Logging & Alerting

AWS Security Workshop

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

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**

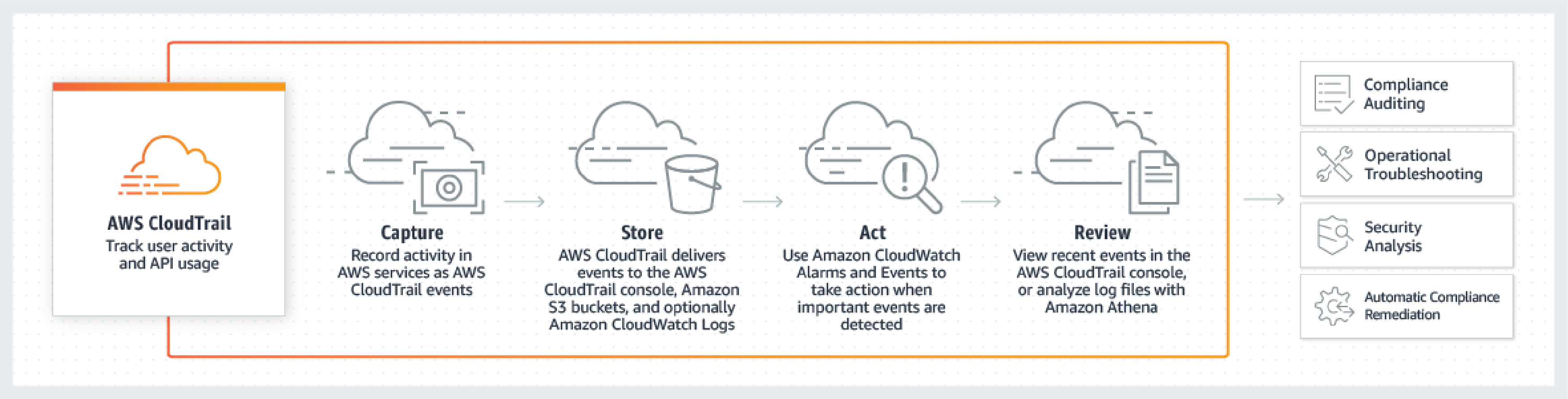
- Managed service to collect and keep your logs
- CloudWatch Logs Agent for Linux and Windows instances
- Integration with **Metrics** and **Alarms**
- Export data to S3 for analytics
- Stream to Amazon ElasticSearch Service or AWS Lambda

AWS CloudTrail

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

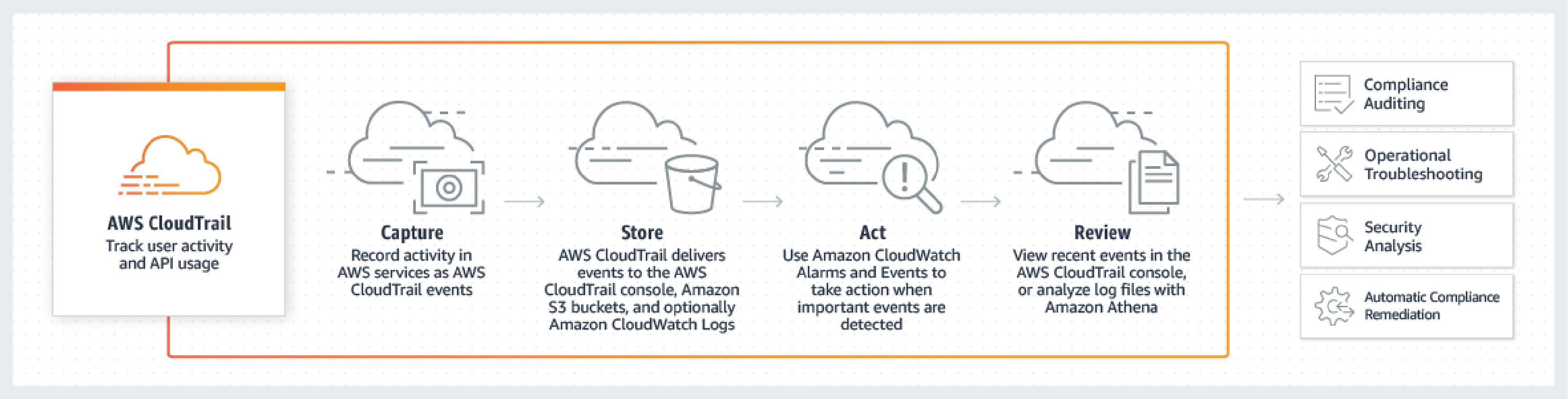


AWS CloudTrail
Track user activity and API usage
Capture
Record activity in AWS services as AWS CloudTrail events
Store
AWS CloudTrail delivers events to the AWS CloudTrail console, Amazon S3 buckets, and optionally Amazon CloudWatch Logs
Act
Use Amazon CloudWatch Alarms and Events to take action when important events are detected
Review
View recent events in the AWS CloudTrail console, or analyze log files with Amazon Athena
Compliance Auditing
Operational Troubleshooting
Security Analysis
Automatic Compliance Remediation

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

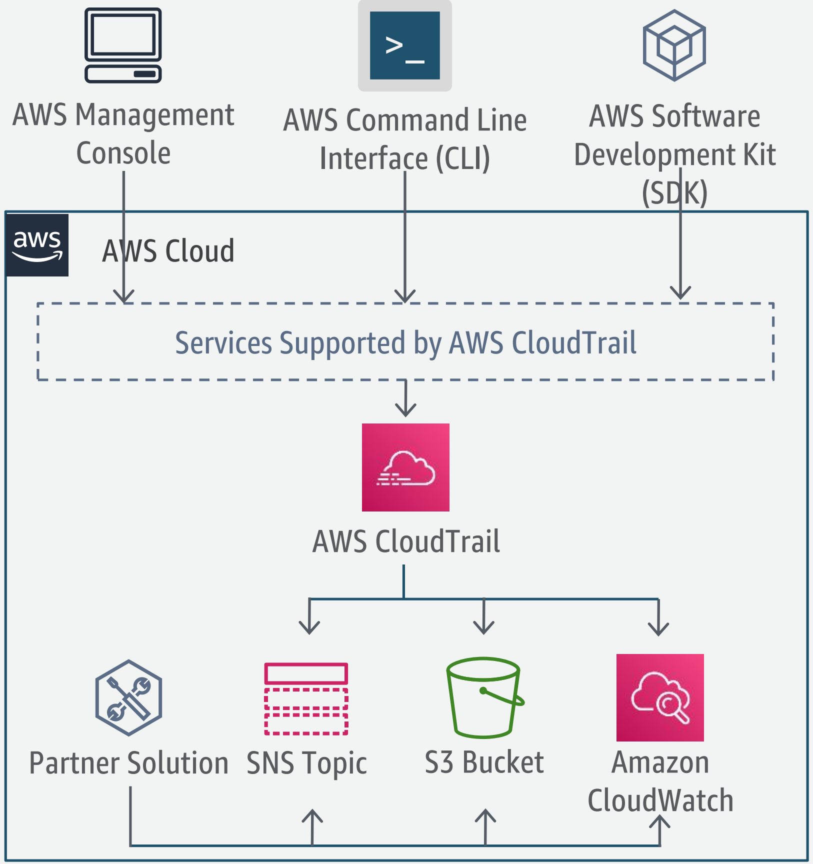

AWS CloudTrail
Track user activity and API usage
Capture
Record activity in AWS services as AWS CloudTrail events
Store
AWS CloudTrail delivers events to the AWS CloudTrail console, Amazon S3 buckets, and optionally Amazon CloudWatch Logs
Act
Use Amazon CloudWatch Alarms and Events to take action when important events are detected
Review
View recent events in the AWS CloudTrail console, or analyze log files with Amazon Athena
Compliance Auditing
Operational Troubleshooting
Security Analysis
Automatic Compliance Remediation

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, ElasticSearch, 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

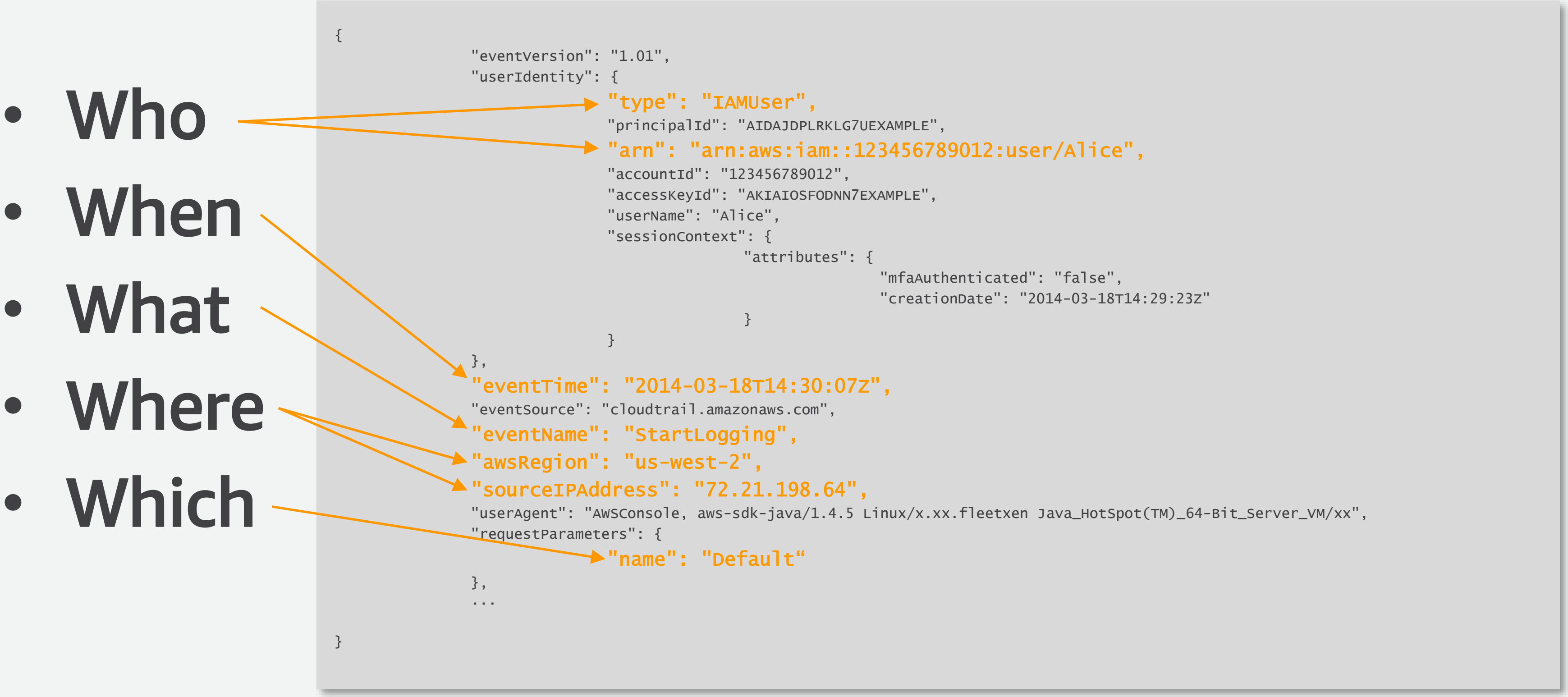
- CloudTrail records API calls in your account and delivers a log file to your S3 bucket.
- Typically, delivers an event within 15 minutes of the API call.
- Log files are delivered approximately every 5 minutes.
- Multiple partners offer integrated solutions to analyze log files.


AWS Management Console
AWS Command Line Interface (CLI)
AWS Software Development Kit (SDK)
AWS Cloud
Services Supported by AWS CloudTrail
AWS CloudTrail
Partner Solution
SNS Topic
S3 Bucket
Amazon CloudWatch

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

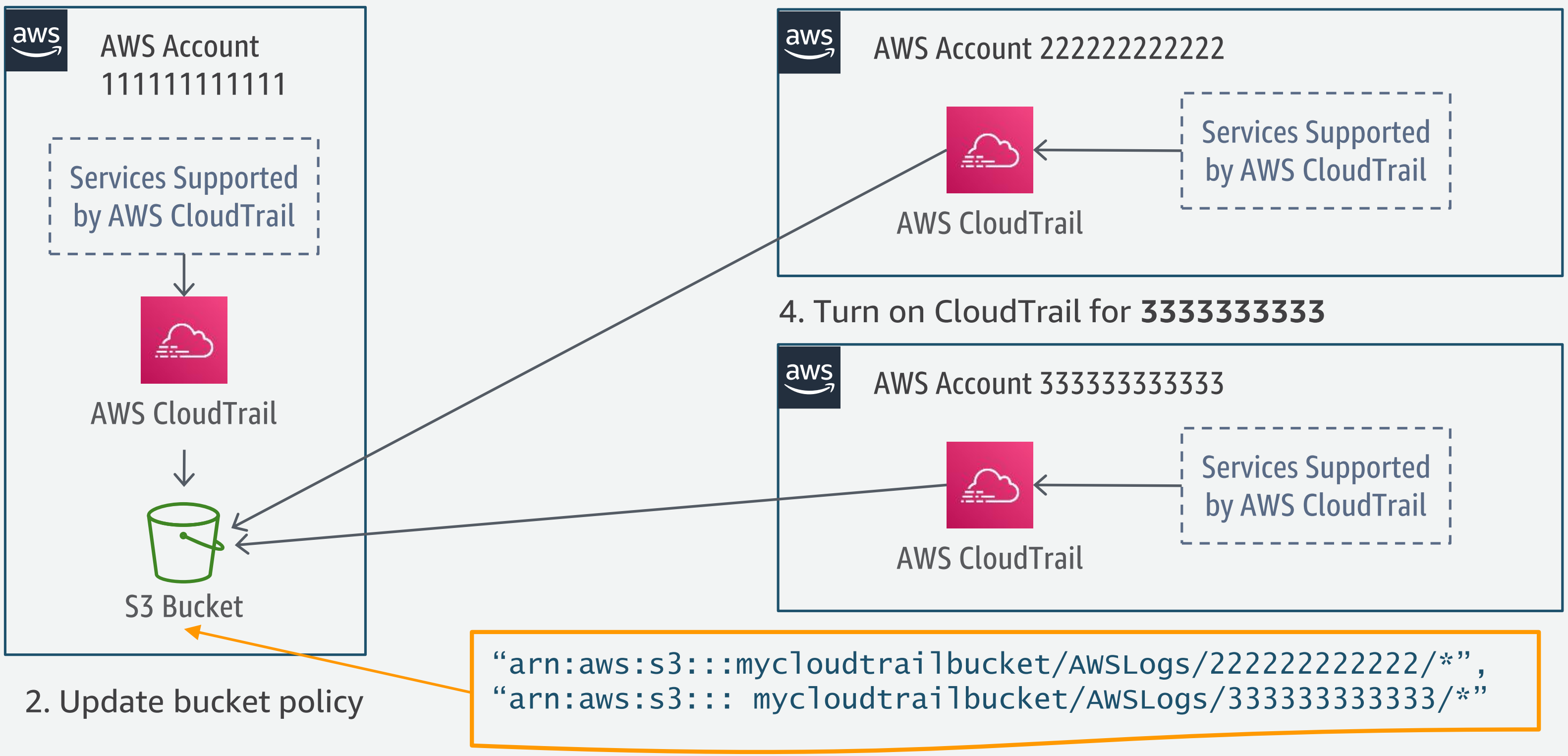
- Many-to-one centralization
    - From multiple regions into one S3 bucket (described before)
    - From multiple accounts into one account’s S3 bucket

