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

aws professional services

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
- …

aws professional services

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

aws professional services

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 professional services

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 professional services
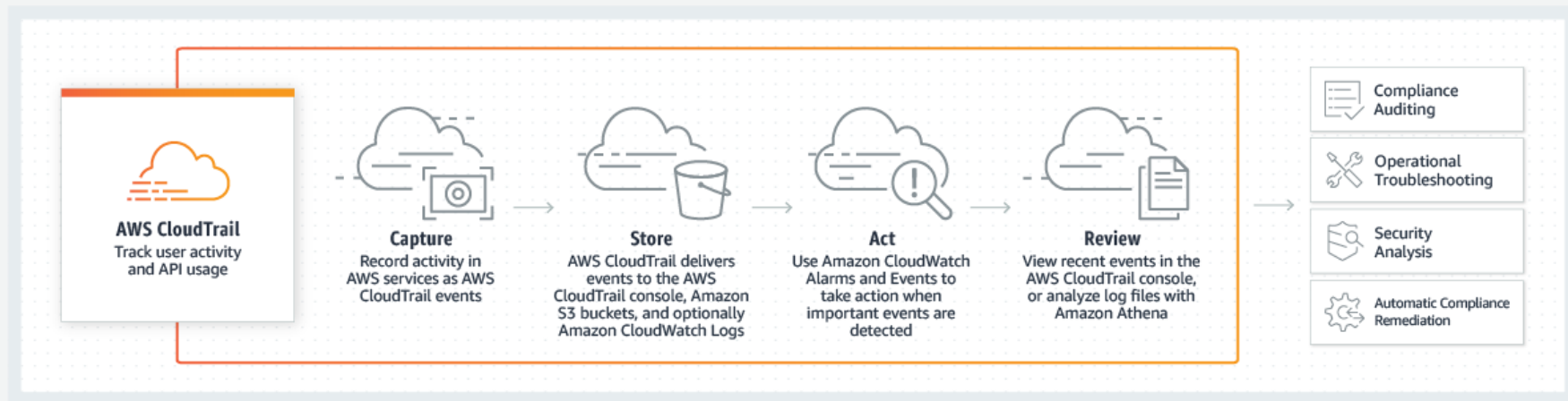
AWS CloudTrail

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 professional services
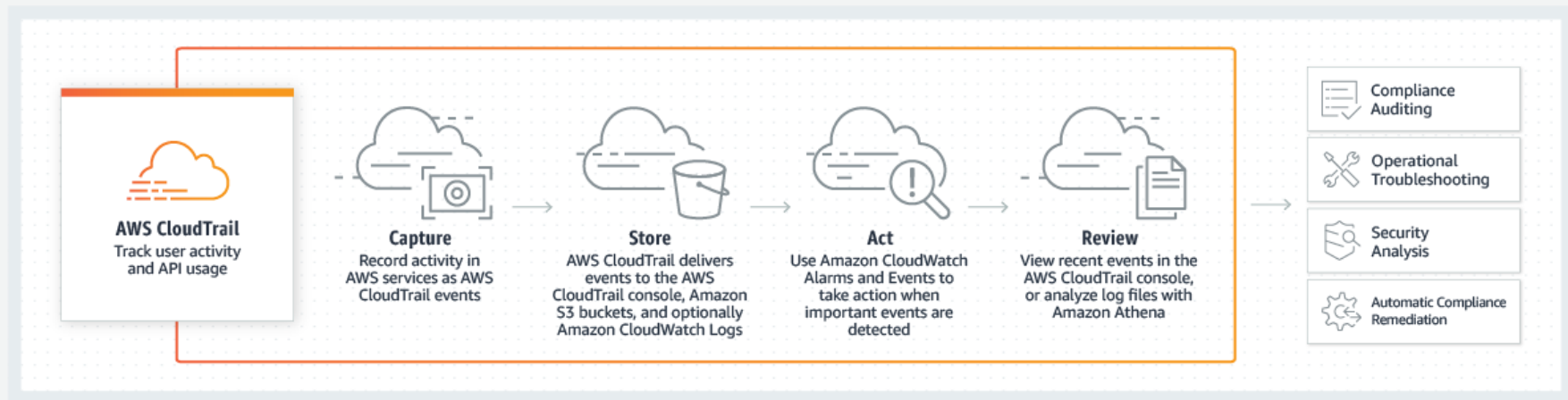
AWS CloudTrail – Common Use Cases

