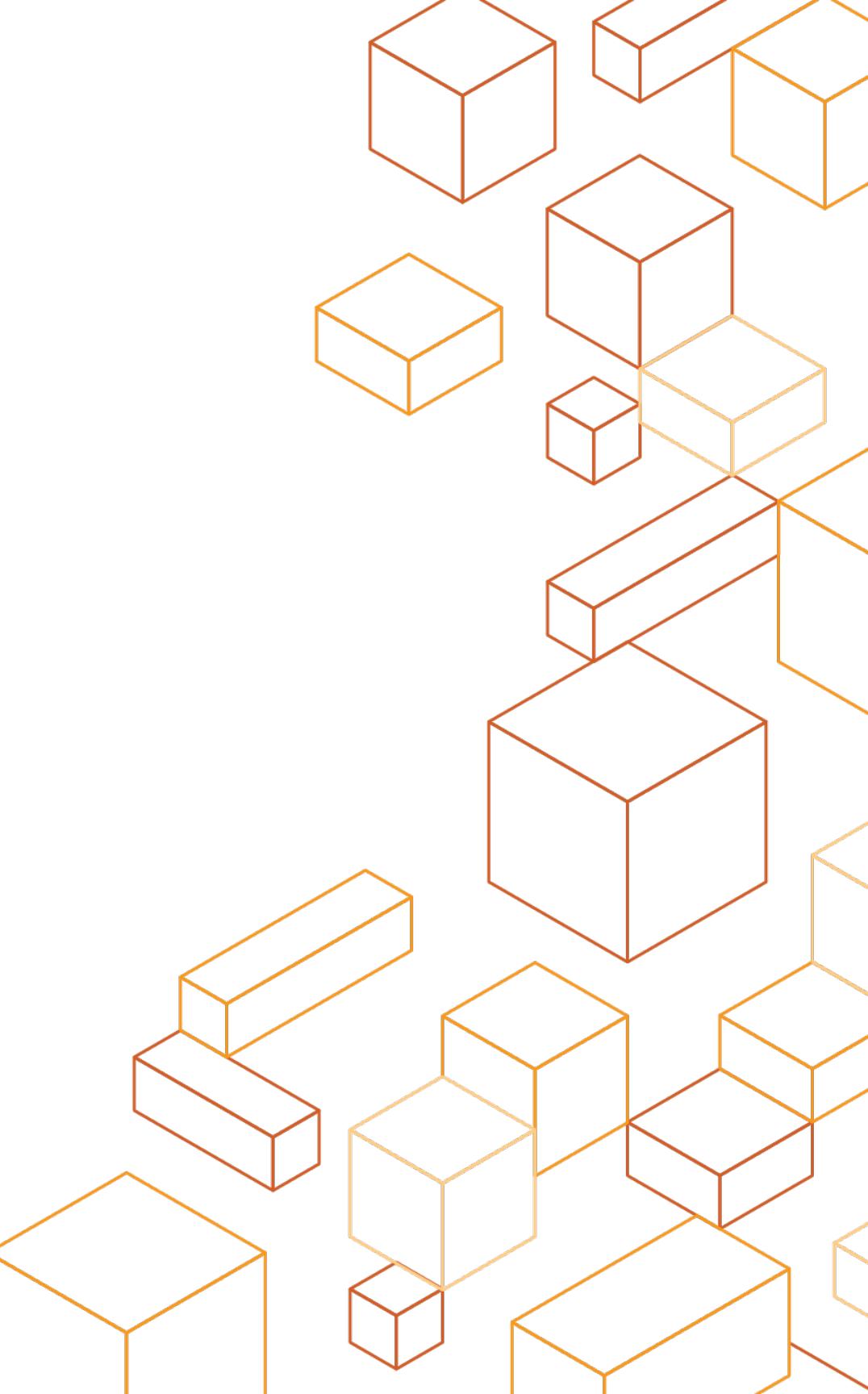




Logging & Monitoring



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

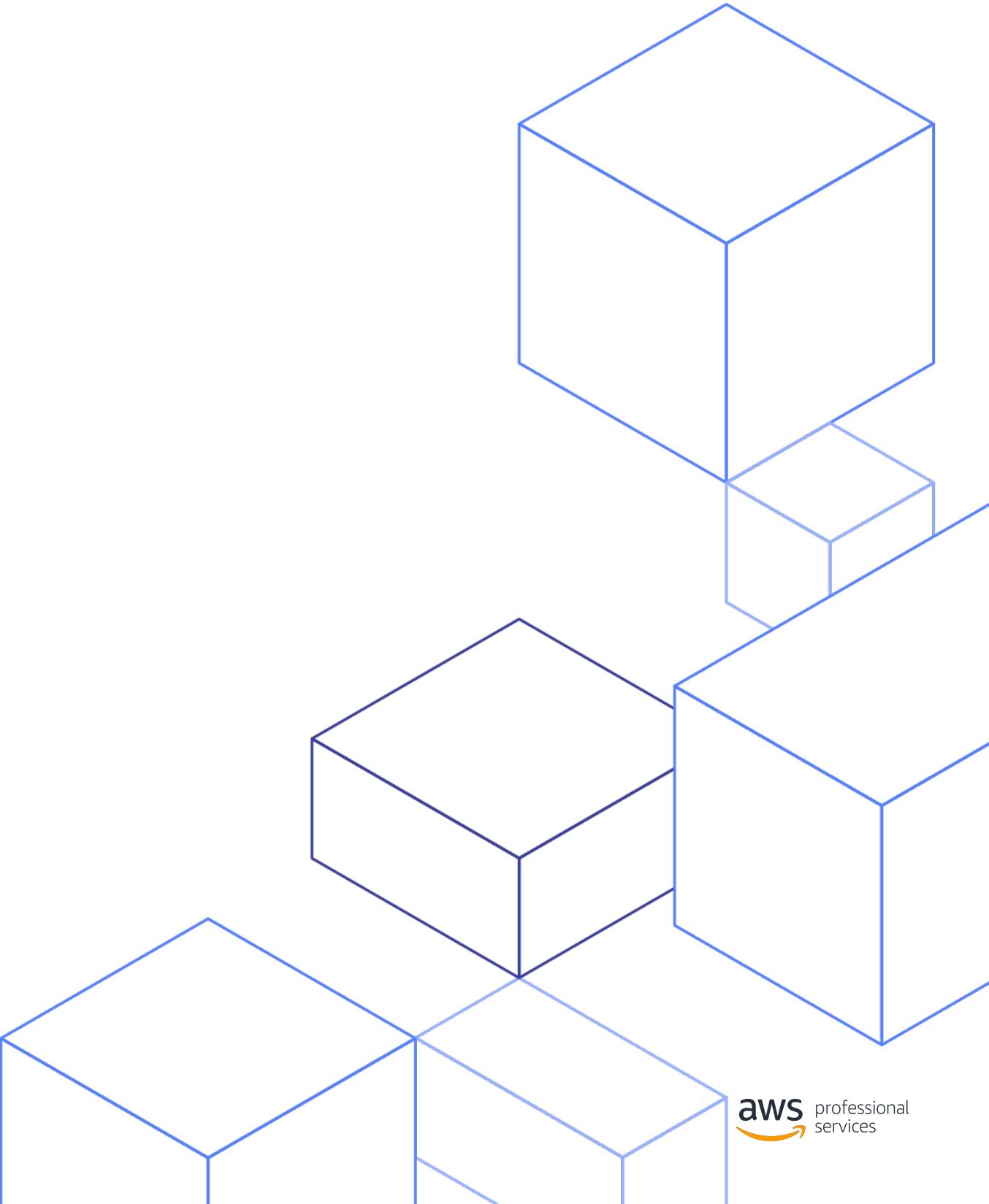
Ubiquitous Logging and Monitoring

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

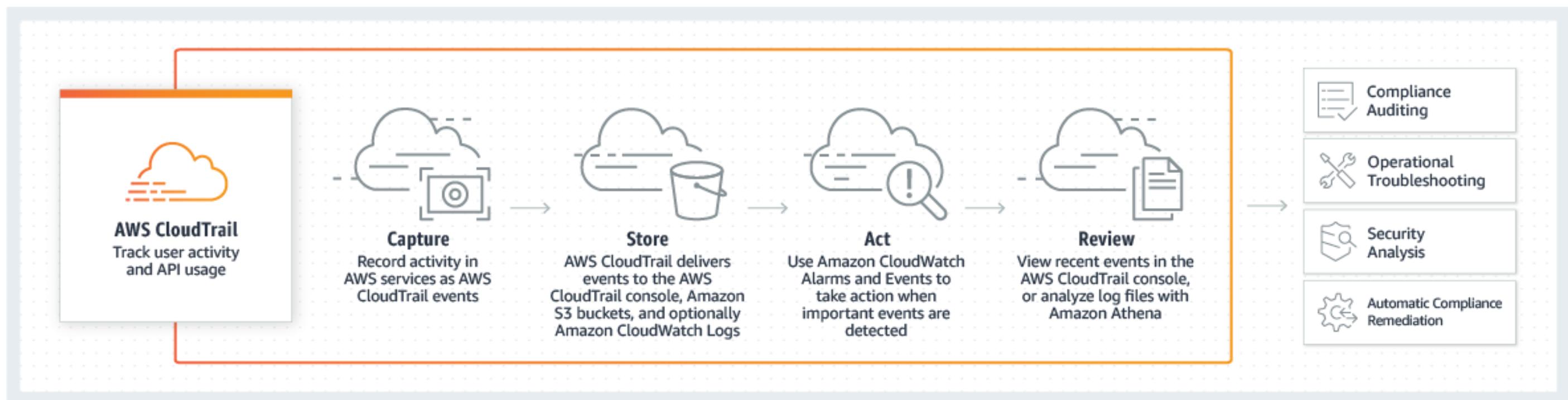
Logging & Monitoring



AWS CloudTrail

What is it?

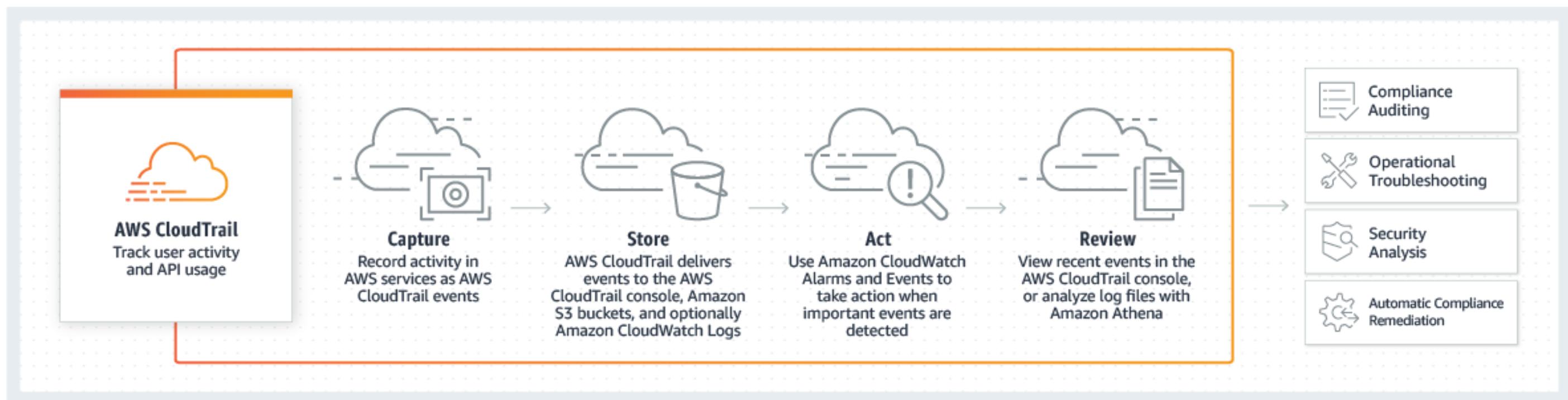
- A service that enables governance, compliance, and operational and risk auditing of your AWS account
- With CloudTrail, you can capture and log events related to API calls and account activity events across your AWS infrastructure and resources



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

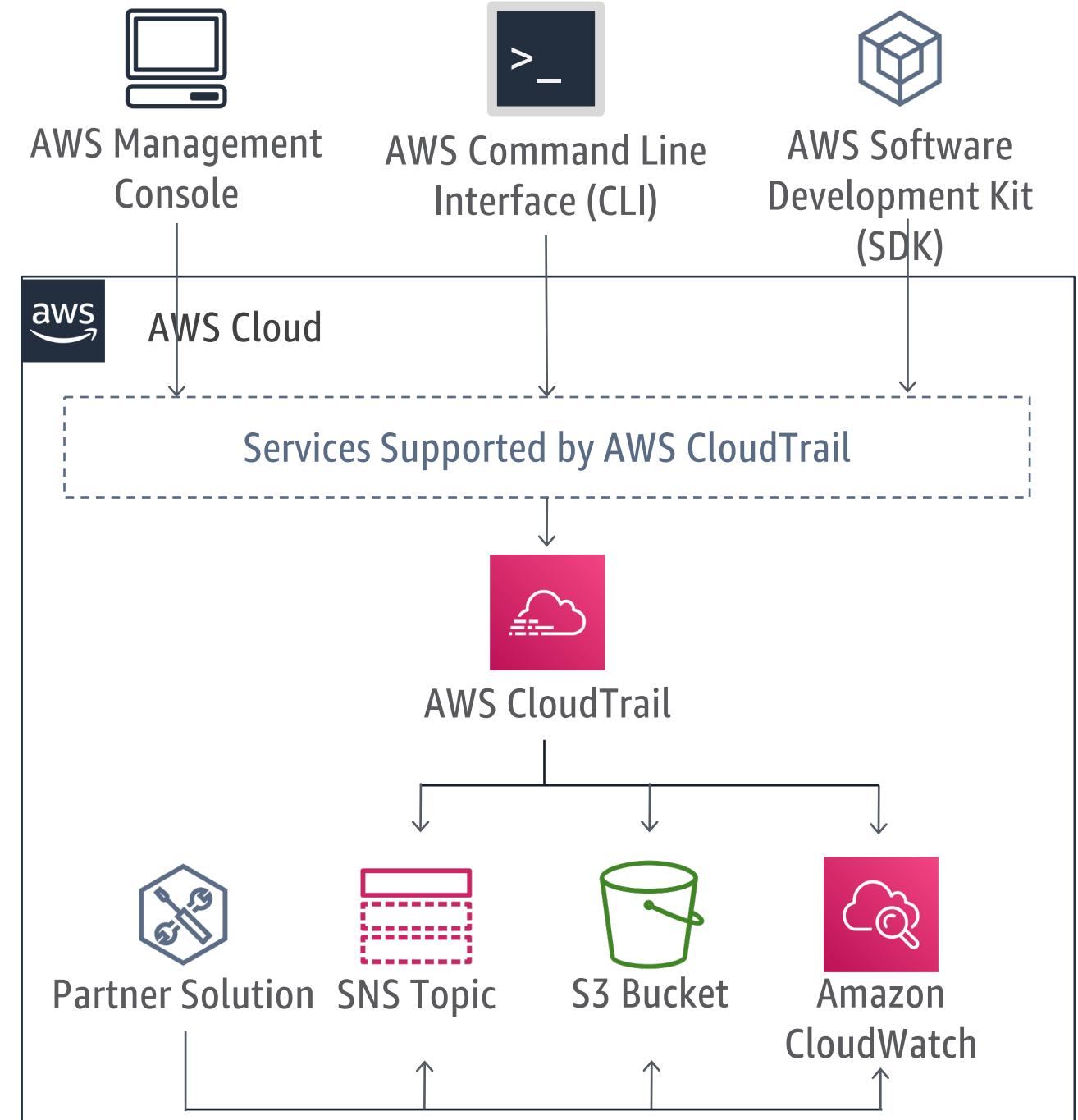


AWS CloudTrail - Common Use Cases

- **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

```
{  
    "eventVersion": "1.01",  
    "userIdentity": {  
        "type": "IAMUser",  
        "principalId": "AIDAJDPLRKLG7UEXAMPLE",  
        "arn": "arn:aws:iam::123456789012:user/Alice",  
        "accountId": "123456789012",  
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",  
        "userName": "Alice",  
        "sessionContext": {  
            "attributes": {  
                "mfaAuthenticated": "false",  
                "creationDate": "2014-03-18T14:29:23Z"  
            }  
        }  
    },  
    "eventTime": "2014-03-18T14:30:07Z",  
    "eventSource": "cloudtrail.amazonaws.com",  
    "eventName": "StartLogging",  
    "awsRegion": "us-west-2",  
    "sourceIPAddress": "72.21.198.64",  
    "userAgent": "AWSConsole, aws-sdk-java/1.4.5 Linux/x.xx.fleetxen Java_HotSpot(TM)_64-Bit_Server_VM/xx",  
    "requestParameters": {  
        "name": "Default"  
    },  
    ...  
}
```