AWS CloudTrail – Centralizing Logs

1. Turn on CloudTrail for **111111111111**

3. Turn on CloudTrail for **222222222222**

4. Turn on CloudTrail for **3333333333**



AWS Account 111111111111

Services Supported by AWS CloudTrail

AWS CloudTrail

S3 Bucket

AWS Account 222222222222

AWS CloudTrail

Services Supported by AWS CloudTrail

AWS Account 333333333333

AWS CloudTrail

Services Supported by AWS CloudTrail

2. Update bucket policy

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

AWS CloudTrail – Centralizing Logs

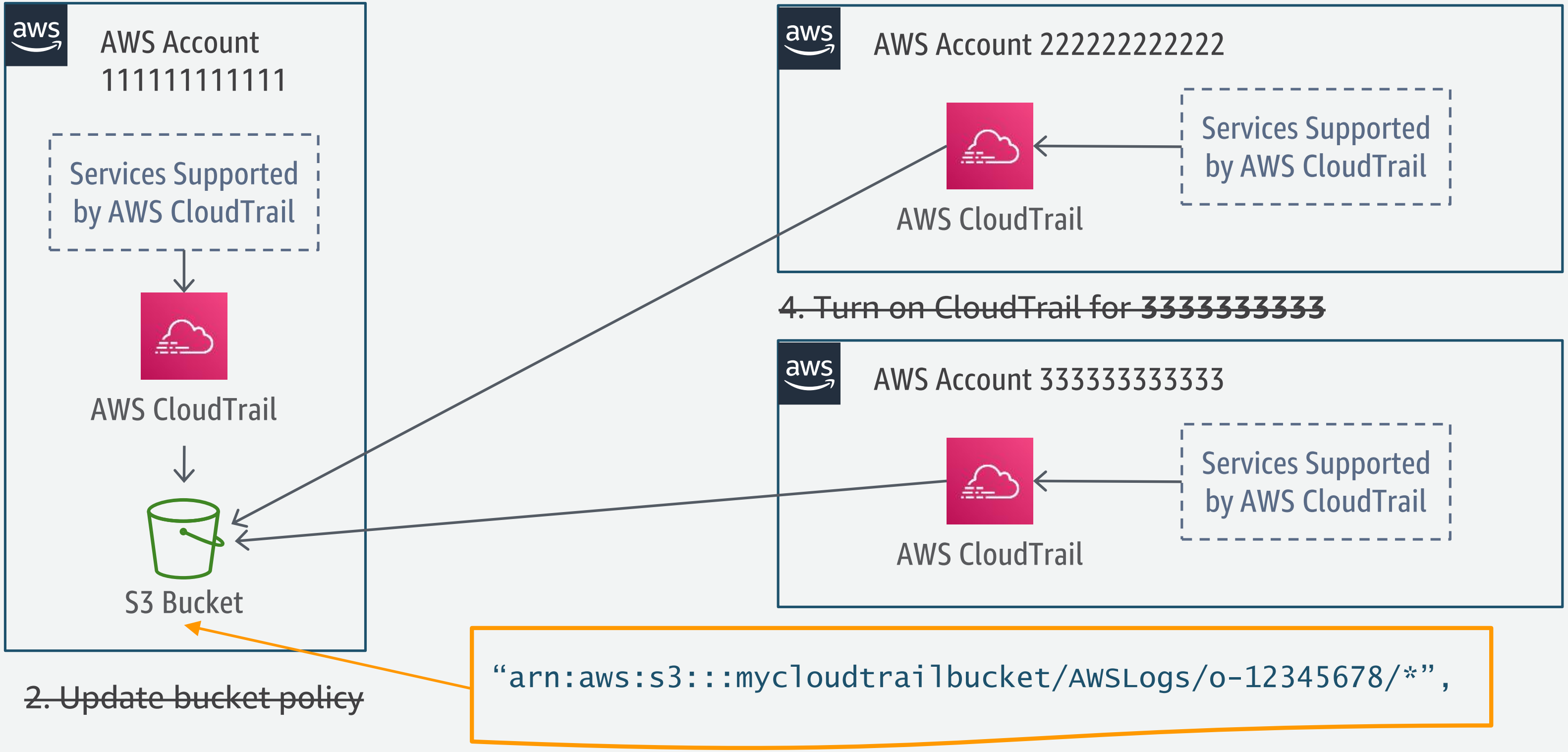
- Centralization within your AWS Organization
  - Enable CloudTrail once in the Master account and have it applied to all AWS accounts
  - log prefix changes from “/AWSLogs/<accountID>/” to “/AWSLogs/<OrganizationID>/” – no more updating of the bucket policy

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**~~

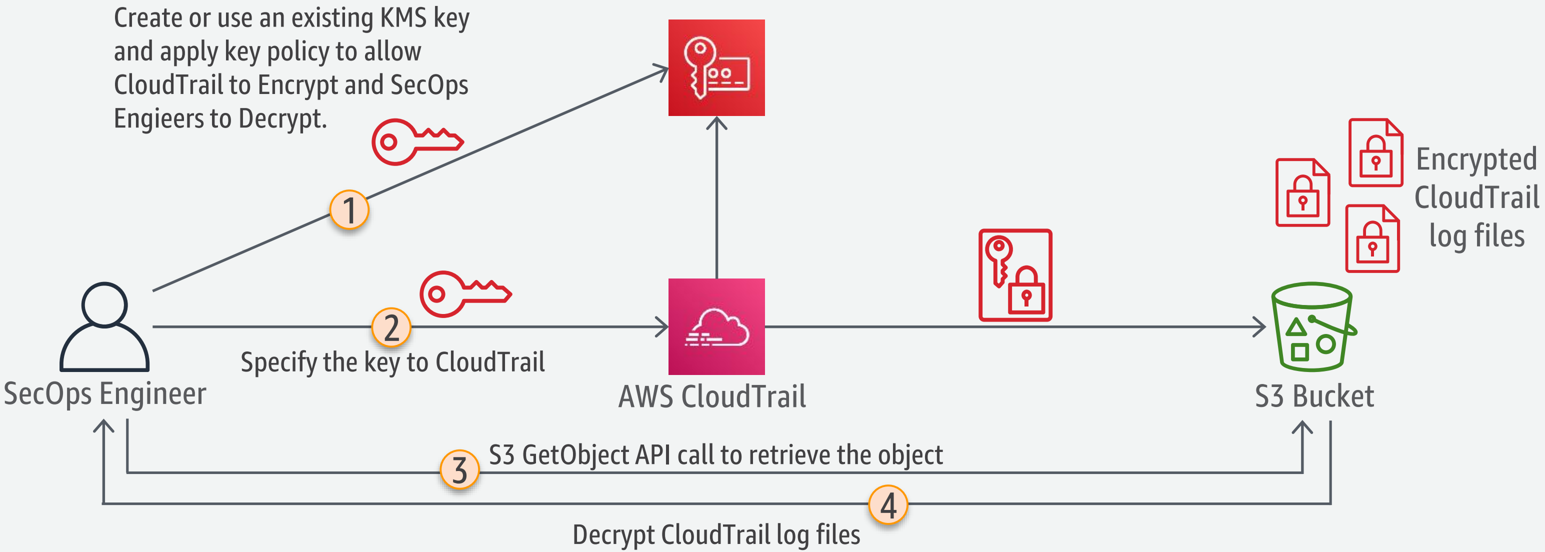


~~4. Turn on CloudTrail for **3333333333**~~

~~2. Update bucket policy~~

```
“arn:aws:s3:::mycloudtrailbucket/AWSLogs/o-12345678/*”,
```

AWS CloudTrail – KMS Encryption



Create or use an existing KMS key and apply key policy to allow CloudTrail to Encrypt and SecOps Engieers to Decrypt.

1

2

Specify the key to CloudTrail

SecOps Engineer

AWS CloudTrail

S3 Bucket

Encrypted CloudTrail log files

3

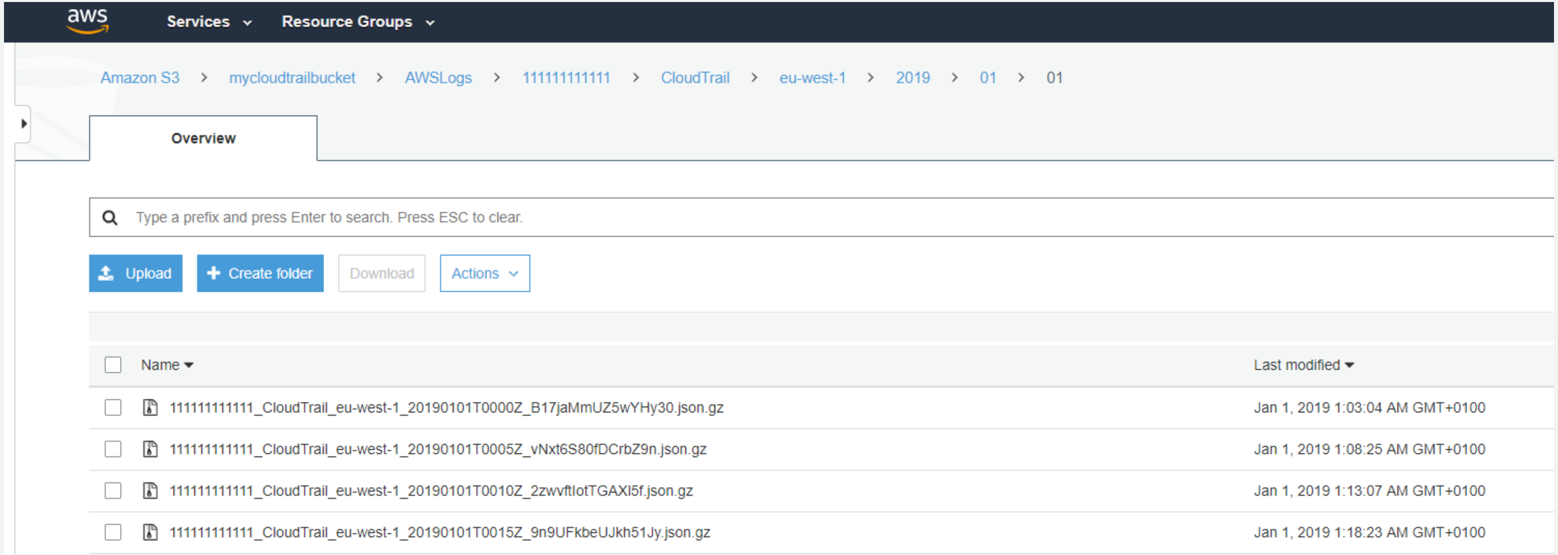
S3 GetObject API call to retrieve the object

4

Decrypt CloudTrail log files

AWS CloudTrail – Storage in S3

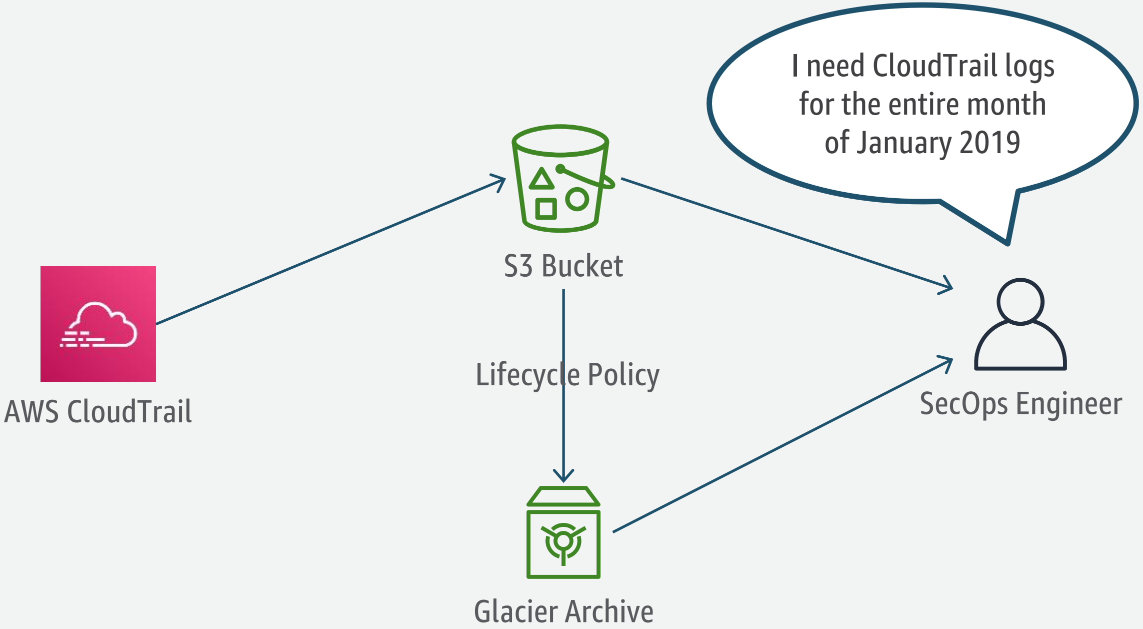
- Default descriptive folder structure makes it easier to store log files from multiple accounts and regions in the same S3 bucket.
- Detailed log file name helps identify the contents of the log file
- Unique identifier in the file name prevents overwriting log files.