- **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 professional services

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 professional services
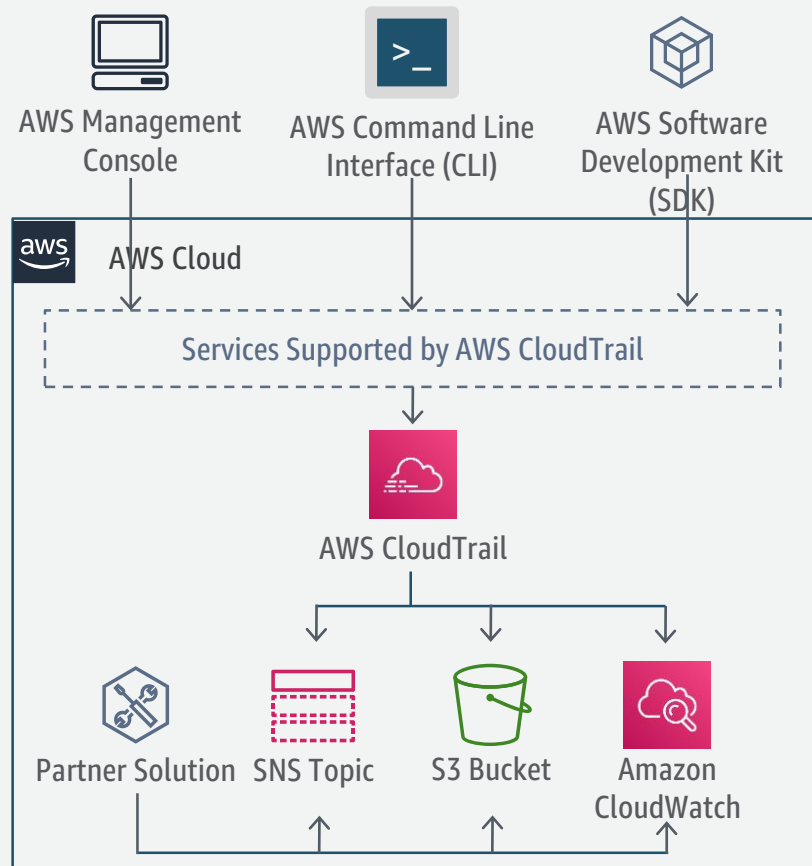
AWS CloudTrail - Security-Relevant Logs

- **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 professional services

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 professional services

AWS CloudTrail - Configuration

- You can create two types of "trails":
    - A trail that applies to <u>all regions</u>
    - A trail that applies to <u>one region</u>

- When you create a <u>trail that applies to all regions</u>, 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 professional services

AWS CloudTrail – Centralizing Logs

- ## Many-to-one centralization
  - From <u>multiple regions</u> into one S3 bucket (described before)
  - From <u>multiple accounts</u> into one account's S3 bucket

aws professional services

AWS CloudTrail – Centralizing Logs

1. Turn on CloudTrail for 111111111111

AWS Account 111111111111

Services Supported by AWS CloudTrail

AWS CloudTrail

S3 Bucket

2. Update bucket policy
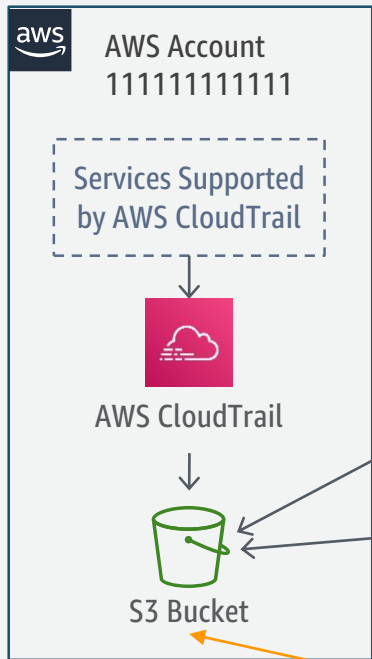
3. Turn on CloudTrail for 222222222222

AWS Account 222222222222

AWS CloudTrail

Services Supported by AWS CloudTrail
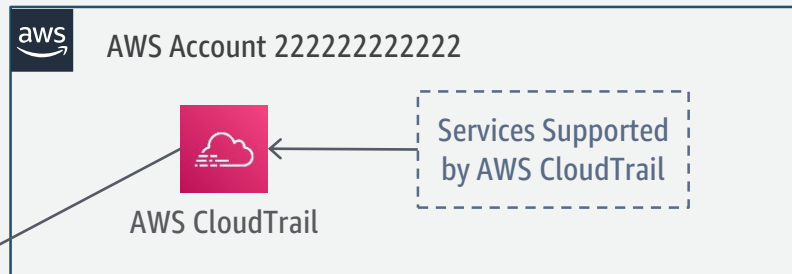
4. Turn on CloudTrail for 3333333333