AWS CloudTrail - Configuration

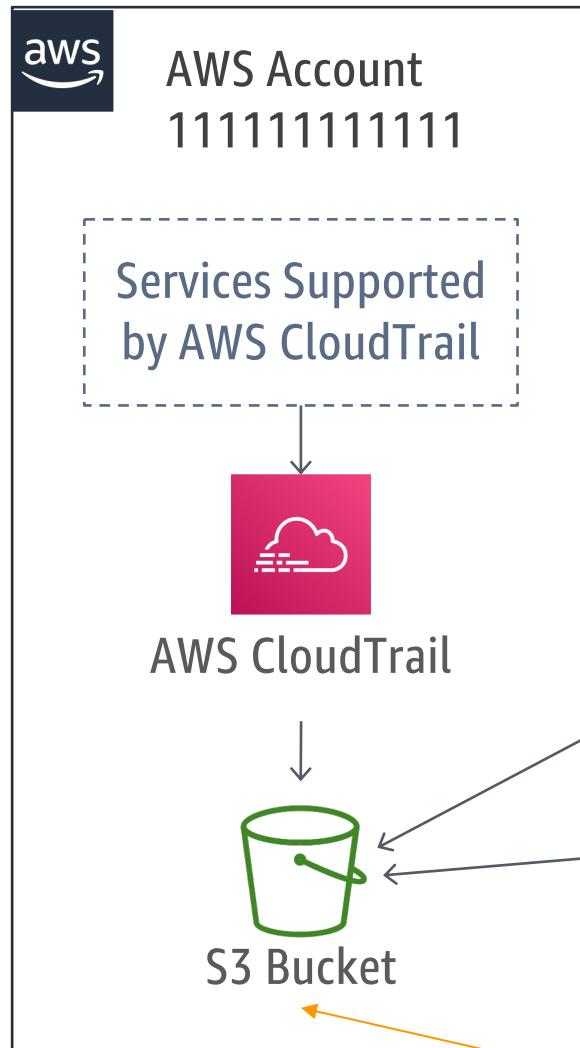
- You can create two types of “trails”:
 - A trail that applies to all regions
 - A trail that applies to one region
- When you create a trail that applies to all regions, CloudTrail creates the same trail in each region, records the log files in each region, and delivers the log files to the single 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

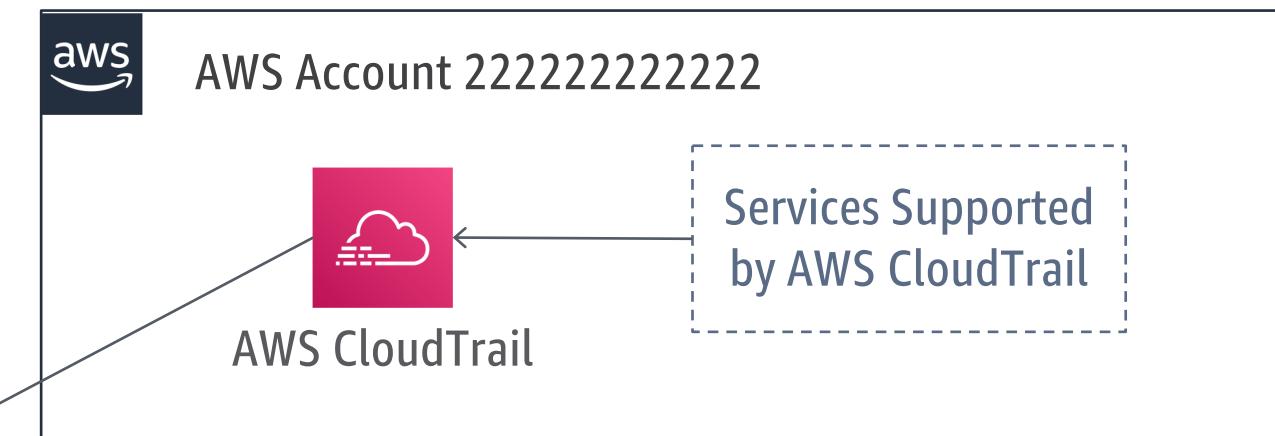
1. Turn on CloudTrail for 111111111111



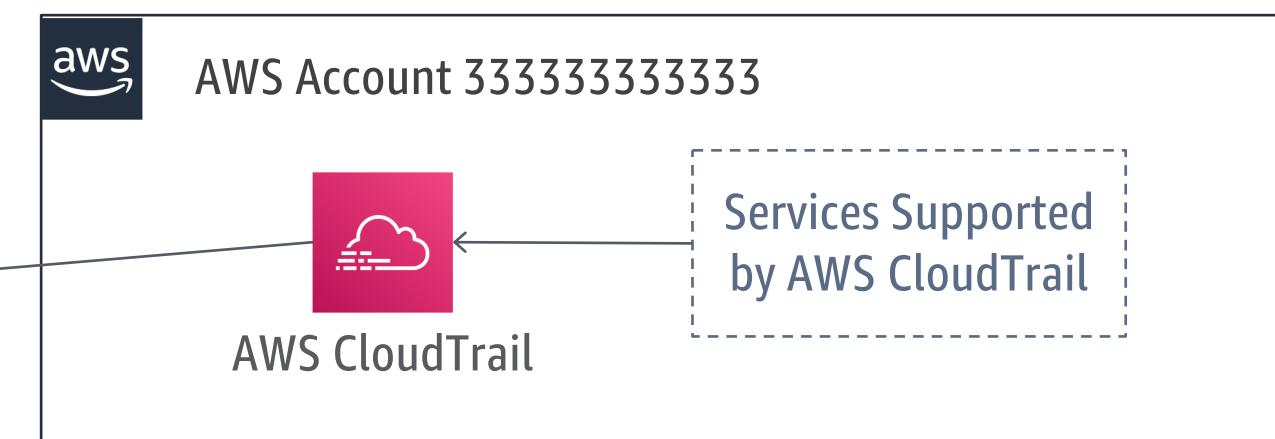
2. Update bucket policy

“arn:aws:s3:::mycloudtrailbucket/AWSLogs/222222222222/*”,
“arn:aws:s3::: mycloudtrailbucket/AWSLogs/333333333333/*”

3. Turn on CloudTrail for 222222222222



4. Turn on CloudTrail for 333333333333



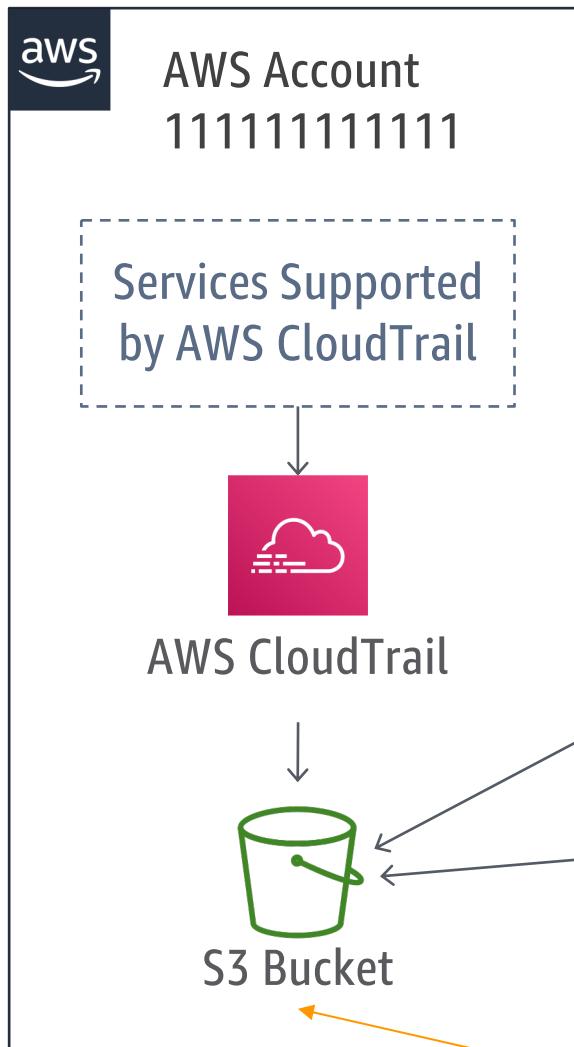
AWS CloudTrail – Centralizing Logs

- 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

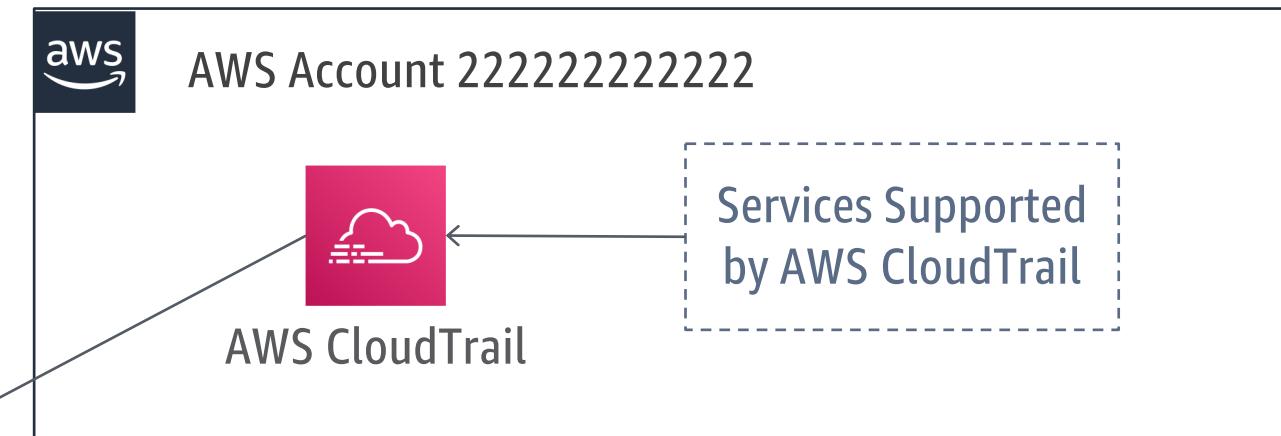
Watch out for multiple trails when enabling in an existing Organization!

AWS CloudTrail – Centralizing Logs

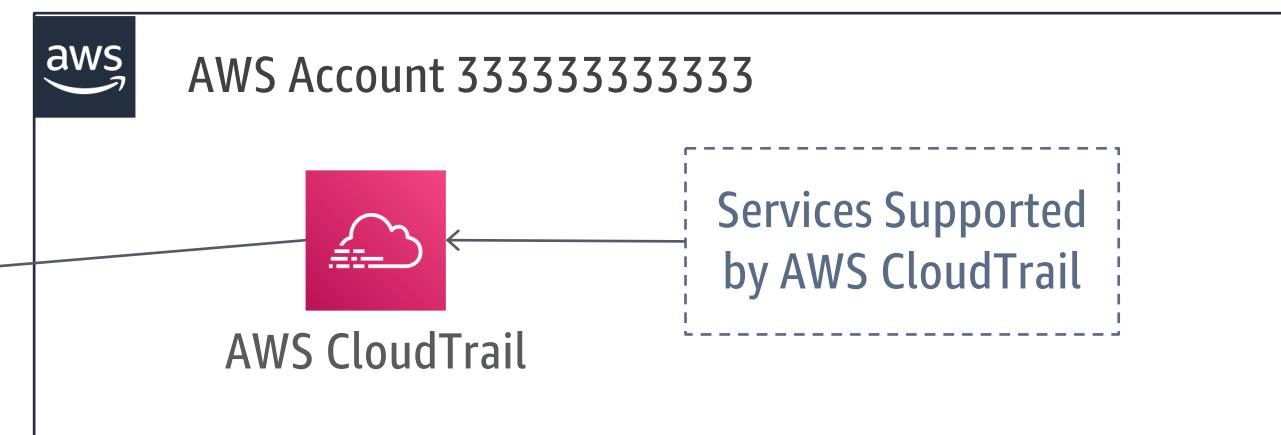
1. Turn on CloudTrail for your Organization



3. Turn on CloudTrail for 222222222222



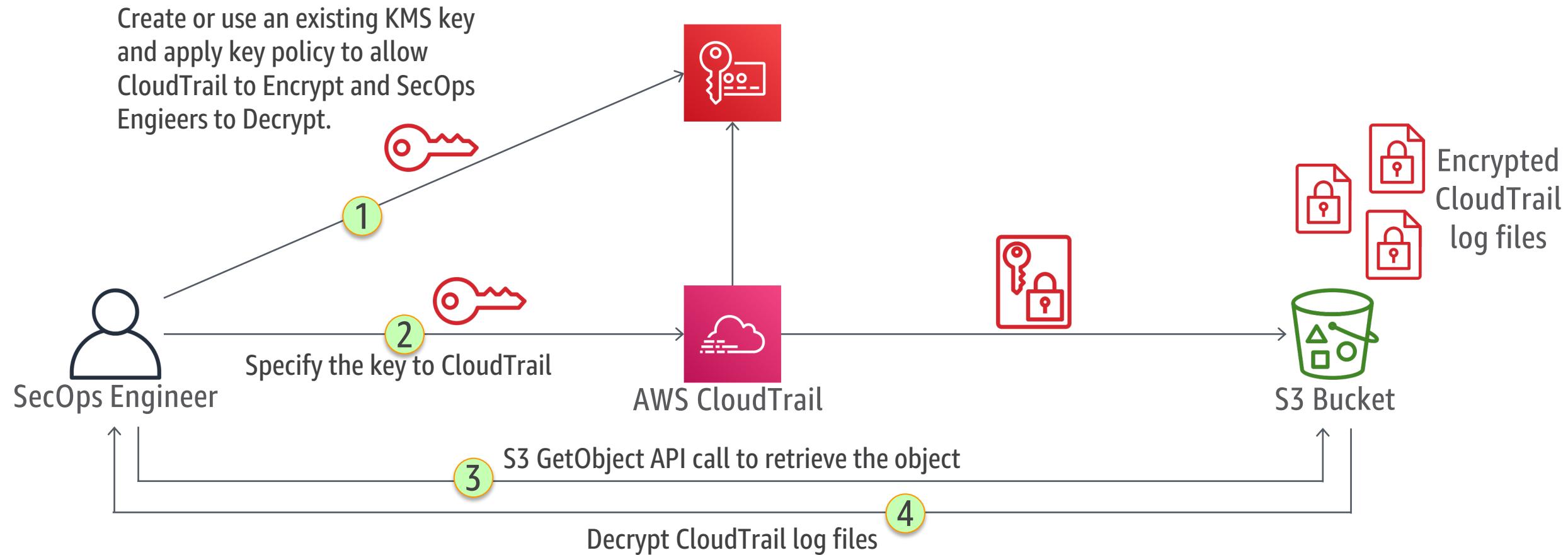
4. Turn on CloudTrail for 333333333333



2. Update bucket policy

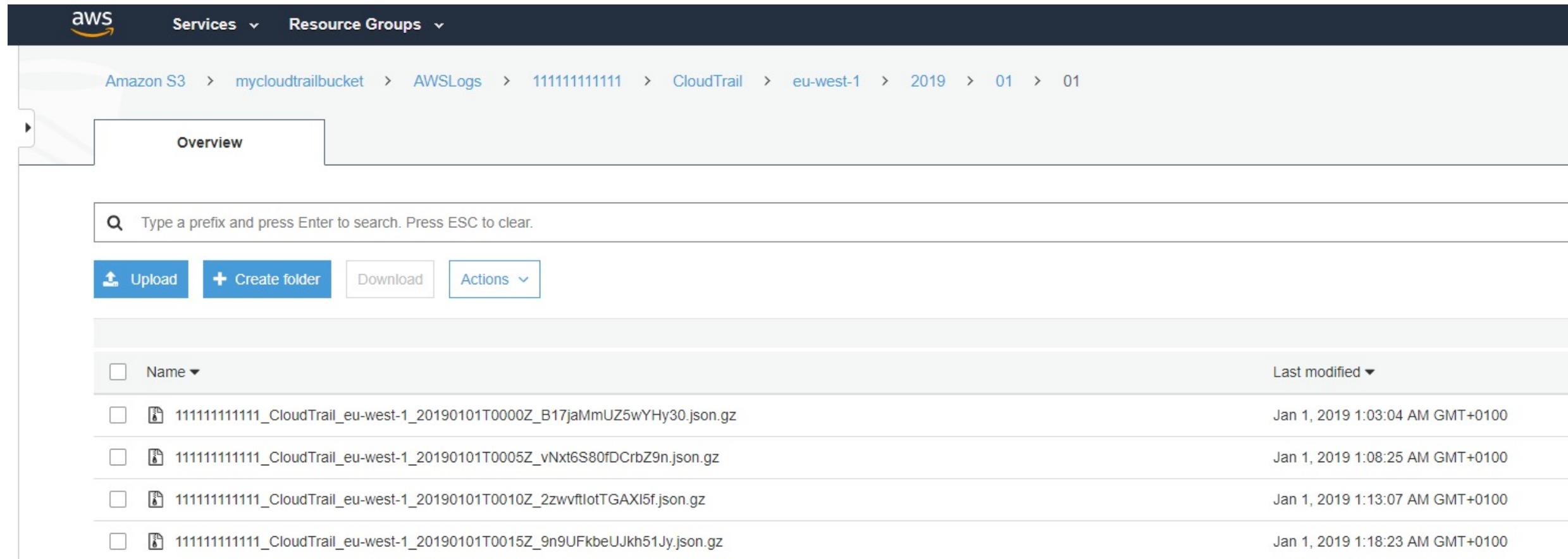
`"arn:aws:s3:::mycloudtrailbucket/AWSLogs/o-12345678/*"`