Amazon S3 > mycloudtrailbucket > AWSLogs > 111111111111 > CloudTrail > eu-west-1 > 2019 > 01 > 01

	Name	Last modified
□	111111111111_CloudTrail_eu-west-1_20190101T0000Z_B17jaMmUZ5wYHy30.json.gz	Jan 1, 2019 1:03:04 AM GMT+0100
□	111111111111_CloudTrail_eu-west-1_20190101T0005Z_vNxt6S80fDCrbZ9n.json.gz	Jan 1, 2019 1:08:25 AM GMT+0100
□	111111111111_CloudTrail_eu-west-1_20190101T0010Z_2zwvftIotTGAXI5f.json.gz	Jan 1, 2019 1:13:07 AM GMT+0100
□	111111111111_CloudTrail_eu-west-1_20190101T0015Z_9n9UFkbeUJkh51Jy.json.gz	Jan 1, 2019 1:18:23 AM GMT+0100

AWS CloudTrail – Lifecycle Management

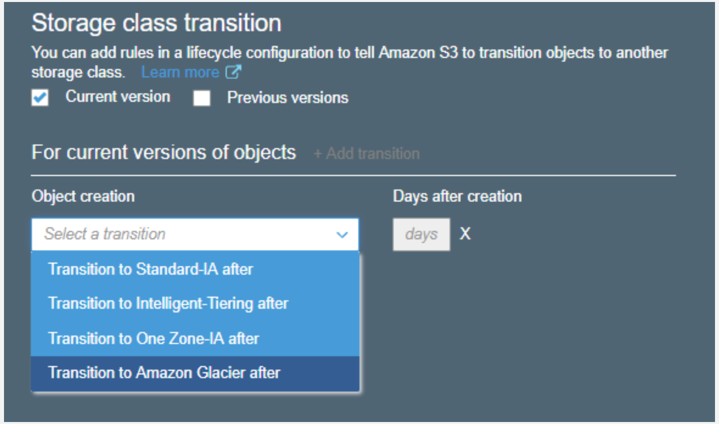


AWS CloudTrail – Lifecycle Management

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

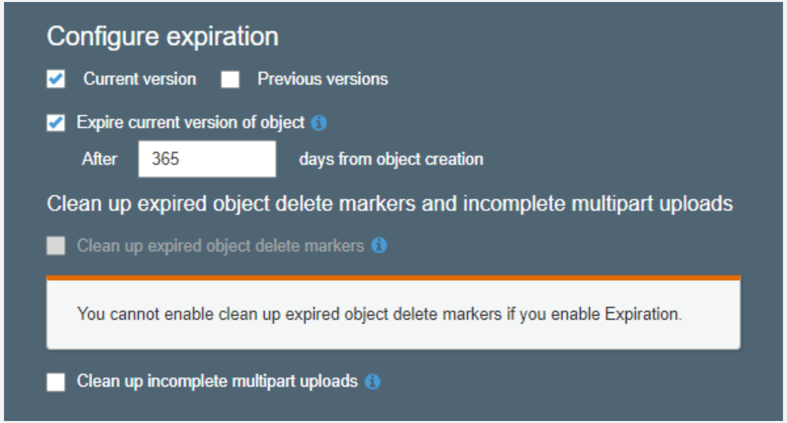
☑ Current version □ Previous versions

For current versions of objects + Add transition

Object creation: Select a transition

Days after creation: 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

After 365 days from object creation

Clean up expired object delete markers and incomplete multipart uploads

□ Clean up expired object delete markers

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

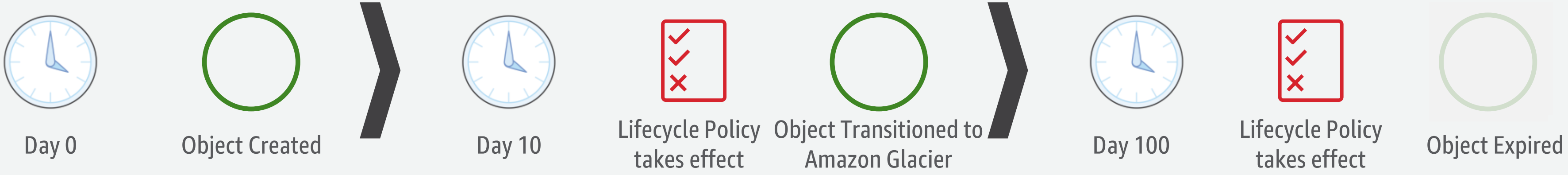
□ Clean up incomplete multipart uploads

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.



Day 0

Object Created

Day 10

Lifecycle Policy takes effect

Object Transitioned to Amazon Glacier

Day 100

Lifecycle Policy takes effect

Object Expired

- 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 – Best Practices

1. **Enable in all regions**

Benefits

- Also tracks unused regions
- Can be done in single configuration step

AWS CloudTrail – Best Practices

1. Enable in all regions
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
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
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
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
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

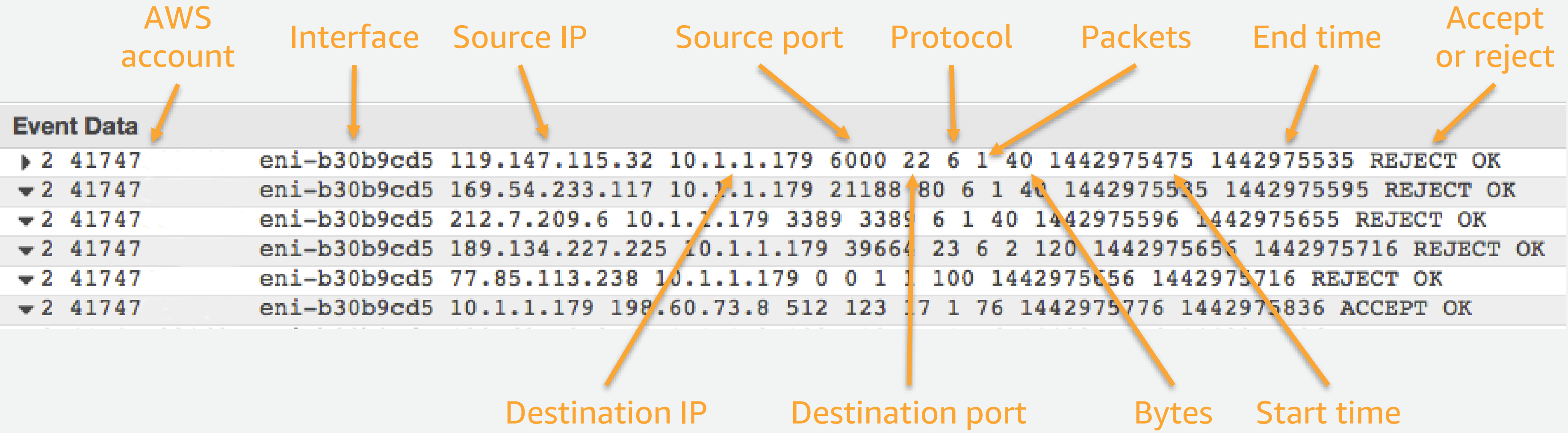
Amazon VPC Flow Logs

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

```
▸ 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
```

Processing Logs

Processing Logs

CloudWatch Logs

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

Amazon Elasticsearch Service Integration (or ELK stack)

- Analytics and Kibana interface

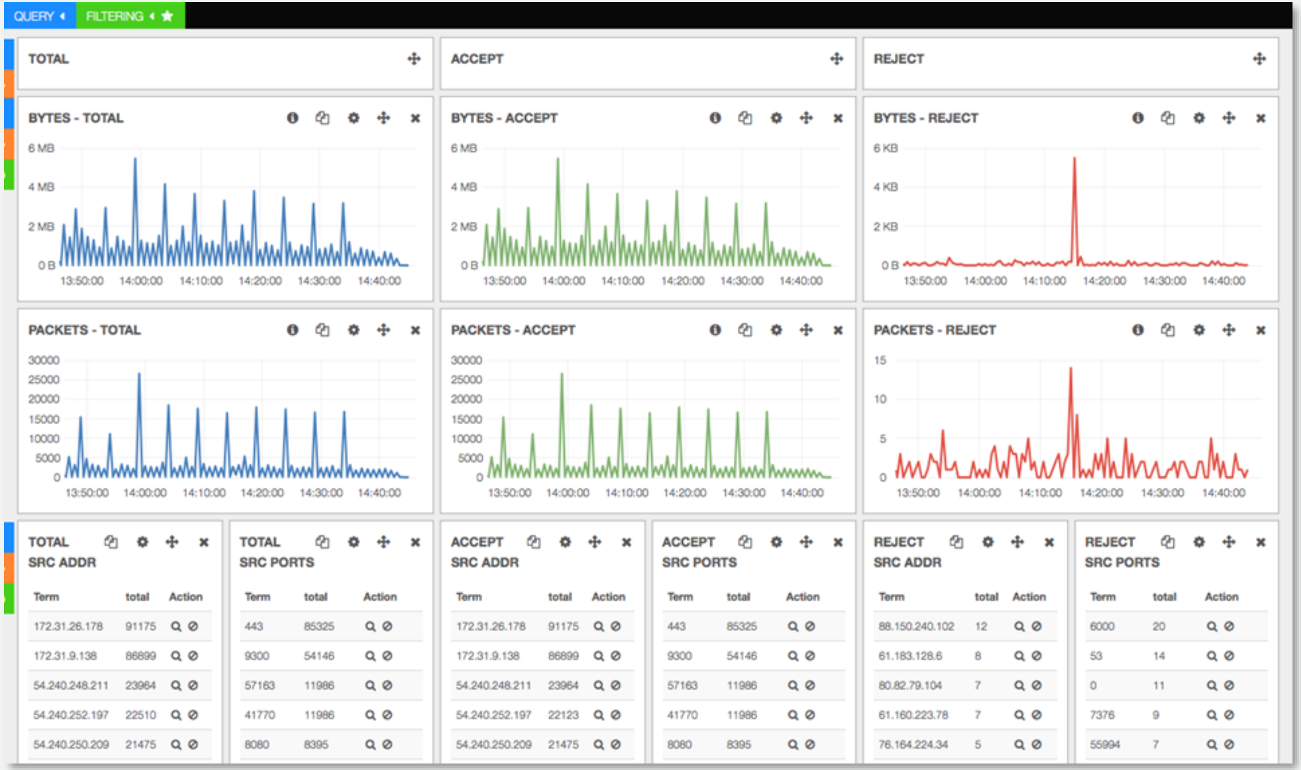
AWS Lambda & Amazon Kinesis Integration

- Custom processing with your code

Export to S3

- SDK & CLI batch export of logs for analytics

Processing Logs – Elasticsearch with Kibana



TOTAL
SRC ADDR

Term	total	Action
172.31.26.178	91175	🔍 ⊘
172.31.9.138	86899	🔍 ⊘
54.240.248.211	23964	🔍 ⊘
54.240.252.197	22510	🔍 ⊘
54.240.250.209	21475	🔍 ⊘

TOTAL
SRC PORTS

Term	total	Action
443	85325	🔍 ⊘
9300	54146	🔍 ⊘
57163	11986	🔍 ⊘
41770	11986	🔍 ⊘
8080	8395	🔍 ⊘

ACCEPT
SRC ADDR

Term	total	Action
172.31.26.178	91175	🔍 ⊘
172.31.9.138	86899	🔍 ⊘
54.240.248.211	23964	🔍 ⊘
54.240.252.197	22123	🔍 ⊘
54.240.250.209	21475	🔍 ⊘

ACCEPT
SRC PORTS

Term	total	Action
443	85325	🔍 ⊘
9300	54146	🔍 ⊘
57163	11986	🔍 ⊘
41770	11986	🔍 ⊘
8080	8395	🔍 ⊘

REJECT
SRC ADDR

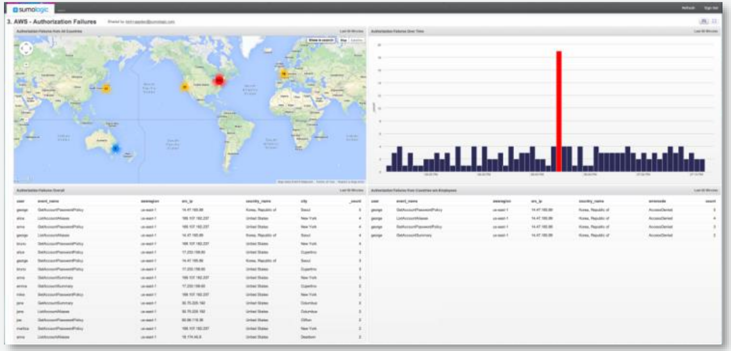
Term	total	Action
88.150.240.102	12	🔍 ⊘
61.183.128.6	8	🔍 ⊘
80.82.79.104	7	🔍 ⊘
61.160.223.78	7	🔍 ⊘
76.164.224.34	5	🔍 ⊘

REJECT
SRC PORTS

Term	total	Action
6000	20	🔍 ⊘
53	14	🔍 ⊘
0	11	🔍 ⊘
7376	9	🔍 ⊘
55994	7	🔍 ⊘

- Amazon Elasticsearch Service
- Amazon CloudWarch Logs Subscription

Processing Logs – Partner Solutions



logentries

boundary

sumologic

Smartronix

Cloud ASSURED

CloudCheckr

STACKDRIVER

ALERTLOGIC
Security. Compliance. Cloud.