AWS Account 333333333333

AWS CloudTrail

Services Supported by AWS CloudTrail

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

aws professional services

AWS CloudTrail – Centralizing Logs

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

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

aws professional services

AWS CloudTrail – Centralizing Logs

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

AWS Account
111111111111

Services Supported
by AWS CloudTrail

AWS CloudTrail

S3 Bucket

AWS Account 222222222222

Services Supported
by AWS CloudTrail

AWS CloudTrail

AWS Account 333333333333

Services Supported
by AWS CloudTrail

AWS CloudTrail

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

aws professional services

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

SecOps Engineer

② Specify the key to CloudTrail

AWS CloudTrail

S3 Bucket

Encrypted CloudTrail log files

③ S3 GetObject API call to retrieve the object

④ Decrypt CloudTrail log files

aws professional services
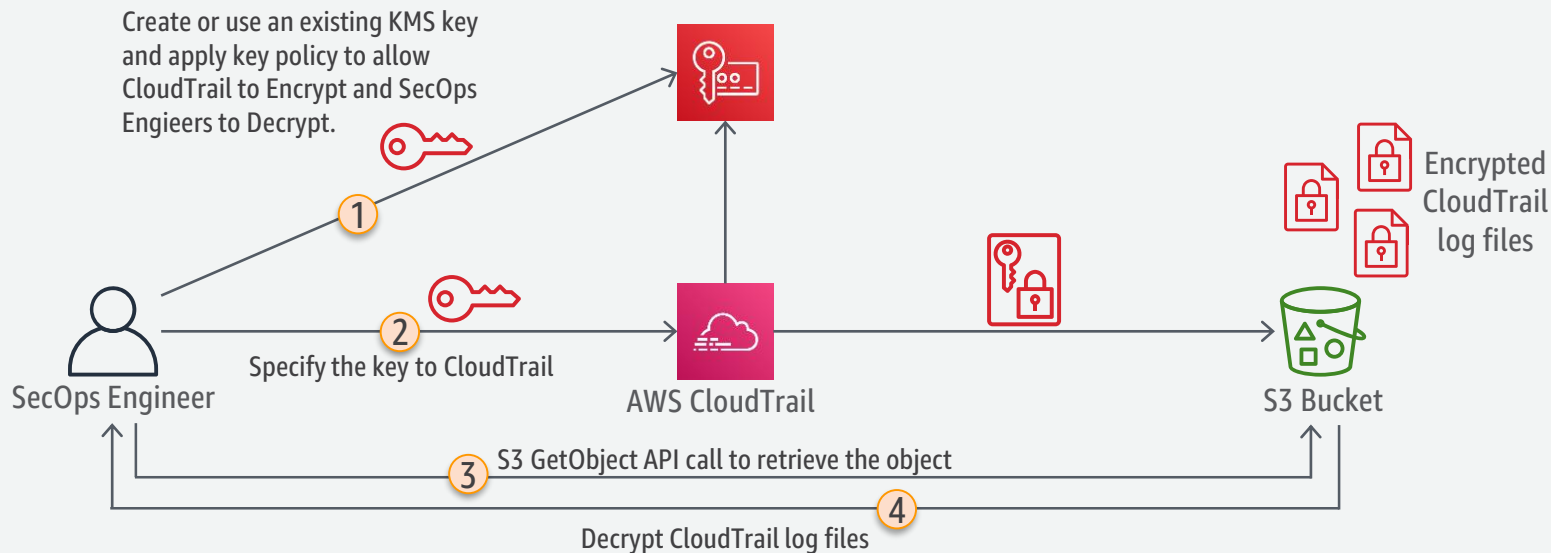
AWS CloudTrail – Storage in S3

- Default descriptive folder structure makes it easier to store log files from multiple accounts and regions in the same S3 bucket.

- Detailed log file name helps identify the contents of the log file

- Unique identifier in the file name prevents overwriting log files.

AWS CloudTrail – Lifecycle Management

AWS CloudTrail – Lifecycle Management

Configured via S3

 Available actions:

- Transition to different storage Tier

- Expire (delete) object

- Transition & Expire

AWS CloudTrail – Lifecycle Management

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

Transition to Amazon Glacier 30 days after creation date.

