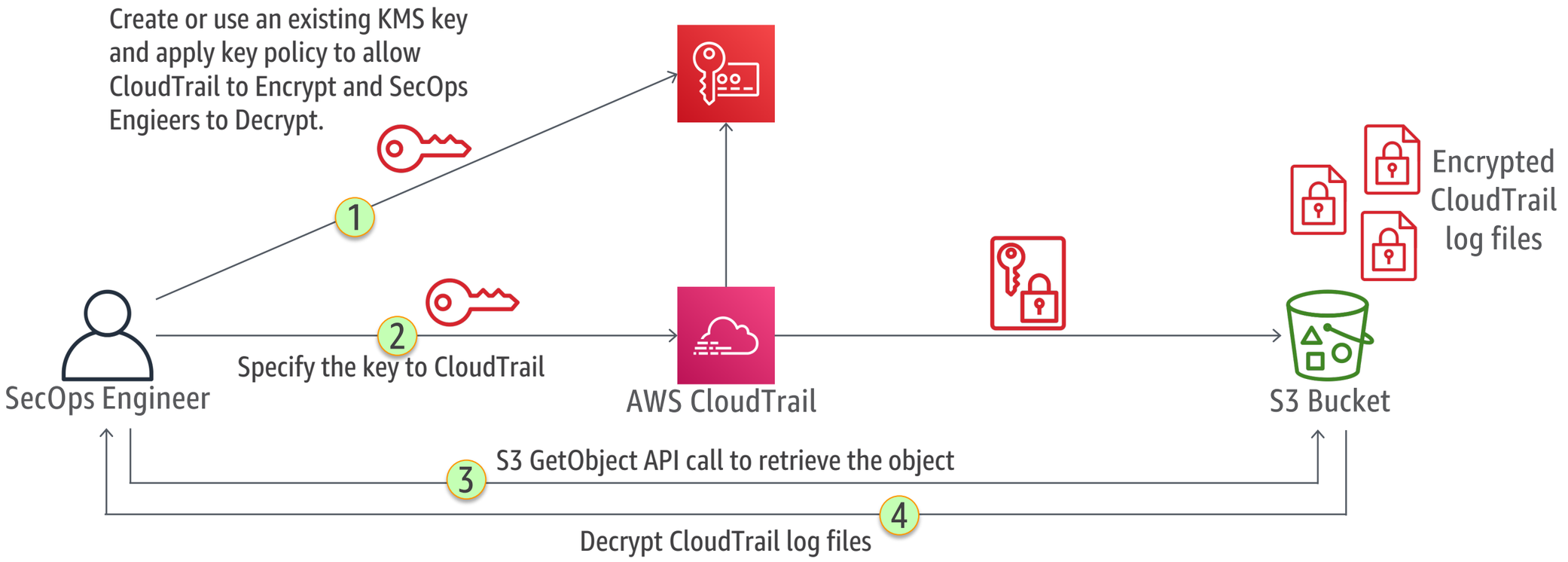
AWS CloudTrail – Centralizing Logs

1. Turn on CloudTrail for **your Organization**



aws professional services

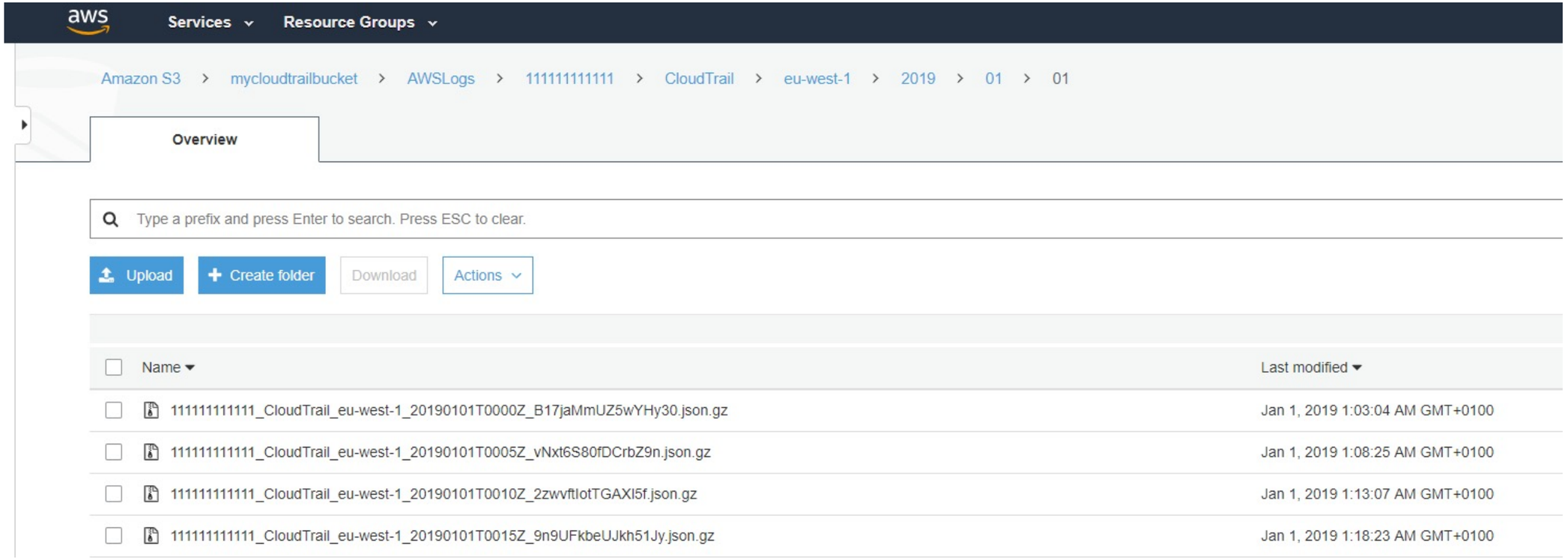
AWS CloudTrail – KMS Encryption



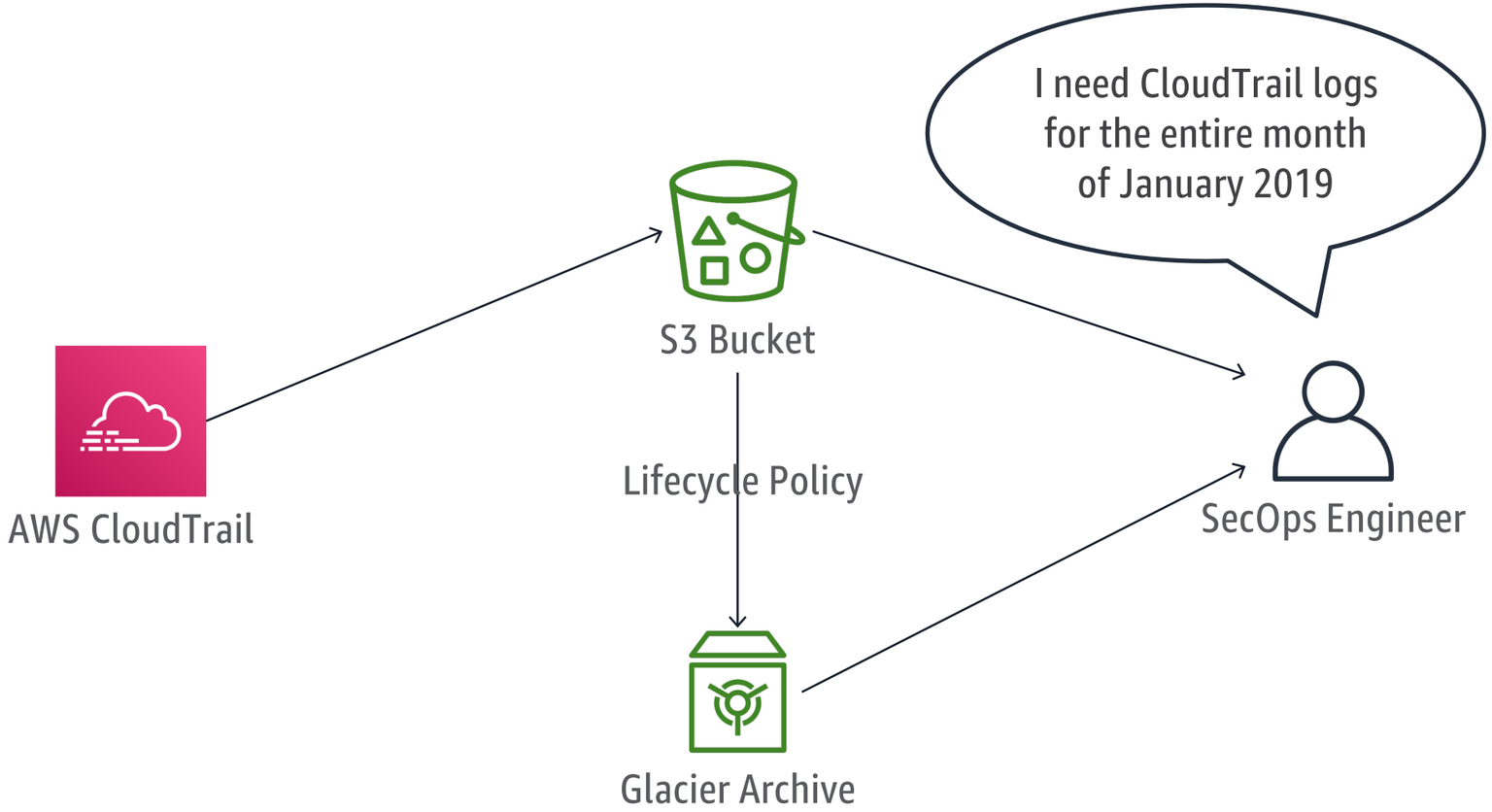
aws professional services

AWS CloudTrail – Storage in S3

- Default descriptive folder structure makes it easier to store log files from multiple accounts and regions in the same S3 bucket.
- Detailed log file name helps identify the contents of the log file
- Unique identifier in the file name prevents overwriting log files.



AWS CloudTrail – Lifecycle Management

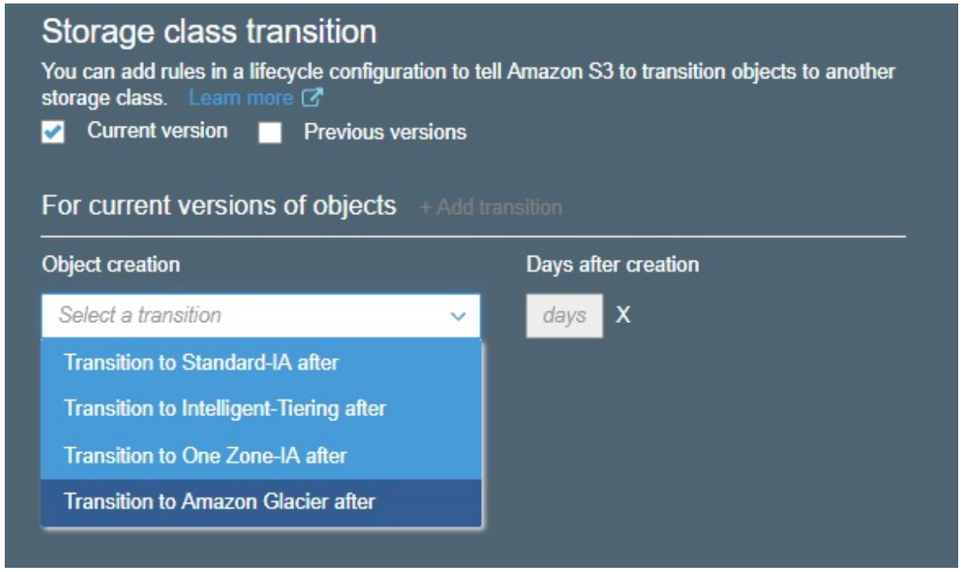


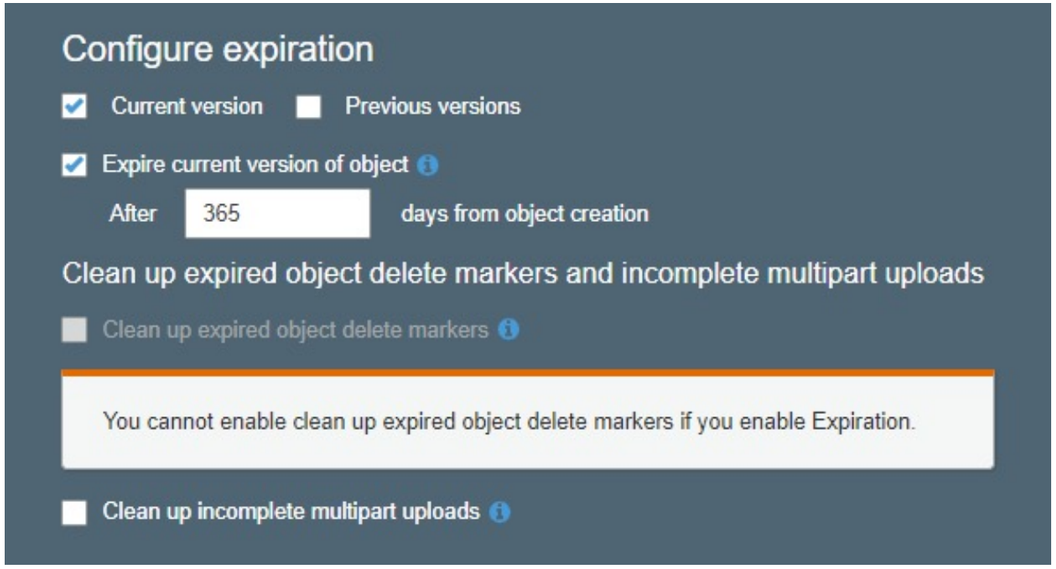
AWS CloudTrail – Lifecycle Management

Configured via S3

Available actions:

- Transition to different storage Tier
- Expire (delete) object
- Transition & Expire





AWS CloudTrail – Lifecycle Management

Lets assume the following rule has been set up for the target bucket:

Transition to Amazon Glacier 30 days after creation date.

Expire 100 days after creation date.

- The object was uploaded to the target bucket on 1-October. The creation date of this object is 1-October.
- On 30-October, 30 days after the object's creation date, the Lifecycle rule takes effect and automatically transitions the object to Amazon Glacier.
- On 9-January, 100 days after the object's creation date, the Lifecycle rule takes effect again and automatically expires the object. The object is now permanently deleted and cannot be recovered.

AWS CloudTrail – Integrity Validation

- To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it, you can use CloudTrail log file integrity validation. Validated log files are invaluable in security and forensic investigations.
- This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. You can use the AWS CLI to validate the files in the location where CloudTrail delivered them.

AWS CloudTrail – Integrity Validation

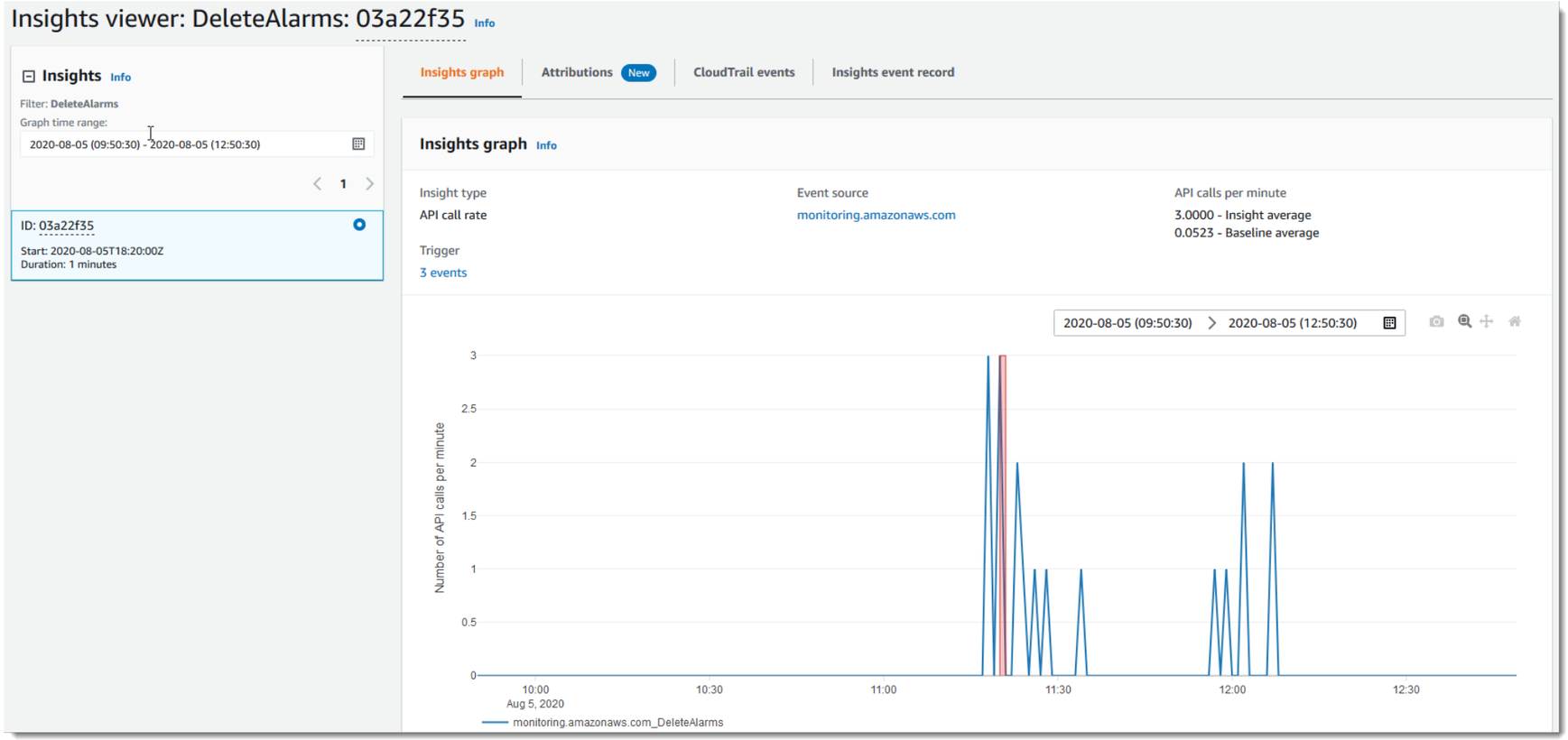
- Once you enable log file integrity validation, CloudTrail will start delivering digest files, on an hourly basis, to the same S3 bucket where you receive your CloudTrail log files, but with a different prefix:
- CloudTrail log files are delivered to:

  `/optional_prefix/AWSLogs/AccountID/CloudTrail/*`
- CloudTrail digest files are delivered to:

  `/optional_prefix/AWSLogs/AccountID/CloudTrail-Digest/*`

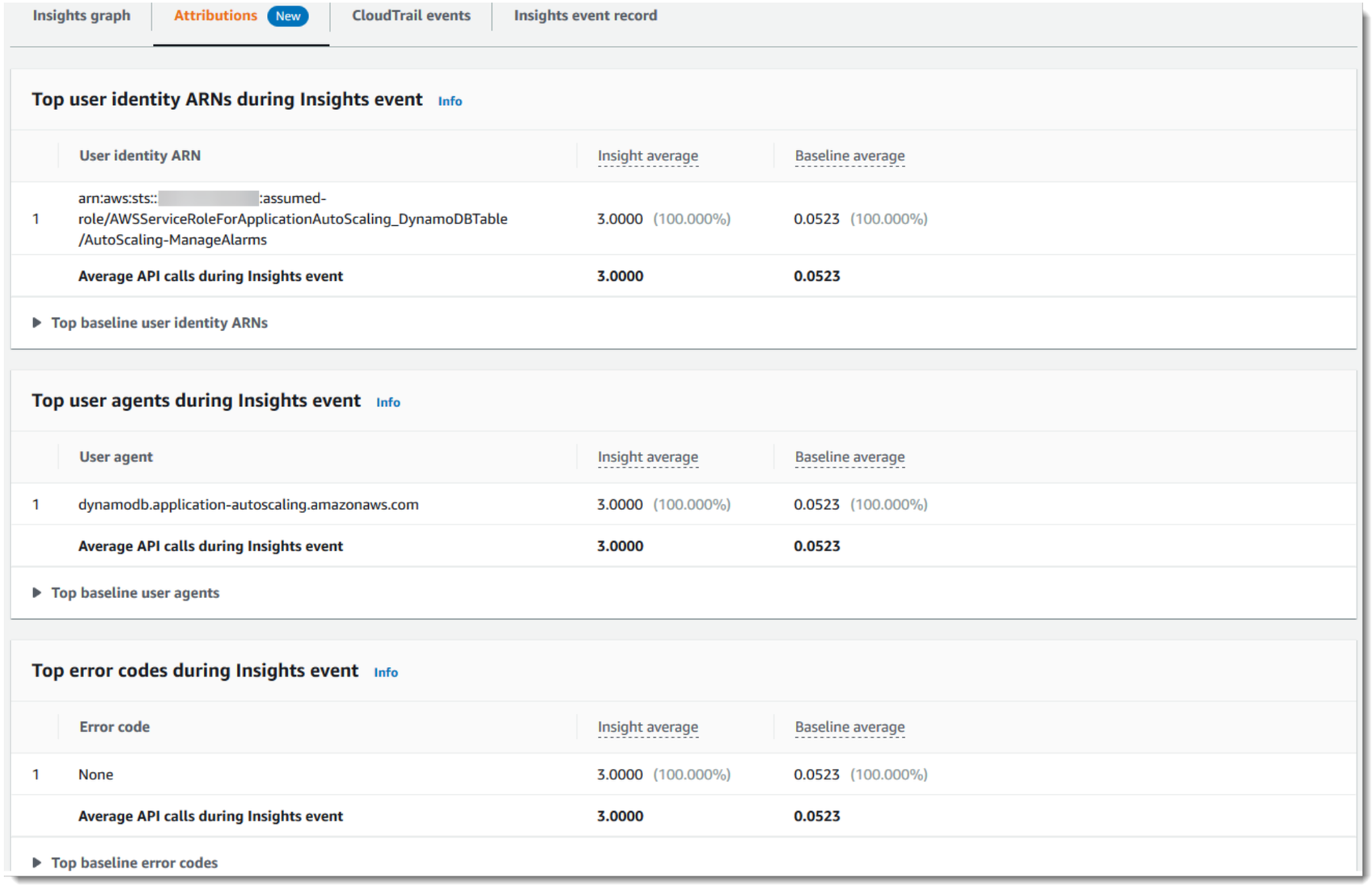
AWS CloudTrail Insights

- Provides insights into unusual write API activity based on anomaly detection.
- Not enabled by default and can take up to 36 hours to be available.



aws professional services

AWS CloudTrail Insights



aws professional services

AWS CloudTrail – Best Practices

1. **Enable in all regions and accounts**

Benefits

- Also tracks unused regions
- Can be done in single configuration step
- Use the organizational trail to automatically onboard all account in an AWS Organization

AWS CloudTrail – Best Practices

1. Enable in all regions and accounts
2. **Enable log file validation**

Benefits

- Ensure log file integrity
- Validated log files are invaluable in security and forensic investigations
- Built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing
- AWS CloudTrail will start delivering digest files on an hourly basis
- Digest files contain hash values of log files delivered and are signed by AWS CloudTrail

AWS CloudTrail – Best Practices

1. Enable in all regions and accounts
2. Enable log file validation
3. **Encrypted logs**

Benefits

- By default, AWS CloudTrail encrypts log files using Amazon S3 server side encryption (SSE-S3)
- You can choose to encrypt using AWS Key Management Service (SSE-KMS)
- Amazon S3 will decrypt on your behalf if your credentials have decrypt permissions

AWS CloudTrail – Best Practices

1. Enable in all regions and accounts
2. Enable log file validation
3. Encrypted logs
4. **Integrate with Amazon CloudWatch Logs**

Benefits

- Simple search
- Configure alerting on events

AWS CloudTrail – Best Practices

1. Enable in all regions and accounts
2. Enable log file validation
3. Encrypted logs
4. Integrate with Amazon CloudWatch Logs
5. **Centralize logs from all accounts**

Benefits

- Configure all accounts to send logs to a central security account
- Reduce risk for log tampering
- Can be easily achieved with AWS Organizations
- Can be combined with S3 Cross-Region Replication

AWS CloudTrail – Best Practices

1. Enable in all regions and accounts
2. Enable log file validation
3. Encrypted logs
4. Integrate with Amazon CloudWatch Logs
5. Centralize logs from all accounts
6. **Apply Lifecycle Policies to logging buckets**

Benefits

- Limit the storage costs of log files
- Prevent manual pruning and the risk of altering of log files
- Automate archival of log files for long-term storage

Amazon VPC Flow Logs

Logging & Monitoring

aws professional services

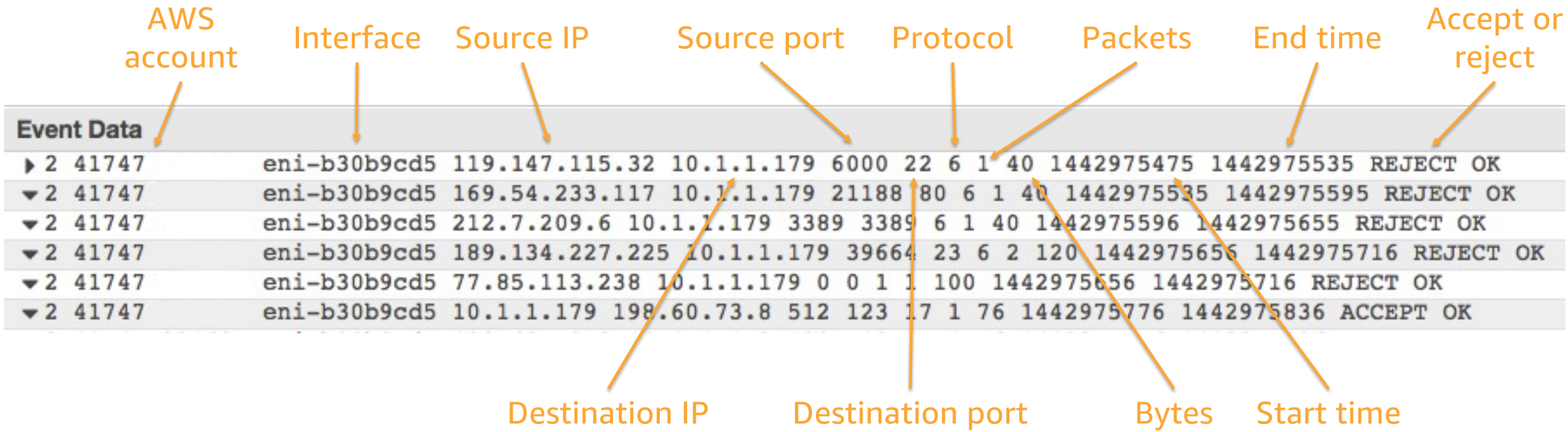
Amazon VPC Flow Logs

- Stores log in AWS CloudWatch Logs
- Can be enabled on
    - Amazon VPC, a subnet, or a network interface
    - Amazon VPC & Subnet enables logging for all interfaces in the VPC/subnet
- Each network interface has a unique log stream
- Flow logs do not capture real-time log streams for your network interfaces
- Filter desired result based on need
    - All, Reject, Accept
    - Troubleshooting or security related with alerting needs?
    - Think before enabling All on VPC, will you use it?

Amazon VPC Flow Logs

- Agentless
- Enable per ENI, per subnet, or per VPC
- Logged to AWS CloudWatch Logs

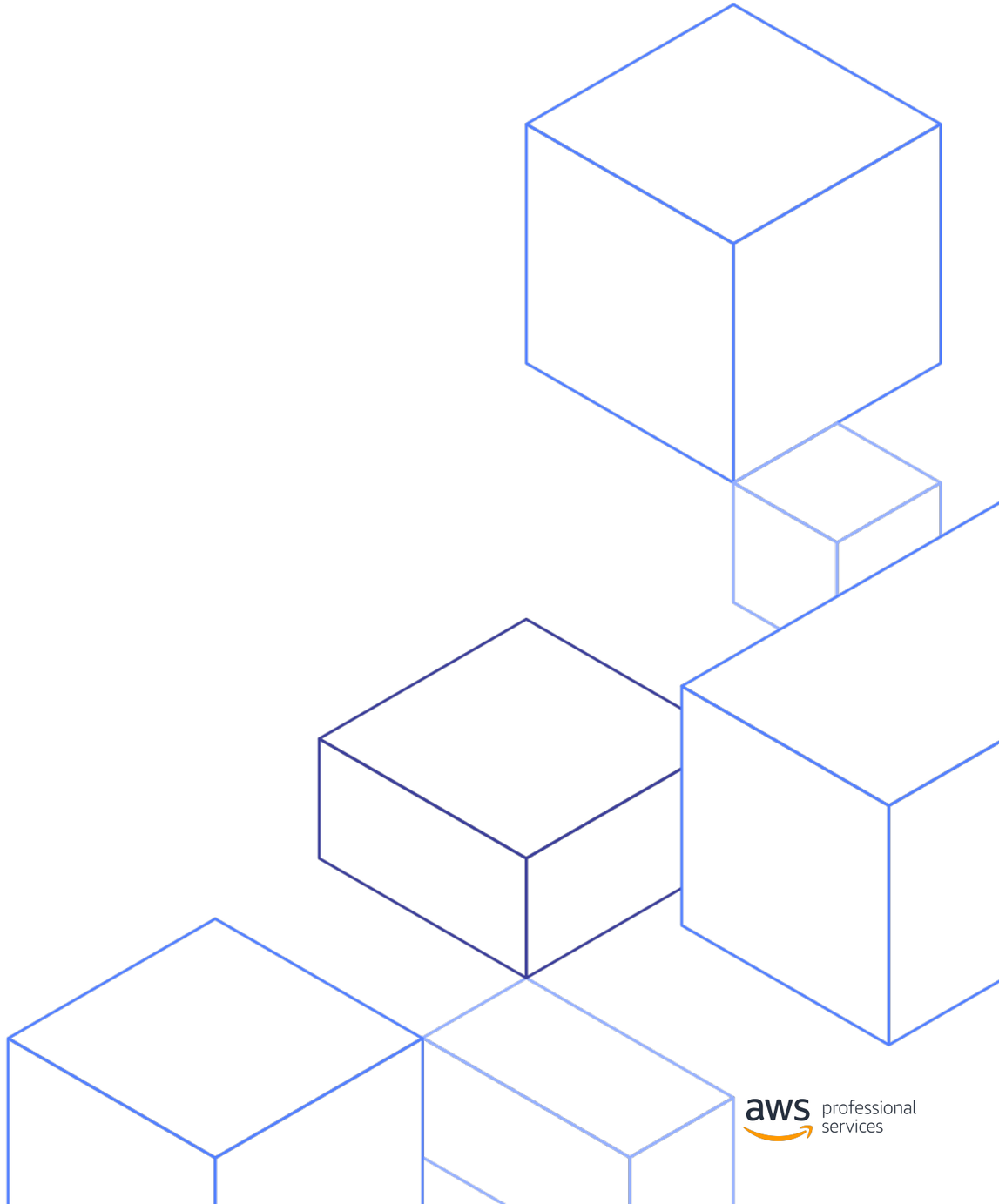
- Create CloudWatch metrics from log data
- Alarm on those metrics



aws professional services

Processing Logs

Logging & Monitoring



aws professional services

Processing Logs

CloudWatch Logs

- Near real-time, aggregate, monitor, store, and search

Amazon OpenSearch Service Integration (or ELK stack)

- Analytics and Kibana interface

AWS Lambda & Amazon Kinesis Integration

- Custom processing with your code

Export to S3

- SDK & CLI batch export of logs for analytics

Amazon OpenSearch Service

(Successor to Amazon Elasticsearch Service)

Logging & Monitoring

aws professional services

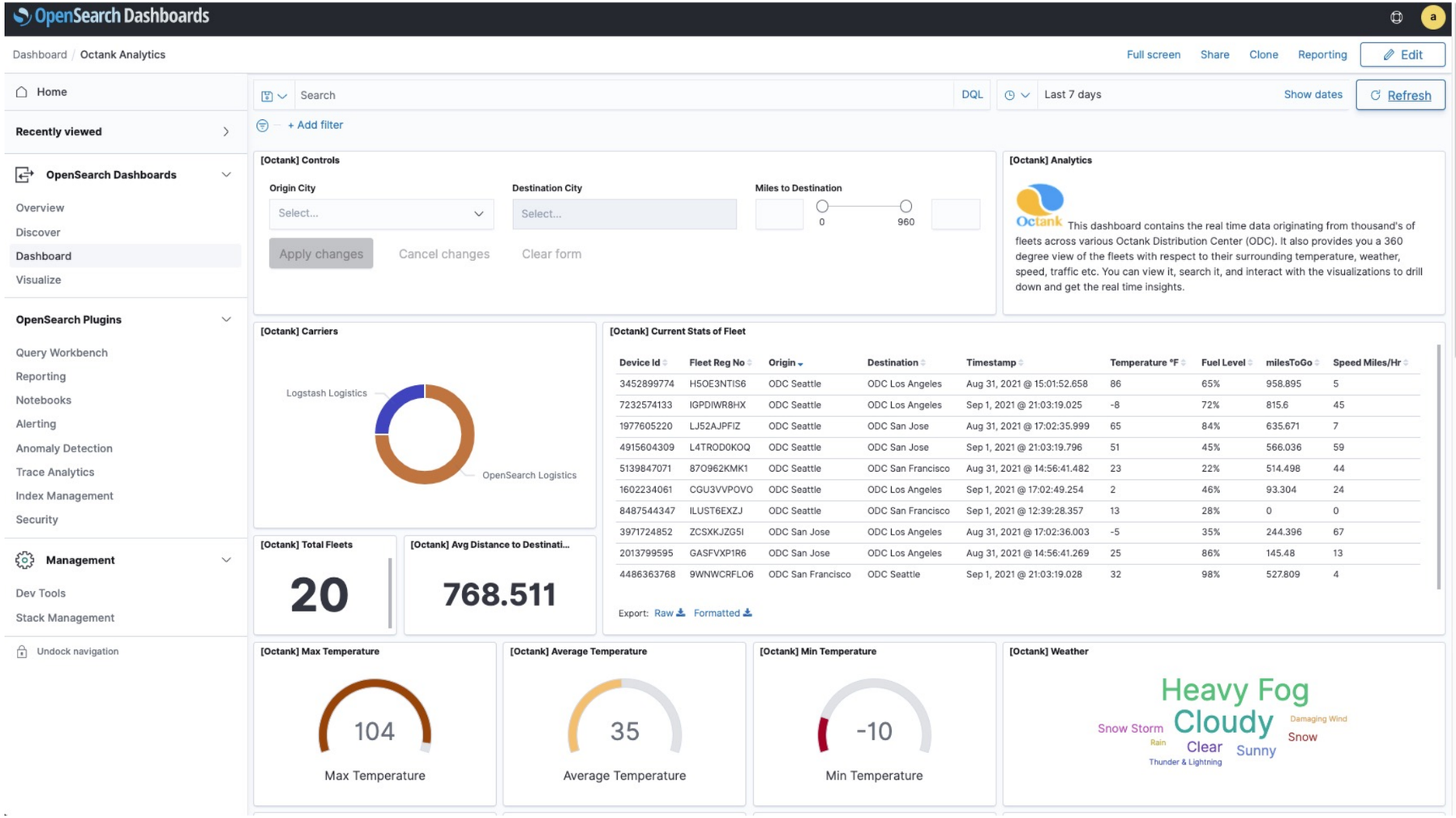
Amazon OpenSearch Service – What is it?

Amazon OpenSearch Service makes it easy for you to perform:

- interactive log analytics
- real-time application monitoring
- website search

OpenSearch is an open source, distributed search and analytics suite derived from Elasticsearch. Amazon OpenSearch Service offers the latest versions of OpenSearch, support for 19 versions of Elasticsearch (1.5 to 7.10 versions), and visualization capabilities powered by OpenSearch Dashboards and Kibana (1.5 to 7.10 versions).