splunk>

DATADOG

LOGGLY

DATAPIPE

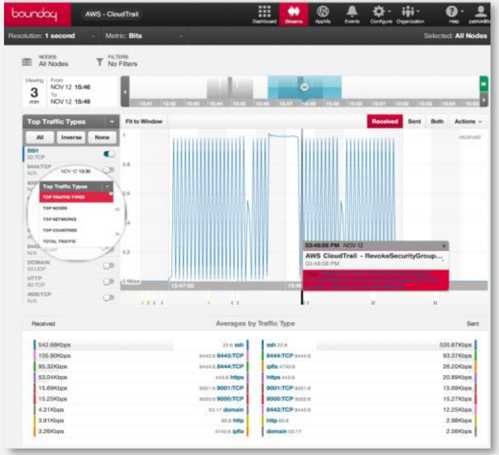
2ND WATCH

CLOUDNEXA

FOGHORN WEBSERVICES

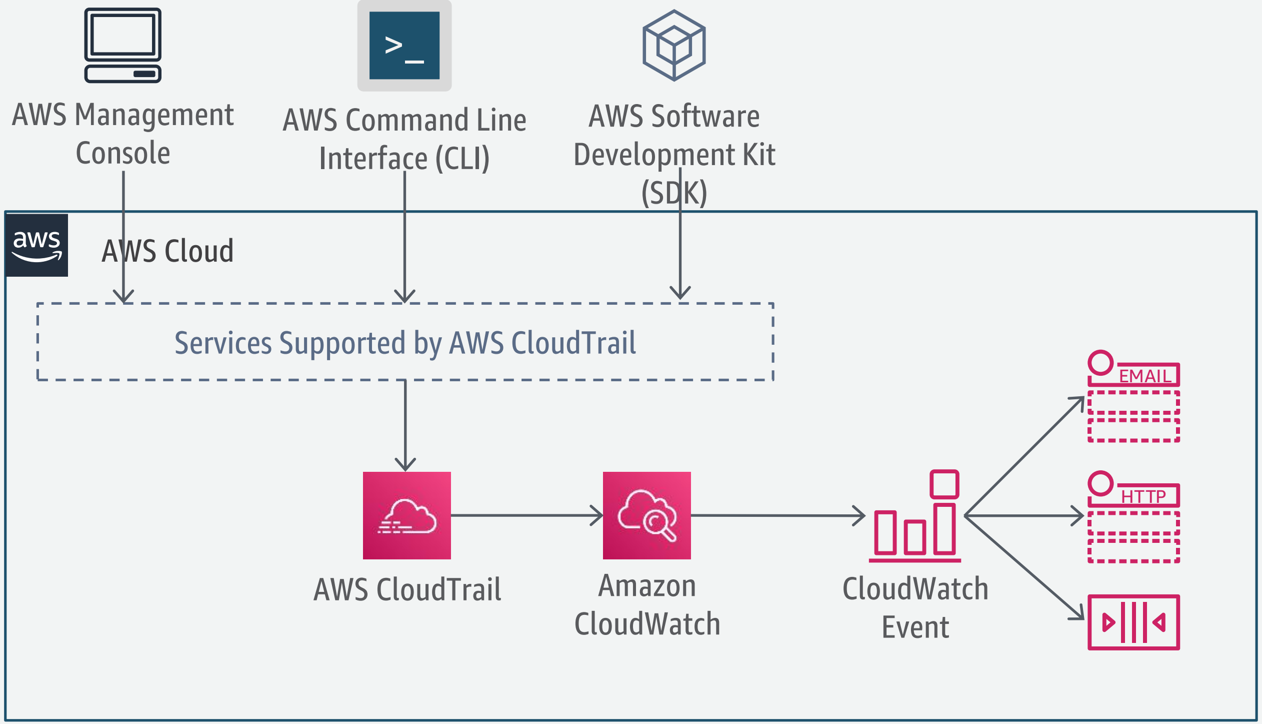
CLOUDLYTICS

graylog



Alerting

Alerting – Receive Notifications of API activity



AWS Management Console

AWS Command Line Interface (CLI)

AWS Software Development Kit (SDK)

AWS Cloud

Services Supported by AWS CloudTrail

AWS CloudTrail

Amazon CloudWatch

CloudWatch Event

Follow-up Actions

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

Alerting - CloudWatch Events

Trigger on event

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

Or Schedule

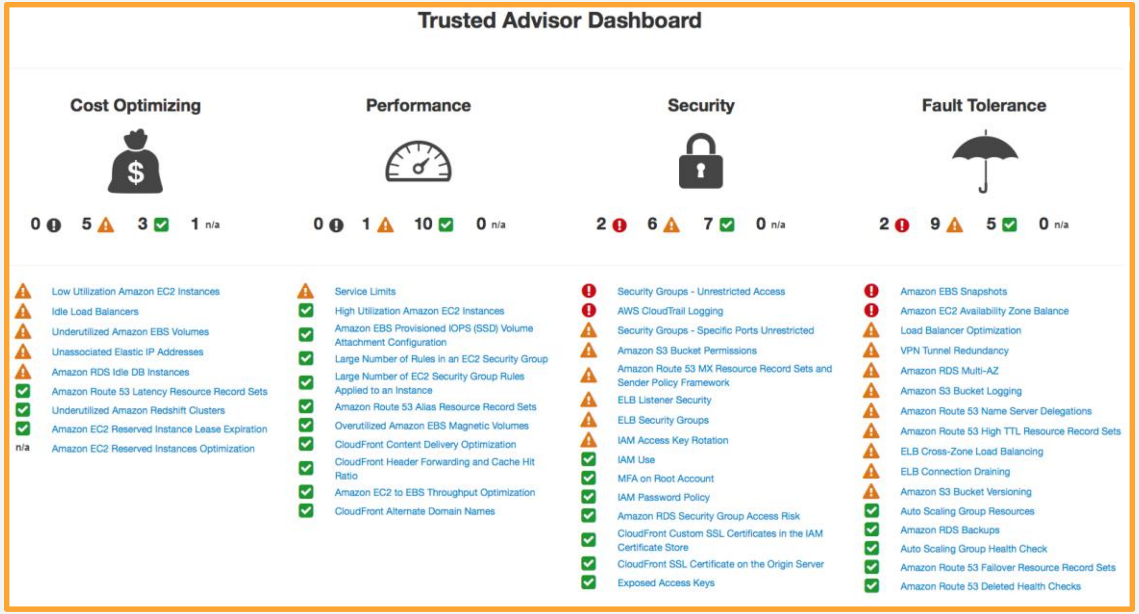
- Cron is in the cloud!
- No more Unreliable Town Clock
- Minimum 1 minute

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



Trusted Advisor Dashboard

Cost Optimizing

0 ❗ 5 ⚠ 3 ☑ 1 n/a

- ⚠ Low Utilization Amazon EC2 Instances
- ⚠ Idle Load Balancers
- ⚠ Underutilized Amazon EBS Volumes
- ⚠ Unassociated Elastic IP Addresses
- ⚠ Amazon RDS Idle DB Instances
- ☑ Amazon Route 53 Latency Resource Record Sets
- ☑ Underutilized Amazon Redshift Clusters
- ☑ Amazon EC2 Reserved Instance Lease Expiration
- n/a Amazon EC2 Reserved Instances Optimization

Performance

0 ❗ 1 ⚠ 10 ☑ 0 n/a

- ⚠ Service Limits
- ☑ High Utilization Amazon EC2 Instances
- ☑ Amazon EBS Provisioned IOPS (SSD) Volume Attachment Configuration
- ☑ Large Number of Rules in an EC2 Security Group
- ☑ Large Number of EC2 Security Group Rules Applied to an Instance
- ☑ Amazon Route 53 Alias Resource Record Sets
- ☑ Overutilized Amazon EBS Magnetic Volumes
- ☑ CloudFront Content Delivery Optimization
- ☑ CloudFront Header Forwarding and Cache Hit Ratio
- ☑ Amazon EC2 to EBS Throughput Optimization
- ☑ CloudFront Alternate Domain Names

Security

2 ❗ 6 ⚠ 7 ☑ 0 n/a

- ❗ Security Groups - Unrestricted Access
- ❗ AWS CloudTrail Logging
- ⚠ Security Groups - Specific Ports Unrestricted
- ⚠ Amazon S3 Bucket Permissions
- ⚠ Amazon Route 53 MX Resource Record Sets and Sender Policy Framework
- ⚠ ELB Listener Security
- ⚠ ELB Security Groups
- ⚠ IAM Access Key Rotation
- ☑ IAM Use
- ☑ MFA on Root Account
- ☑ IAM Password Policy
- ☑ Amazon RDS Security Group Access Risk
- ☑ CloudFront Custom SSL Certificates in the IAM Certificate Store
- ☑ CloudFront SSL Certificate on the Origin Server
- ☑ Exposed Access Keys

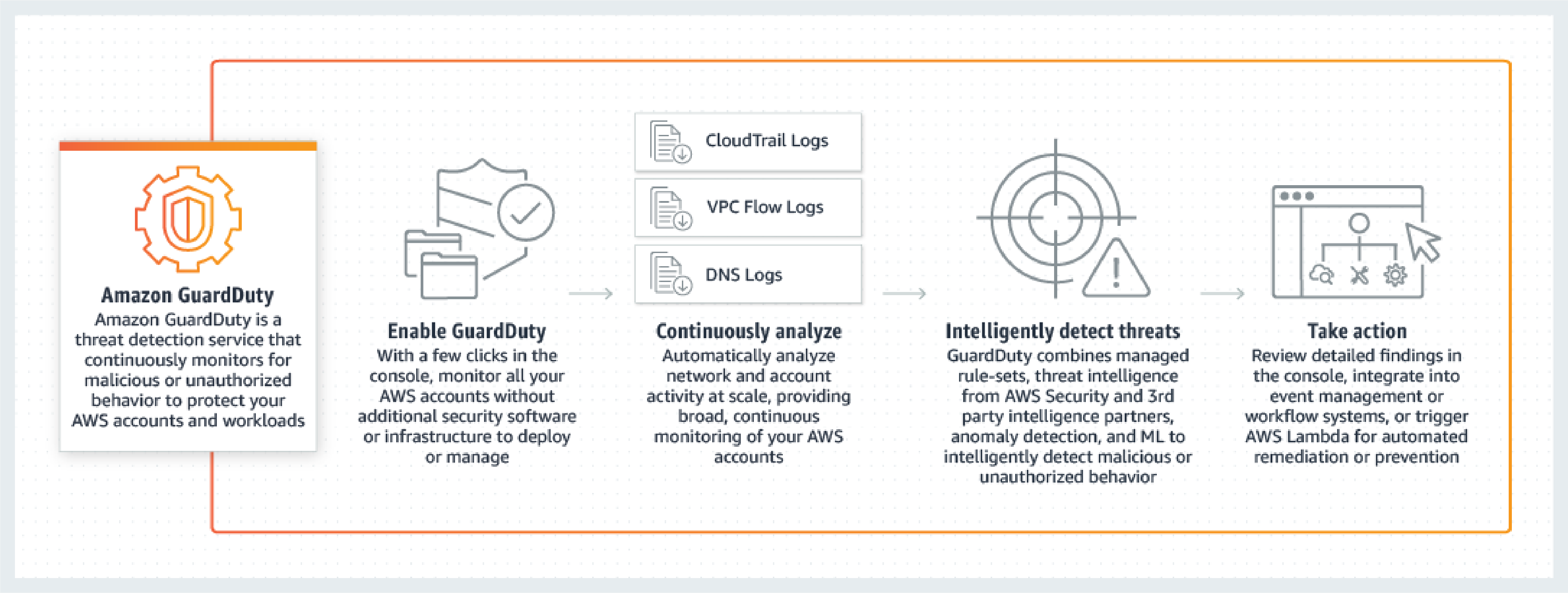
Fault Tolerance

2 ❗ 9 ⚠ 5 ☑ 0 n/a

- ❗ Amazon EBS Snapshots
- ❗ Amazon EC2 Availability Zone Balance
- ⚠ Load Balancer Optimization
- ⚠ VPN Tunnel Redundancy
- ⚠ Amazon RDS Multi-AZ
- ⚠ Amazon S3 Bucket Logging
- ⚠ Amazon Route 53 Name Server Delegations
- ⚠ Amazon Route 53 High TTL Resource Record Sets
- ⚠ ELB Cross-Zone Load Balancing
- ⚠ ELB Connection Draining
- ⚠ Amazon S3 Bucket Versioning
- ☑ Auto Scaling Group Resources
- ☑ Amazon RDS Backups
- ☑ Auto Scaling Group Health Check
- ☑ Amazon Route 53 Failover Resource Record Sets
- ☑ Amazon Route 53 Deleted Health Checks

Amazon GuardDuty

Amazon GuardDuty



Amazon GuardDuty
Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to protect your AWS accounts and workloads

Enable GuardDuty
With a few clicks in the console, monitor all your AWS accounts without additional security software or infrastructure to deploy or manage

CloudTrail Logs

VPC Flow Logs

DNS Logs

Continuously analyze
Automatically analyze network and account activity at scale, providing broad, continuous monitoring of your AWS accounts

Intelligently detect threats
GuardDuty combines managed rule-sets, threat intelligence from AWS Security and 3rd party intelligence partners, anomaly detection, and ML to intelligently detect malicious or unauthorized behavior

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

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).