AWS CloudTrail – KMS Encryption



AWS CloudTrail – Storage in S3

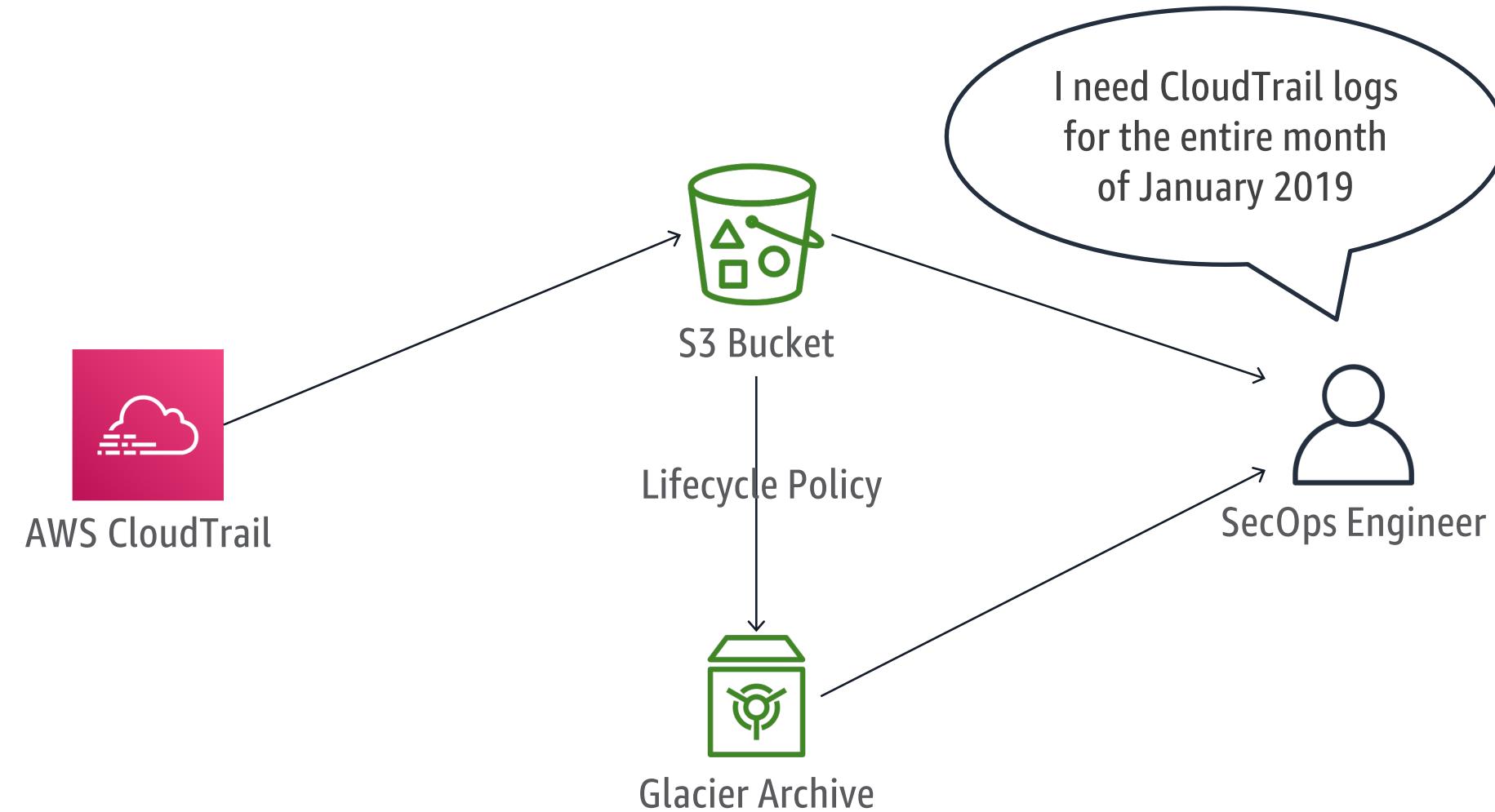
- Default descriptive folder structure makes it easier to store log files from multiple accounts and regions in the same S3 bucket.
- Detailed log file name helps identify the contents of the log file
- Unique identifier in the file name prevents overwriting log files.



The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, and 'Resource Groups' dropdown. Below the navigation bar, the breadcrumb navigation shows the path: Amazon S3 > mycloudtrailbucket > AWSLogs > 111111111111 > CloudTrail > eu-west-1 > 2019 > 01 > 01. The main content area has a title 'Overview' and a search bar with placeholder text 'Type a prefix and press Enter to search. Press ESC to clear.' Below the search bar are four buttons: 'Upload' (blue), '+ Create folder' (blue), 'Download' (light blue), and 'Actions' (light blue). The main table lists five log files:

	Name	Last modified
<input type="checkbox"/>	111111111111_CloudTrail_eu-west-1_20190101T0000Z_B17jaMmUZ5wYHy30.json.gz	Jan 1, 2019 1:03:04 AM GMT+0100
<input type="checkbox"/>	111111111111_CloudTrail_eu-west-1_20190101T0005Z_vNxt6S80fDCrbZ9n.json.gz	Jan 1, 2019 1:08:25 AM GMT+0100
<input type="checkbox"/>	111111111111_CloudTrail_eu-west-1_20190101T0010Z_2zwvftlotTGAXI5f.json.gz	Jan 1, 2019 1:13:07 AM GMT+0100
<input type="checkbox"/>	111111111111_CloudTrail_eu-west-1_20190101T0015Z_9n9UFkbeUJkh51Jy.json.gz	Jan 1, 2019 1:18:23 AM GMT+0100

AWS CloudTrail – Lifecycle Management



AWS CloudTrail – Lifecycle Management

Configured via S3

Available actions:

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

Storage class transition

You can add rules in a lifecycle configuration to tell Amazon S3 to transition objects to another storage class. [Learn more](#)

Current version Previous versions

For current versions of objects [+ Add transition](#)

Object creation	Days after creation
Select a transition	days X
Transition to Standard-IA after	
Transition to Intelligent-Tiering after	
Transition to One Zone-IA after	
Transition to Amazon Glacier after	

Configure expiration

Current version Previous versions

Expire current version of object [i](#)

After days from object creation

Clean up expired object delete markers and incomplete multipart uploads

Clean up expired object delete markers [i](#)

You cannot enable clean up expired object delete markers if you enable Expiration.

Clean up incomplete multipart uploads [i](#)

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

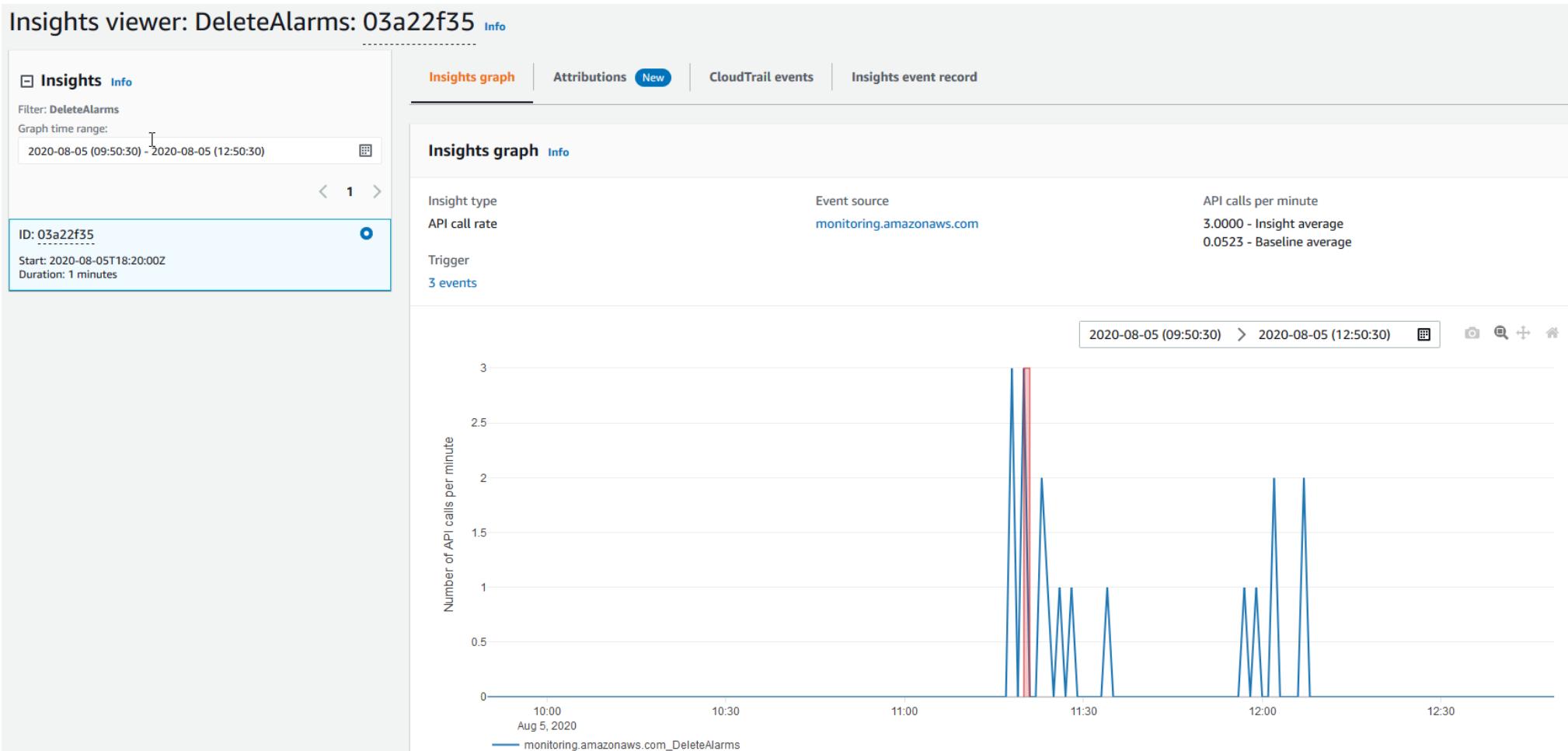
- To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it, you can use CloudTrail log file integrity validation. Validated log files are invaluable in security and forensic investigations.
- This feature is built using industry standard algorithms: SHA-256 for 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 CloudTrail Insights

Top user identity ARNs during Insights event Info			
	User identity ARN	Insight average	Baseline average
1	arn:aws:sts::████████:assumed-role/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable/AutoScaling-ManageAlarms	3.0000 (100.000%)	0.0523 (100.000%)
Average API calls during Insights event		3.0000	0.0523
► Top baseline user identity ARNs			
Top user agents during Insights event Info			
	User agent	Insight average	Baseline average
1	dynamodb.application-autoscaling.amazonaws.com	3.0000 (100.000%)	0.0523 (100.000%)
Average API calls during Insights event		3.0000	0.0523
► Top baseline user agents			
Top error codes during Insights event Info			
	Error code	Insight average	Baseline average
1	None	3.0000 (100.000%)	0.0523 (100.000%)
Average API calls during Insights event		3.0000	0.0523
► Top baseline error codes			

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



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

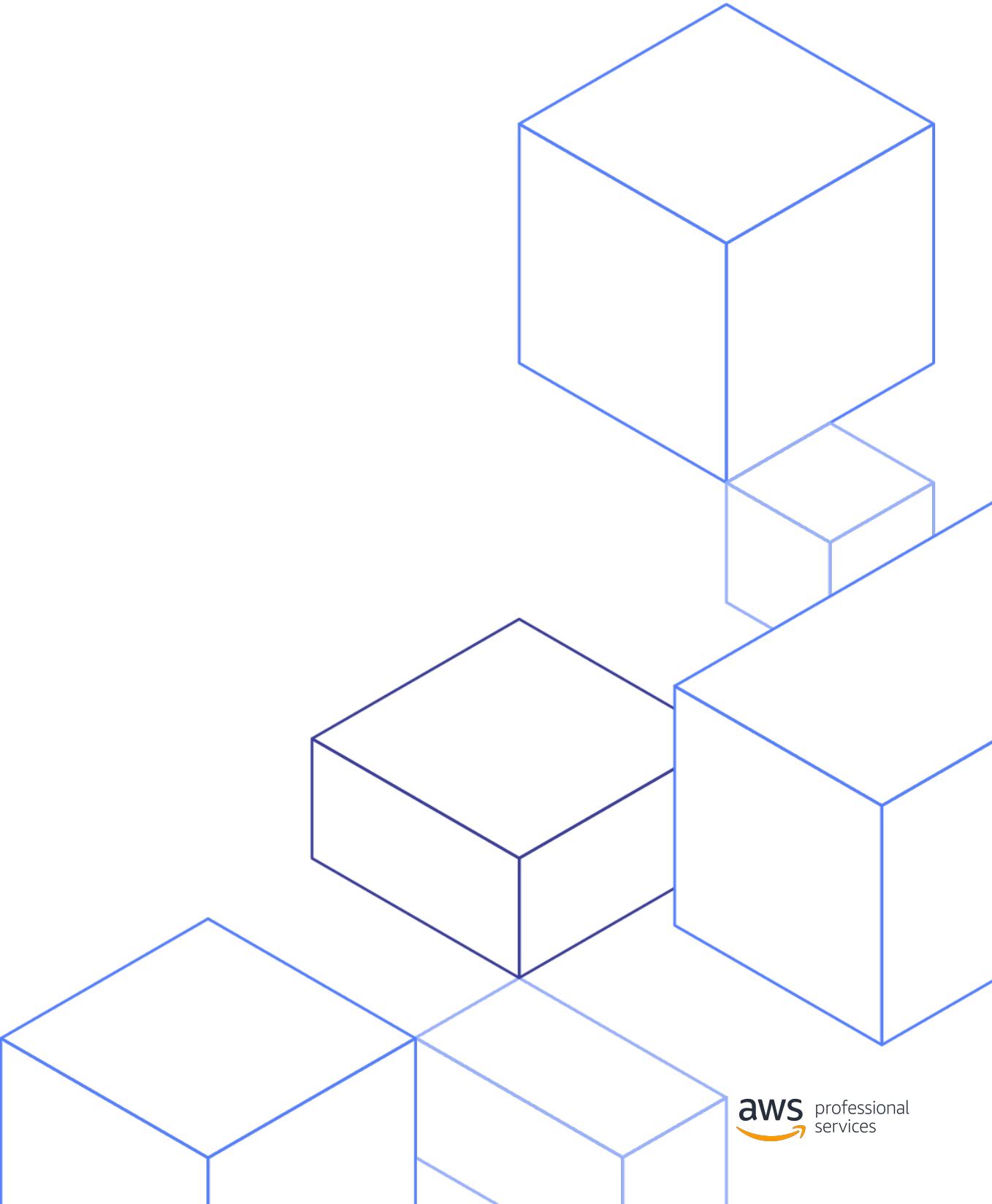
Event Data	AWS account	Interface	Source IP	Source port	Protocol	Packets	End time	Accept or reject
► 2 41747		eni-b30b9cd5	119.147.115.32	10.1.1.179 6000	22 6 1 40	1442975475	1442975535	REJECT OK
▼ 2 41747		eni-b30b9cd5	169.54.233.117	10.1.1.179 21188	80 6 1 40	1442975535	1442975595	REJECT OK
▼ 2 41747		eni-b30b9cd5	212.7.209.6	10.1.1.179 3389	3389 6 1 40	1442975596	1442975655	REJECT OK
▼ 2 41747		eni-b30b9cd5	189.134.227.225	10.1.1.179 39664	23 6 2 120	1442975656	1442975716	REJECT OK
▼ 2 41747		eni-b30b9cd5	77.85.113.238	10.1.1.179 0 0 1 1	100 1442975656	1442975716	REJECT OK	
▼ 2 41747		eni-b30b9cd5	10.1.1.179	198.60.73.8 512	123 17 1 76	1442975776	1442975836	ACCEPT OK

Annotations pointing to specific columns:

- AWS account: Points to the second column.
- Interface: Points to the third column.
- Source IP: Points to the fourth column.
- Source port: Points to the fifth column.
- Protocol: Points to the sixth column.
- Packets: Points to the seventh column.
- End time: Points to the eighth column.
- Accept or reject: Points to the ninth column.
- Destination IP: Points to the fourth column.
- Destination port: Points to the fifth column.
- Bytes: Points to the seventh column.
- Start time: Points to the eighth column.