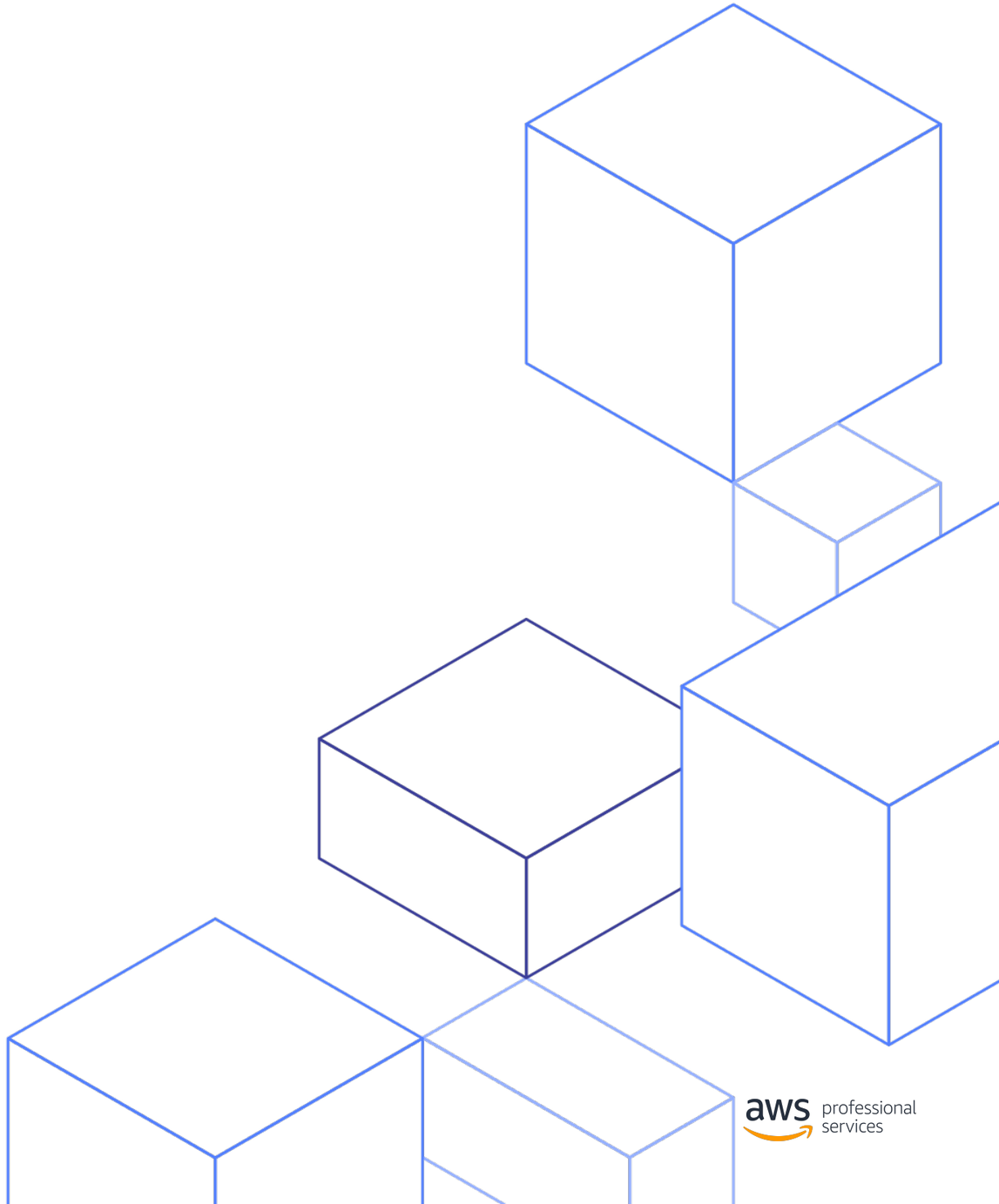
Amazon OpenSearch Service – Dashboards



aws professional services

Amazon Athena

Logging & Monitoring



aws professional services

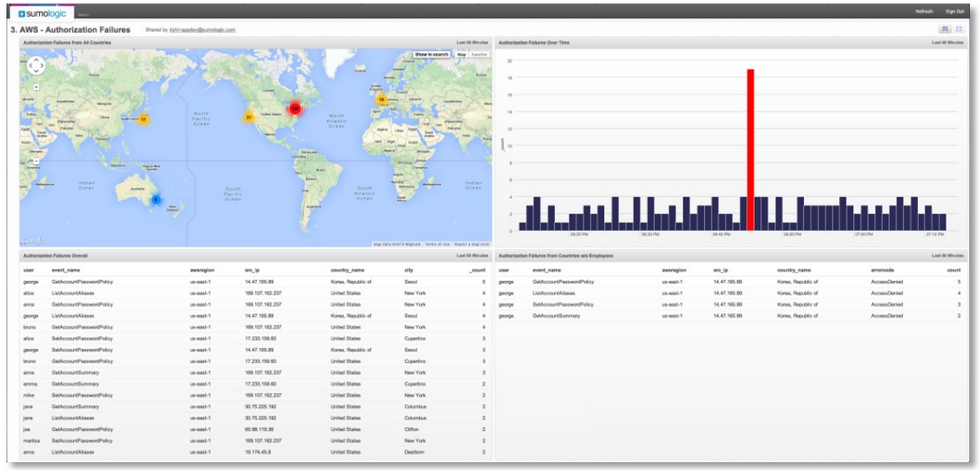
Amazon Athena – What is it?

Amazon Athena is an interactive query service that makes it easy to analyze data directly on Amazon S3 using Standard SQL

Amazon Athena – Why?

1. Decouple storage from compute
2. Serverless – No infrastructure or resources to manage
3. Pay only for data scanned
4. Schema on read – Same data, many views
5. Secure – IAM for authentication; Encryption at rest & in transit
6. Standard compliant and open storage file formats
7. Built on powerful community supported OSS solutions

Processing Logs – Partner Solutions



logentries

bounday

sumologic

Smartronix

Cloud ASSURED

CloudCheckr

ALERTLOGIC
Security. Compliance. Cloud.

STACKDRIVER

splunk>

DATADOG

LOGGLY

DATAPIPE

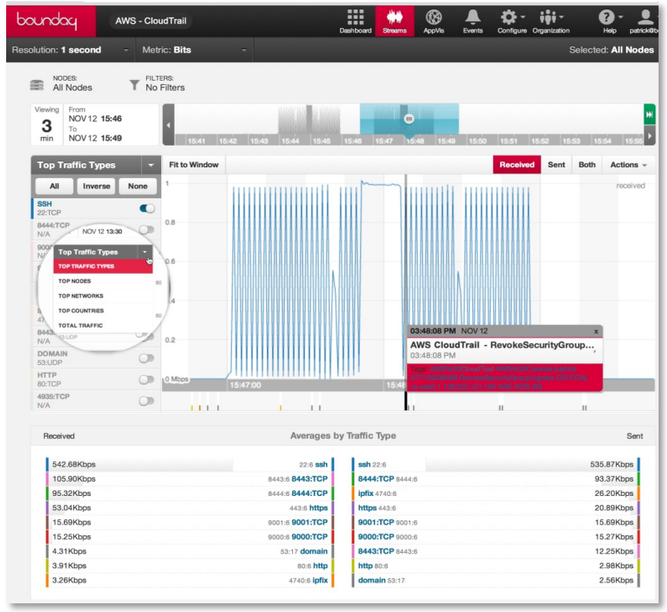
2ND WATCH

CLOUDNEXA

FOGHORN WEBSERVICES

CLOUDLYTICS

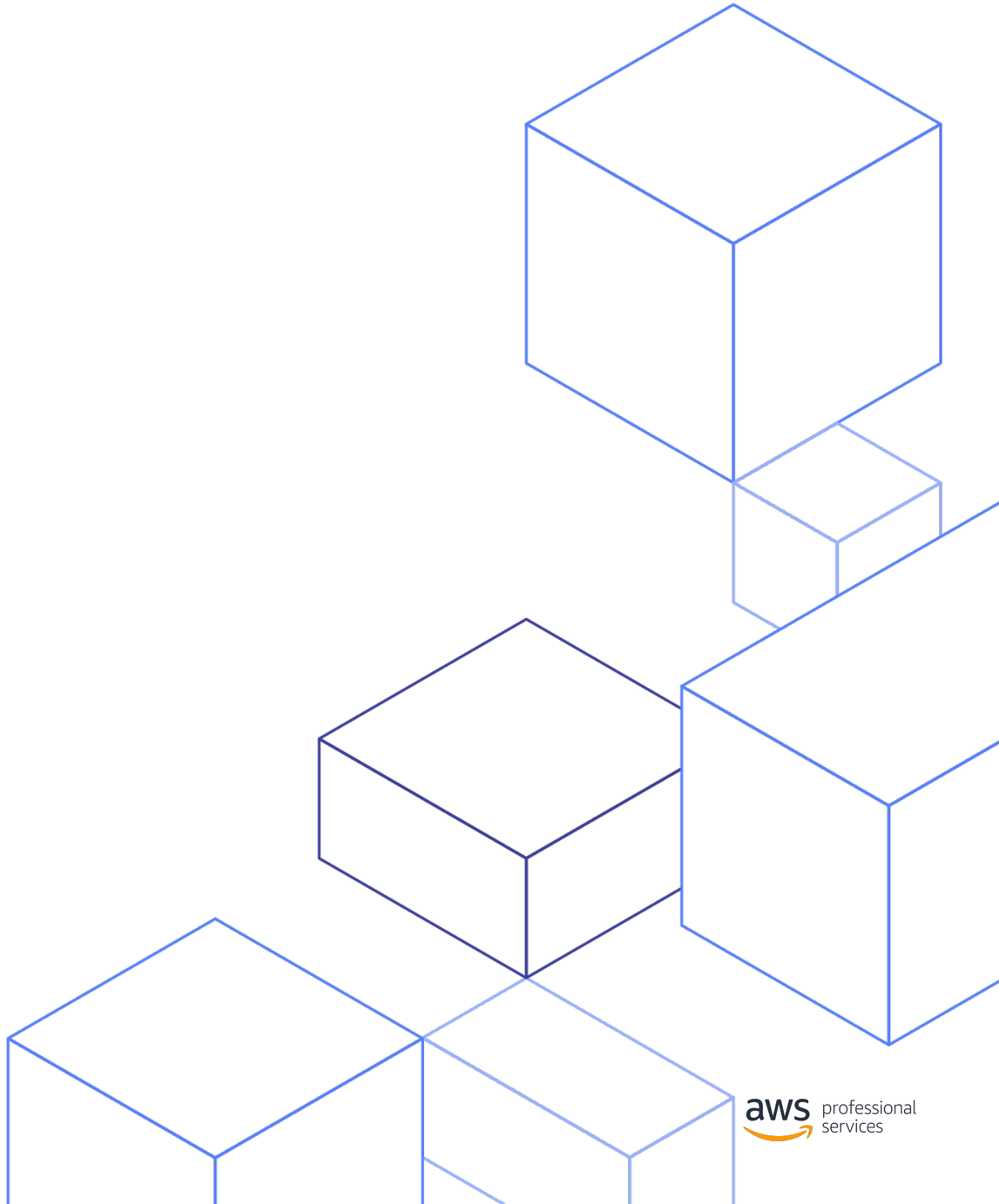
graylog



aws professional services

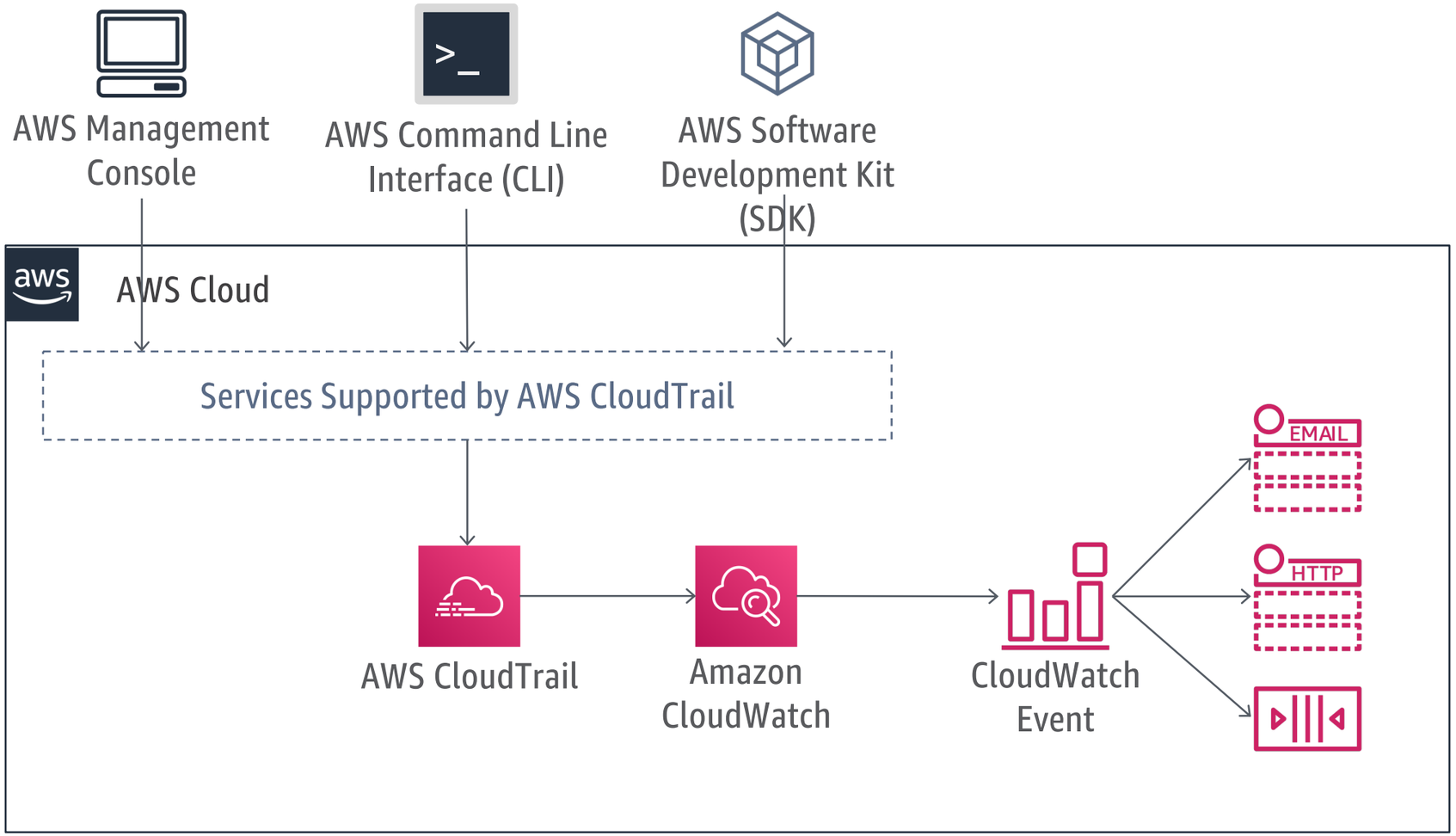
Alerting

Logging & Monitoring



aws professional services

Alerting – Receive Notifications of API activity



Follow-up Actions

- Create a Ticket
- Send an E-Mail
- Automatically Remediate
- Message somebody on Slack

aws professional services

Alerting - EventBridge Events

Trigger on event

- Amazon EC2 instance state change notification
- AWS API call (very specific)
- Auto Scaling
- AWS Config

Or Schedule

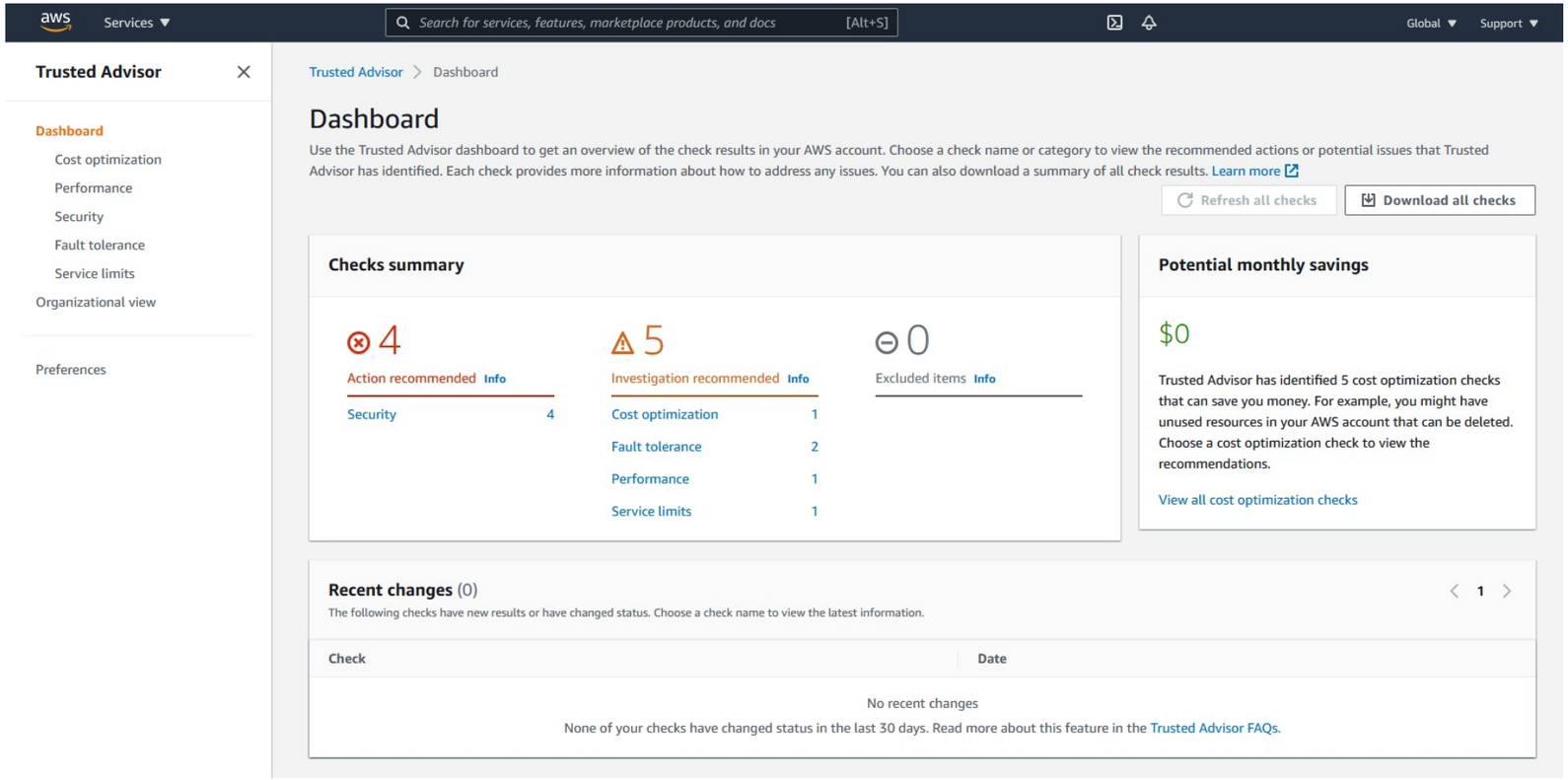
- Cron is in the cloud!
- No more Unreliable Town Clock
- Minimum 1 minute

Single event can have multiple targets

Alerting – Trusted Advisor

Security configuration checks of your AWS environment:

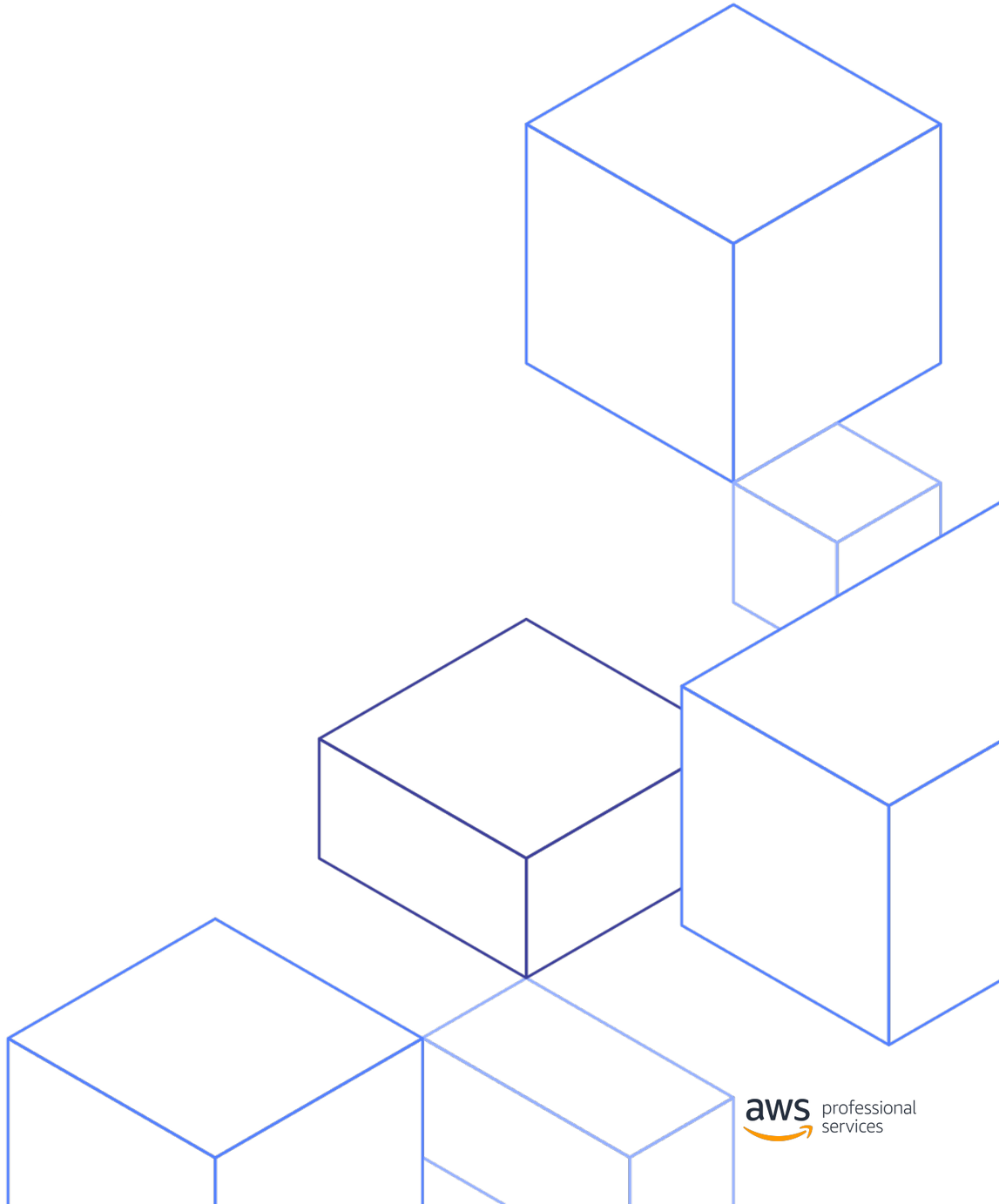
- Open ports
- Unrestricted access
- CloudTrail Logging
- S3 Bucket Permissions
- Multi-factor auth
- Password Policy
- DB Access Risk
- DNS Records
- Load Balancer config



aws professional services

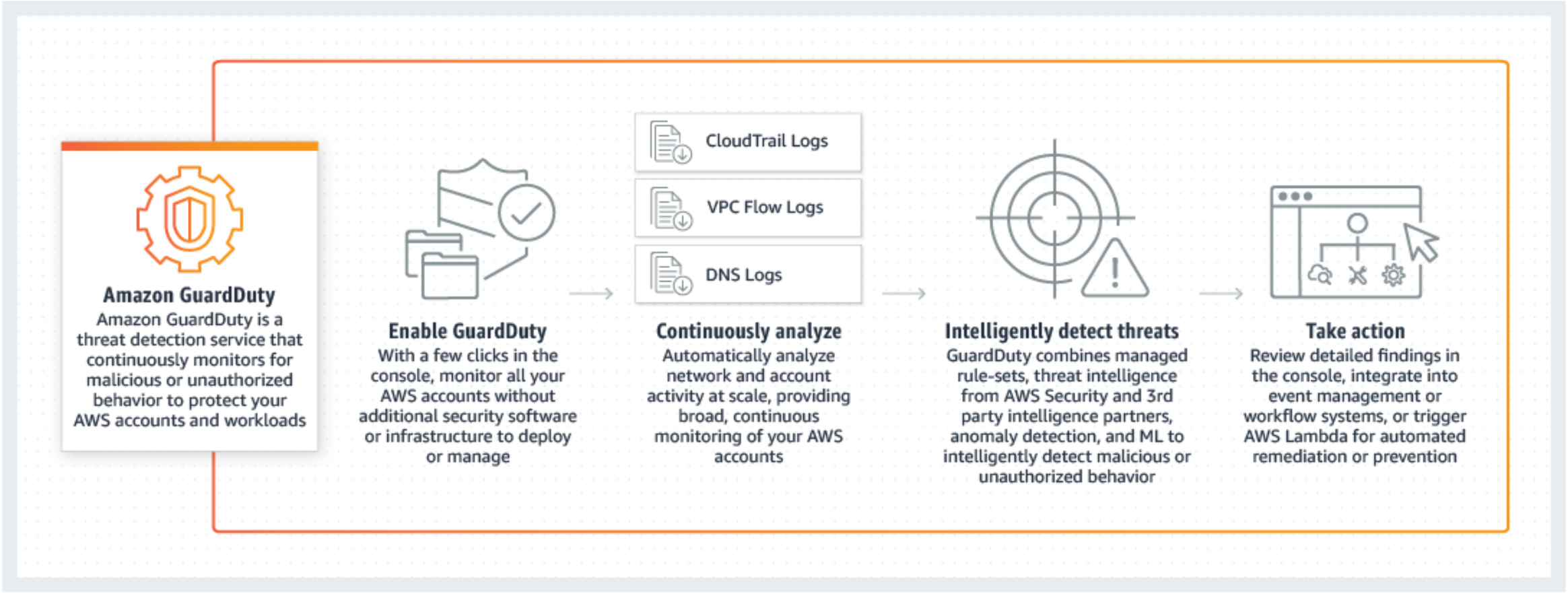
Amazon GuardDuty

Logging & Monitoring



aws professional services

Amazon GuardDuty



aws professional services

Amazon GuardDuty – Service Benefits

- Managed Threat Detection Service
- Easy One-Click Activation without Architectural or Performance Impact
- Continuous Monitoring of AWS Accounts and Resources
- Discover Threats Related to EC2 and IAM
- Instant On Provides Findings in Minutes
- No Agents, no Sensors, no Network Appliances
- Global Coverage, Regional Results
- Built In Anomaly Detection with Machine Learning
- Partner Integrations for Additional Protections
- Cost Effective Simple Pricing

Amazon GuardDuty – Data Sources

VPC Flow Logs

- Flow Logs for VPCs Do Not Need to Be Turned On to Generate Findings, data is consumed through independent duplicate stream.
- Suggested Turning On VPC Flow Logs to Augment Data Analysis (charges apply).

DNS Logs

- DNS Logs are based on queries made from EC2 instances to known questionable domains.
- DNS Logs are in addition to Route 53 query logs. Route 53 is not required for GuardDuty to generate DNS based findings.

CloudTrail Events

- CloudTrail history of AWS API calls used to access the Management Console, SDKs , CLI, etc. presented by GuardDuty.
- Identification of user and account activity including source IP address used to make the calls.

Amazon GuardDuty – S3 protection

- S3 protection enables Amazon GuardDuty to monitor object-level API operations to identify potential security risks within your S3 buckets.
- GuardDuty monitors CloudTrail management events by default for all accounts that have enabled GuardDuty
- CloudTrail S3 data event logs are a configurable data source in GuardDuty
- By default, S3 protection is enabled for new detectors

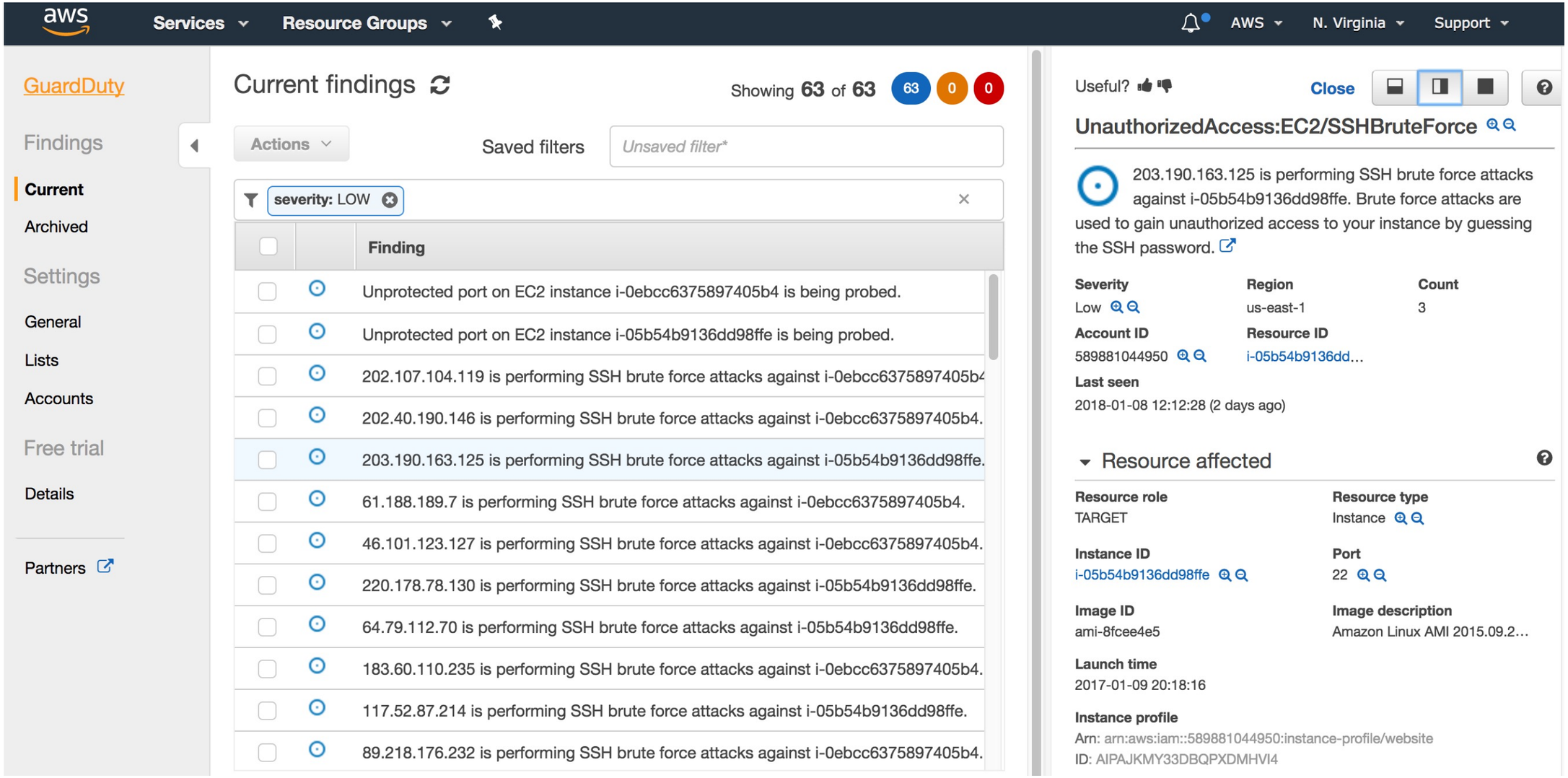
Management events for S3 include operations such as:

- **ListBuckets**
- **DeleteBuckets**
- **PutBucketReplication**

Data events for S3 include object-level API operations, such as:

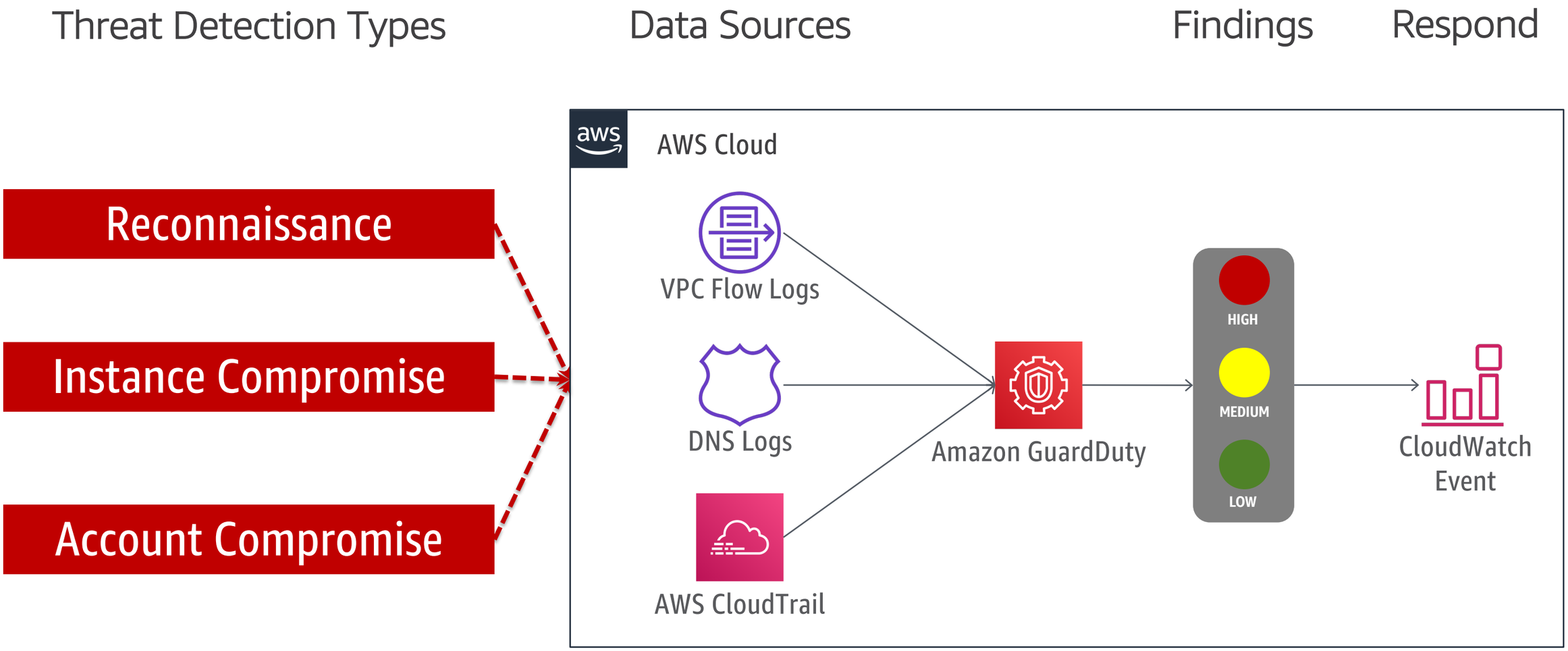
- **GetObject**
- **ListObjects**
- **DeleteObject**
- **PutObject**

Amazon GuardDuty – Findings

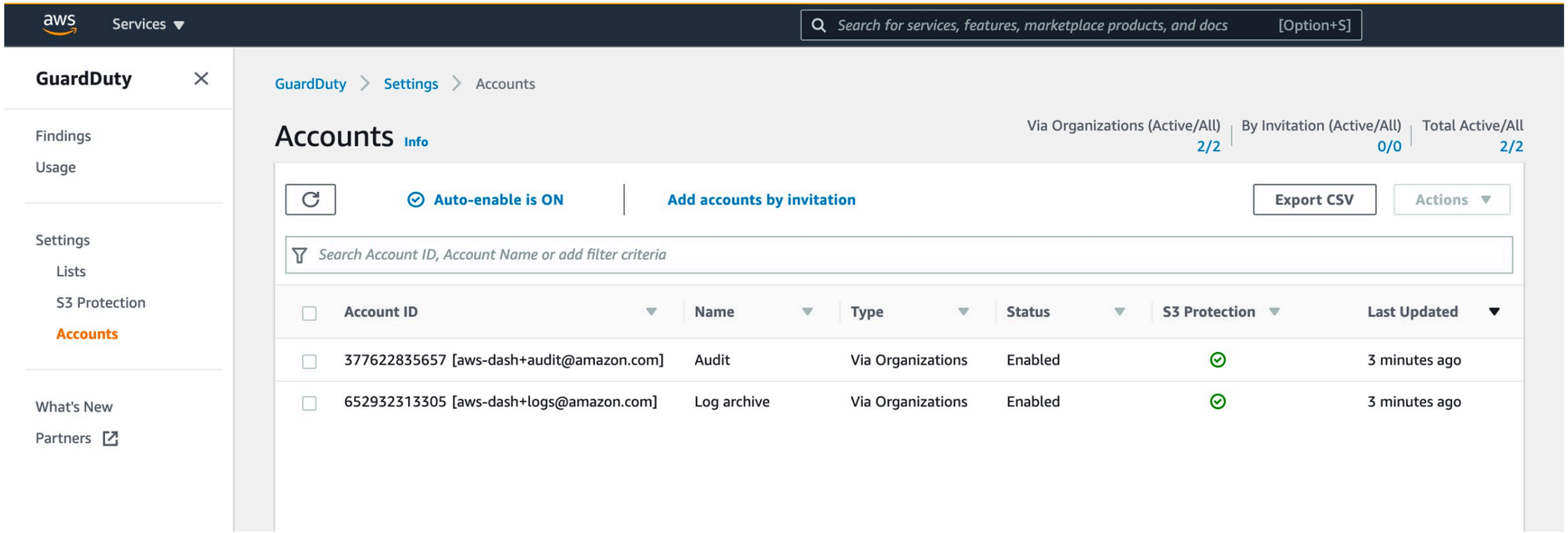


aws professional services

Amazon GuardDuty – Threat Detection



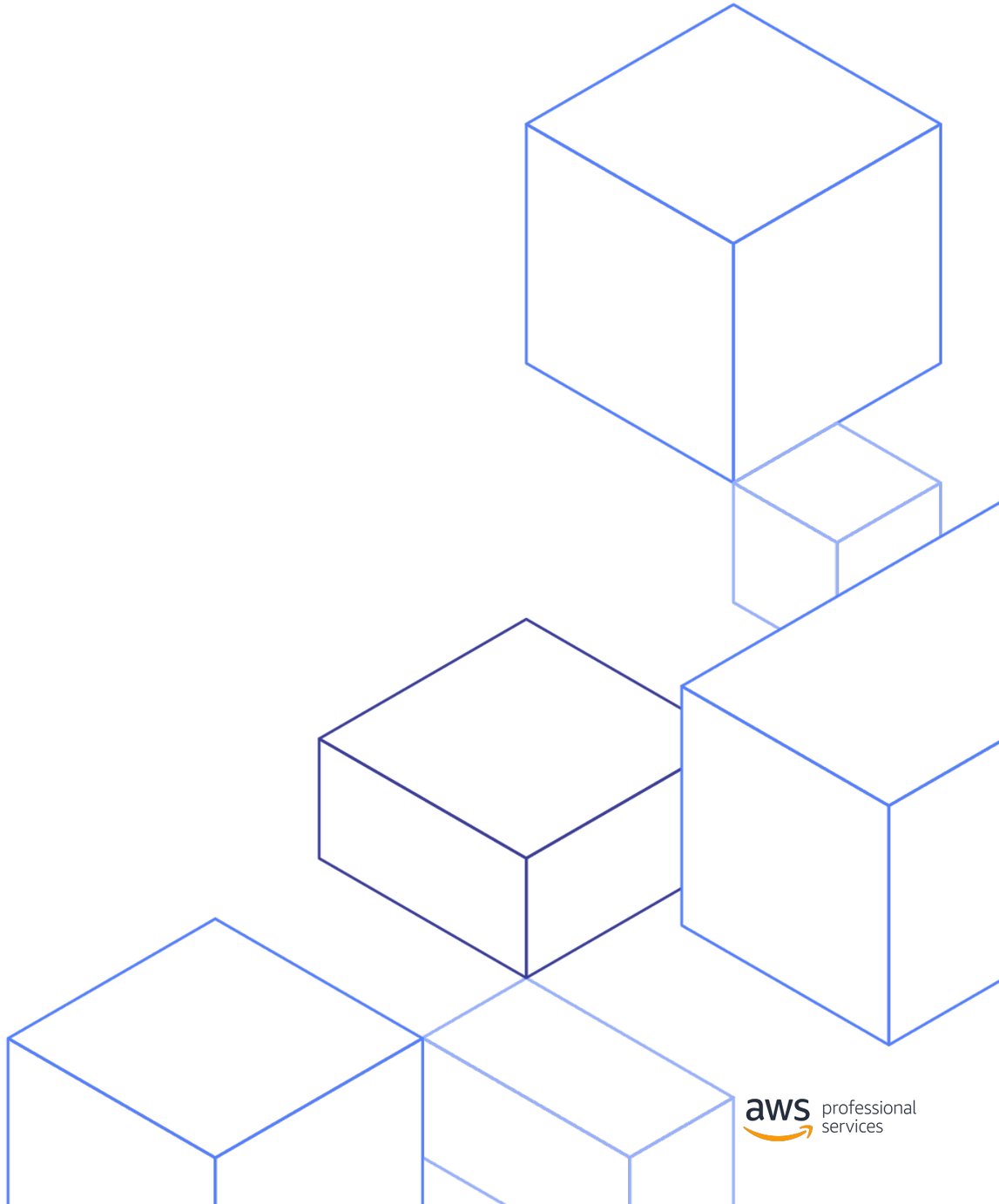
Amazon GuardDuty – Organization Support



- When you use GuardDuty with an AWS Organizations organization, you can designate any account within the organization to be the GuardDuty delegated administrator.
- This admin can enable and manage GuardDuty for all accounts in the organization **within that Region**.