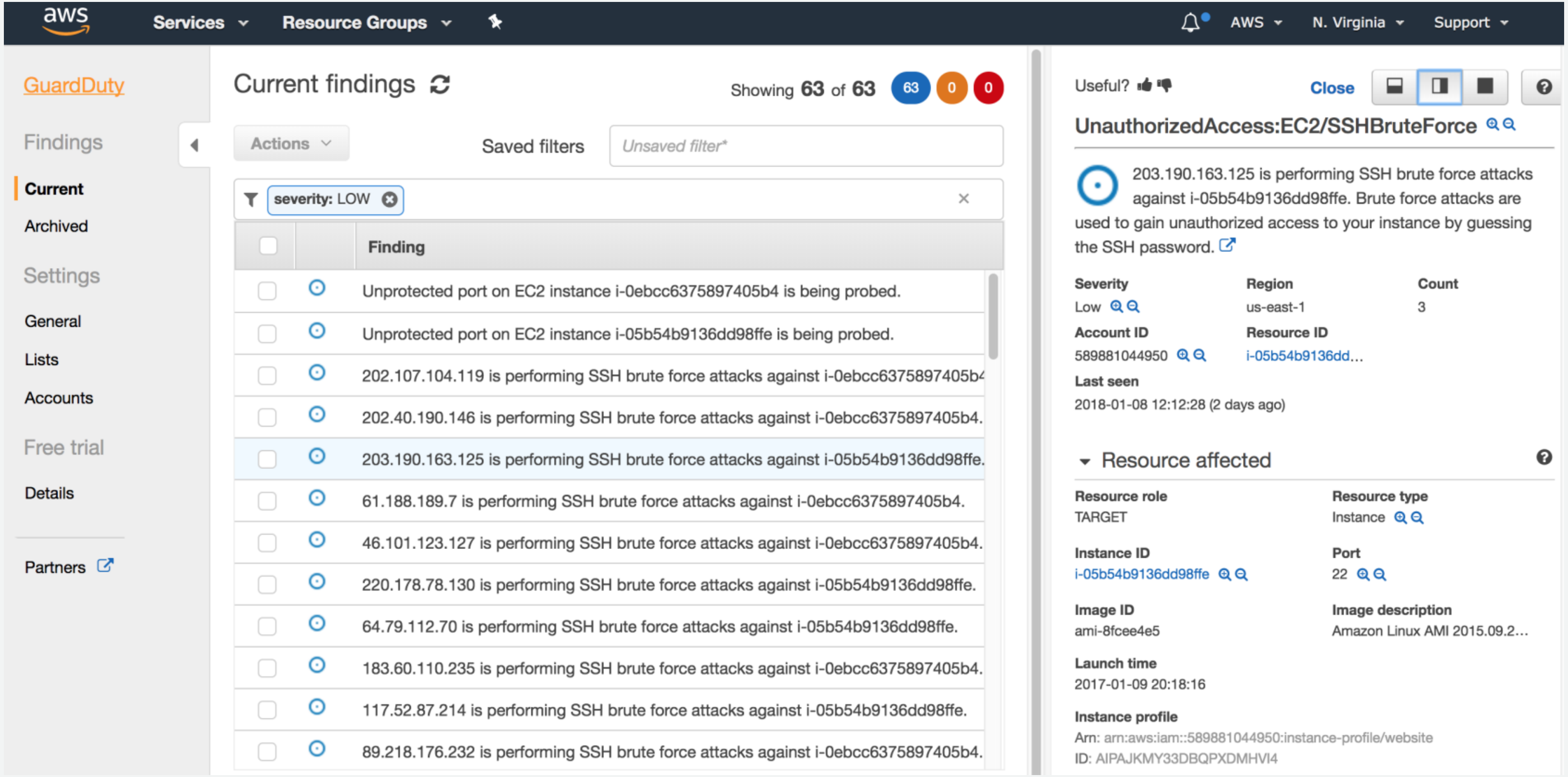
DNS Logs

- 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 – Findings



Current findings

Showing 63 of 63 63 0 0

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**	
589881044950	i-05b54b9136dd...	

Last seen
2018-01-08 12:12:28 (2 days ago)

Resource affected

Resource role	Resource type
TARGET	Instance
Instance ID	**Port**
i-05b54b9136dd98ffe	22
Image ID	**Image description**
ami-8fcee4e5	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