Processing Logs

Logging & Monitoring



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



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

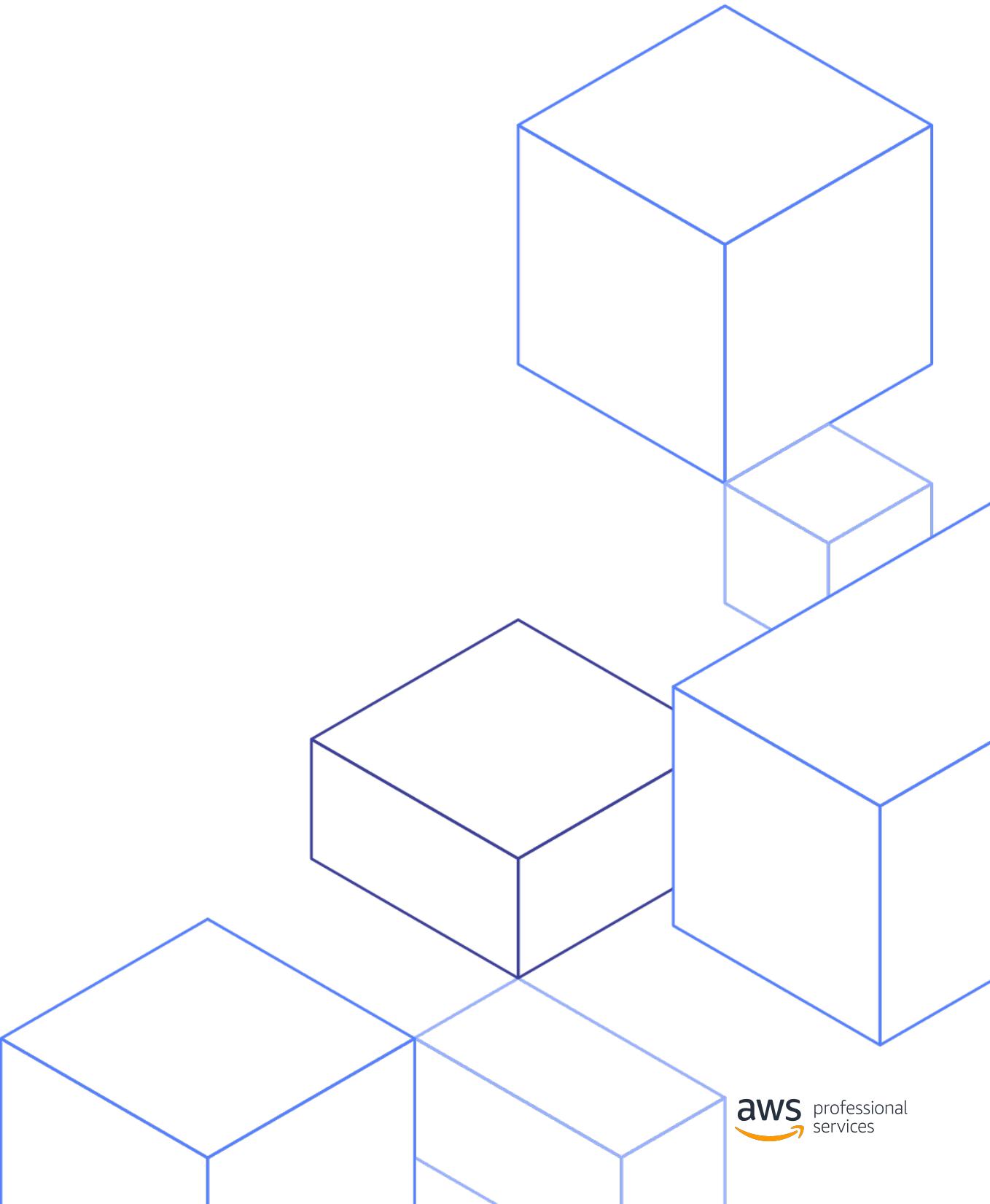
The screenshot shows the Amazon OpenSearch Dashboards interface with the following details:

- Header:** OpenSearch Dashboards, Dashboard / Octank Analytics, Full screen, Share, Clone, Reporting, Edit, Refresh.
- Left Sidebar:** Home, Recently viewed (Octank Analytics), OpenSearch Dashboards (Overview, Discover, Dashboard, Visualize), OpenSearch Plugins (Query Workbench, Reporting, Notebooks, Alerting, Anomaly Detection, Trace Analytics, Index Management, Security), Management (Dev Tools, Stack Management).
- Top Right Controls:** DQL, Last 7 days, Show dates, Refresh.
- [Octank] Controls:** Origin City (Select...), Destination City (Select...), Miles to Destination (0 to 960).
- [Octank] Analytics:** A panel describing the Octank dashboard, stating it contains real-time data from thousands of fleets across various Octank Distribution Centers (ODC). It provides a 360-degree view of fleets with respect to their surrounding temperature, weather, speed, traffic, etc. You can view it, search it, and interact with the visualizations to drill down and get real-time insights.
- [Octank] Carriers:** A donut chart showing Logstash Logistics (blue) and OpenSearch Logistics (orange).
- [Octank] Current Stats of Fleet:** A table listing fleet statistics.

Device Id	Fleet Reg No	Origin	Destination	Timestamp	Temperature °F	Fuel Level	milesToGo	Speed Miles/Hr
3452899774	H50E3NTIS6	ODC Seattle	ODC Los Angeles	Aug 31, 2021 @ 15:01:52.658	86	65%	958.895	5
7232574133	IGPDIWR8HX	ODC Seattle	ODC Los Angeles	Sep 1, 2021 @ 21:03:19.025	-8	72%	815.6	45
1977605220	LJ52AJPFIZ	ODC Seattle	ODC San Jose	Aug 31, 2021 @ 17:02:35.999	65	84%	635.671	7
4915604309	L4TROD0KQ	ODC Seattle	ODC San Jose	Sep 1, 2021 @ 21:03:19.796	51	45%	566.036	59
5139847071	870962KMK1	ODC Seattle	ODC San Francisco	Aug 31, 2021 @ 14:56:41.482	23	22%	514.498	44
1602234061	CGU3VVPVO	ODC Seattle	ODC Los Angeles	Sep 1, 2021 @ 17:02:49.254	2	46%	93.304	24
8487544347	ILUST6EXZJ	ODC Seattle	ODC San Francisco	Sep 1, 2021 @ 12:39:28.357	13	28%	0	0
3971724852	ZCSXKJZG5I	ODC San Jose	ODC Los Angeles	Aug 31, 2021 @ 17:02:36.003	-5	35%	244.396	67
2013799595	GASFVXP1R6	ODC San Jose	ODC Los Angeles	Aug 31, 2021 @ 14:56:41.269	25	86%	145.48	13
4486363768	9WNWCRFL06	ODC San Francisco	ODC Seattle	Sep 1, 2021 @ 21:03:19.028	32	98%	527.809	4
- [Octank] Total Fleets:** 20
- [Octank] Avg Distance to Destination:** 768.511
- [Octank] Max Temperature:** 104 (Max Temperature)
- [Octank] Average Temperature:** 35 (Average Temperature)
- [Octank] Min Temperature:** -10 (Min Temperature)
- [Octank] Weather:** Heavy Fog, Cloudy, Damaging Wind, Snow Storm, Rain, Clear, Thunder & Lightning, Sunny, Snow.

Amazon Athena

Logging & Monitoring



Amazon Athena – What is it?

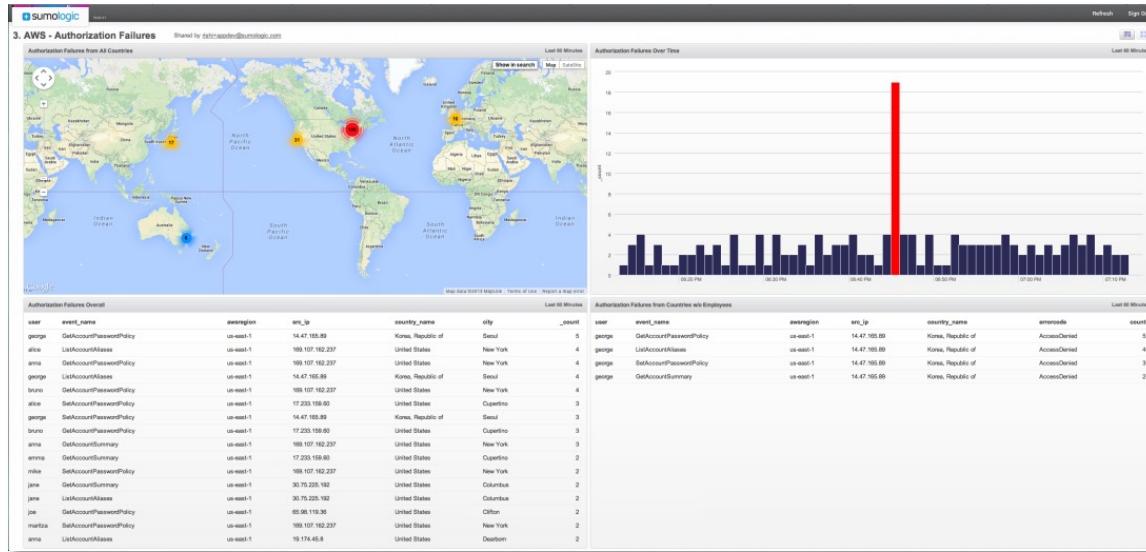
Amazon Athena is an **interactive query service** that makes it easy to analyze data directly on Amazon S3 using Standard SQL

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

+ sumologic

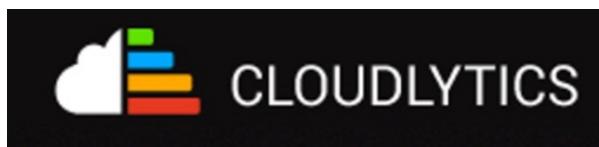
 ALERTLOGIC
Security. Compliance. Cloud.