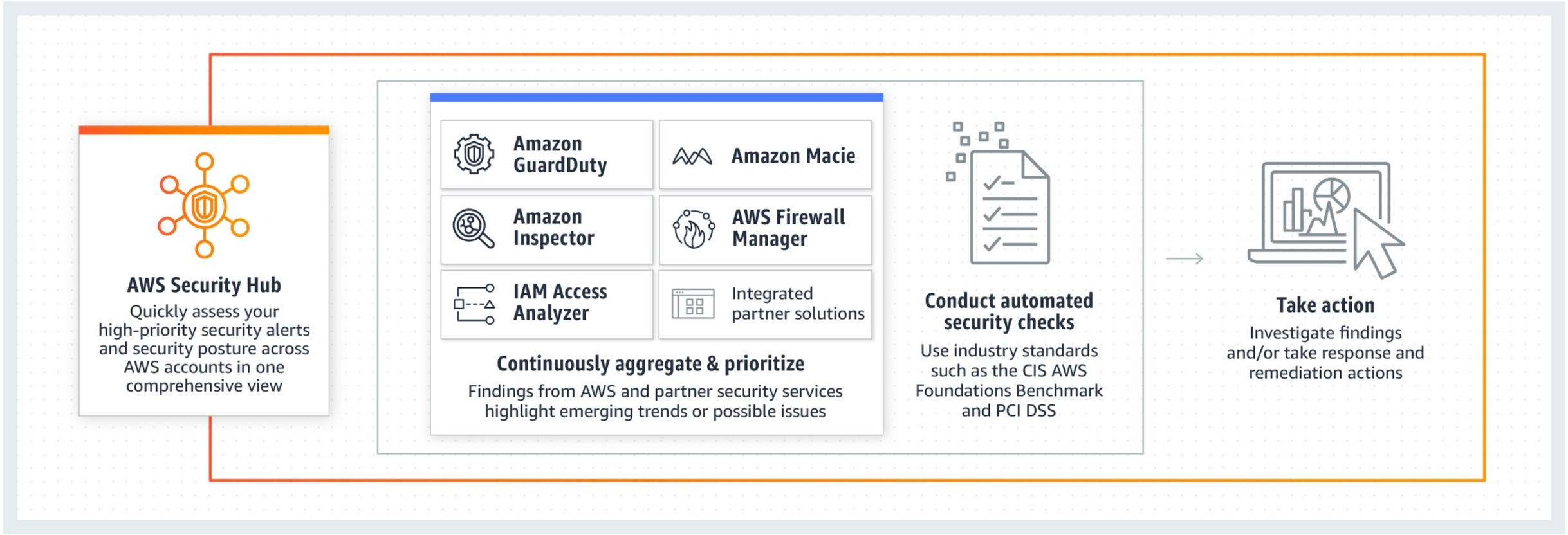
AWS Security Hub

Logging & Monitoring



aws professional services

AWS Security Hub - Overview



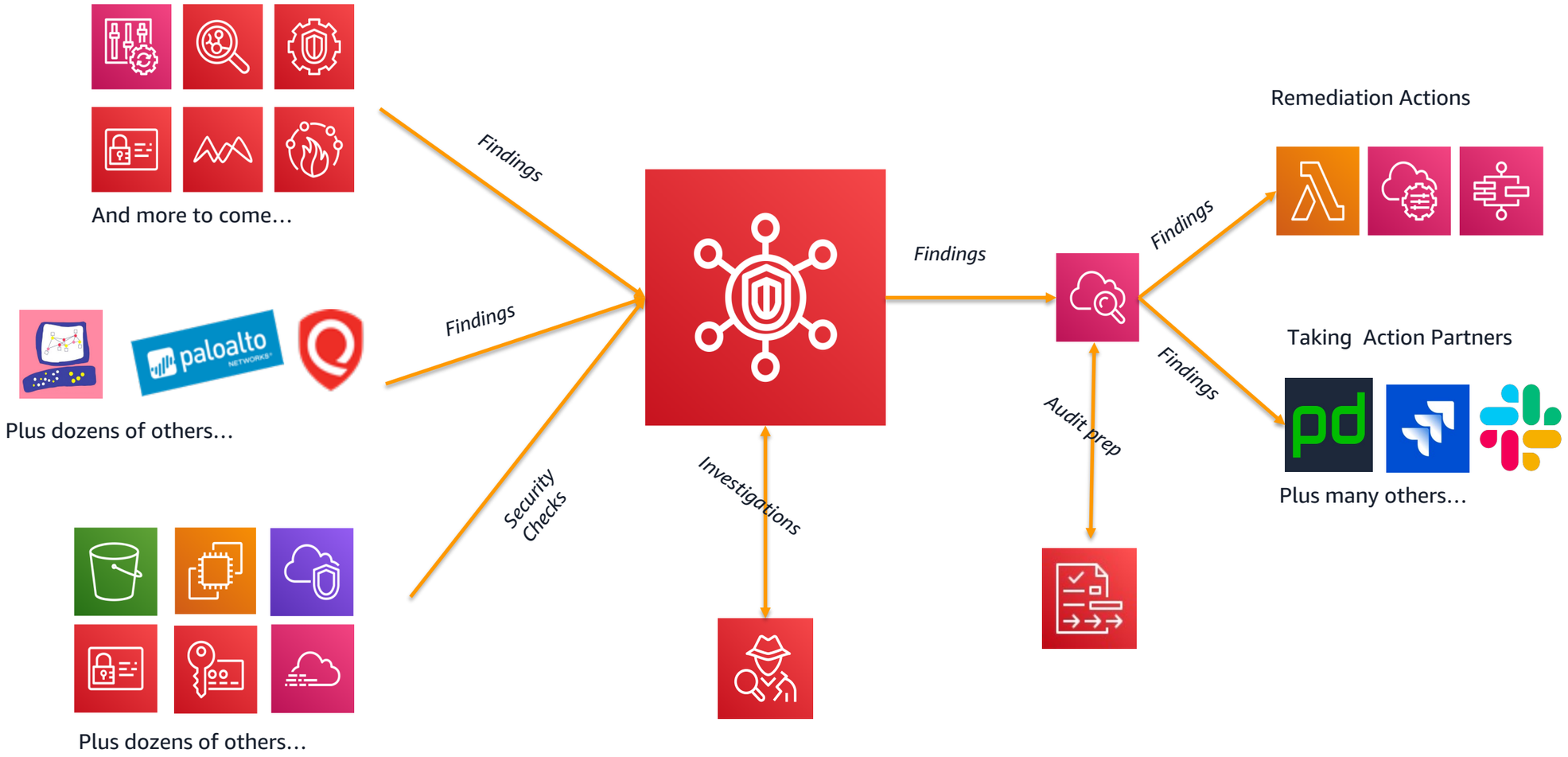
AWS Security Hub - Benefits

Compliance standards

Aggregated findings across accounts & regions

Insights

AWS Security Hub – Information Flows

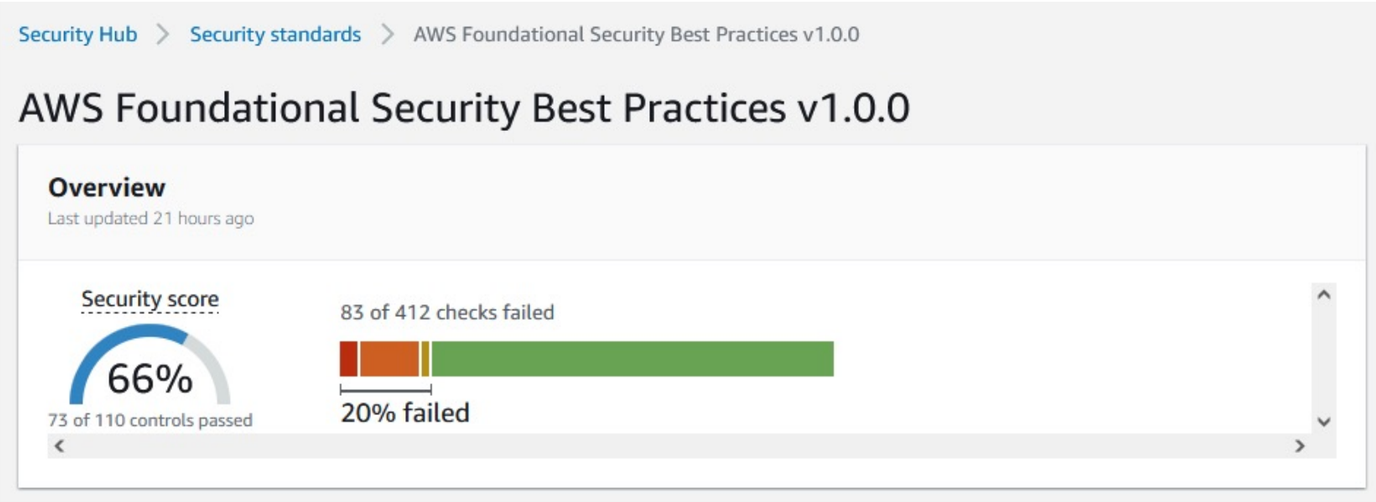


aws professional services

AWS Security Hub - Compliance Standards

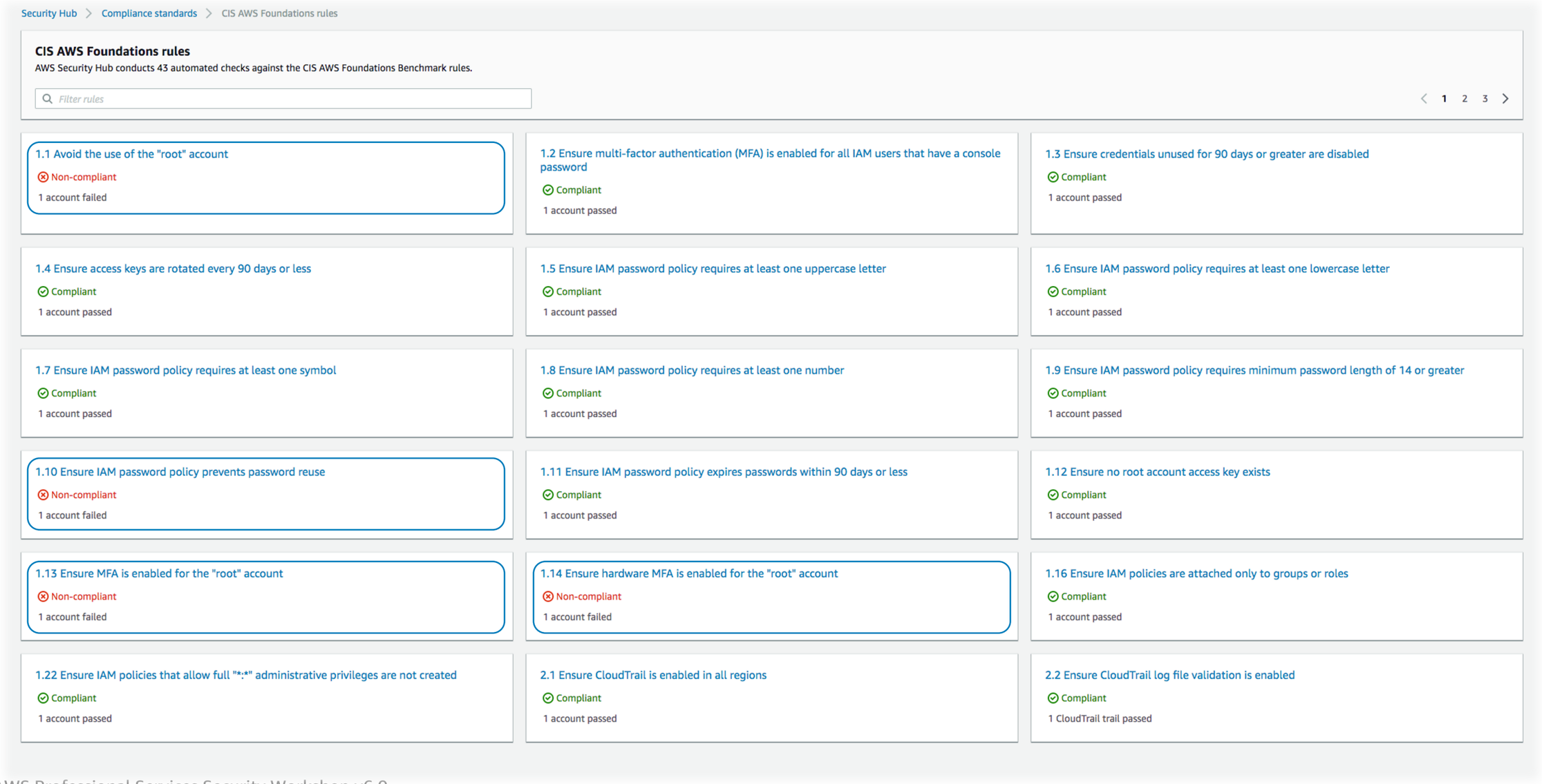
Three standards currently available:

- AWS Foundational Security Best Practices
- CIS AWS Foundations Benchmark
- PCI DSS v3.2.1