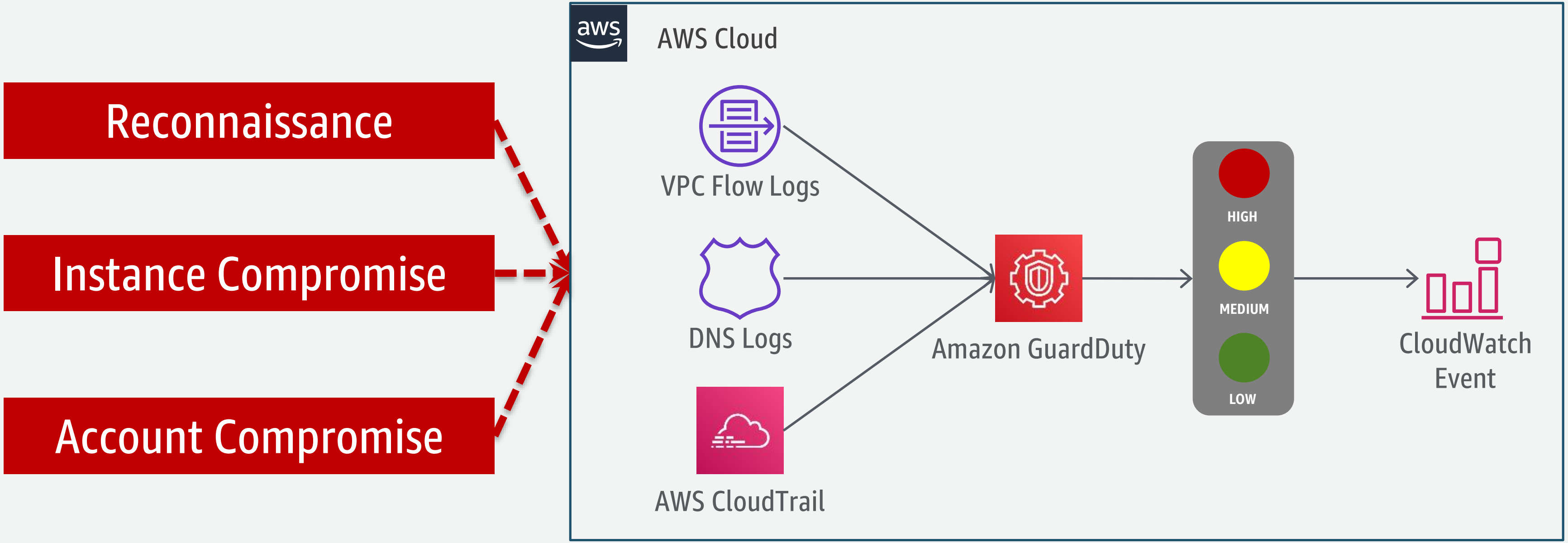
Amazon GuardDuty – Threat Detection

Threat Detection Types

Data Sources

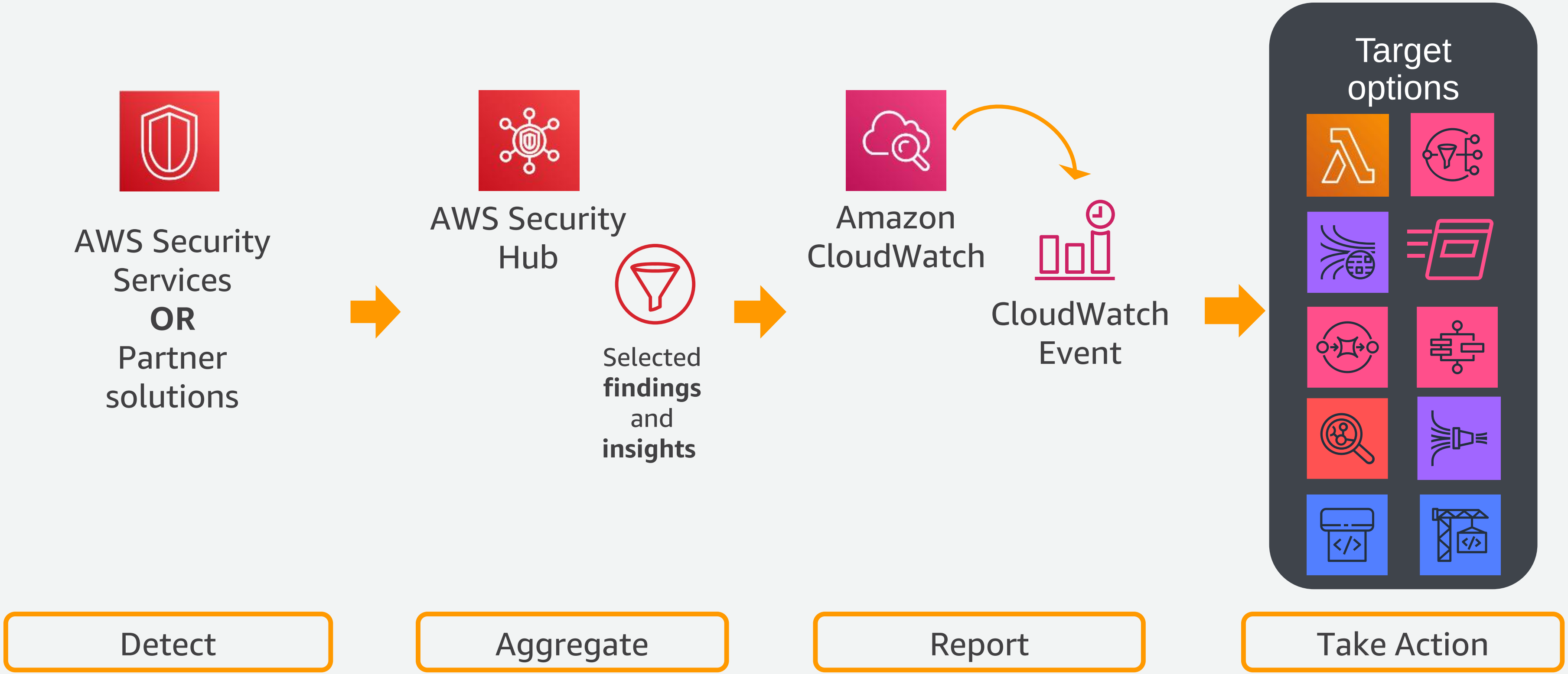
Findings

Respond



AWS Security Hub

AWS Security Hub



AWS Security Services **OR** Partner solutions

AWS Security Hub

Selected **findings** and **insights**

Amazon CloudWatch

CloudWatch Event

Target options

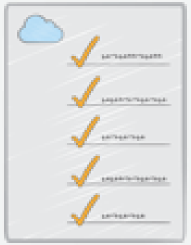
Detect

Aggregate

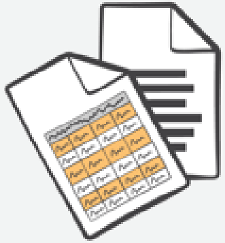
Report

Take Action

AWS Security Hub - Benefits



Compliance standards



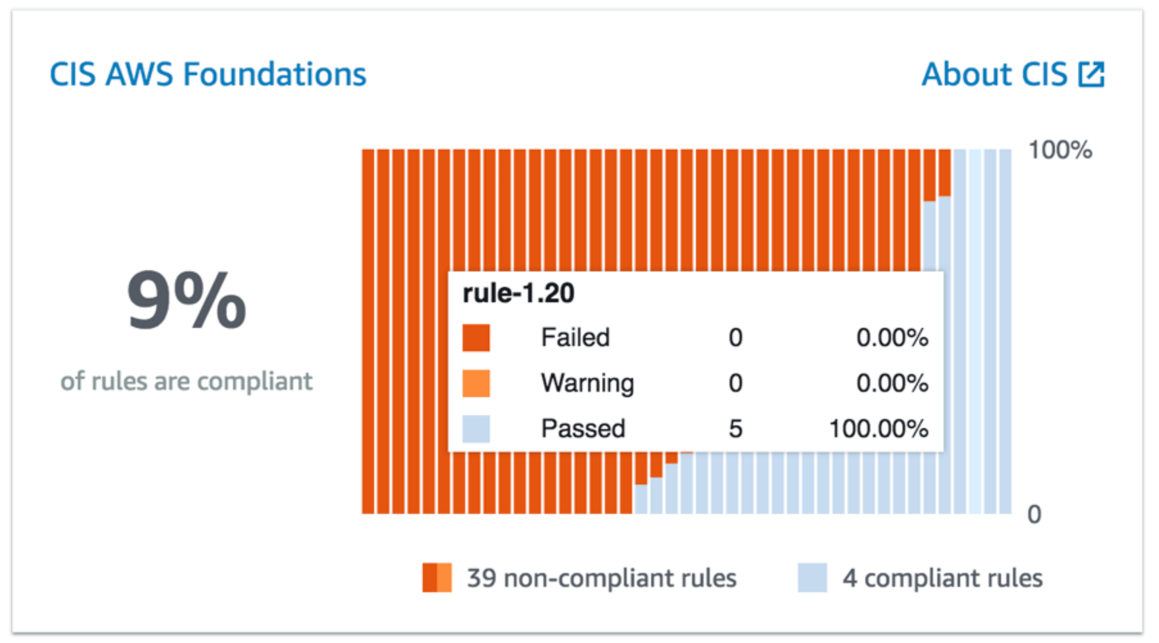
Aggregated findings

Insights

AWS Security Hub - Automated compliance checks

CIS Center for Internet Security®

43 fully automated, nearly continuous checks



CIS AWS Foundations

About CIS ↗

9%

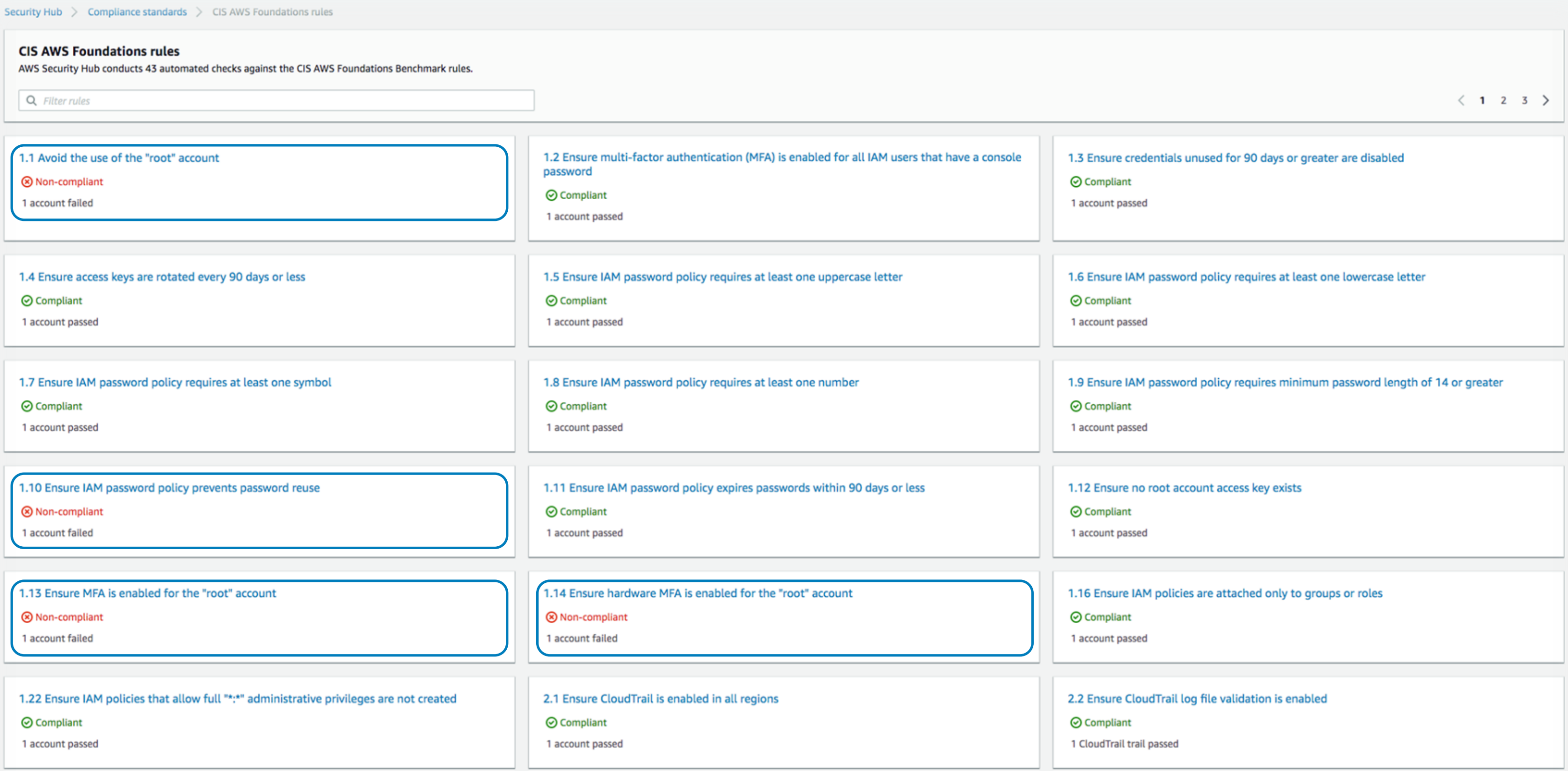
of rules are compliant

rule-1.20

🟥	Failed	0	0.00%
🟧	Warning	0	0.00%
🟦	Passed	5	100.00%

🟥🟧 39 non-compliant rules 🟦 4 compliant rules

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.

1.1 Avoid the use of the "root" account
⊗ Non-compliant
1 account failed

1.2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password
✓ Compliant
1 account passed

1.3 Ensure credentials unused for 90 days or greater are disabled
✓ Compliant
1 account passed

1.4 Ensure access keys are rotated every 90 days or less
✓ Compliant
1 account passed

1.5 Ensure IAM password policy requires at least one uppercase letter
✓ Compliant
1 account passed

1.6 Ensure IAM password policy requires at least one lowercase letter
✓ Compliant
1 account passed

1.7 Ensure IAM password policy requires at least one symbol
✓ Compliant
1 account passed

1.8 Ensure IAM password policy requires at least one number
✓ Compliant
1 account passed

1.9 Ensure IAM password policy requires minimum password length of 14 or greater
✓ Compliant
1 account passed

1.10 Ensure IAM password policy prevents password reuse
⊗ Non-compliant
1 account failed

1.11 Ensure IAM password policy expires passwords within 90 days or less
✓ Compliant
1 account passed

1.12 Ensure no root account access key exists
✓ Compliant
1 account passed

1.13 Ensure MFA is enabled for the "root" account
⊗ Non-compliant
1 account failed

1.14 Ensure hardware MFA is enabled for the "root" account
⊗ Non-compliant
1 account failed

1.16 Ensure IAM policies are attached only to groups or roles
✓ Compliant
1 account passed

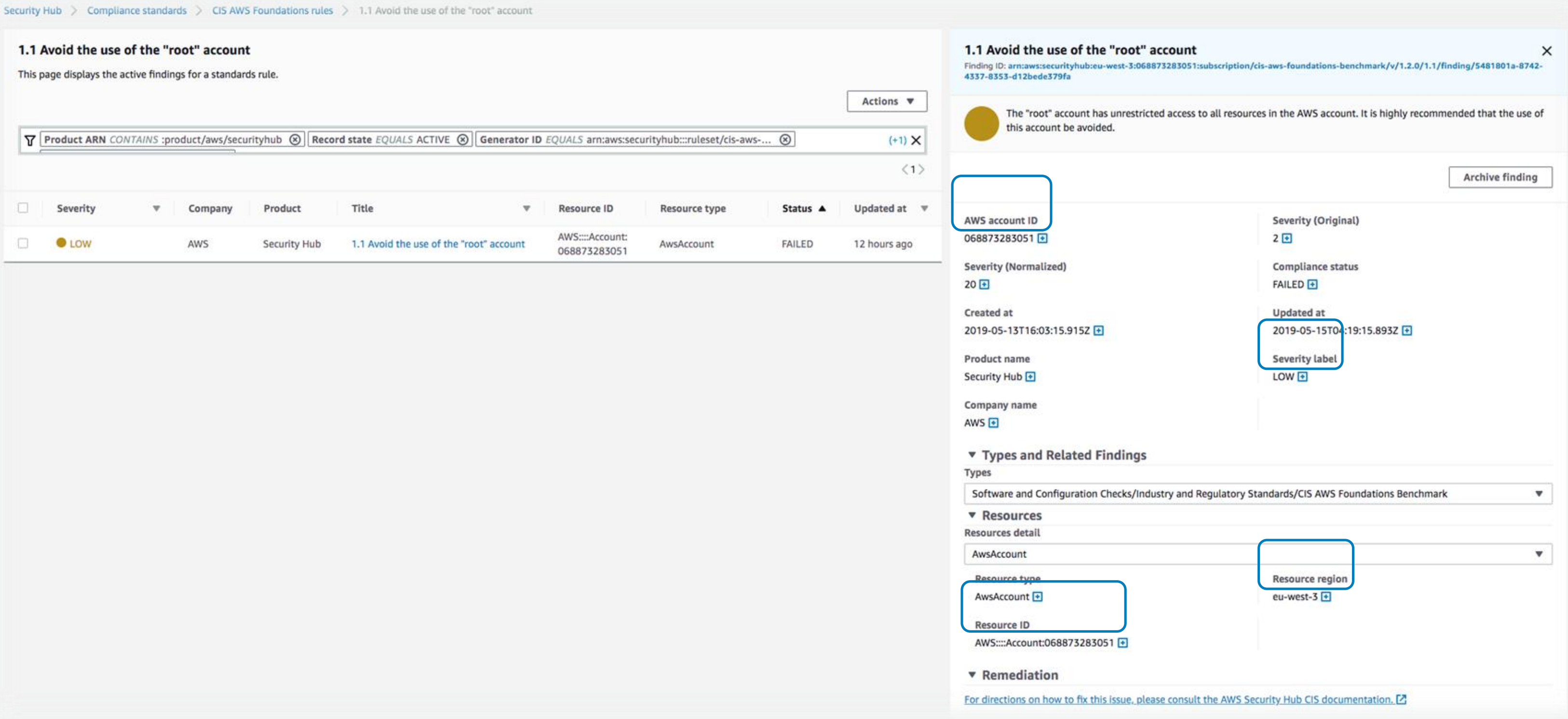
1.22 Ensure IAM policies that allow full "*:*" administrative privileges are not created
✓ Compliant
1 account passed

2.1 Ensure CloudTrail is enabled in all regions
✓ Compliant
1 account passed

2.2 Ensure CloudTrail log file validation is enabled
✓ 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

1.1 Avoid the use of the "root" account

This page displays the active findings for a standards rule.

Product ARN *CONTAINS* :product/aws/securityhub ⊗ | Record state *EQUALS* ACTIVE ⊗ | Generator ID *EQUALS* arn:aws:securityhub:::ruleset/cis-aws-... ⊗ (+1) ✕

□	Severity	Company	Product	Title	Resource ID	Resource type	Status ▲	Updated at
□	● LOW	AWS	Security Hub	1.1 Avoid the use of the "root" account	AWS::::Account: 068873283051	AwsAccount	FAILED	12 hours ago

1.1 Avoid the use of the "root" account ✕

Finding ID: 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 "root" account has unrestricted access to all resources in the AWS account. It is highly recommended that the use of this account be avoided.

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
Product name Security Hub	**Severity label** LOW
Company name AWS	

▼ **Types and Related Findings**

Types

Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark ▼

▼ **Resources**

Resources detail

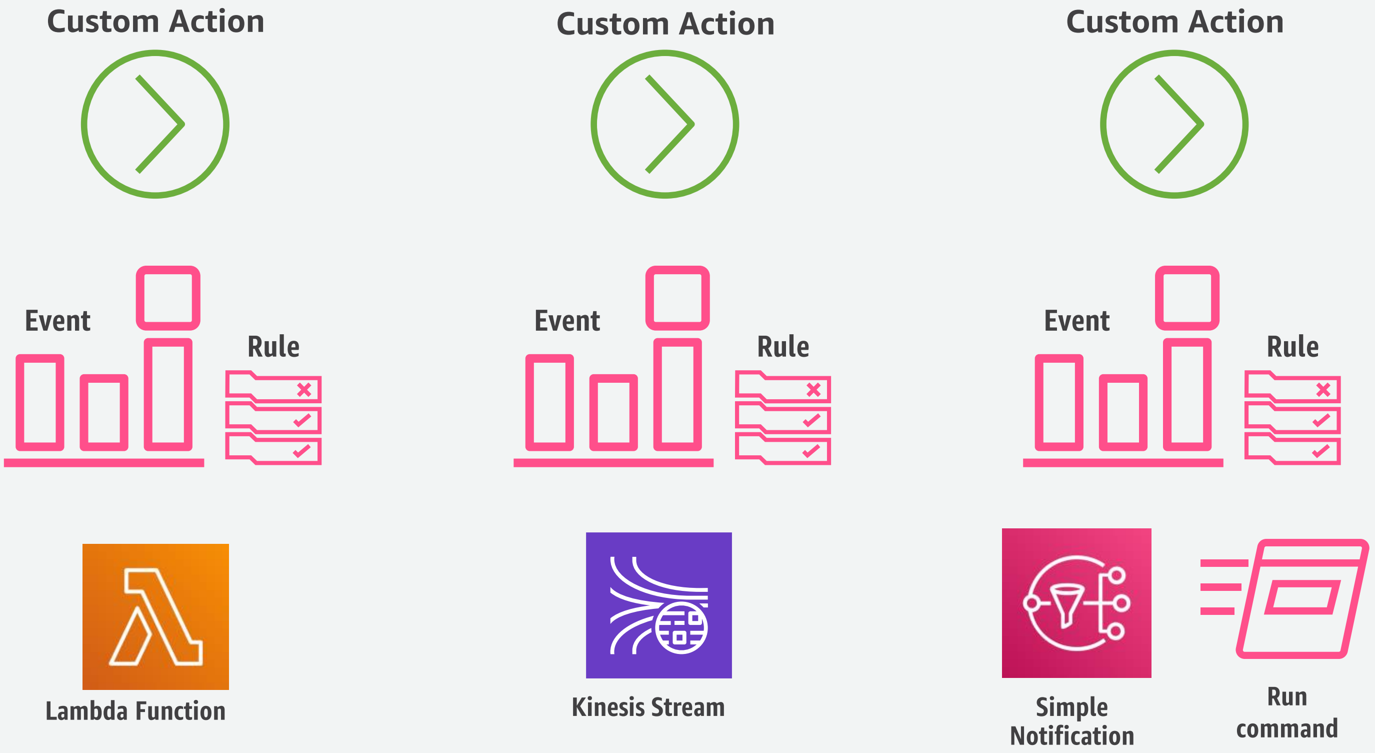
AwsAccount ▼

Resource type AwsAccount	**Resource region** eu-west-3
Resource ID AWS::::Account:068873283051	

▼ **Remediation**

For directions on how to fix this issue, please consult the AWS Security Hub CIS documentation.