Expire 100 days after creation date.

Day 0 — Object Created — Day 10 — Lifecycle Policy takes effect — Object Transitioned to Amazon Glacier — Day 100 — Lifecycle Policy takes effect — Object Expired
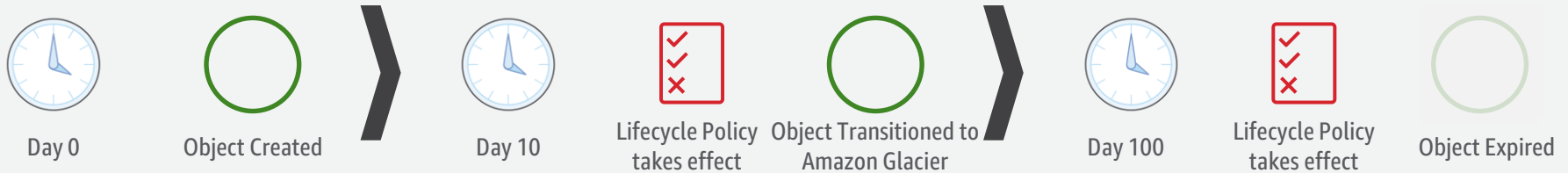
- The object was uploaded to the target bucket on 1-October. The creation date of this object is 1-October.
- On 30-October, 30 days after the object's creation date, the Lifecycle rule takes effect and automatically transitions the object to Amazon Glacier.
- On 9-January, 100 days after the object's creation date, the Lifecycle rule takes effect again and automatically expires the object. The object is now permanently deleted and cannot be recovered.

aws professional services

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 professional services

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 professional services

AWS CloudTrail – Best Practices

1. **Enable in all regions**

Benefits

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

aws professional services

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 professional services

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 professional services

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 professional services

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 professional services

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

aws professional services

Amazon VPC Flow Logs

- Stores log in AWS CloudWatch Logs
- Can be enabled on
  - Amazon VPC, a subnet, or a network interface
  - Amazon VPC & Subnet enables logging for all interfaces in the VPC/subnet
- Each network interface has a unique log stream
- Flow logs <u>do not capture real-time</u> 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?

aws professional services

Amazon VPC Flow Logs

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

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

AWS account   Interface   Source IP   Source port   Protocol   Packets   End time   Accept or reject