 LOGGLY

 DATAPIPE

 FOGHORN
WEBSERVICES

 2ND WATCH

 CLOUDLYTICS

STACKDRIVER

splunk®



 CLOUDNEXA

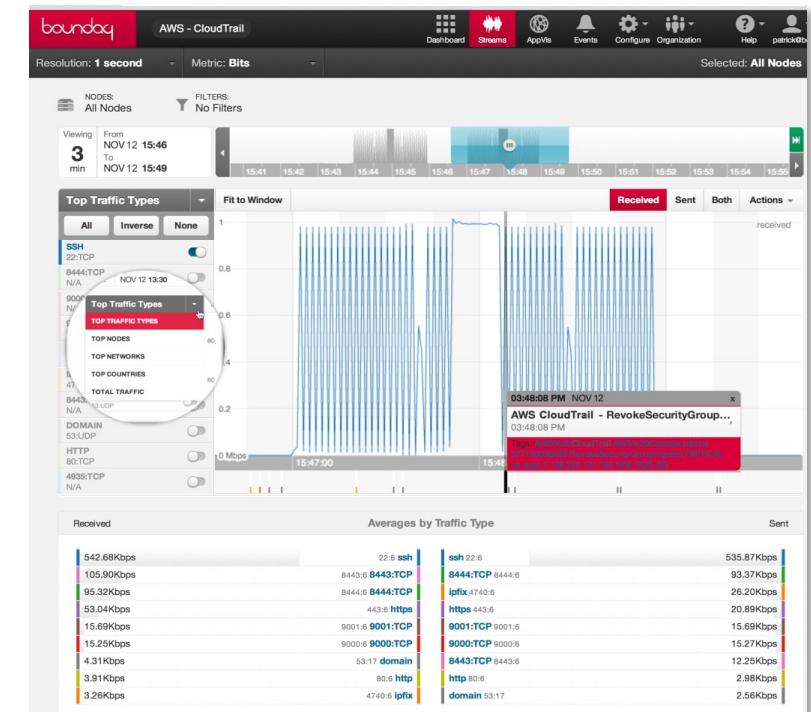
graylog

boundary

smartronix

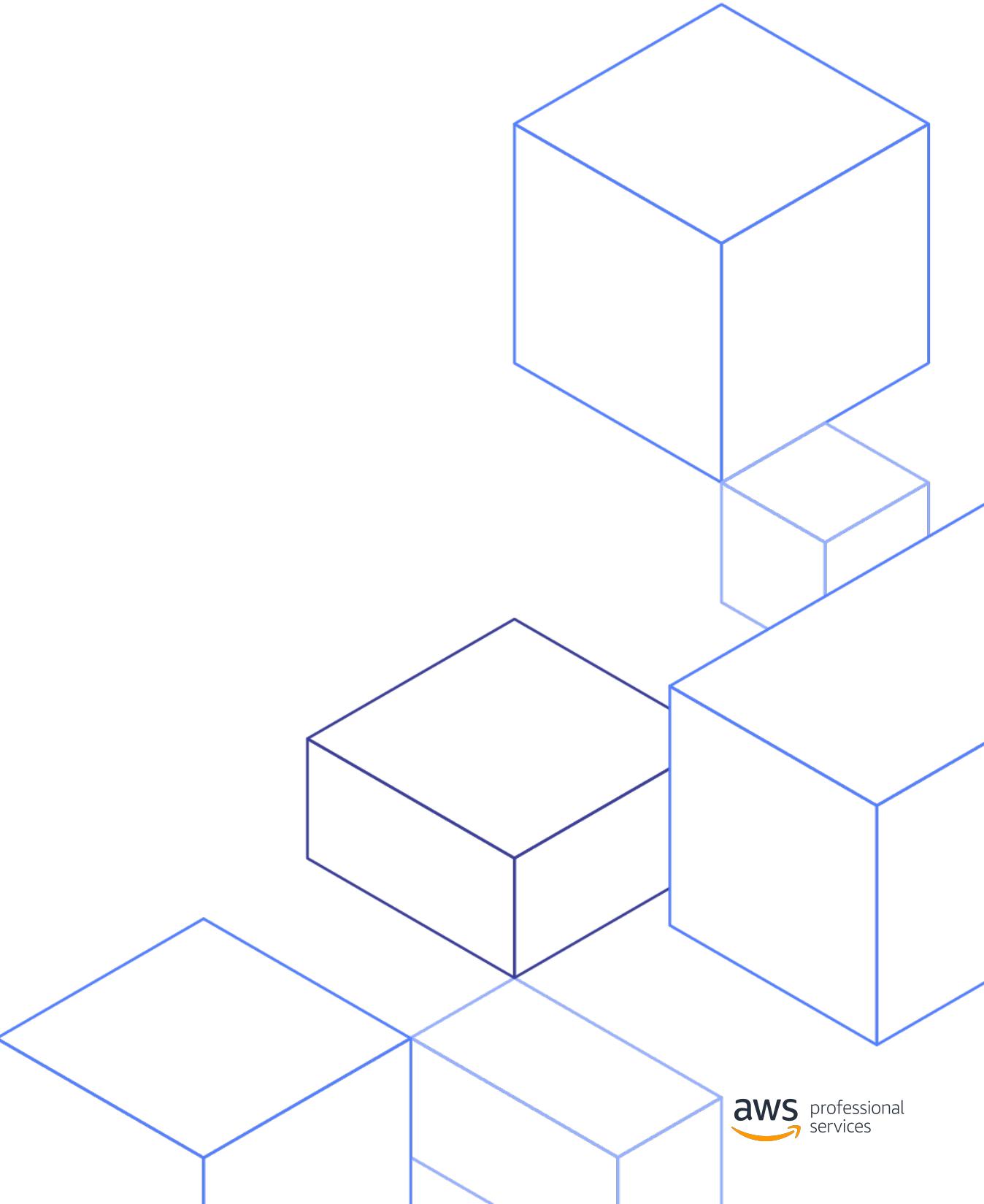
Cloud ASSURED

CloudCheckr

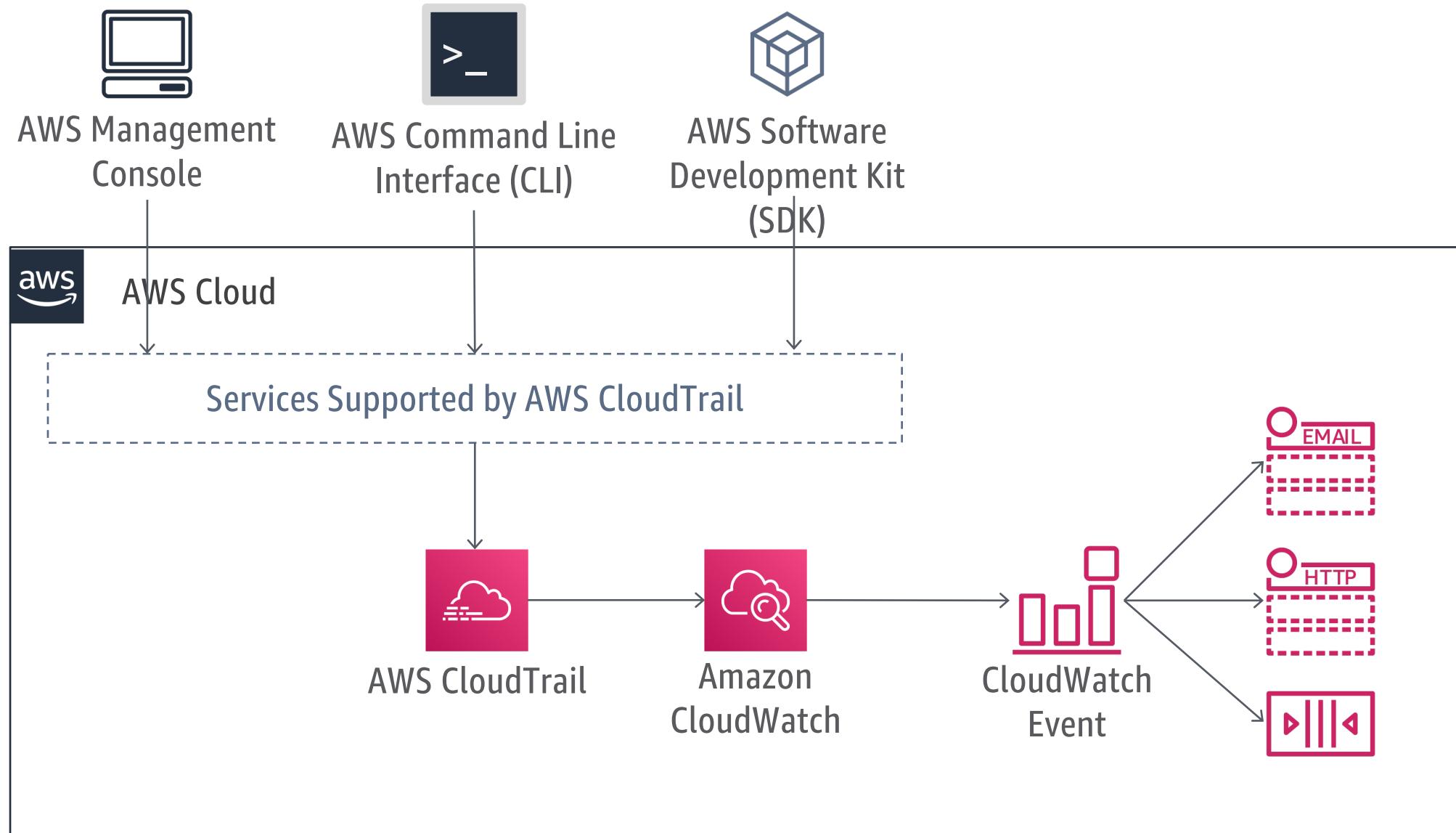


Alerting

Logging & Monitoring



Alerting – Receive Notifications of API activity



Follow-up Actions

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

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

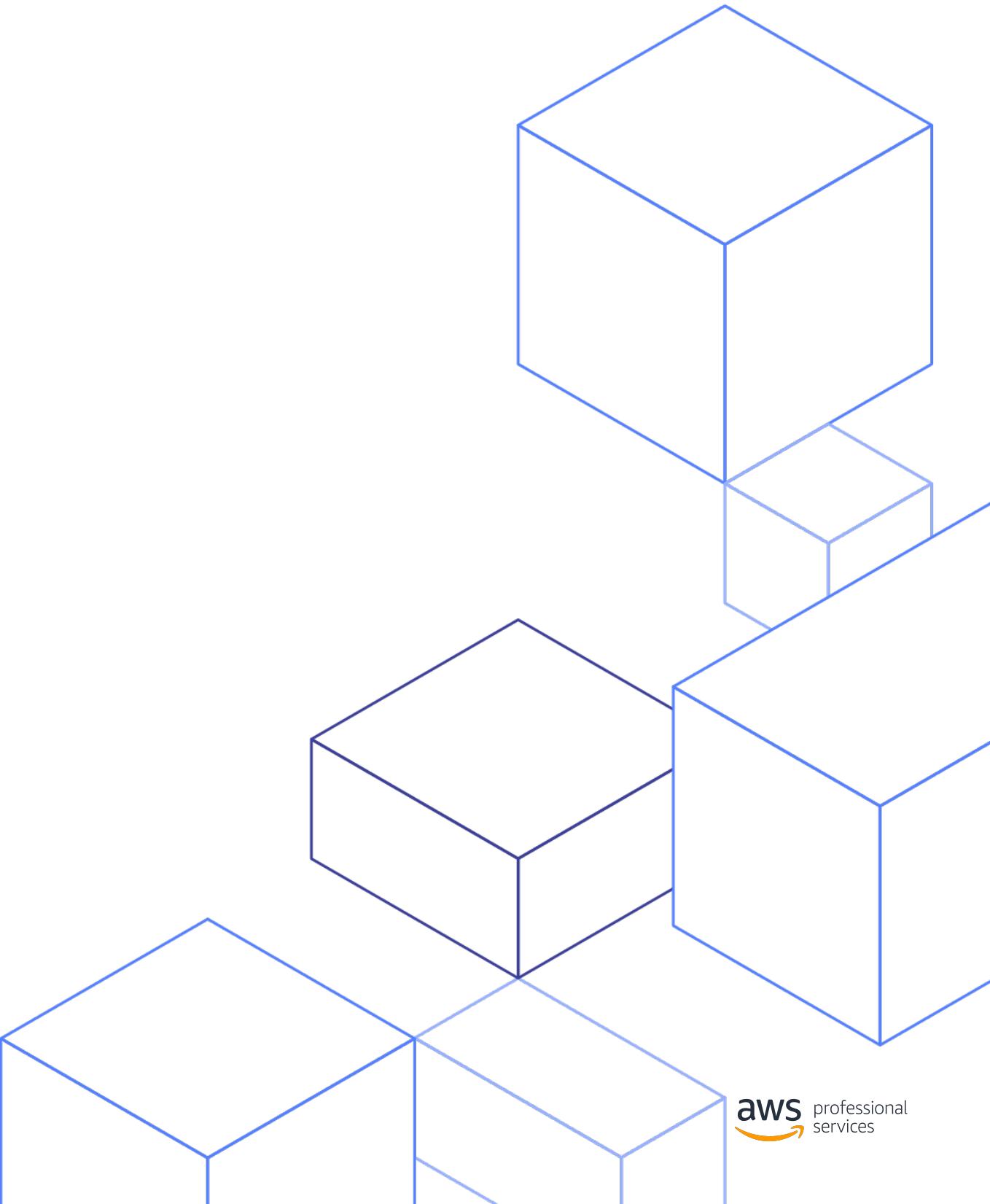
Security configuration checks of your AWS environment:

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

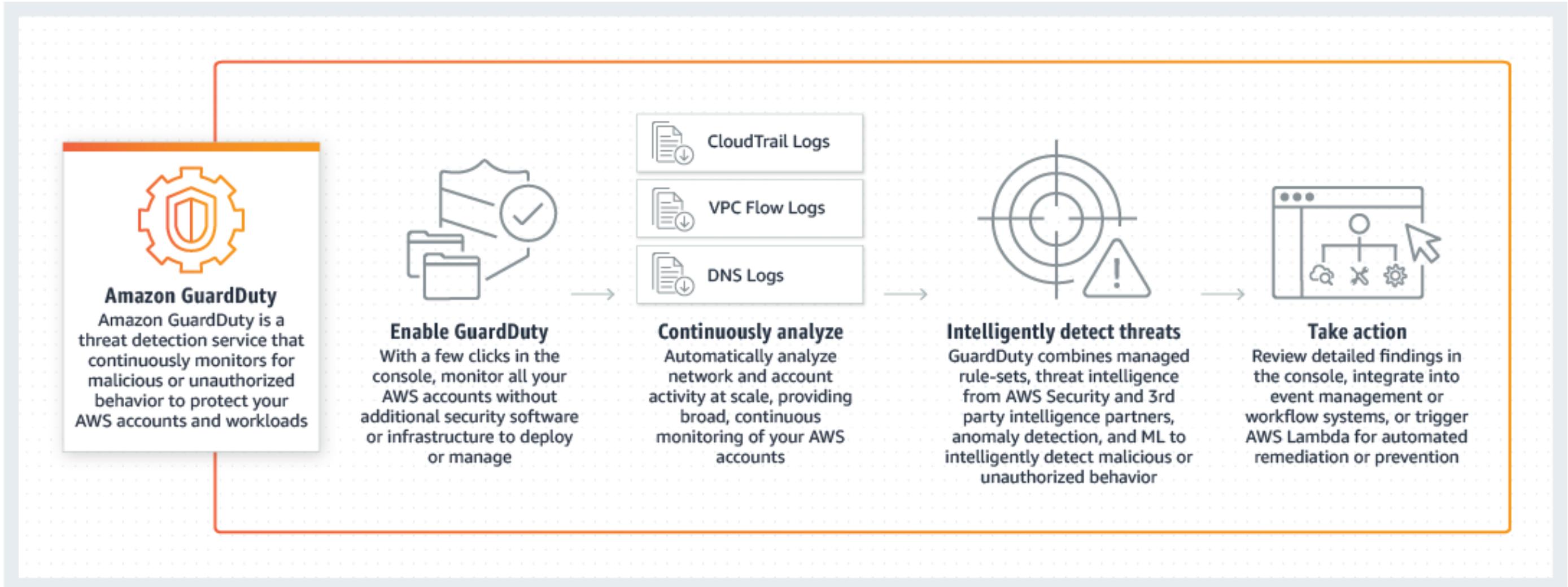
The screenshot shows the AWS Trusted Advisor dashboard. On the left, a sidebar menu includes 'Dashboard' (selected), 'Cost optimization', 'Performance', 'Security', 'Fault tolerance', 'Service limits', and 'Organizational view'. Below the sidebar are 'Preferences' and 'Logout' buttons. The main content area has a header 'Trusted Advisor > Dashboard'. It features a 'Checks summary' section with three categories: 'Action recommended' (4 items, Security), 'Investigation recommended' (5 items, Cost optimization, Fault tolerance, Performance, Service limits), and 'Excluded items' (0). A 'Potential monthly savings' section shows '\$0' and notes that Trusted Advisor has identified 5 cost optimization checks. The 'Recent changes (0)' section indicates 'No recent changes' and provides a link to 'Trusted Advisor FAQs'.

Amazon GuardDuty

Logging & Monitoring



Amazon GuardDuty



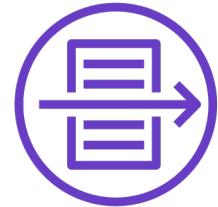
Amazon GuardDuty – Service Benefits

- 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



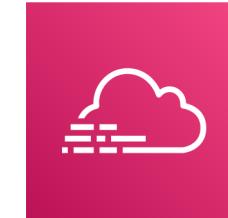
- Flow Logs for VPCs Do Not Need to Be Turned On to Generate Findings, data is consumed through independent duplicate stream.
- Suggested Turning On VPC Flow Logs to Augment Data Analysis (charges apply).

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

The screenshot shows the AWS GuardDuty findings interface. On the left, a sidebar navigation includes options like Findings, Current, Archived, Settings, General, Lists, Accounts, Free trial, Details, and Partners. The main area displays 'Current findings' with 63 results, filtered by 'severity: LOW'. A detailed view of an 'UnauthorizedAccess:EC2/SSHBruteForce' finding is shown on the right, with a summary and a table of affected resources.

Current findings (Showing 63 of 63)

Actions Saved filters Unsaved filter*

severity: LOW

Finding
Unprotected port on EC2 instance i-0ebcc6375897405b4 is being probed.
Unprotected port on EC2 instance i-05b54b9136dd98ffe is being probed.
202.107.104.119 is performing SSH brute force attacks against i-0ebcc6375897405b4.
202.40.190.146 is performing SSH brute force attacks against i-0ebcc6375897405b4.
203.190.163.125 is performing SSH brute force attacks against i-05b54b9136dd98ffe.
61.188.189.7 is performing SSH brute force attacks against i-0ebcc6375897405b4.
46.101.123.127 is performing SSH brute force attacks against i-0ebcc6375897405b4.
220.178.78.130 is performing SSH brute force attacks against i-05b54b9136dd98ffe.
64.79.112.70 is performing SSH brute force attacks against i-05b54b9136dd98ffe.
183.60.110.235 is performing SSH brute force attacks against i-0ebcc6375897405b4.
117.52.87.214 is performing SSH brute force attacks against i-05b54b9136dd98ffe.
89.218.176.232 is performing SSH brute force attacks against i-0ebcc6375897405b4.

UnauthorizedAccess:EC2/SSHBruteForce

203.190.163.125 is performing SSH brute force attacks against i-05b54b9136dd98ffe. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.

Severity	Region	Count
Low	us-east-1	3
Account ID	Resource ID	i-05b54b9136dd...
589881044950		
Last seen	2018-01-08 12:12:28 (2 days ago)	
Resource affected		
Resource role	Resource type	Instance
TARGET		
Instance ID	Port	22
i-05b54b9136dd98ffe		
Image ID	Image description	ami-8fceee4e5 Amazon Linux AMI 2015.09.2...
Launch time	2017-01-09 20:18:16	
Instance profile	Arn: arn:aws:iam::589881044950:instance-profile/website ID: AIPAJKMY33DBQPXDMHVI4	

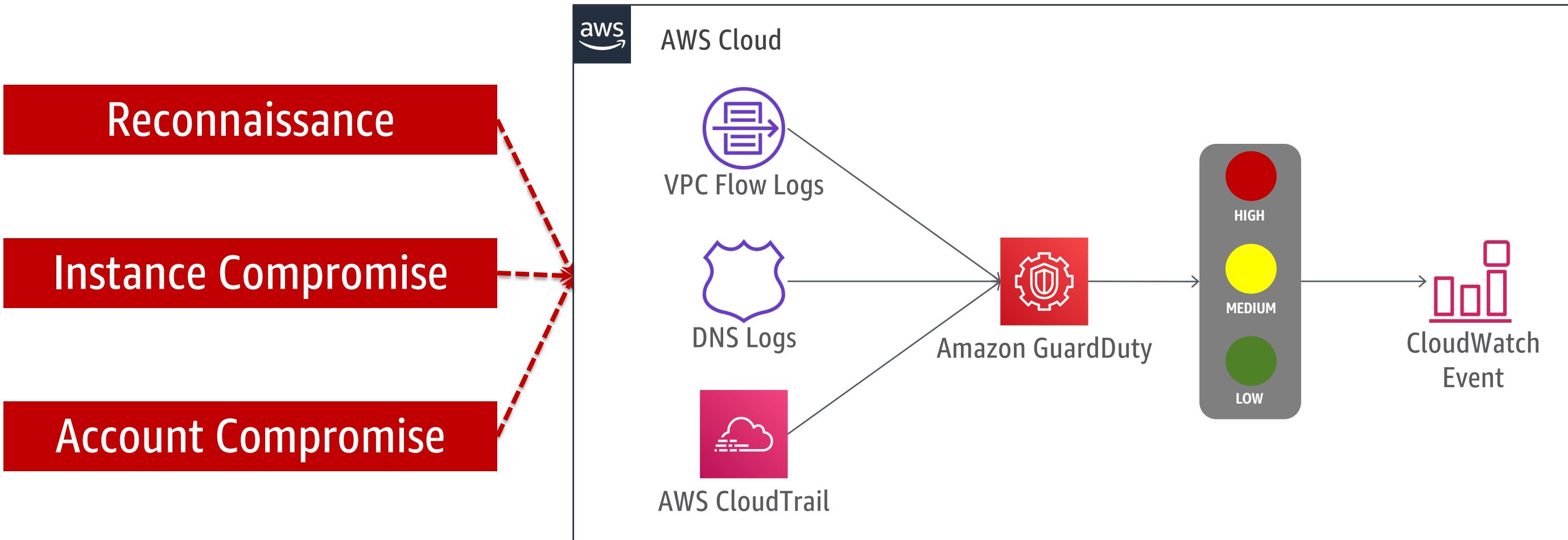
Amazon GuardDuty – Threat Detection

Threat Detection Types

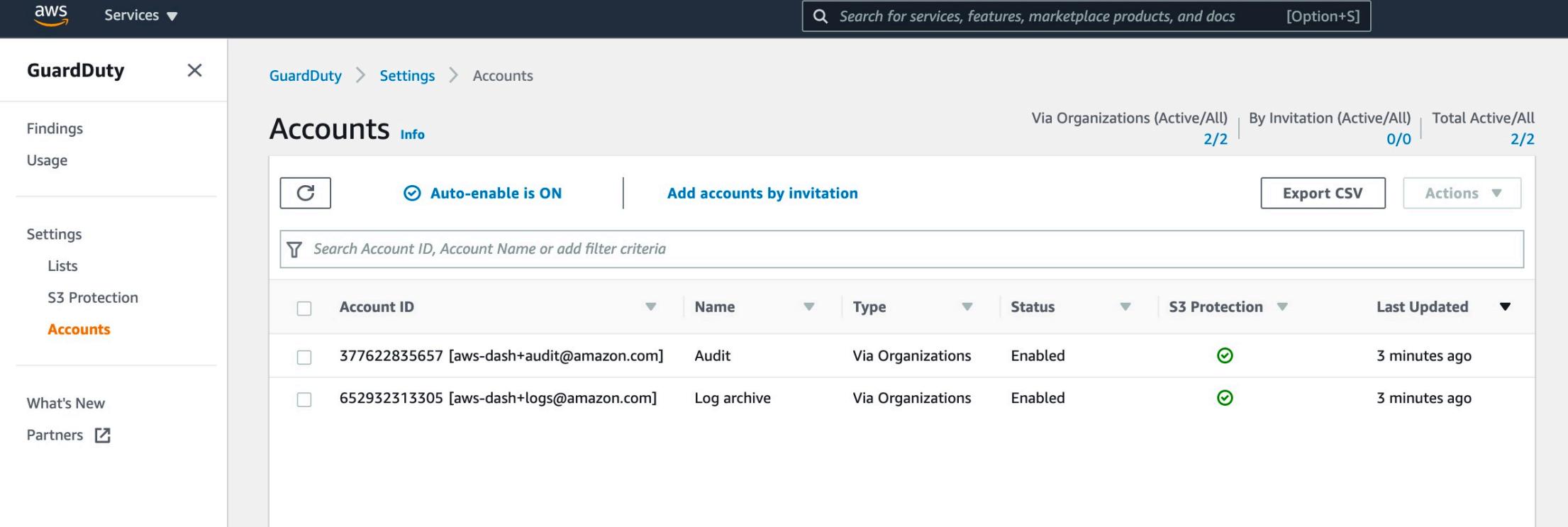
Data Sources

Findings

Respond



Amazon GuardDuty – Organization Support



The screenshot shows the AWS GuardDuty service interface. In the left sidebar, 'GuardDuty' is selected under the 'Accounts' section. The main content area is titled 'Accounts' and shows two accounts listed:

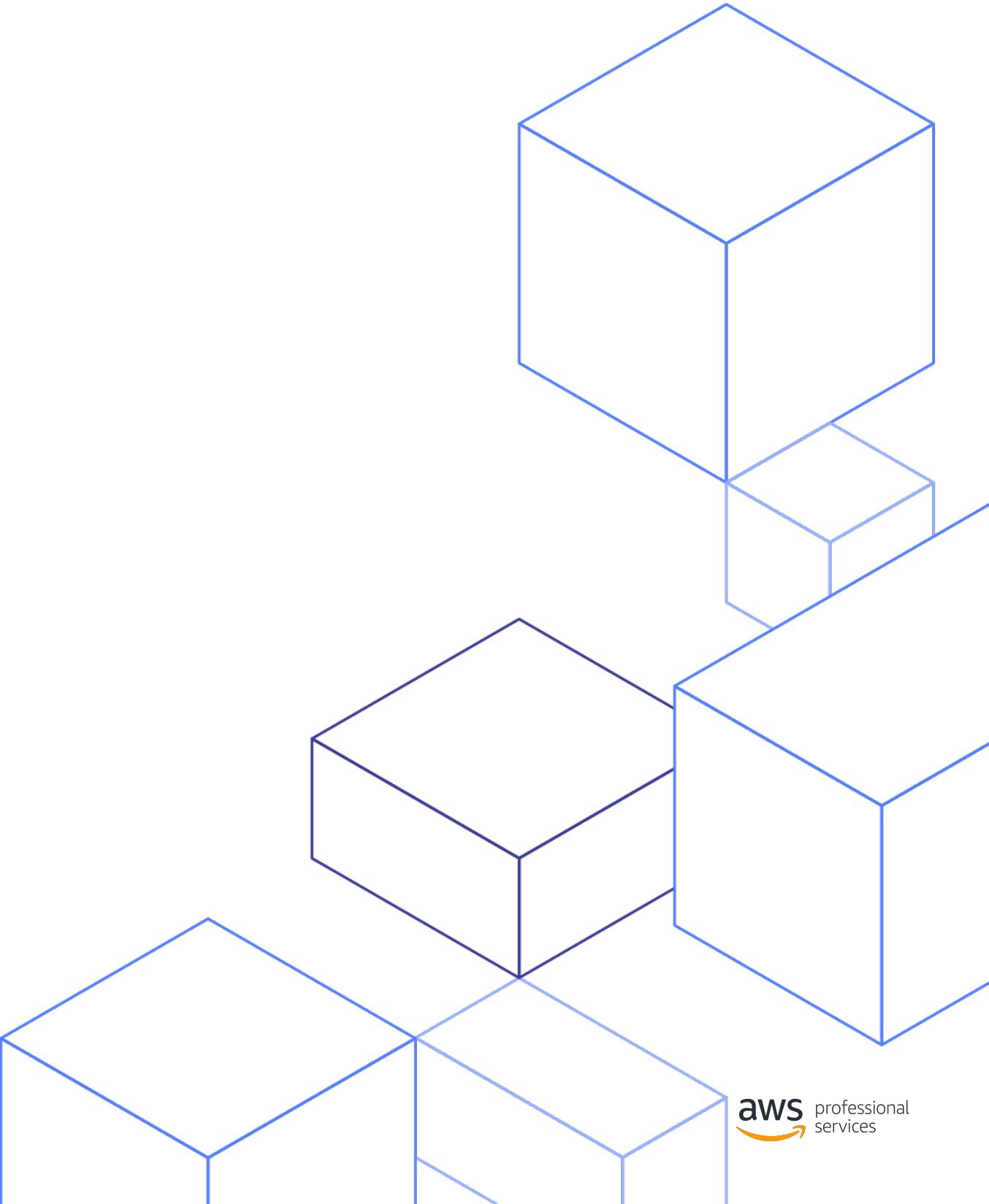
Account ID	Name	Type	Status	S3 Protection	Last Updated
377622835657 [aws-dash+audit@amazon.com]	Audit	Via Organizations	Enabled	✓	3 minutes ago
652932313305 [aws-dash+logs@amazon.com]	Log archive	Via Organizations	Enabled	✓	3 minutes ago

At the top right, there are three filters: 'Via Organizations (Active/All) 2/2', 'By Invitation (Active/All) 0/0', and 'Total Active/All 2/2'. There are also 'Export CSV' and 'Actions' buttons.

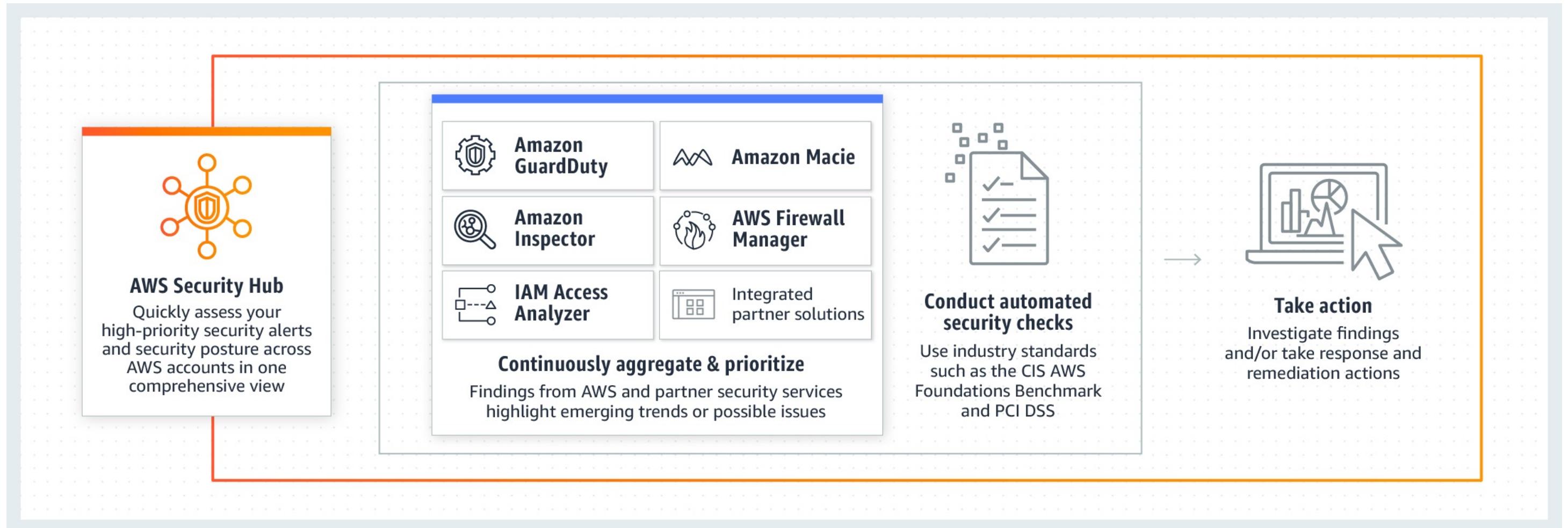
- When you use GuardDuty with an AWS Organizations organization, you can designate any account within the organization to be the GuardDuty delegated administrator.
- This admin can enable and manage GuardDuty for all accounts in the organization **within that Region**.

AWS Security Hub

Logging & Monitoring



AWS Security Hub - Overview



AWS Security Hub - Benefits



Compliance
standards

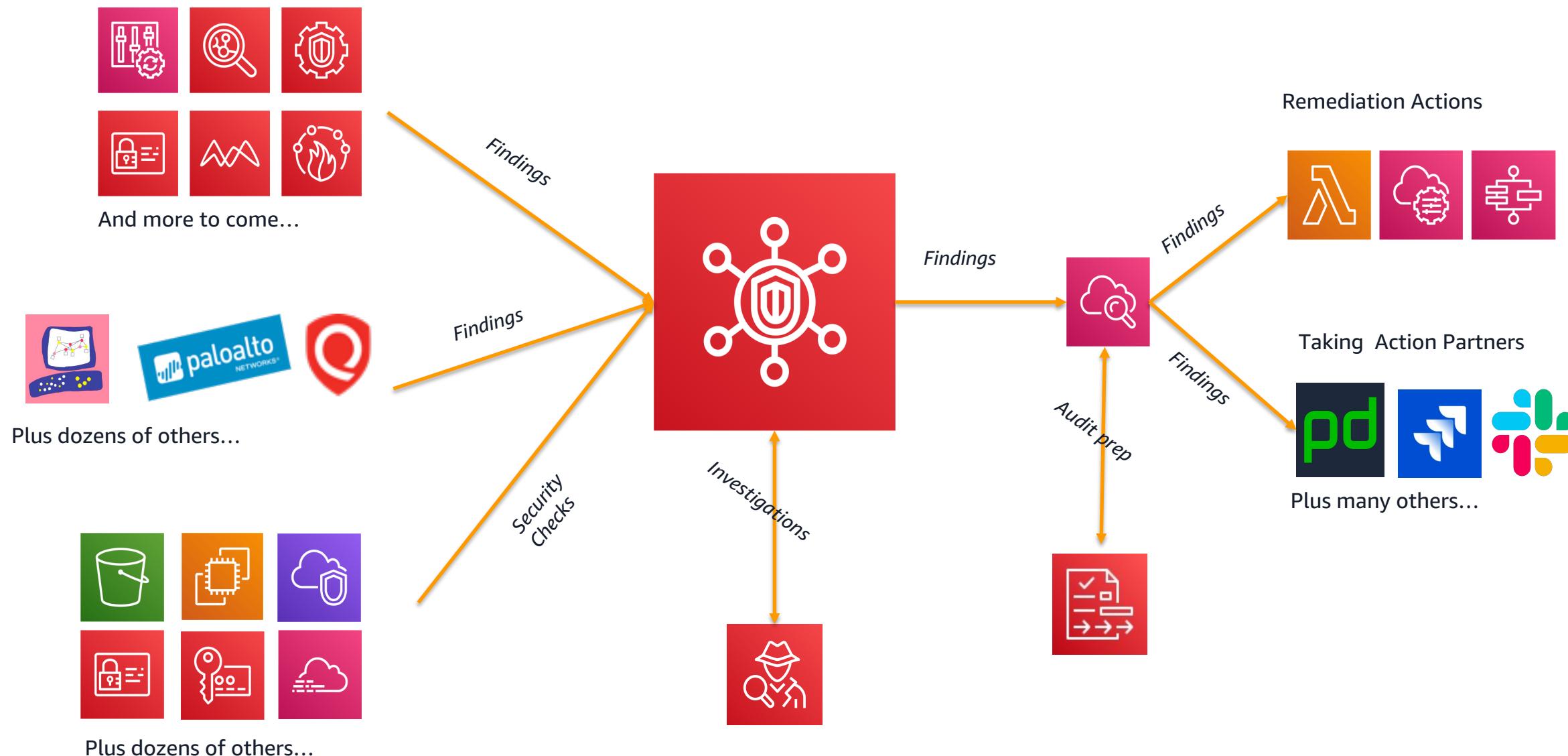


Aggregated
findings across
accounts & regions



Insights

AWS Security Hub – Information Flows



AWS Security Hub - Compliance Standards

Three standards currently available:

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



AWS Security Hub - Compliance Standards

Security Hub > Compliance standards > CIS AWS Foundations rules

CIS AWS Foundations rules		
AWS Security Hub conducts 43 automated checks against the CIS AWS Foundations Benchmark rules.		
<input type="text"/> Filter rules < 1 2 3 >		
1.1 Avoid the use of the "root" account <input checked="" type="radio"/> Non-compliant 1 account failed	1.2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password <input checked="" type="radio"/> Compliant 1 account passed	1.3 Ensure credentials unused for 90 days or greater are disabled <input checked="" type="radio"/> Compliant 1 account passed
1.4 Ensure access keys are rotated every 90 days or less <input checked="" type="radio"/> Compliant 1 account passed	1.5 Ensure IAM password policy requires at least one uppercase letter <input checked="" type="radio"/> Compliant 1 account passed	1.6 Ensure IAM password policy requires at least one lowercase letter <input checked="" type="radio"/> Compliant 1 account passed
1.7 Ensure IAM password policy requires at least one symbol <input checked="" type="radio"/> Compliant 1 account passed	1.8 Ensure IAM password policy requires at least one number <input checked="" type="radio"/> Compliant 1 account passed	1.9 Ensure IAM password policy requires minimum password length of 14 or greater <input checked="" type="radio"/> Compliant 1 account passed
1.10 Ensure IAM password policy prevents password reuse <input checked="" type="radio"/> Non-compliant 1 account failed	1.11 Ensure IAM password policy expires passwords within 90 days or less <input checked="" type="radio"/> Compliant 1 account passed	1.12 Ensure no root account access key exists <input checked="" type="radio"/> Compliant 1 account passed
1.13 Ensure MFA is enabled for the "root" account <input checked="" type="radio"/> Non-compliant 1 account failed	1.14 Ensure hardware MFA is enabled for the "root" account <input checked="" type="radio"/> Non-compliant 1 account failed	1.16 Ensure IAM policies are attached only to groups or roles <input checked="" type="radio"/> Compliant 1 account passed
1.22 Ensure IAM policies that allow full ":" administrative privileges are not created <input checked="" type="radio"/> Compliant 1 account passed	2.1 Ensure CloudTrail is enabled in all regions <input checked="" type="radio"/> Compliant 1 account passed	2.2 Ensure CloudTrail log file validation is enabled <input checked="" type="radio"/> Compliant 1 CloudTrail trail passed

AWS Security Hub - Compliance Standards

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

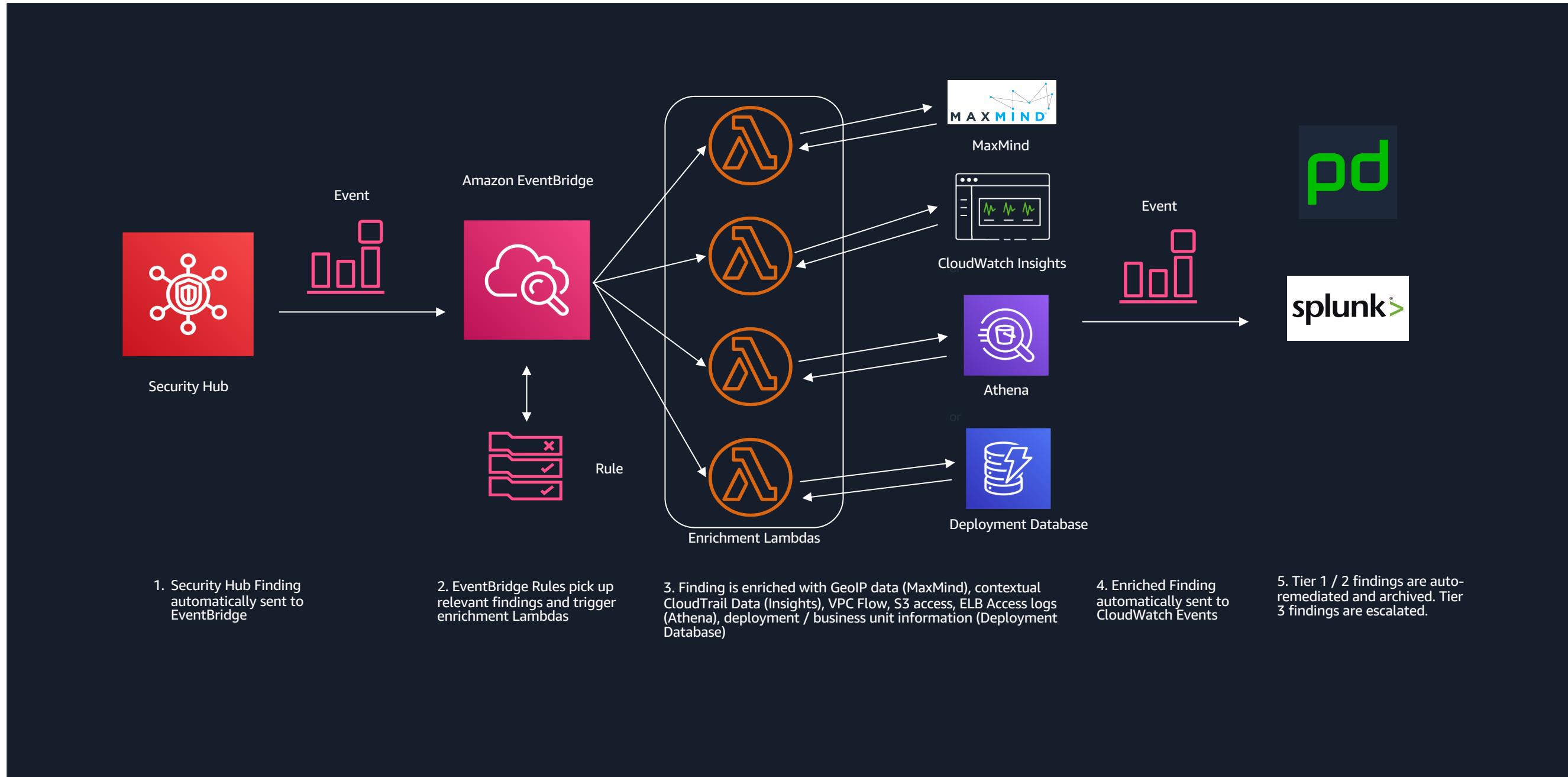
Security Hub > Compliance standards > CIS AWS Foundations rules > 1.1 Avoid the use of the "root" account

The screenshot shows the AWS Security Hub interface. On the left, a list view displays a single finding titled '1.1 Avoid the use of the "root" account'. The finding is categorized under 'CIS AWS Foundations rules' and has a status of 'FAILED'. On the right, a detailed view of the same finding is shown. The finding ID is arn:aws:securityhub:eu-west-3:068873283051:subscription/cis-aws-foundations-benchmark/v/1.2.0/1.1/finding/5481801a-8742-4337-8353-d12bede379fa. The description states: 'The "root" account has unrestricted access to all resources in the AWS account. It is highly recommended that the use of this account be avoided.' The finding details include:

- AWS account ID:** 068873283051
- Severity (Original):** 2
- Severity (Normalized):** 20
- Compliance status:** FAILED
- Created at:** 2019-05-13T16:03:15.915Z
- Updated at:** 2019-05-15T04:19:15.893Z
- Severity label:** LOW
- Product name:** Security Hub
- Company name:** AWS
- Resource type:** AwsAccount
- Resource ID:** AWS::::Account:068873283051
- Resource region:** eu-west-3

Below the finding details, there is a section for 'Types and Related Findings' which lists 'Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark'. There is also a 'Remediation' section with a link to the AWS Security Hub CIS documentation.