Custom Actions in Security Hub



Custom Action

Event

Rule

Lambda Function

Custom Action

Event

Rule

Kinesis Stream

Custom Action

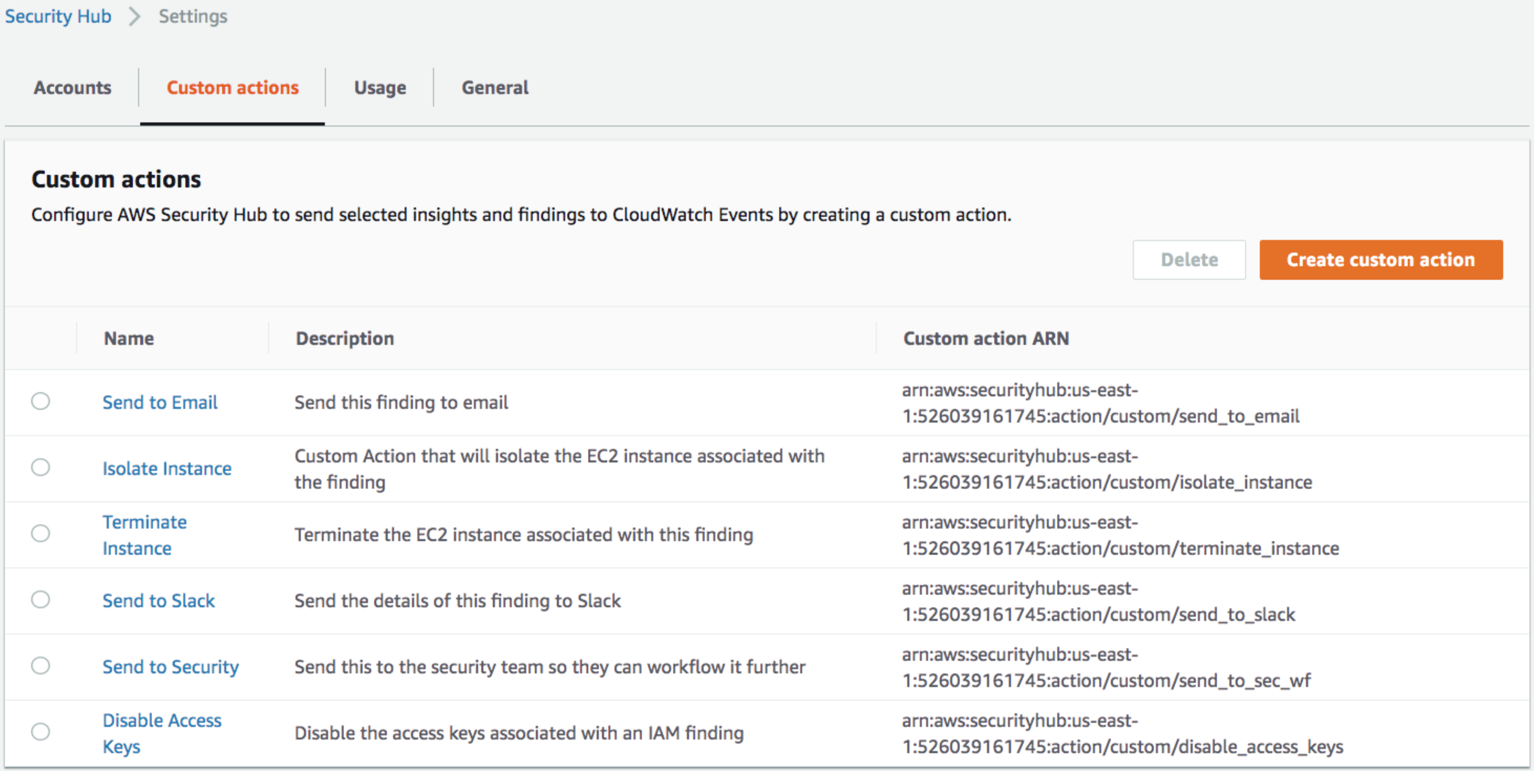
Event

Rule

Simple Notification

Run command

Custom Actions in Security Hub



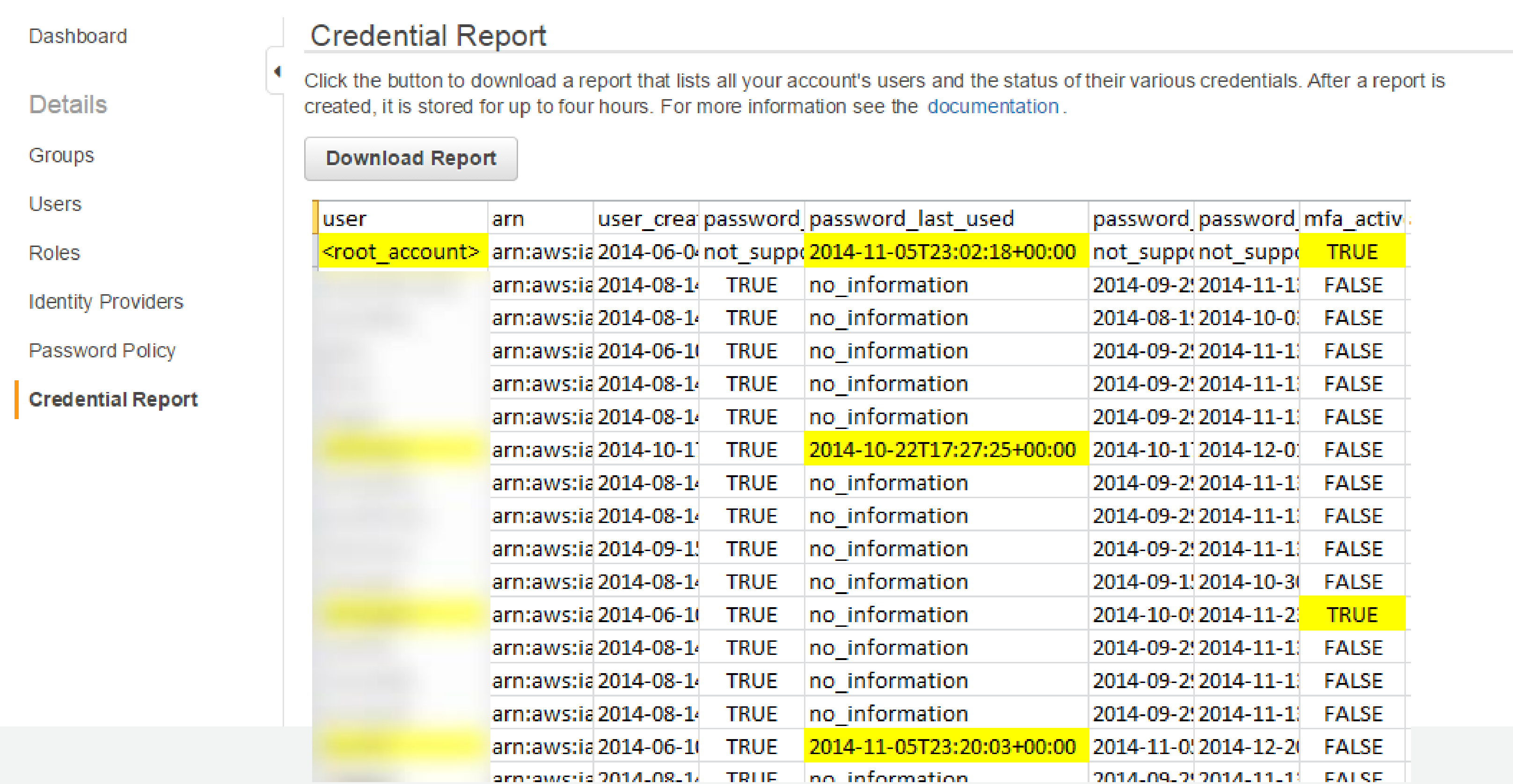
Custom actions

Configure AWS Security Hub to send selected insights and findings to CloudWatch Events by creating a custom action.

	Name	Description	Custom action ARN
○	Send to Email	Send this finding to email	arn:aws:securityhub:us-east-1:526039161745:action/custom/send_to_email
○	Isolate Instance	Custom Action that will isolate the EC2 instance associated with the finding	arn:aws:securityhub:us-east-1:526039161745:action/custom/isolate_instance
○	Terminate Instance	Terminate the EC2 instance associated with this finding	arn:aws:securityhub:us-east-1:526039161745:action/custom/terminate_instance
○	Send to Slack	Send the details of this finding to Slack	arn:aws:securityhub:us-east-1:526039161745:action/custom/send_to_slack
○	Send to Security	Send this to the security team so they can workflow it further	arn:aws:securityhub:us-east-1:526039161745:action/custom/send_to_sec_wf
○	Disable Access Keys	Disable the access keys associated with an IAM finding	arn:aws:securityhub:us-east-1:526039161745:action/custom/disable_access_keys

Auditing Your AWS Environment

Auditing – IAM 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.

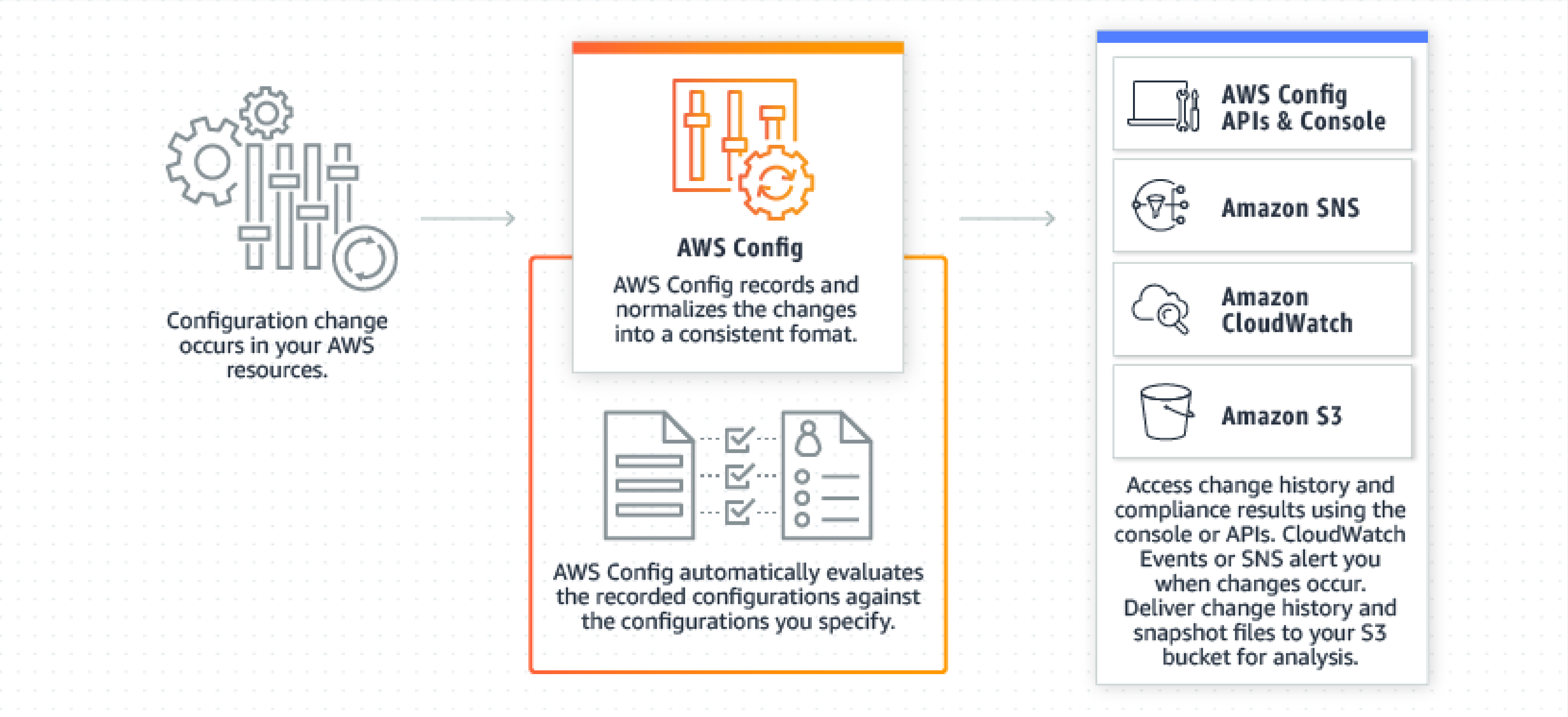
user	arn	user_crea	password_	password_last_used	password_	password_	mfa_activ
<root_account>	arn:aws:ia	2014-06-0	not_suppo	2014-11-05T23:02:18+00:00	not_suppo	not_suppo	TRUE
[redacted]	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
[redacted]	arn:aws:ia	2014-08-1	TRUE	no_information	2014-08-1	2014-10-0	FALSE
[redacted]	arn:aws:ia	2014-06-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
[redacted]	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
[redacted]	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
[redacted]	arn:aws:ia	2014-10-1	TRUE	2014-10-22T17:27:25+00:00	2014-10-1	2014-12-0	FALSE
[redacted]	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
[redacted]	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
[redacted]	arn:aws:ia	2014-09-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
[redacted]	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-1	2014-10-3	FALSE
[redacted]	arn:aws:ia	2014-06-1	TRUE	no_information	2014-10-0	2014-11-2	TRUE
[redacted]	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
[redacted]	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
[redacted]	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE
[redacted]	arn:aws:ia	2014-06-1	TRUE	2014-11-05T23:20:03+00:00	2014-11-0	2014-12-2	FALSE
[redacted]	arn:aws:ia	2014-08-1	TRUE	no_information	2014-09-2	2014-11-1	FALSE

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



Configuration change occurs in your AWS resources.

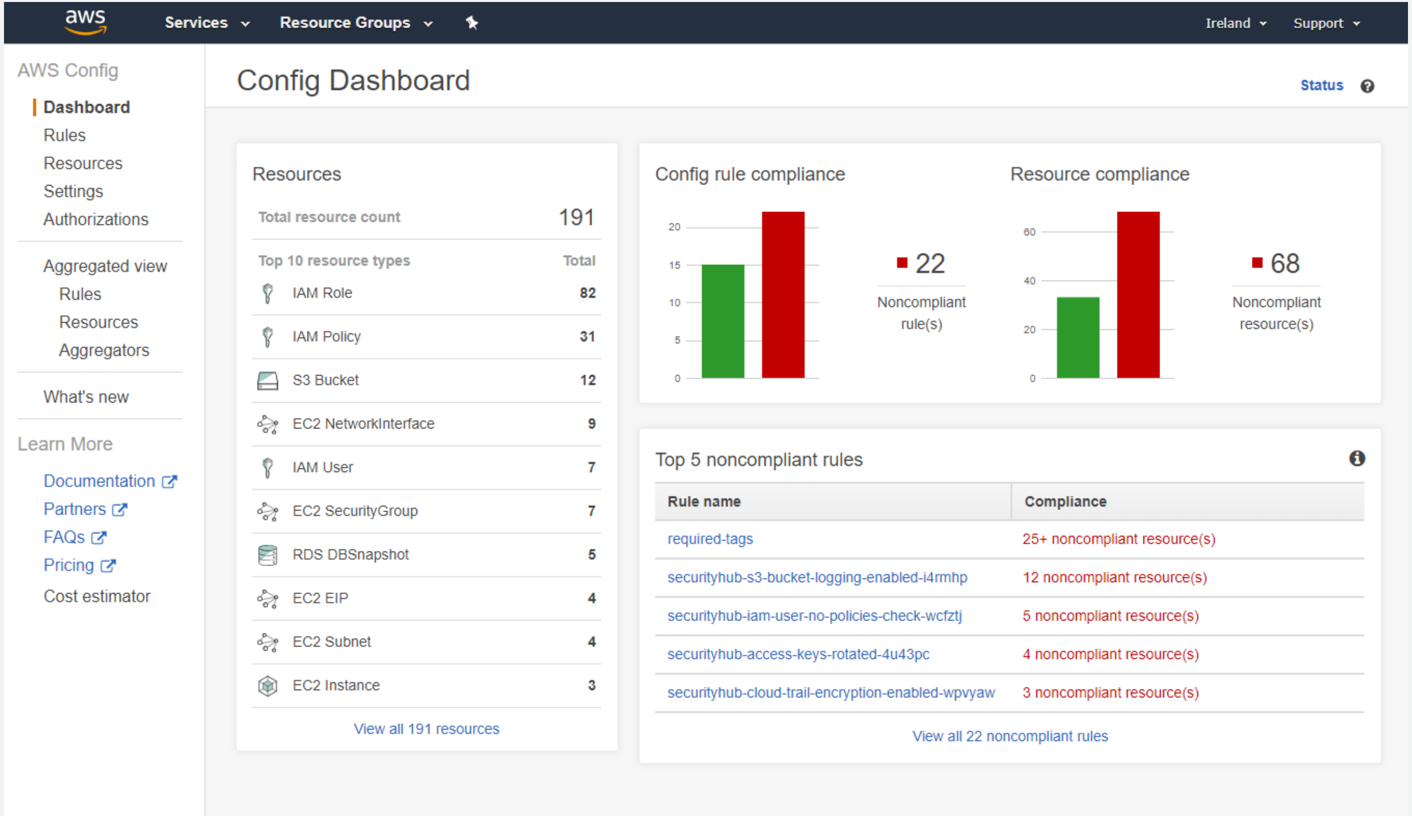
AWS Config

AWS Config records and normalizes the changes into a consistent fomat.