aws professional services

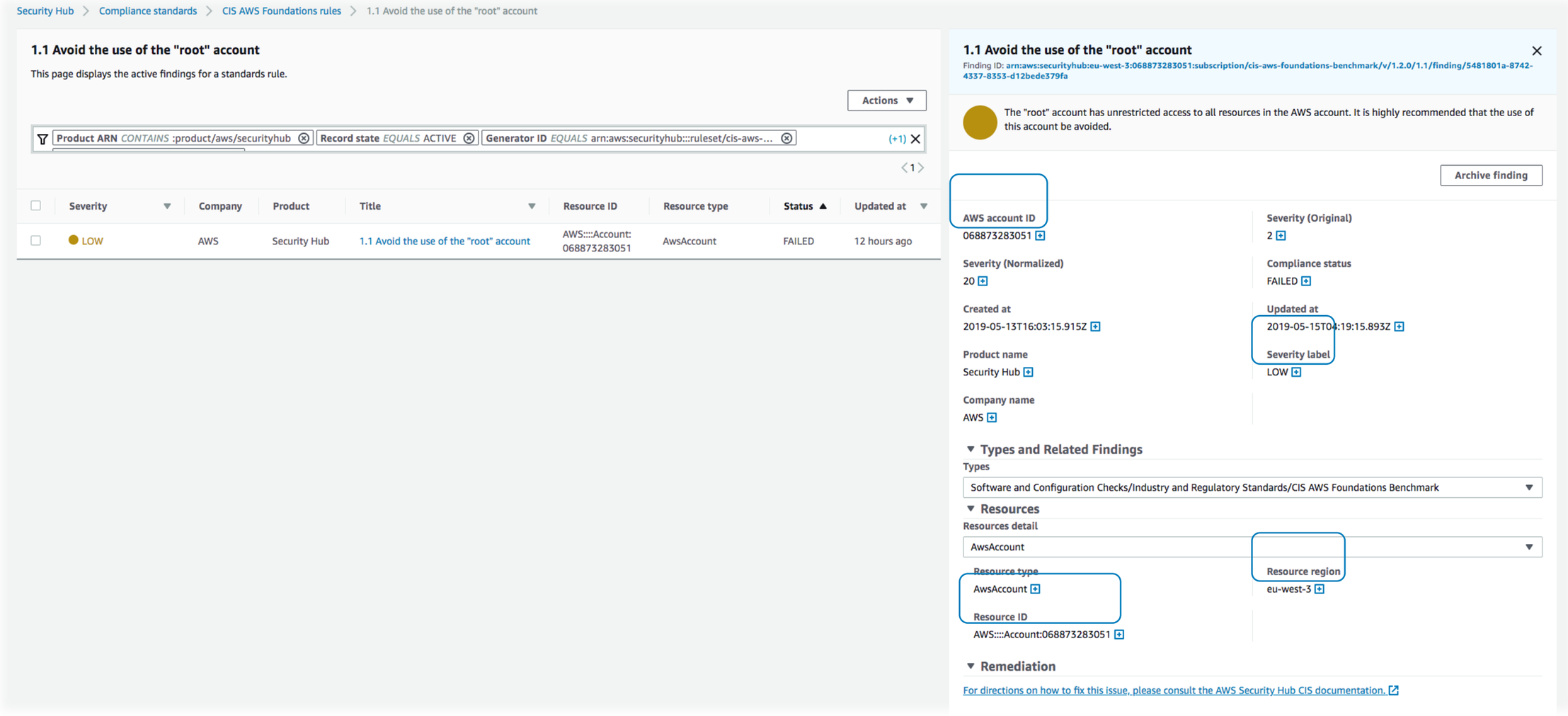
AWS Security Hub - Compliance Standards



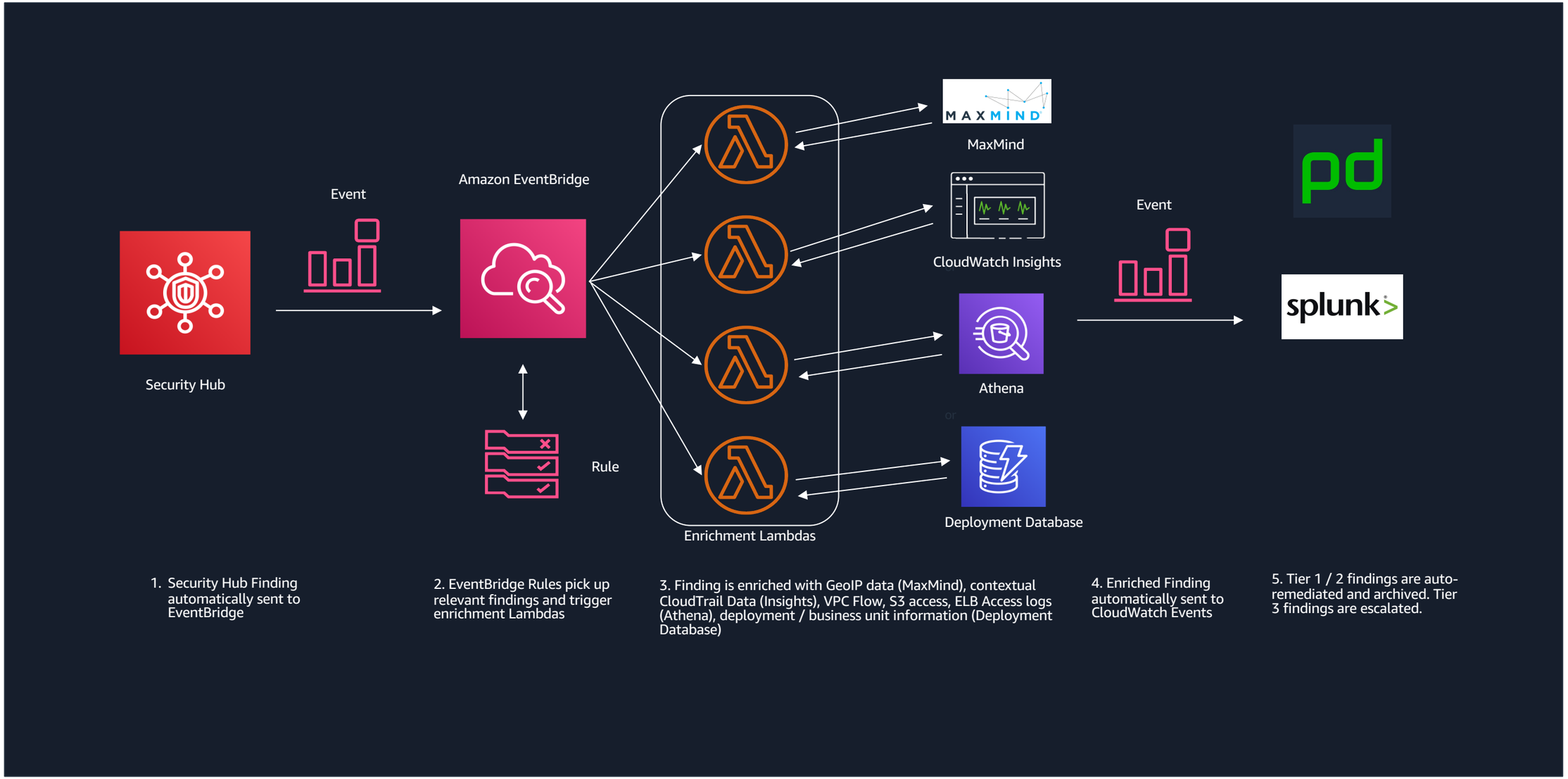
aws professional services

AWS Security Hub - Compliance Standards

Example: 1.1 Avoid the use of the "root" account



AWS Security Hub – Example Customer Architecture



AWS Security Hub – Best Practices

1. Turn on Security Hub in all accounts and all regions using AWS Labs script
2. Upload your GuardDuty master/member hierarchy
3. Enable Config if you don't have it on in all accounts; leave the CIS standard enabled
4. Integrate and enable your existing security products. There are 30 integrations today and more to come.
5. Use tags for access control and cost allocation
6. Evaluate your costs during the free trial
7. Customize your insights using the managed insights as templates
8. Integrate your "taking action" products, such as ticketing, chat, on-call management, and SOAR products using CloudWatch Events
9. Build out customized semi- and/or fully automated remediation playbooks using CloudWatch events plus Automation documents and/or Step Functions

https://aws.amazon.com/blogs/security/nine-aws-security-hub-best-practices/

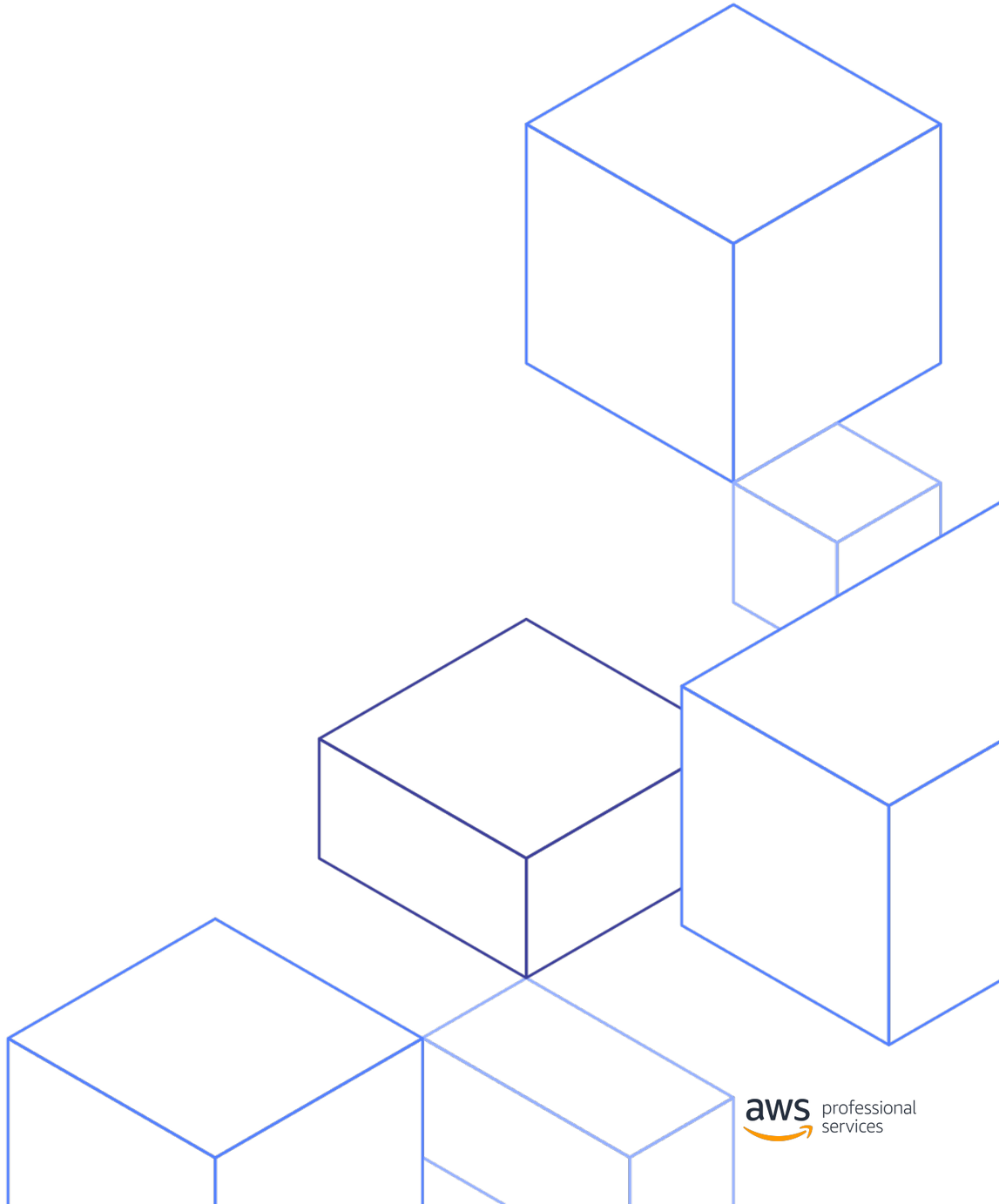
AWS Security Hub – Key Takeaways

- Automatically evaluate your compliance against key standards with one-click, frictionless enablement
- Centralize all of your findings without the need to parse and normalize via the AWS Security Findings Format
- Prioritize findings using insights for efficient response and remediation
- Take actions on findings automatically or semi-automatically using CloudWatch events
- View and understand your security and compliance state in one place

aws professional services

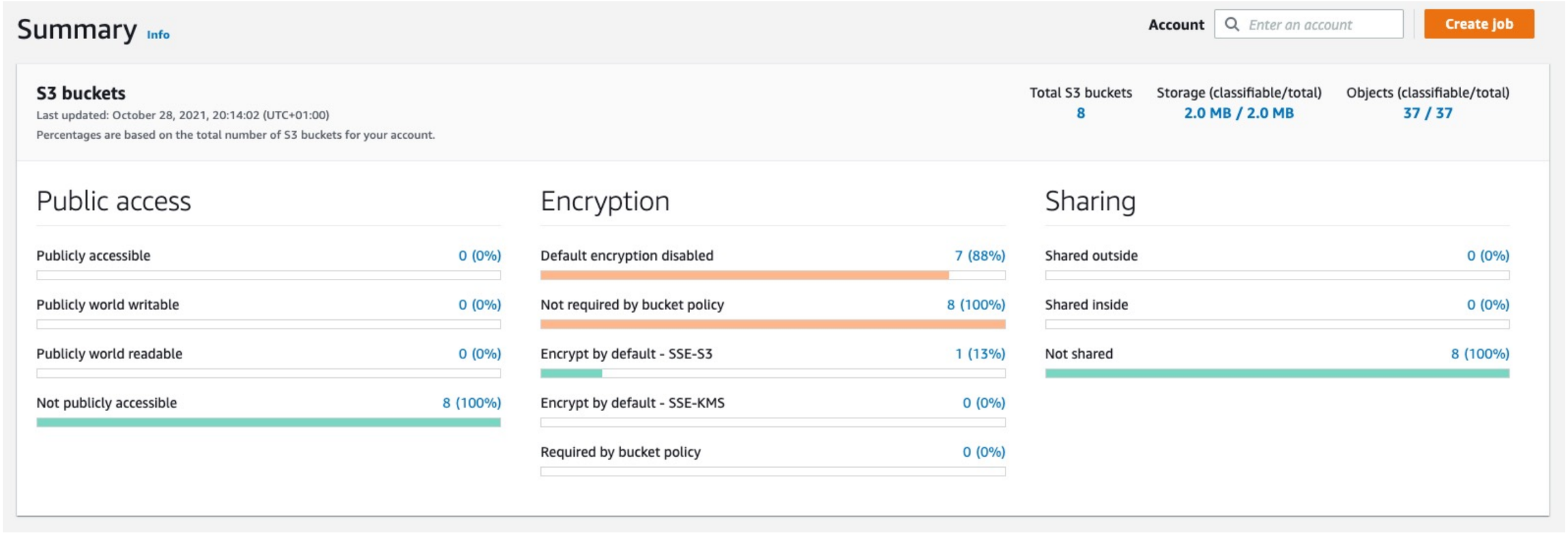
Amazon Macie

Logging & Monitoring



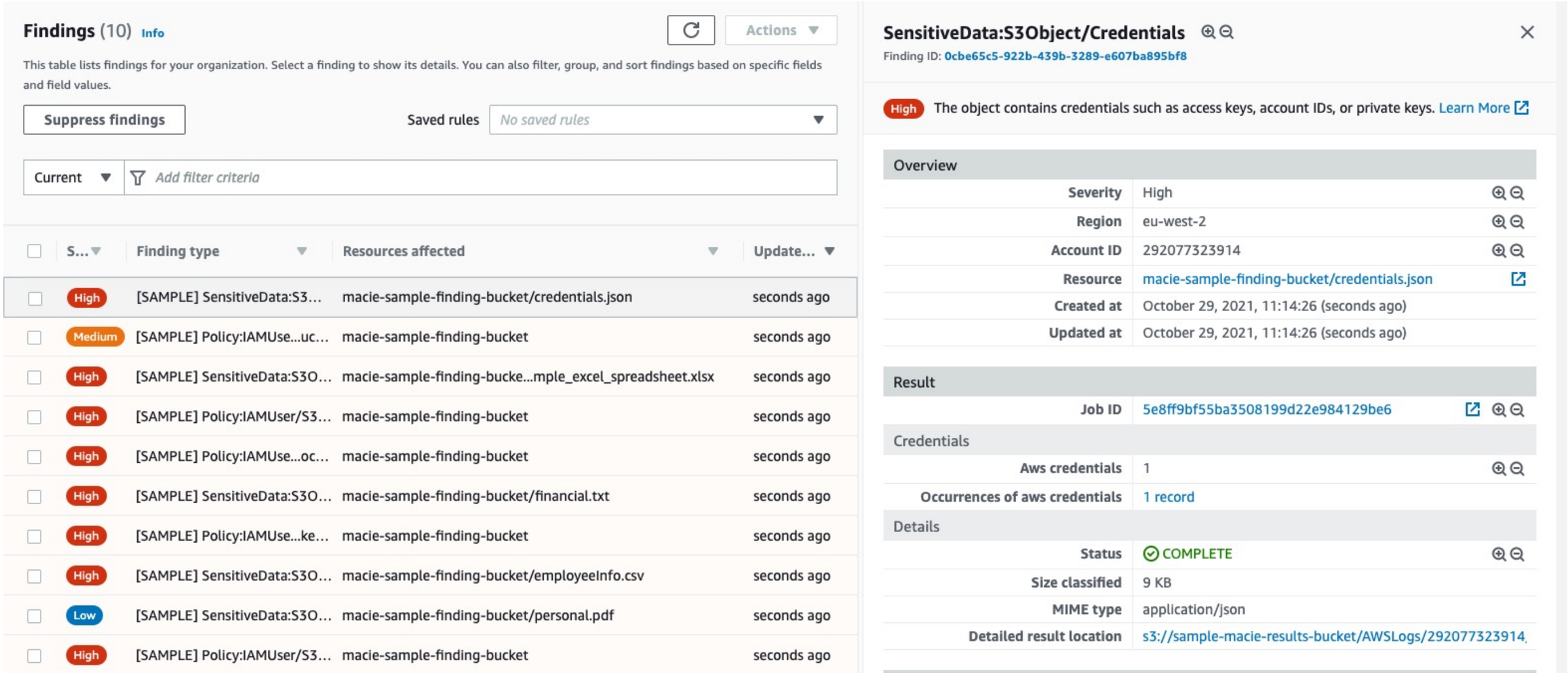
aws professional services

Amazon Macie - Dashboard



aws professional services

Amazon Macie – PII Monitoring



Findings (10) Info

Actions

This table lists findings for your organization. Select a finding to show its details. You can also filter, group, and sort findings based on specific fields and field values.

Suppress findings

Saved rules: No saved rules

Current | Add filter criteria

S...	Finding type	Resources affected	Update...
High	[SAMPLE] SensitiveData:S3...	macie-sample-finding-bucket/credentials.json	seconds ago
Medium	[SAMPLE] Policy:IAMUse...uc...	macie-sample-finding-bucket	seconds ago
High	[SAMPLE] SensitiveData:S3O...	macie-sample-finding-bucke...mple_excel_spreadsheet.xlsx	seconds ago
High	[SAMPLE] Policy:IAMUser/S3...	macie-sample-finding-bucket	seconds ago
High	[SAMPLE] Policy:IAMUse...oc...	macie-sample-finding-bucket	seconds ago
High	[SAMPLE] SensitiveData:S3O...	macie-sample-finding-bucket/financial.txt	seconds ago
High	[SAMPLE] Policy:IAMUse...ke...	macie-sample-finding-bucket	seconds ago
High	[SAMPLE] SensitiveData:S3O...	macie-sample-finding-bucket/employeeInfo.csv	seconds ago
Low	[SAMPLE] SensitiveData:S3O...	macie-sample-finding-bucket/personal.pdf	seconds ago
High	[SAMPLE] Policy:IAMUser/S3...	macie-sample-finding-bucket	seconds ago

SensitiveData:S3Object/Credentials

Finding ID: 0cbe65c5-922b-439b-3289-e607ba895bf8

High The object contains credentials such as access keys, account IDs, or private keys. Learn More

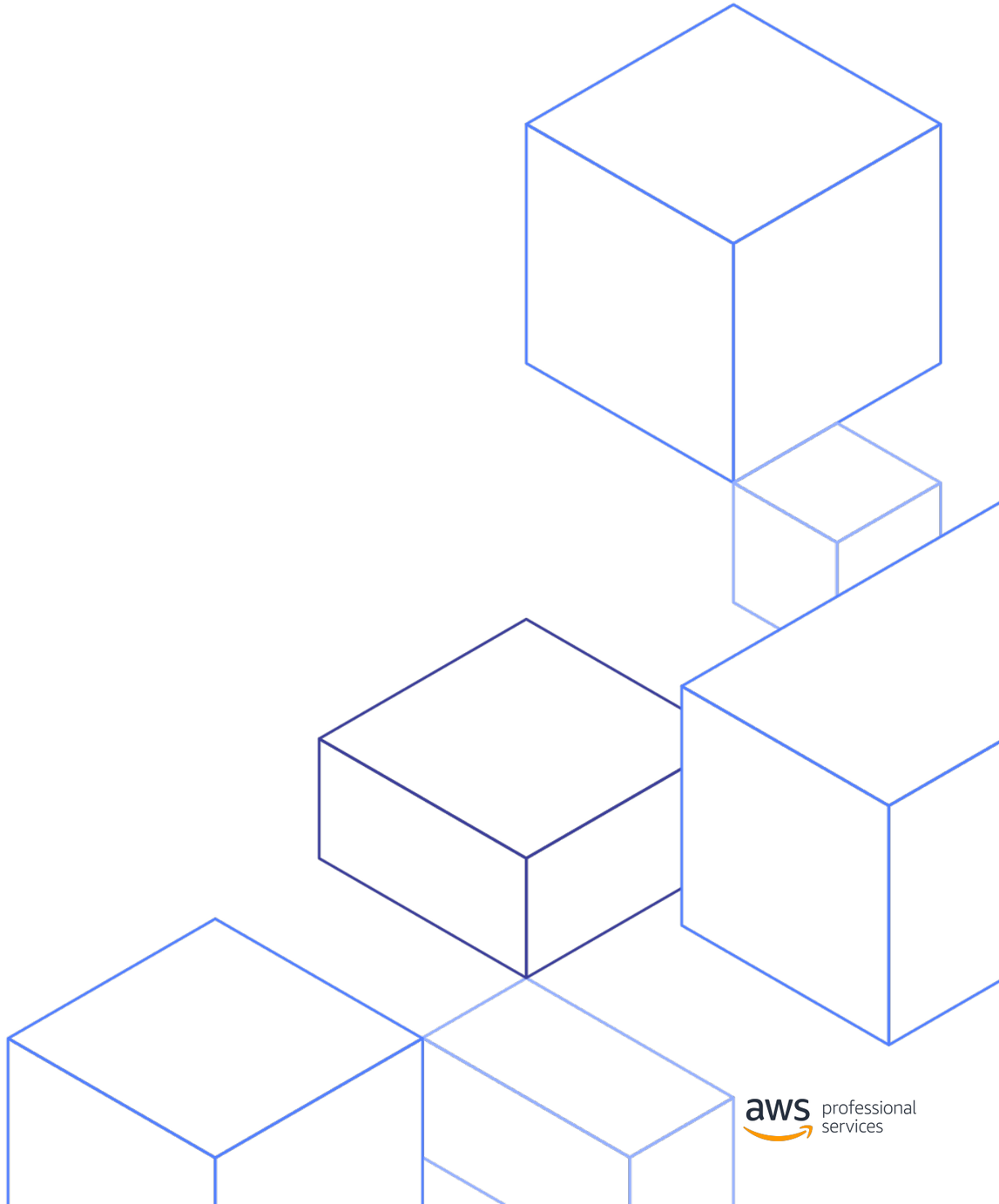
Overview	
Severity	High
Region	eu-west-2
Account ID	292077323914
Resource	macie-sample-finding-bucket/credentials.json
Created at	October 29, 2021, 11:14:26 (seconds ago)
Updated at	October 29, 2021, 11:14:26 (seconds ago)