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

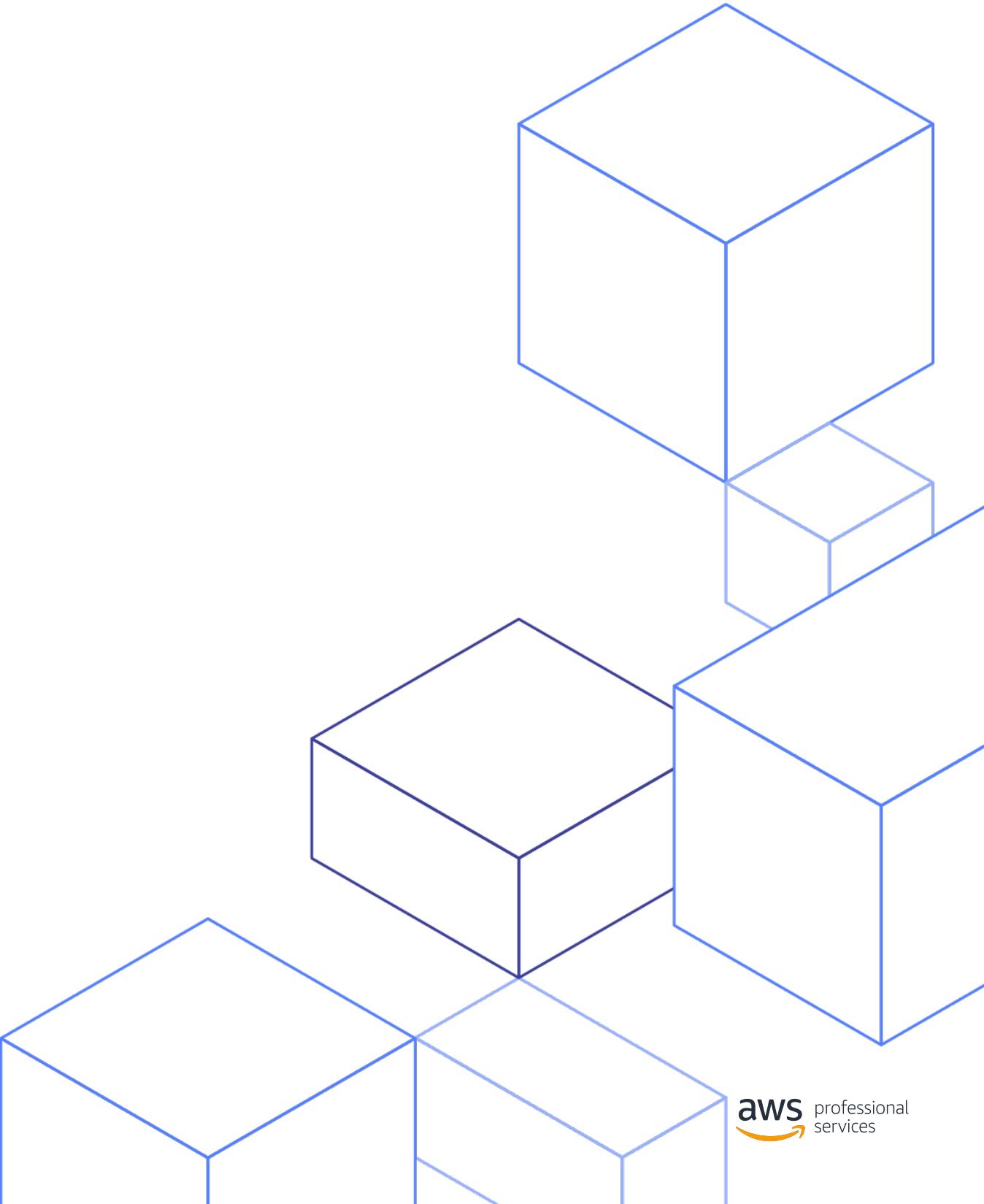
<https://aws.amazon.com/blogs/security/nine-aws-security-hub-best-practices/>

AWS Security Hub – Key Takeaways

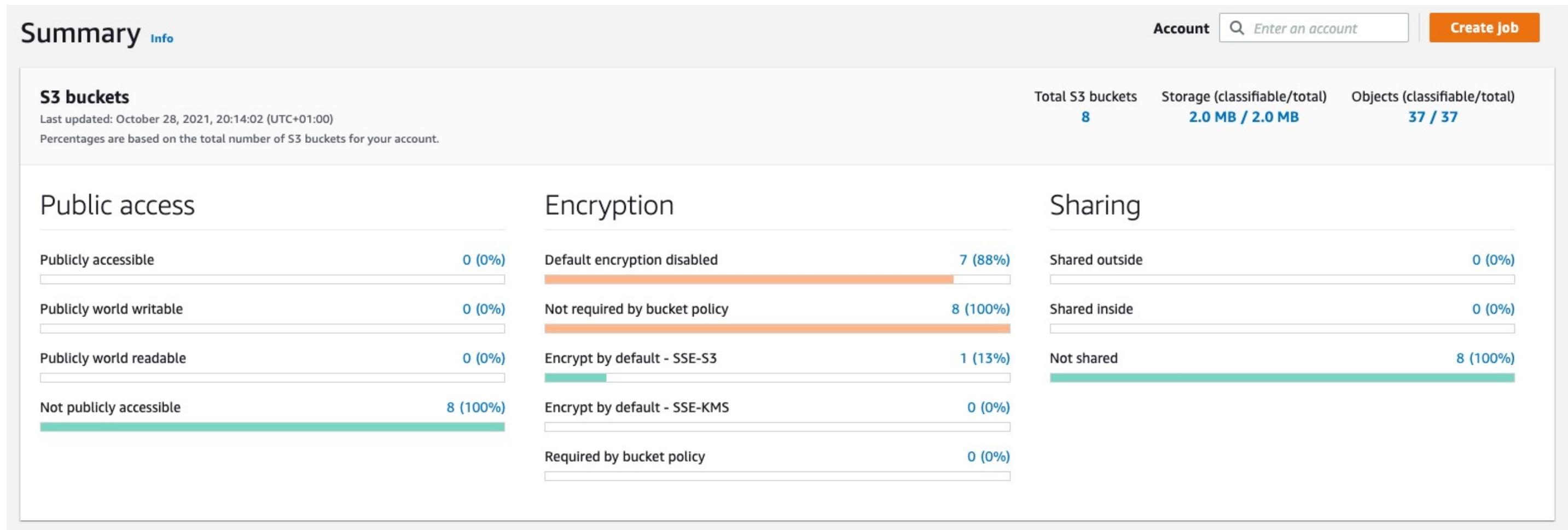
- Automatically evaluate your compliance against key standards with one-click, frictionless enablement
- Centralize all of your findings without the need to parse and normalize via the AWS Security Findings Format
- Prioritize findings using insights for efficient response and remediation
- Take actions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

Amazon Macie

Logging & Monitoring



Amazon Macie - Dashboard



Amazon Macie – PII Monitoring

Findings (10) [Info](#)

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](#) [Actions ▾](#)

Saved rules [No saved rules](#)

Current [▼](#) [Add filter criteria](#)

	Finding type	Resources affected	Updated
<input type="checkbox"/>	High [SAMPLE] SensitiveData:S3...	macie-sample-finding-bucket/credentials.json	seconds ago
<input type="checkbox"/>	Medium [SAMPLE] Policy:IAMUser...uc...	macie-sample-finding-bucket	seconds ago
<input type="checkbox"/>	High [SAMPLE] SensitiveData:S3O...	macie-sample-finding-bucket/excel_spreadsheet.xlsx	seconds ago
<input type="checkbox"/>	High [SAMPLE] Policy:IAMUser/S3...	macie-sample-finding-bucket	seconds ago
<input type="checkbox"/>	High [SAMPLE] Policy:IAMUser...oc...	macie-sample-finding-bucket	seconds ago
<input type="checkbox"/>	High [SAMPLE] SensitiveData:S3O...	macie-sample-finding-bucket/financial.txt	seconds ago
<input type="checkbox"/>	High [SAMPLE] Policy:IAMUser...ke...	macie-sample-finding-bucket	seconds ago
<input type="checkbox"/>	High [SAMPLE] SensitiveData:S3O...	macie-sample-finding-bucket/employeeInfo.csv	seconds ago
<input type="checkbox"/>	Low [SAMPLE] SensitiveData:S3O...	macie-sample-finding-bucket/personal.pdf	seconds ago
<input type="checkbox"/>	High [SAMPLE] Policy:IAMUser/S3...	macie-sample-finding-bucket	seconds ago

SensitiveData:S3Object/Credentials [⊕](#) [⊖](#) [X](#)

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

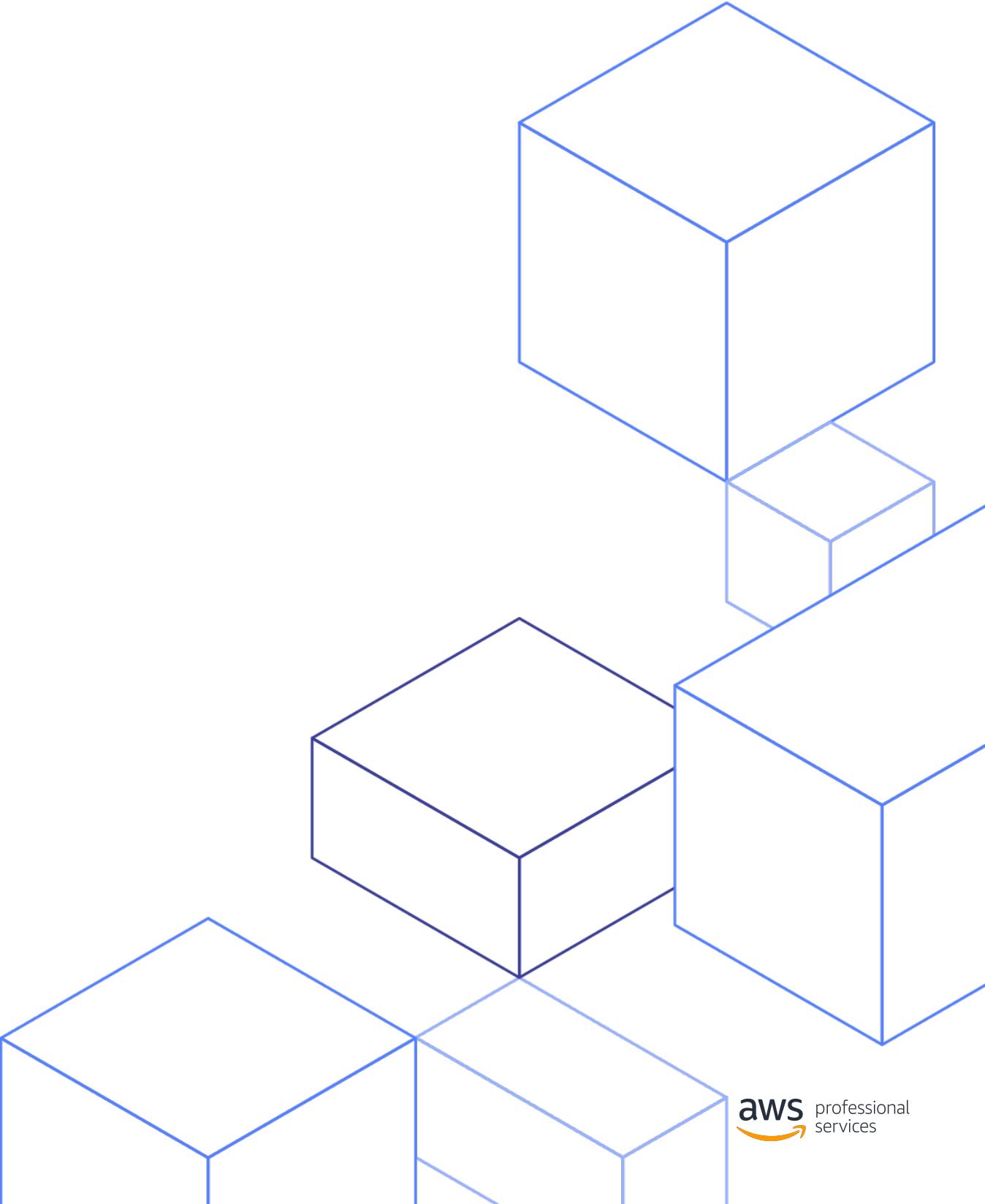
Aws credentials	1	⊕ ⊖
Occurrences of aws credentials	1 record	

Details

Status	COMPLETE	⊕ ⊖
Size classified	9 KB	
MIME type	application/json	
Detailed result location	s3://sample-macie-results-bucket/AWSLogs/292077323914/	

Auditing your AWS Environment

Logging & Monitoring



Auditing – IAM Credential Report

Dashboard

Details

Groups

Users

Roles

Identity Providers

Password Policy

Credential Report

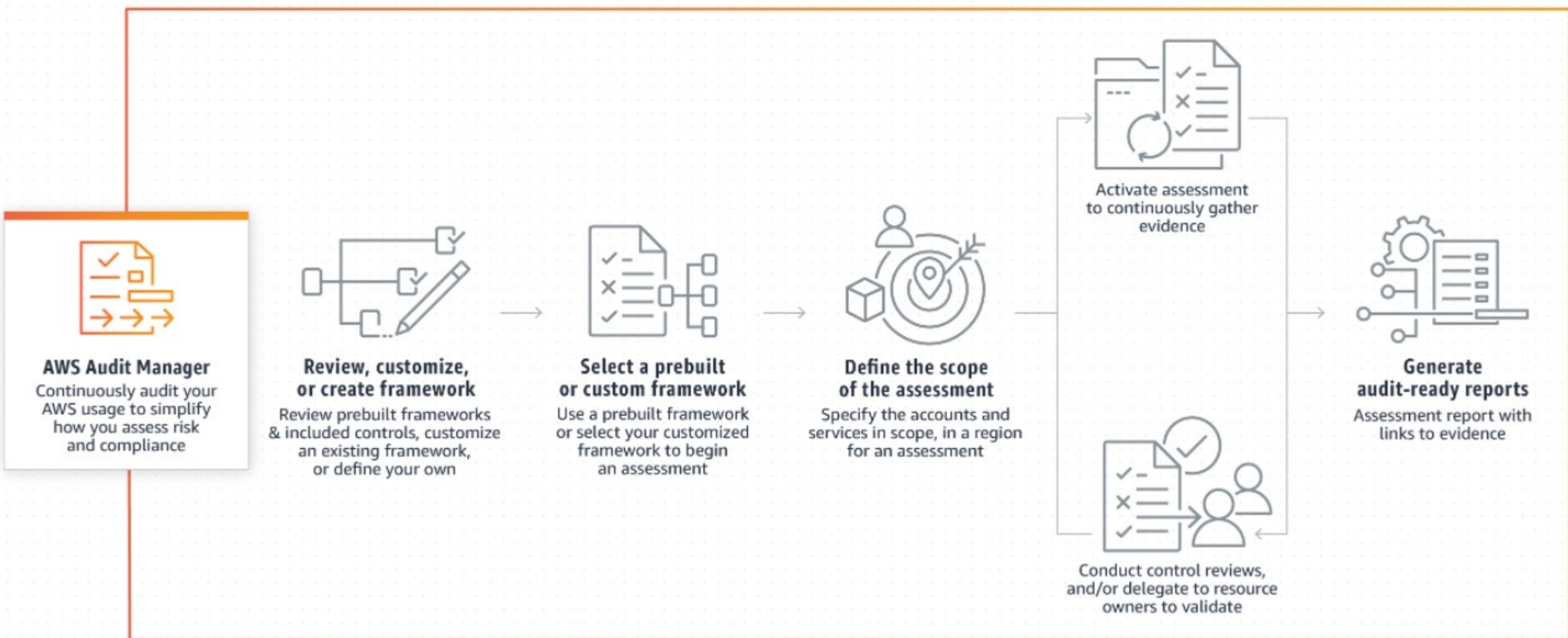
Credential Report

Click the button to download a report that lists all your account's users and the status of their various credentials. After a report is created, it is stored for up to four hours. For more information see the [documentation](#).