AWS Config automatically evaluates the recorded configurations against the configurations you specify.

Access change history and compliance results using the console or APIs. CloudWatch Events or SNS alert you when changes occur. Deliver change history and snapshot files to your S3 bucket for analysis.

Auditing – AWS Config



Config Dashboard

Resources

Total resource count	191
Top 10 resource types	**Total**
IAM Role	82
IAM Policy	31
S3 Bucket	12
EC2 NetworkInterface	9
IAM User	7
EC2 SecurityGroup	7
RDS DBSnapshot	5
EC2 EIP	4
EC2 Subnet	4
EC2 Instance	3

View all 191 resources

Config rule compliance

🟥 22 Noncompliant rule(s)

Resource compliance

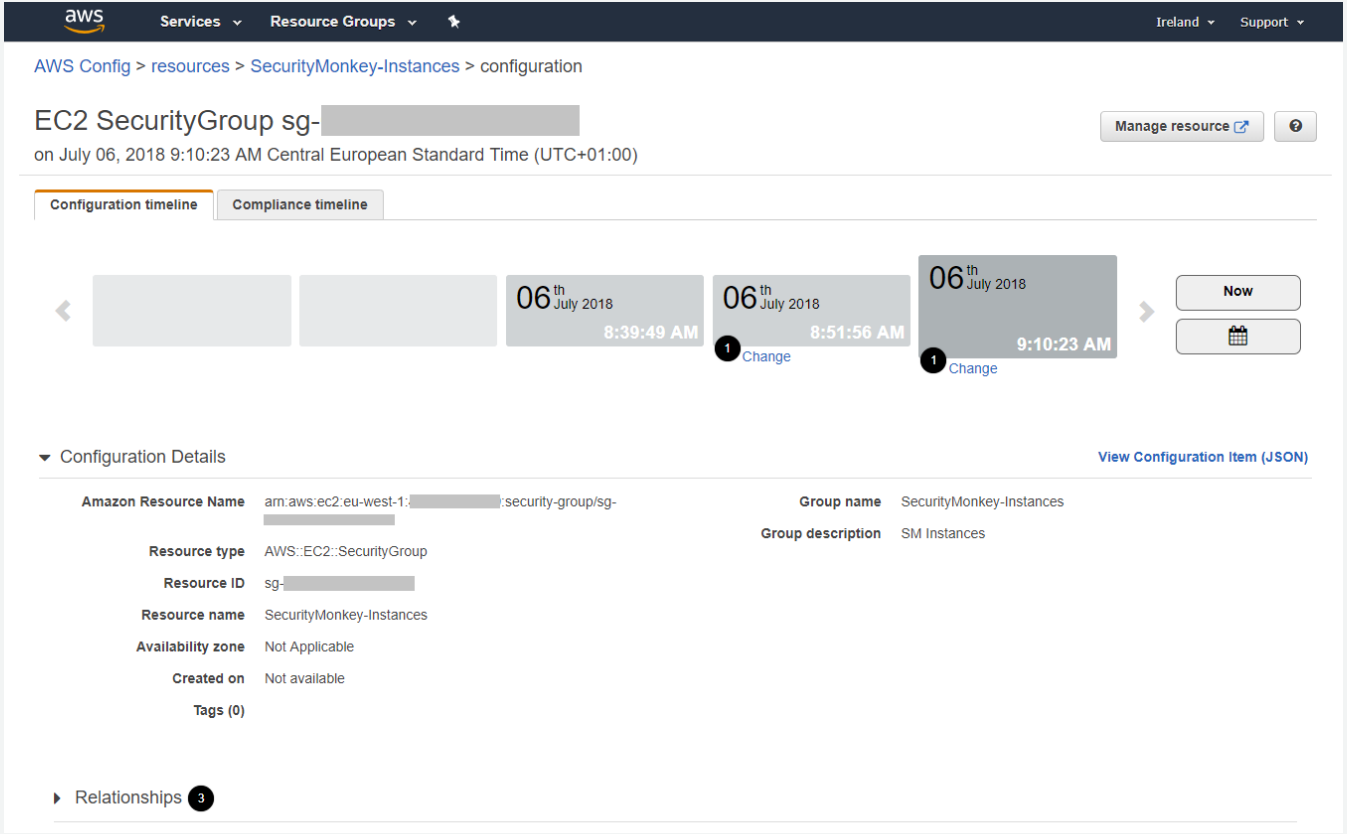
🟥 68 Noncompliant resource(s)

Top 5 noncompliant rules

Rule name	Compliance
required-tags	25+ noncompliant resource(s)
securityhub-s3-bucket-logging-enabled-i4rmhp	12 noncompliant resource(s)
securityhub-iam-user-no-policies-check-wcfztj	5 noncompliant resource(s)
securityhub-access-keys-rotated-4u43pc	4 noncompliant resource(s)
securityhub-cloud-trail-encryption-enabled-wpvyaw	3 noncompliant resource(s)

View all 22 noncompliant rules

Auditing – AWS Config



AWS Config > resources > SecurityMonkey-Instances > configuration

EC2 SecurityGroup sg-[redacted]

on July 06, 2018 9:10:23 AM Central European Standard Time (UTC+01:00)

06th July 2018 8:39:49 AM

06th July 2018 8:51:56 AM

1 Change

06th July 2018 9:10:23 AM

1 Change

Configuration Details

View Configuration Item (JSON)

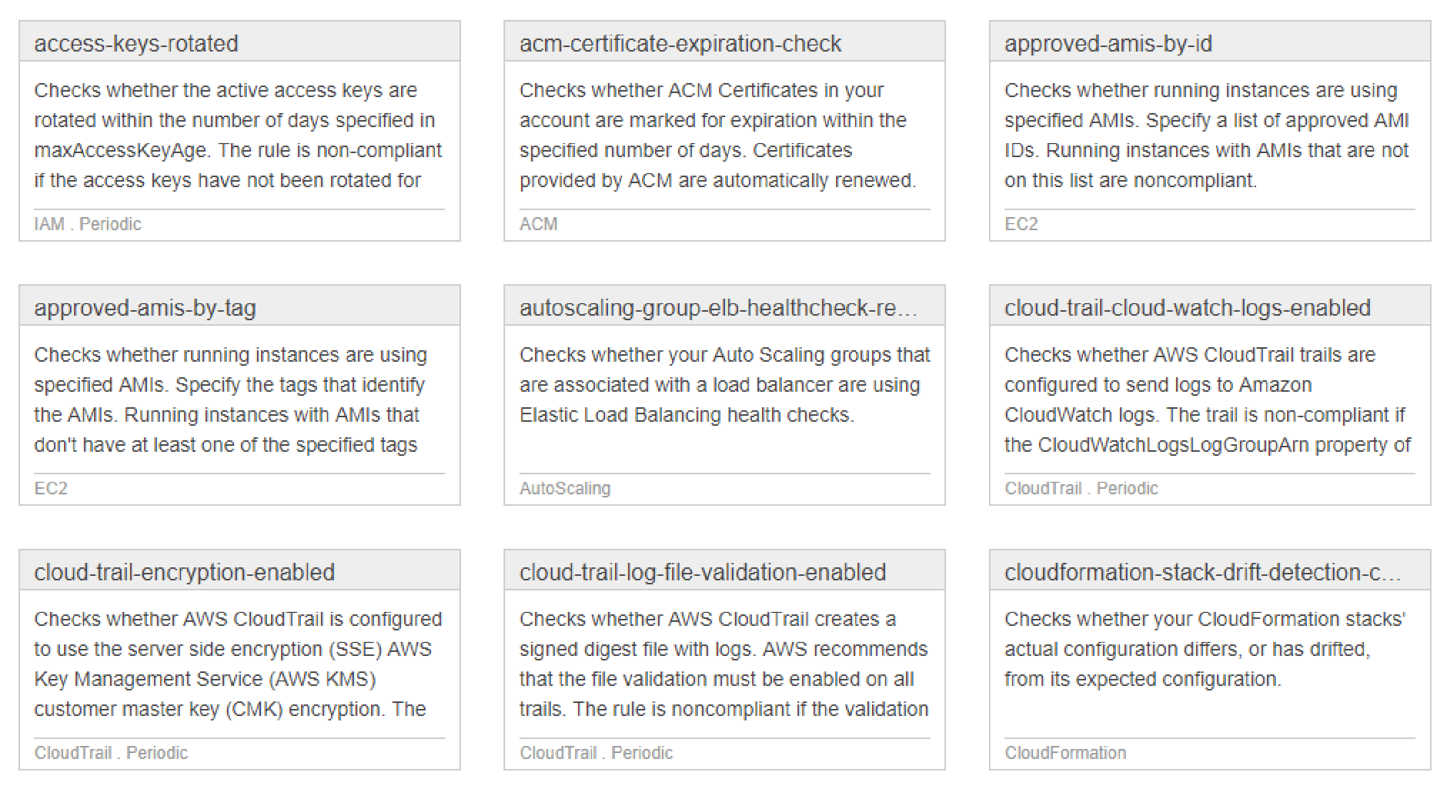
Amazon Resource Name	arn:aws:ec2:eu-west-1:[redacted]:security-group/sg-[redacted]	Group name	SecurityMonkey-Instances
Resource type	AWS::EC2::SecurityGroup	Group description	SM Instances
Resource ID	sg-[redacted]		
Resource name	SecurityMonkey-Instances		
Availability zone	Not Applicable		
Created on	Not available		
Tags (0)			

Relationships 3

Auditing – AWS Config Rules

- continuous and automated compliance validation against the specified configuration
- 80+ AWS Managed Rules available out of the box
- Ability to implement your own rules
- More information is provided in the ‘Security Automation’ workshop

Auditing – AWS Config Rules



access-keys-rotated

Checks whether the active access keys are rotated within the number of days specified in maxAccessKeyAge. The rule is non-compliant if the access keys have not been rotated for

IAM . Periodic

acm-certificate-expiration-check

Checks whether ACM Certificates in your account are marked for expiration within the specified number of days. Certificates provided by ACM are automatically renewed.

ACM

approved-amis-by-id

Checks whether running instances are using specified AMIs. Specify a list of approved AMI IDs. Running instances with AMIs that are not on this list are noncompliant.

EC2

approved-amis-by-tag

Checks whether running instances are using specified AMIs. Specify the tags that identify the AMIs. Running instances with AMIs that don't have at least one of the specified tags

EC2

autoscaling-group-elb-healthcheck-re...

Checks whether your Auto Scaling groups that are associated with a load balancer are using Elastic Load Balancing health checks.

AutoScaling

cloud-trail-cloud-watch-logs-enabled

Checks whether AWS CloudTrail trails are configured to send logs to Amazon CloudWatch logs. The trail is non-compliant if the CloudWatchLogsLogGroupArn property of

CloudTrail . Periodic

cloud-trail-encryption-enabled

Checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The

CloudTrail . Periodic

cloud-trail-log-file-validation-enabled

Checks whether AWS CloudTrail creates a signed digest file with logs. AWS recommends that the file validation must be enabled on all trails. The rule is noncompliant if the validation

CloudTrail . Periodic

cloudformation-stack-drift-detection-c...

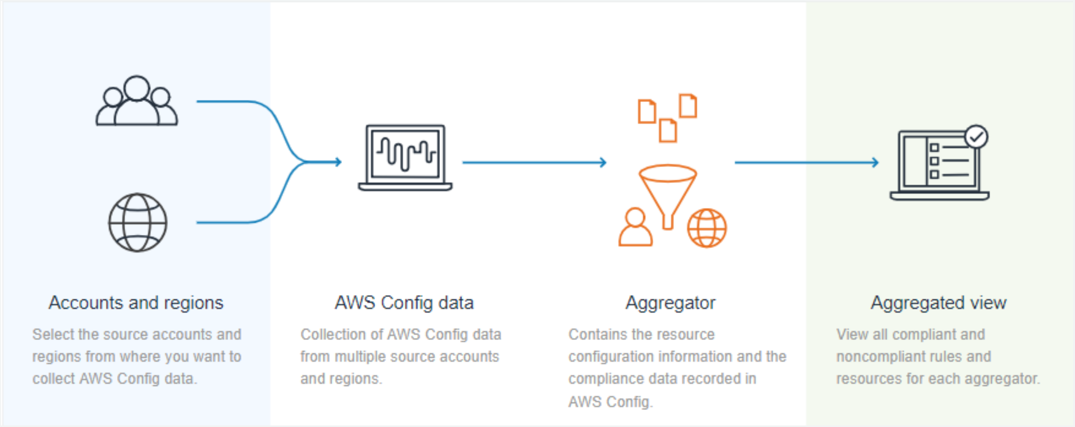
Checks whether your CloudFormation stacks' actual configuration differs, or has drifted, from its expected configuration.

CloudFormation

Auditing – AWS Config

Best practice: 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



Accounts and regions

Select the source accounts and regions from where you want to collect AWS Config data.

AWS Config data

Collection of AWS Config data from multiple source accounts and regions.

Aggregator

Contains the resource configuration information and the compliance data recorded in AWS Config.

Aggregated view

View all compliant and noncompliant rules and resources for each aggregator.

Questions?