Result	
Job ID	5e8ff9bf55ba3508199d22e984129be6
Credentials	
Aws credentials	1
Occurrences of aws credentials	1 record
Details	
Status	COMPLETE
Size classified	9 KB
MIME type	application/json
Detailed result location	s3://sample-macie-results-bucket/AWSLogs/292077323914

aws professional services

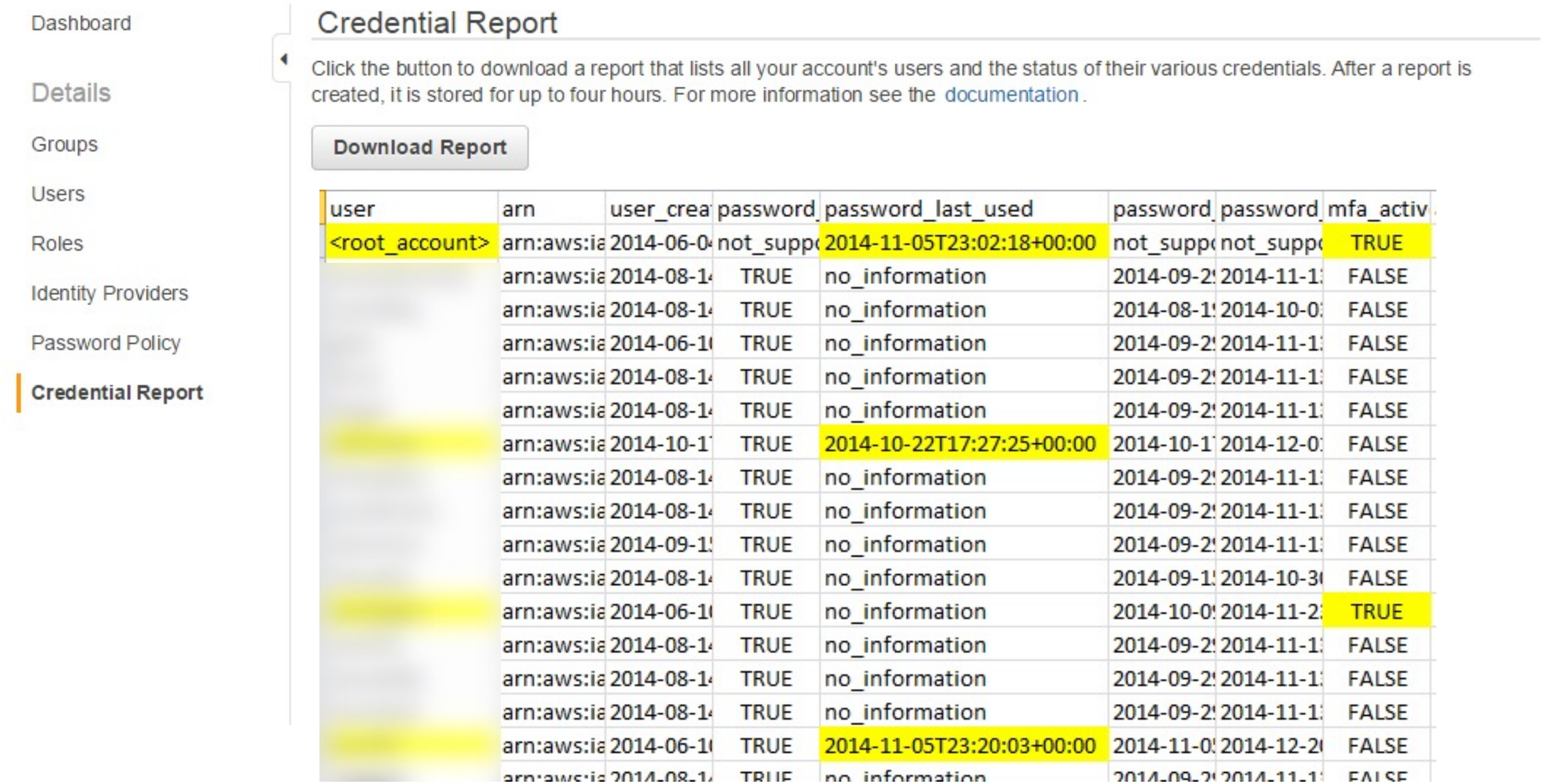
Auditing your AWS Environment

Logging & Monitoring



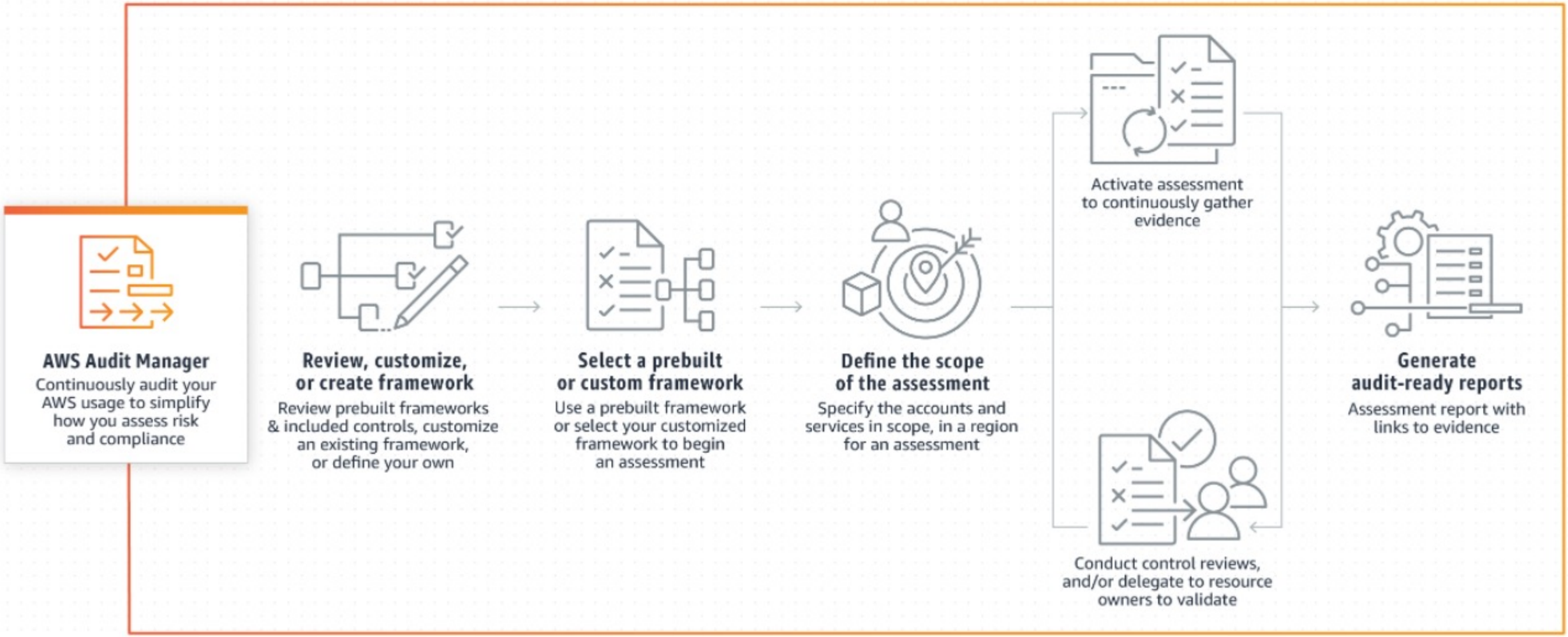
aws professional services

Auditing – IAM Credential Report



aws professional services

AWS Audit Manager

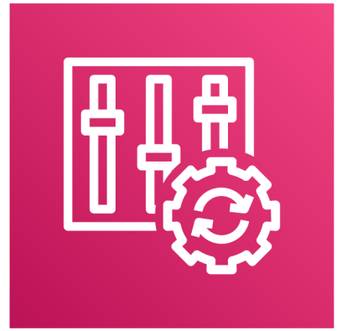


aws professional services

Auditing – AWS Config

What **Resources** exist within my AWS Environment?

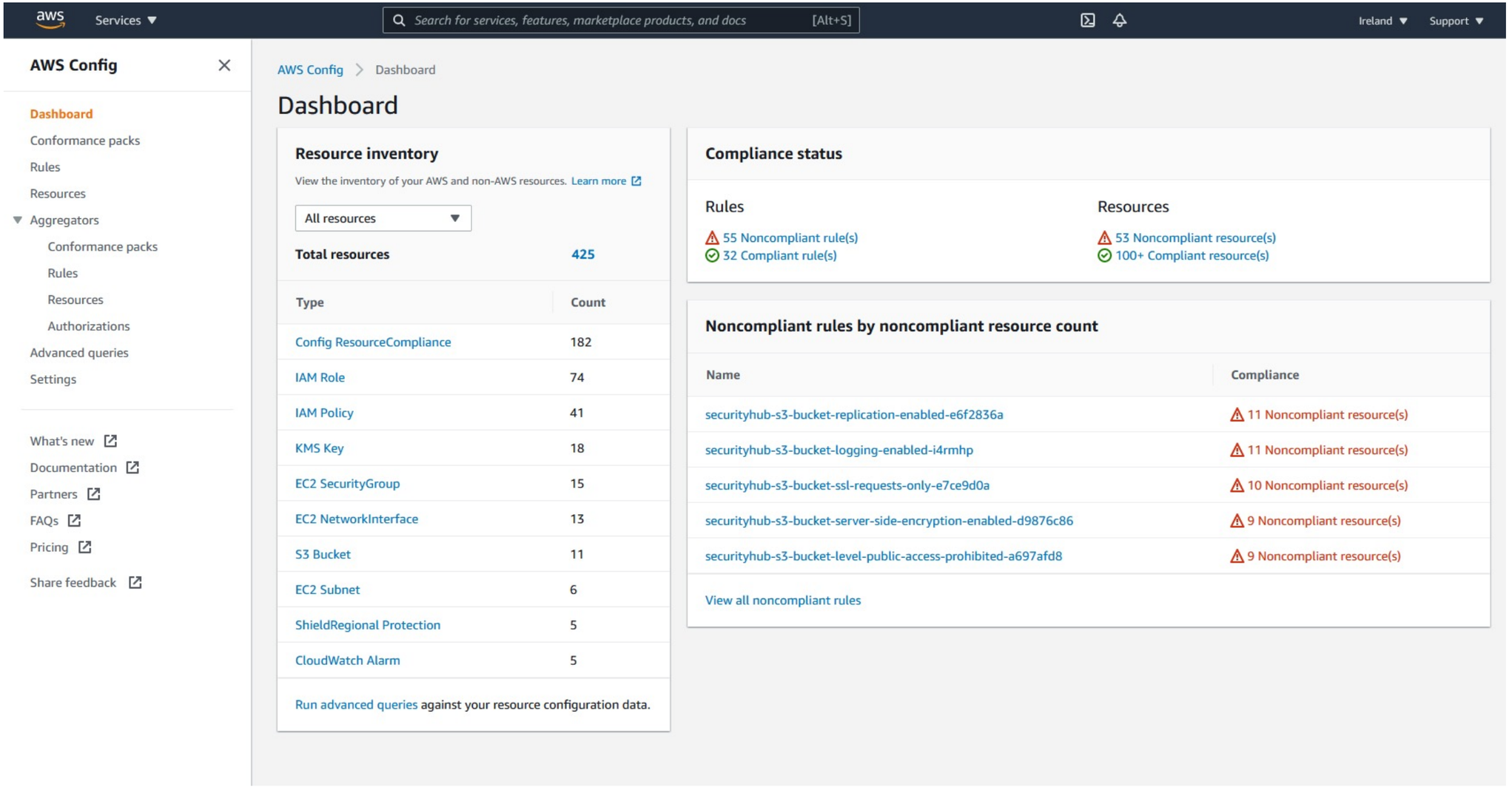
- Get inventory of AWS resources
- Discover new and deleted resources
- Record configuration changes continuously
- Get notified when configurations change
- Know resource relationships dependencies



Auditing – AWS Config

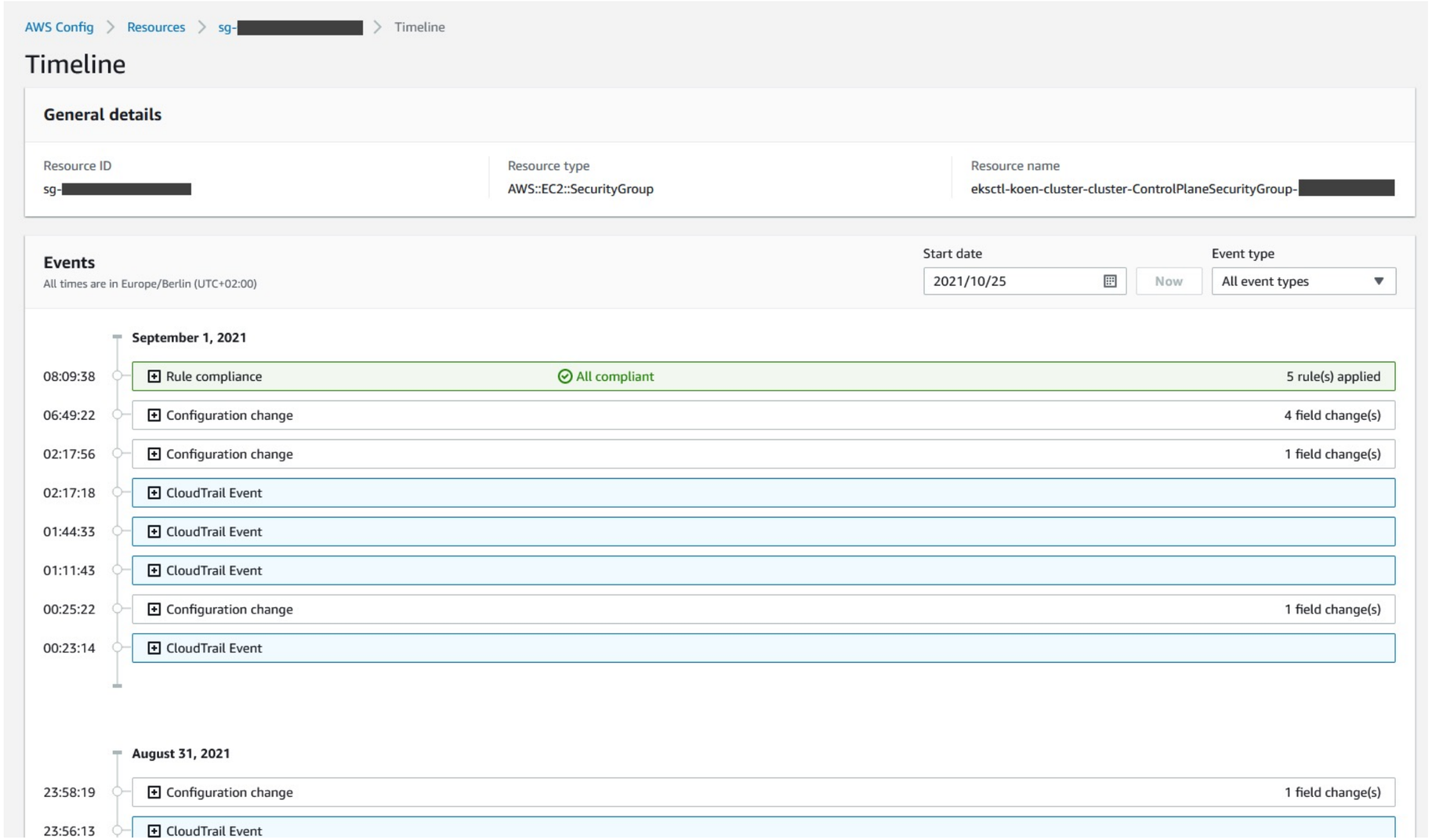
- Continuously tracks resource configuration changes (not just API changes).
- Evaluates the configuration against policies defined using AWS Config rules.
- Alerts if the configuration is noncompliant using Amazon SNS and CloudWatch Event.