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 1442975655 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
```

Destination IP   Destination port   Bytes   Start time

aws professional services

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

aws professional services

Processing Logs – Elasticsearch with Kibana
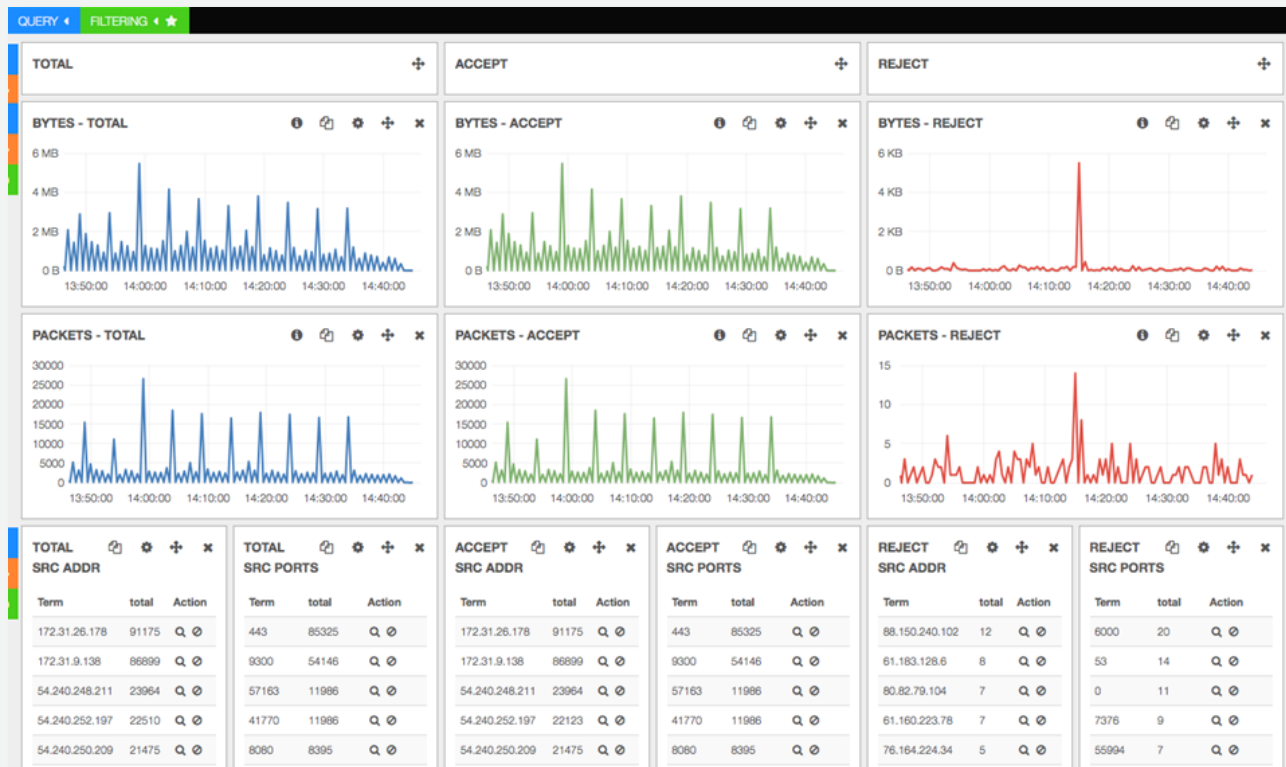
- Amazon Elasticsearch Service
- Amazon CloudWarch Logs Subscription

aws professional services

Processing Logs – Partner Solutions
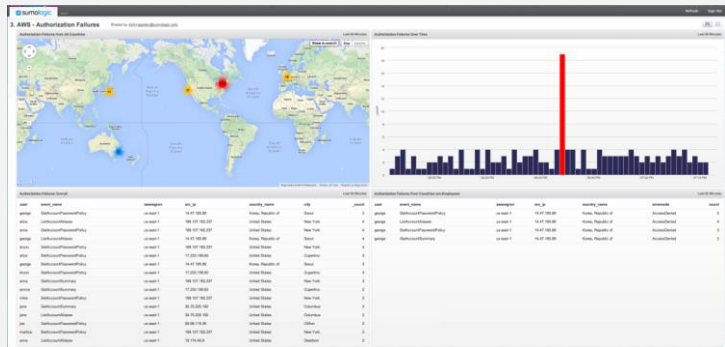
Alerting

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

EMAIL

HTTP
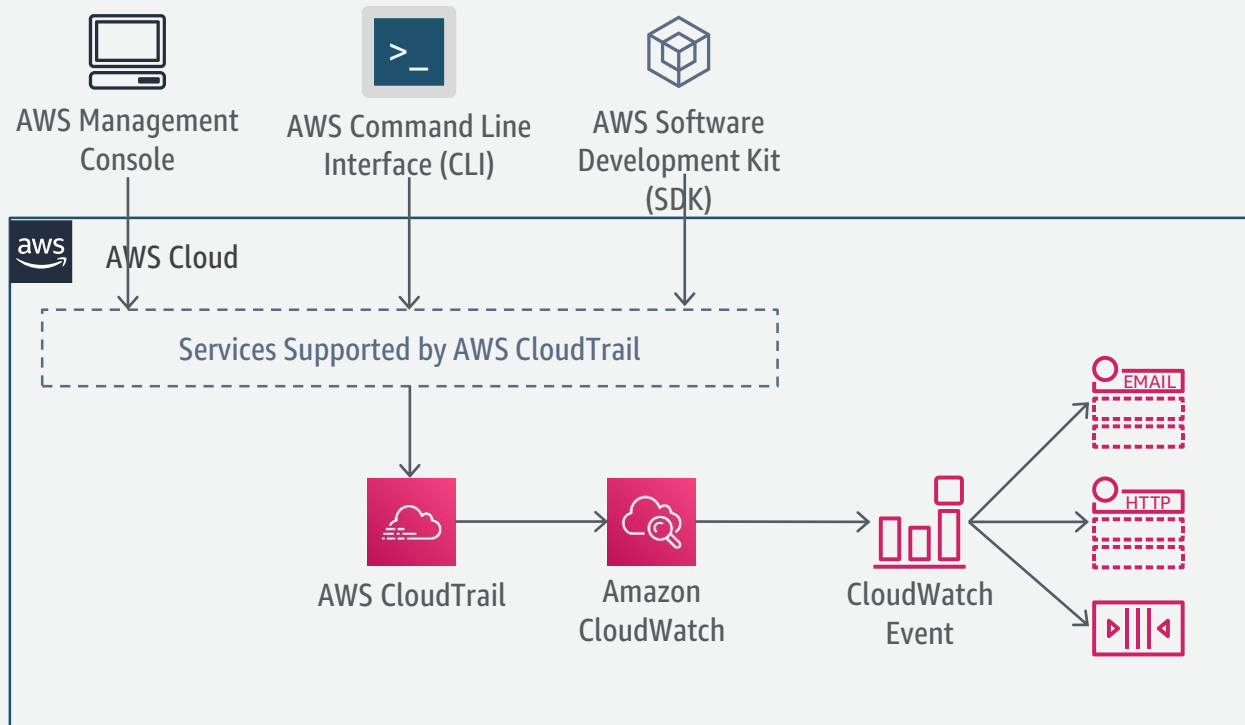
Follow-up Actions
- Create a Ticket
- Send an E-Mail
- Automatically Remediate
- Message somebody on Slack

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

aws professional services

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	Performance	Security	Fault Tolerance
0 ⓘ 5 ⚠ 3 ✅ 1 n/a	0 ⓘ 1 ⚠ 10 ✅ 0 n/a	2 ⓘ 6 ⚠ 7 ✅ 0 n/a	2 ⓘ 9 ⚠ 5 ✅ 0 n/a

Amazon GuardDuty

aws professional services

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

aws professional services

Amazon GuardDuty – Service Benefits