Download Report

user	arn	user_creation_date	password_status	password_last_used	password_expires	password_enabled	mfa_active
<root_account>	arn:aws:iam::123456789012:root	2014-06-01T00:00:00Z	not_supported	2014-11-05T23:02:18+00:00	2014-11-05T23:02:18+00:00	not_supported	TRUE
	arn:aws:iam::123456789012:root	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-15T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-08-14T00:00:00Z	TRUE	no_information	2014-08-14T00:00:00Z	2014-10-01T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-06-10T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-15T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-15T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-15T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-10-15T00:00:00Z	TRUE	2014-10-22T17:27:25+00:00	2014-10-15T00:00:00Z	2014-12-01T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-15T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-15T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-09-15T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-15T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-15T00:00:00Z	2014-10-31T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-06-10T00:00:00Z	TRUE	no_information	2014-10-01T00:00:00Z	2014-11-28T00:00:00Z	TRUE
	arn:aws:iam::123456789012:root	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-15T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-15T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-15T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-06-10T00:00:00Z	TRUE	2014-11-05T23:20:03+00:00	2014-11-05T23:20:03+00:00	2014-12-21T00:00:00Z	FALSE
	arn:aws:iam::123456789012:root	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-15T00:00:00Z	FALSE

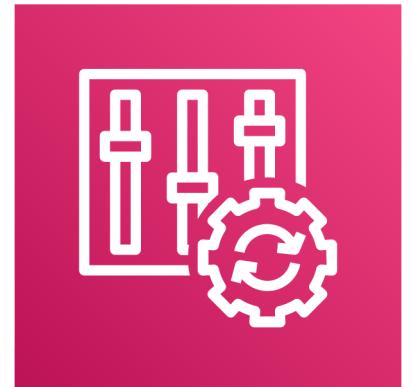
AWS Audit Manager



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

The screenshot shows the AWS Config Dashboard. On the left, a sidebar menu includes options like Dashboard, Conformance packs, Rules, Resources, Aggregators, Settings, and links to What's new, Documentation, Partners, FAQs, Pricing, and Share feedback. The main content area has a breadcrumb navigation bar: AWS Config > Dashboard. The dashboard features three main sections: Resource inventory, Compliance status, and Noncompliant rules by noncompliant resource count.

Resource inventory: Shows a total of 425 resources. A dropdown menu is set to "All resources". The table below lists resource types and their counts:

Type	Count
Config ResourceCompliance	182
IAM Role	74
IAM Policy	41
KMS Key	18
EC2 SecurityGroup	15
EC2 NetworkInterface	13
S3 Bucket	11
EC2 Subnet	6
ShieldRegional Protection	5
CloudWatch Alarm	5

Compliance status: Displays the following counts:

Rules	Resources
⚠️ 55 Noncompliant rule(s)	⚠️ 53 Noncompliant resource(s)
✅ 32 Compliant rule(s)	✅ 100+ Compliant resource(s)

Noncompliant rules by noncompliant resource count: A table listing rules and their associated noncompliant resources:

Name	Compliance
securityhub-s3-bucket-replication-enabled-e6f2836a	⚠️ 11 Noncompliant resource(s)
securityhub-s3-bucket-logging-enabled-i4rmhp	⚠️ 11 Noncompliant resource(s)
securityhub-s3-bucket-ssl-requests-only-e7ce9d0a	⚠️ 10 Noncompliant resource(s)
securityhub-s3-bucket-server-side-encryption-enabled-d9876c86	⚠️ 9 Noncompliant resource(s)
securityhub-s3-bucket-level-public-access-prohibited-a697af8	⚠️ 9 Noncompliant resource(s)

[View all noncompliant rules](#)

Auditing – AWS Config

AWS Config > Resources > sg-[REDACTED] > Timeline

Timeline

General details

Resource ID	sg-[REDACTED]	Resource type	AWS::EC2::SecurityGroup	Resource name	eksctl-koen-cluster-cluster-ControlPlaneSecurityGroup-[REDACTED]
-------------	---------------	---------------	-------------------------	---------------	--

Events
All times are in Europe/Berlin (UTC+02:00)

	Start date	Event type
2021/10/25	Now	All event types

September 1, 2021

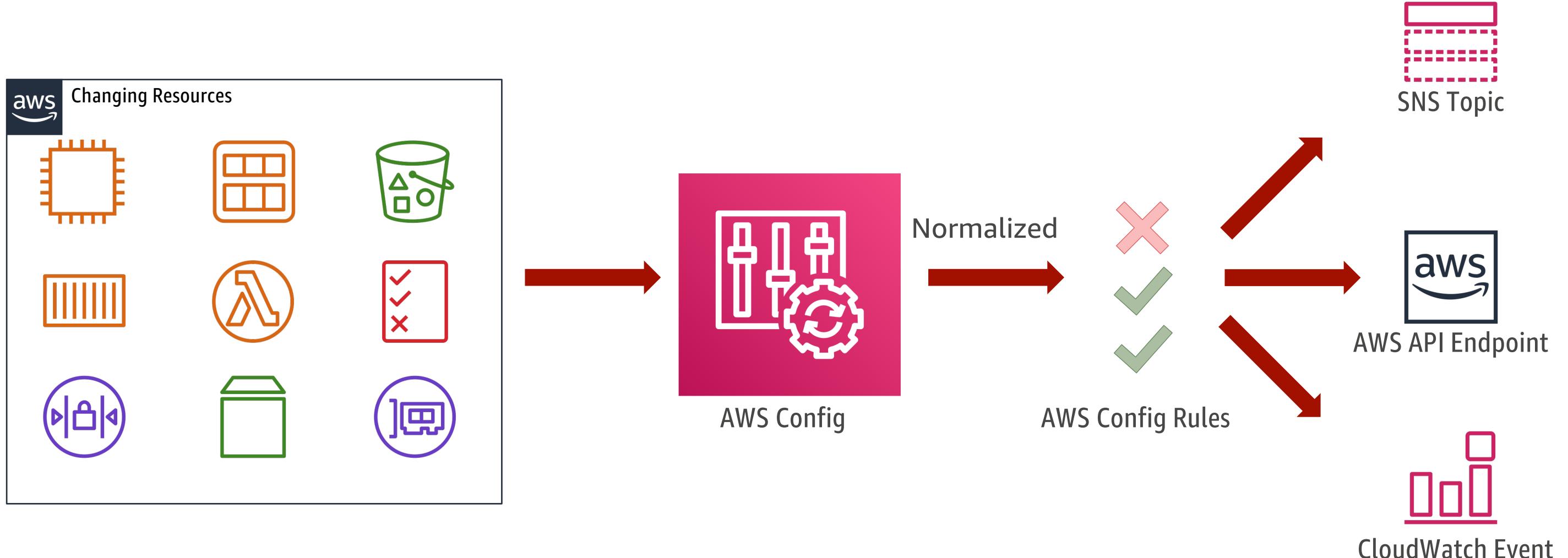
08:09:38	[+] Rule compliance	All compliant	5 rule(s) applied
06:49:22	[+] Configuration change		4 field change(s)
02:17:56	[+] Configuration change		1 field change(s)
02:17:18	[+] CloudTrail Event		
01:44:33	[+] CloudTrail Event		
01:11:43	[+] CloudTrail Event		
00:25:22	[+] Configuration change		1 field change(s)
00:23:14	[+] CloudTrail Event		

August 31, 2021

23:58:19	[+] Configuration change		1 field change(s)
23:56:13	[+] CloudTrail Event		

The screenshot shows the AWS Config Timeline interface for a specific security group. It displays a timeline of events from September 1, 2021, and August 31, 2021. The events are categorized by type: Rule compliance, Configuration change, and CloudTrail Event. The Rule compliance event on September 1st is marked as 'All compliant' and shows 5 rule(s) applied. There are multiple configuration changes and CloudTrail events throughout the period. The interface includes filters for start date (set to 2021/10/25), now, and all event types.

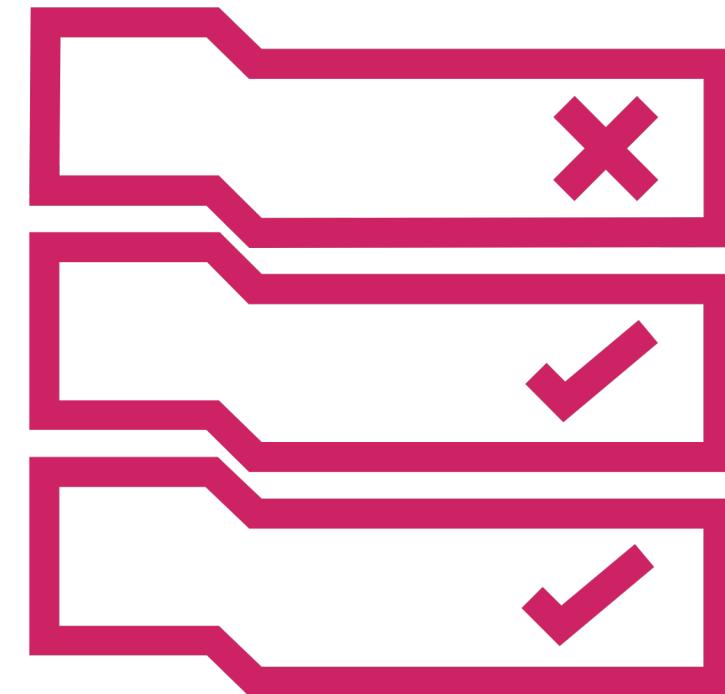
AWS Config Rules



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 Config > Rules

Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the compliance results.

Rules				
	Name	Remediation action	Type	Compliance
<input checked="" type="radio"/>	securityhub-cloud-trail-encryption-enabled-wpvyaw	Not set	AWS managed	⚠ 3 Noncompliant resource(s)
<input type="radio"/>	encrypted-volumes	Not set	AWS managed	-
<input checked="" type="radio"/>	securityhub-beanstalk-enhanced-health-reporting-enabled-9249bb2b	Not set	AWS managed	-
<input type="radio"/>	approved-amis-by-id	AWS-TerminateEC2Instance	AWS managed	-
<input checked="" type="radio"/>	securityhub-acm-certificate-expiration-check-8243709c	Not set	AWS managed	-
<input checked="" type="radio"/>	securityhub-api-gw-xray-enabled-953fe989	Not set	AWS managed	⚠ 1 Noncompliant resource(s)
<input type="radio"/>	s3-bucket-public-write-prohibited	Not set	AWS managed	✓ Compliant
<input type="radio"/>	s3-bucket-public-read-prohibited	Not set	AWS managed	✓ Compliant
<input checked="" type="radio"/>	securityhub-alb-http-drop-invalid-header-enabled-a13e32b3	Not set	AWS managed	⚠ 1 Noncompliant resource(s)
<input checked="" type="radio"/>	securityhub-aurora-mysql-backtracking-enabled-3ee12ac5	Not set	AWS managed	-

AWS Config Rules – Review Compliance (Aggregated)

Screenshot of the AWS Config Aggregators overview dashboard for Koen-Org.

Aggregator overview for Koen-Org

Data displayed in the dashboard is received from multiple aggregation sources and is refreshed at different intervals. Data might be delayed by a few minutes.

Resource inventory

Type	Resource count
Config ResourceCompliance	345
IAM Role	148
IAM Policy	82
KMS Key	30
EC2 SecurityGroup	26
EC2 NetworkInterface	16
S3 Bucket	16
CloudWatch Alarm	14
EC2 Subnet	10
ShieldRegional Protection	7

Compliance status

41.26%

Config rule compliance

⚠ 84 Noncompliant rule(s)
✓ 59 Compliant rule(s)

Top 5 noncompliant rules

Rule name	Region	Account	Compliance
securityhub-s3-bucket-replication-enabled-e6f2836a	eu-west-1	[REDACTED]	⚠ 11 Noncompliant resource(s)
securityhub-s3-bucket-logging-enabled-i4rmhp	eu-west-1	[REDACTED]	⚠ 11 Noncompliant resource(s)
securityhub-s3-bucket-ssl-requests-only-e7ce9d0a	eu-west-1	[REDACTED]	⚠ 10 Noncompliant resource(s)
securityhub-s3-bucket-level-public-access-prohibited-a697af8	eu-west-1	[REDACTED]	⚠ 9 Noncompliant resource(s)
securityhub-s3-bucket-server-side-encryption-enabled-d9876c86	eu-west-1	[REDACTED]	⚠ 9 Noncompliant resource(s)

[View all noncompliant rules](#)

Accounts by resource count

Account	Resource count
[REDACTED]	796

Accounts by noncompliant rules

Account	Compliance
[REDACTED]	⚠ 84 Noncompliant rule(s)

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

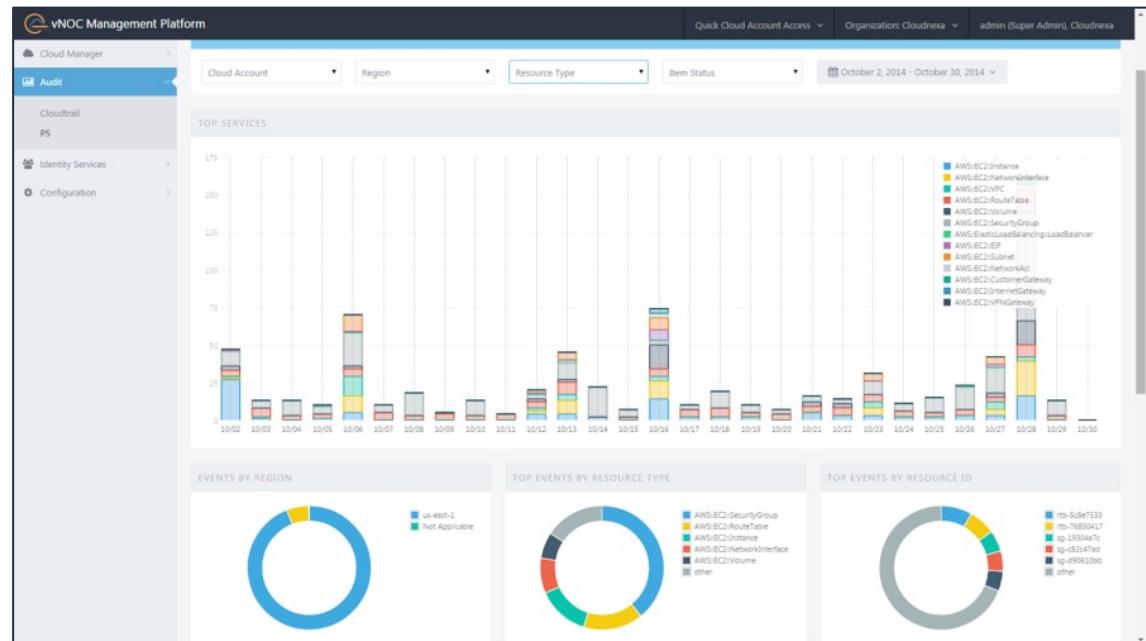
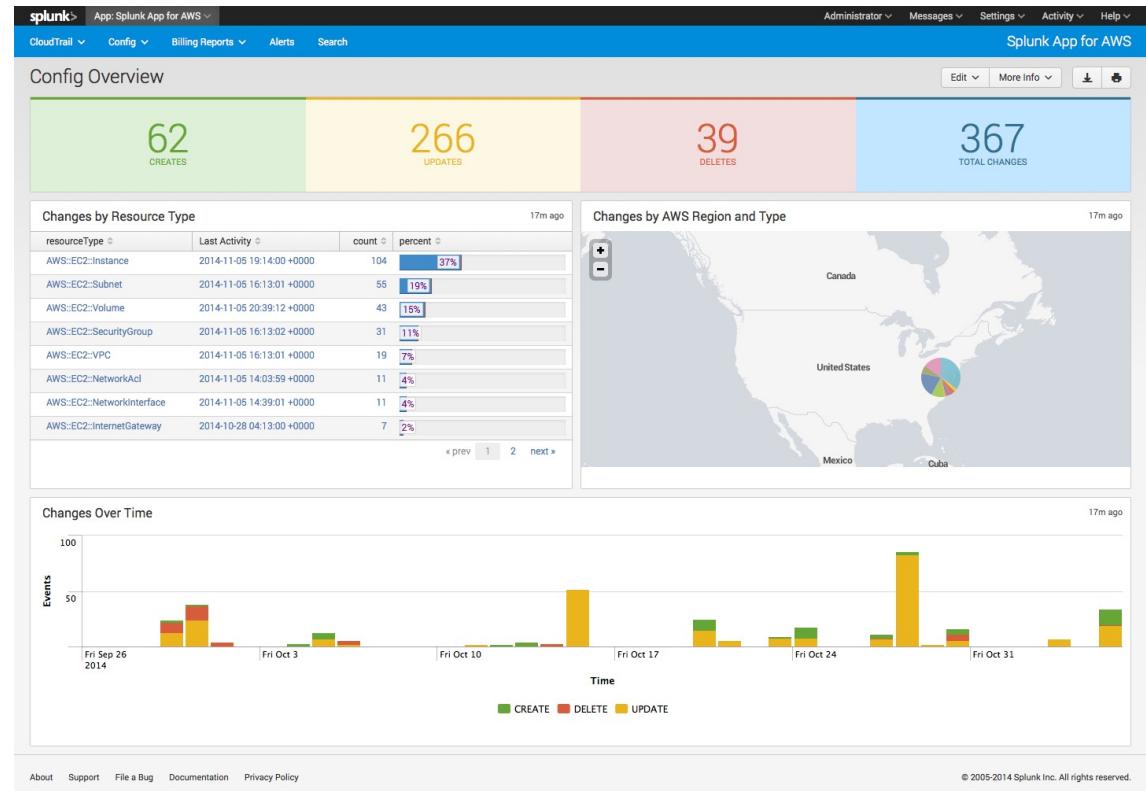
```
config.putEvaluations(putEvaluationsRequest, function (err,  
data) {  
    if (err) {  
        context.fail(err);  
    } else {  
        context.succeed(data);  
    }  
});
```

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 Config Rules Partners



ALERT LOGIC®

CloudHealth®



evident.io

 ALLGRESS™


 TREND
MICRO™

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





Questions