Auditing – AWS Config



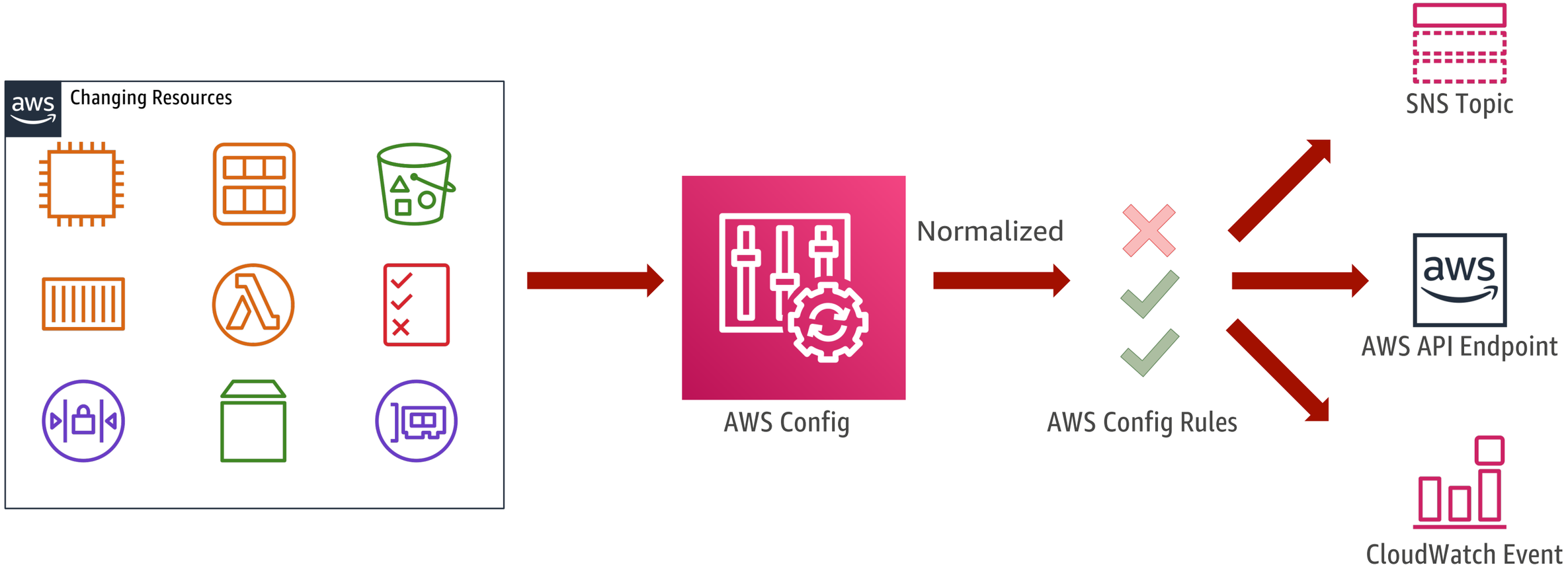
aws professional services

Auditing – AWS Config



aws professional services

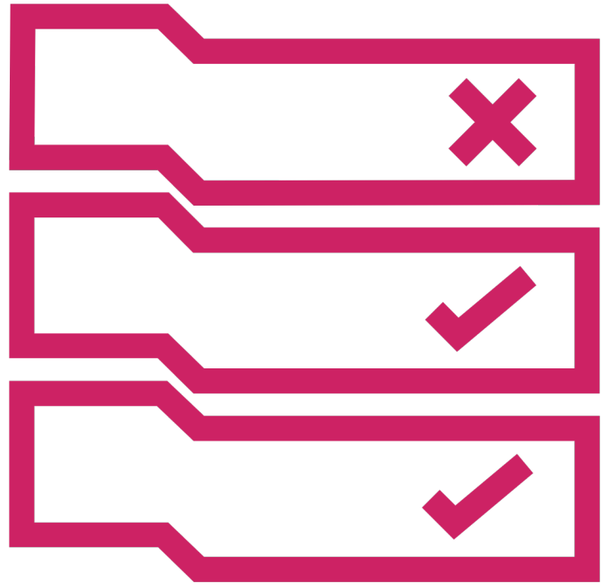
AWS Config Rules



AWS Config Rules

Continuous and automated compliance validation against the specified configuration

- AWS managed rules
  - Defined by AWS
  - Require minimal (or no) configuration
  - Rules are maintained by AWS
  - 200+ AWS managed rules available
- Customer managed rules
  - Authored by you using AWS Lambda
  - Rules execute in your account
  - You maintain the rule

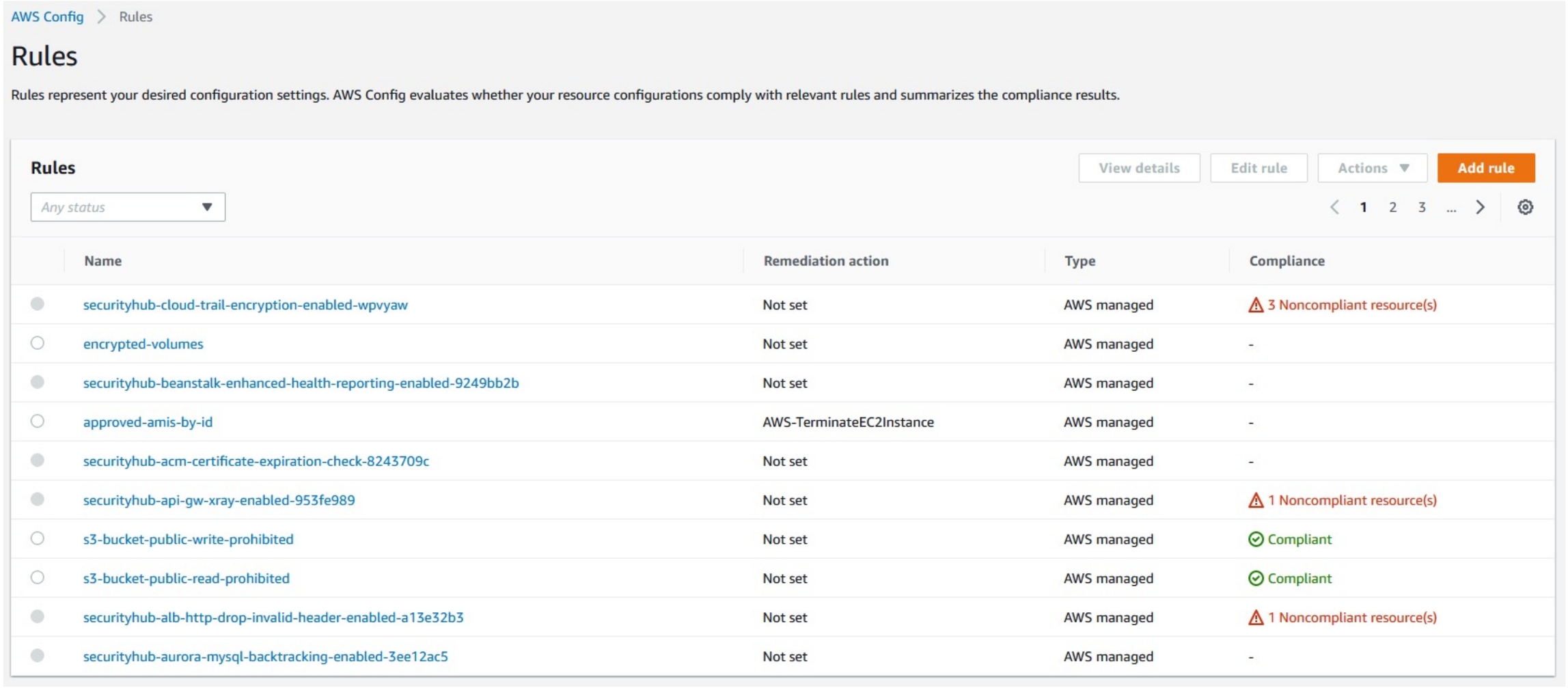


AWS Config Rules - Triggers

Two types of Triggers:

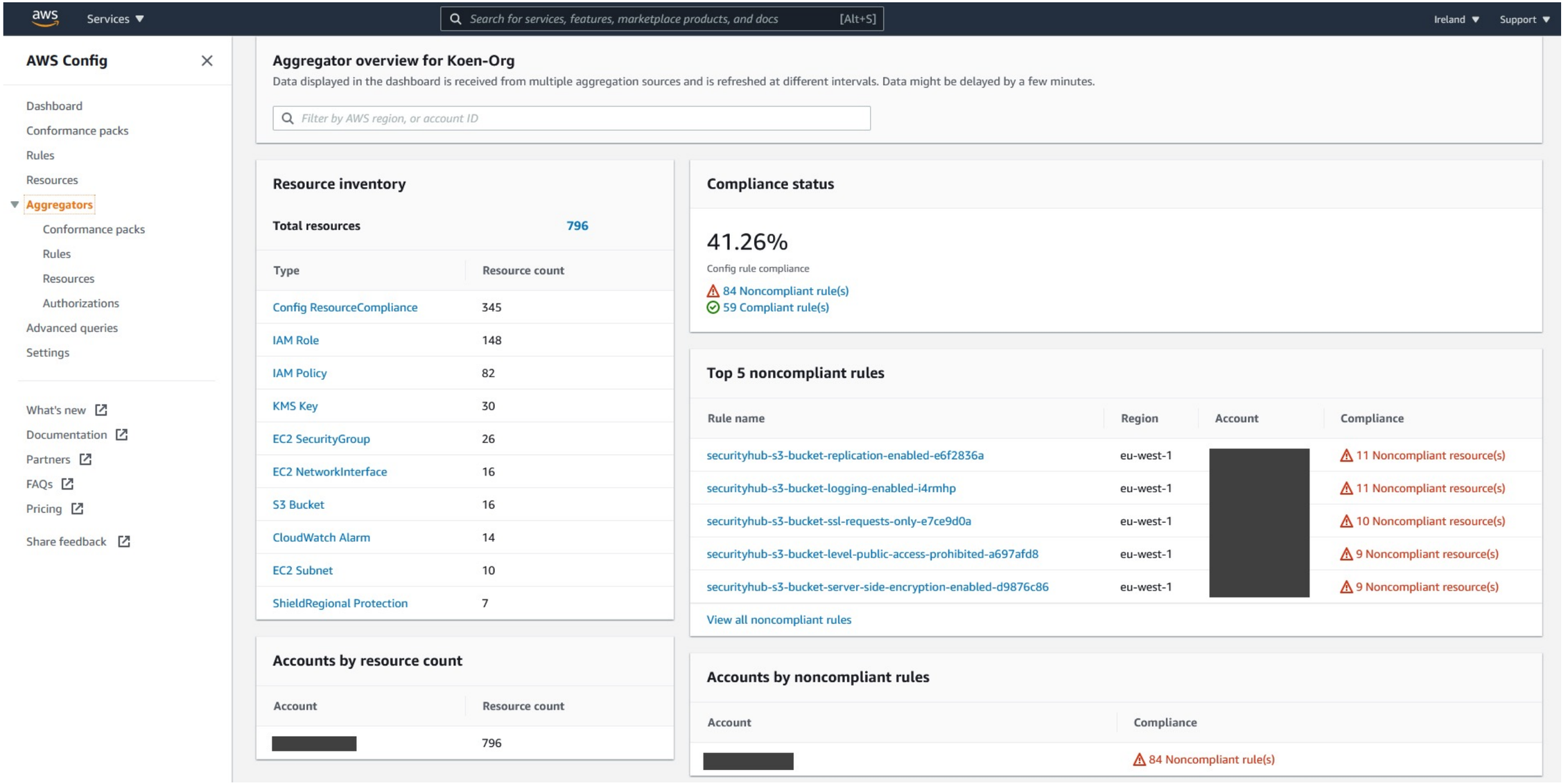
- Triggered by **resource change**: rules are invoked when a specified resource type has changed
    - Scope:
        - Tag key/value (eg: Env / Prod)
        - Supported resource types (eg: AWS::S3::Bucket)
        - Specific resource ID (eg: i-1234567890abcdef0)
- Triggered **periodically**: rules are invoked on a specified schedule
    - Useful for checking long-running resources and resources that are not natively supported by AWS Config

AWS Config Rules – Review Compliance



aws professional services

AWS Config Rules – Review Compliance (Aggregated)



aws professional services

AWS Config Rules – Custom Config Rules

- Codify and automate your own security controls
- Get started with the AWS Rule Development Kit (RDK)
- Get started with samples in AWS Lambda
- Implement guidelines for security best practices and compliance
- Use rules from various AWS Partners
- View compliance in one dashboard across your AWS accounts and regions

AWS Community repository of custom Config rules
https://github.com/awslabs/aws-config-rules

Contains Node and Python samples for Custom Rules for AWS Config

AWS Config Rules – Evaluating Compliance

```
function hasExpectedSecurityGroup(expectedSecurityGroupId,
securityGroups) {
    for (var i = 0; i < securityGroups.length; i++) {
        var securityGroup = securityGroups[i];
        if (securityGroup.groupId ===
expectedSecurityGroupId) {
            return true;
        }
    }
    return false;
}
```

AWS Config Rules – Recording Compliance State

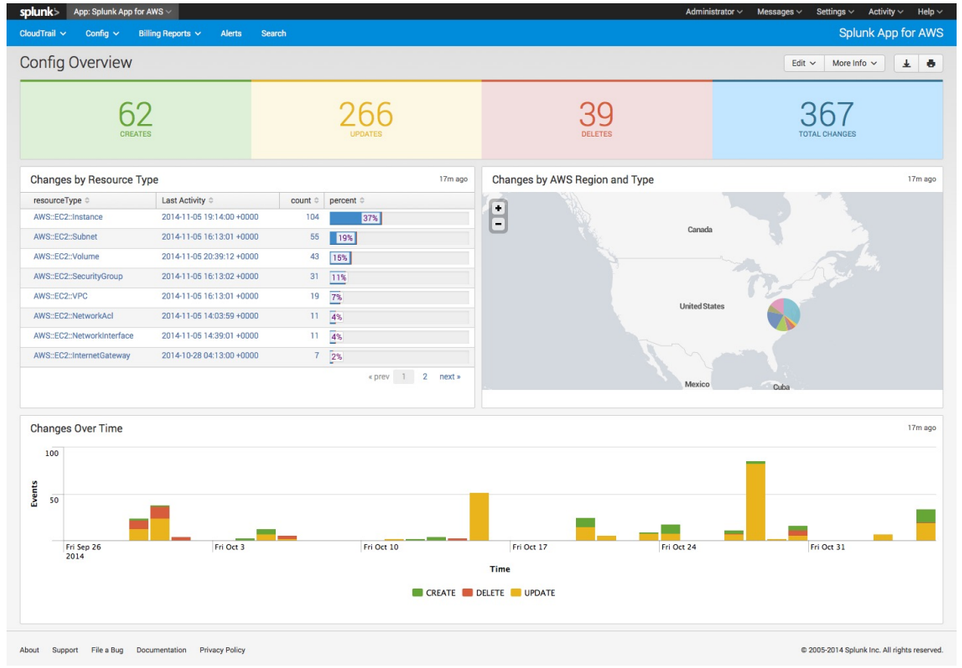
```
config.putEvaluations(putEvaluationsRequest, function (err,
data) {
    if (err) {
        context.fail(err);
    } else {
        context.succeed(data);
    }
});
```

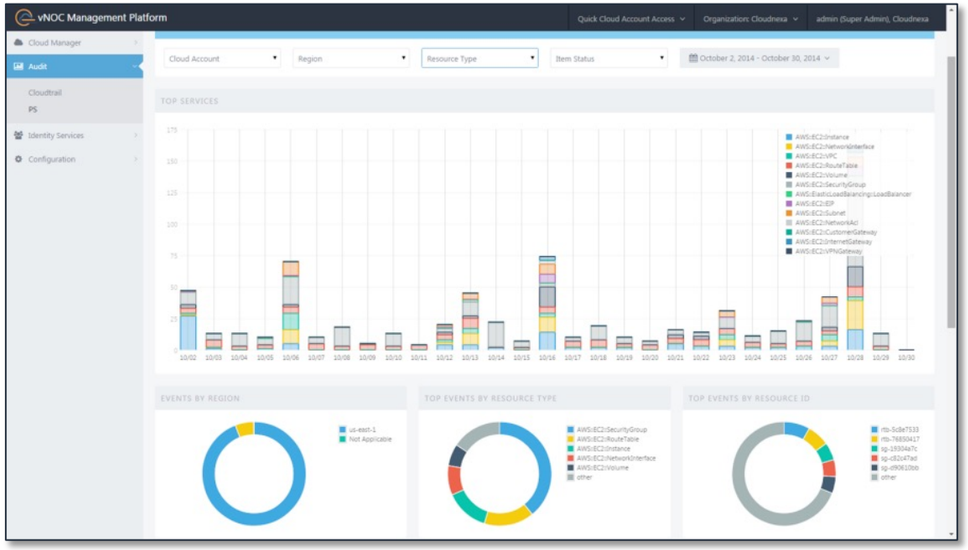
AWS Config Rules – Automatic Remediation

- Config Rules support automatic remediation
- YAML/JSON based AWS Systems Manager Automation Documents
- Pre-defined and custom documents can be used

AWS Config Partners

- 2nd Watch
- CloudCheckr
- CloudNexa
- CloudHealth
- Evident.IO
- Red Hat Cloud Forms
- RedSeal Networks
- Splunk
- Alertlogic – Cloud Insight
- Allgress





aws professional services

AWS Config Rules Partners

CloudHealth®

evident.io

ALLGRESS™

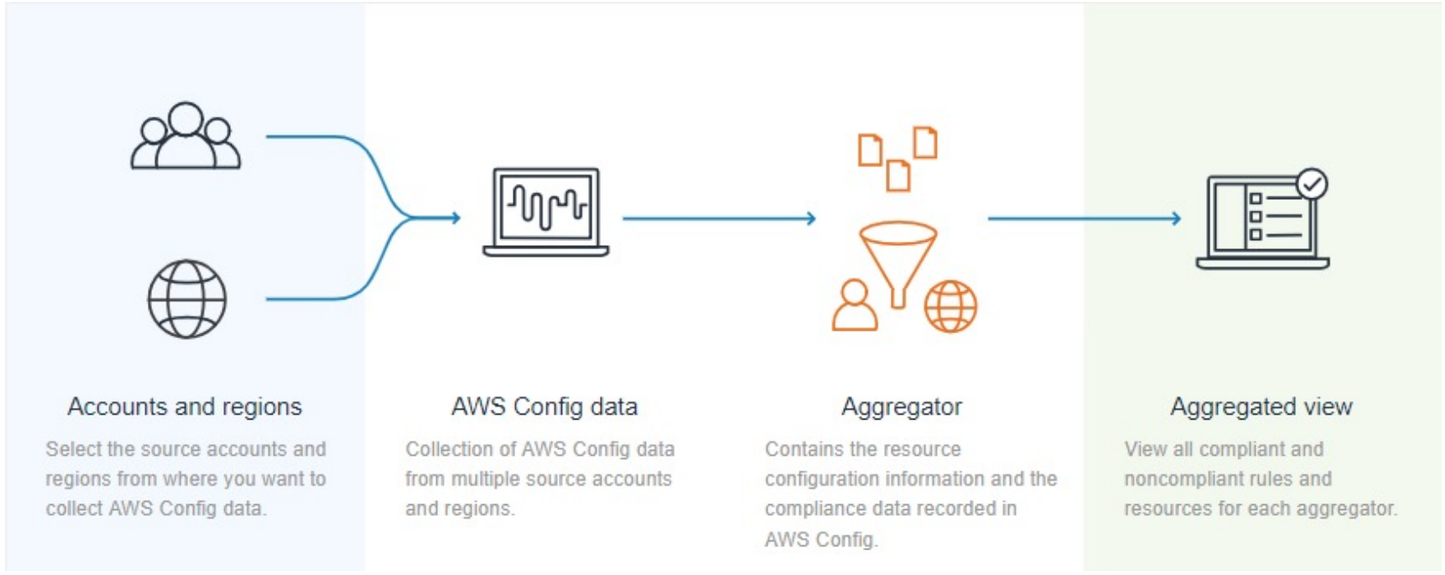
TREND MICRO™

aws professional services

AWS Config Best Practices

Use multi-account, multi-region data aggregation feature in AWS Config

- Based on your AWS Organization or invite individual AWS accounts
- Aggregates resource configuration and AWS Config rule compliance data
- Use a delegated administrator account



aws professional services

Questions