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

Amazon GuardDuty – Data Sources

VPC Flow Logs

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

DNS Logs

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

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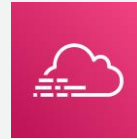
- CloudTrail history of AWS API calls used to access the Management Console, SDKs , CLI, etc. presented by GuardDuty.
- Identification of user and account activity including source IP address used to make the calls.

aws professional services

Amazon GuardDuty – Findings

Amazon GuardDuty – Threat Detection

Threat Detection Types Data Sources Findings Respond

Reconnaissance

Instance Compromise

Account Compromise

AWS Cloud

VPC Flow Logs

DNS Logs

AWS CloudTrail

Amazon GuardDuty

HIGH
MEDIUM
LOW

CloudWatch Event

aws professional services

AWS Security Hub

aws professional services
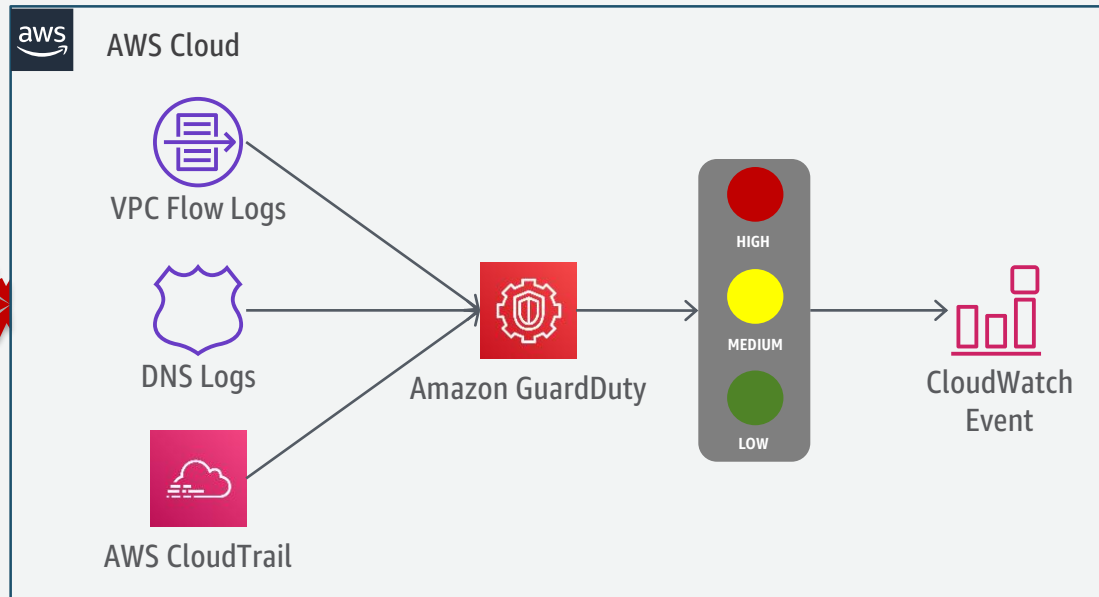
AWS Security Hub

AWS Security Services OR Partner solutions

AWS Security Hub

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

Amazon CloudWatch

CloudWatch Event

Target options

| Detect | Aggregate | Report | Take Action |
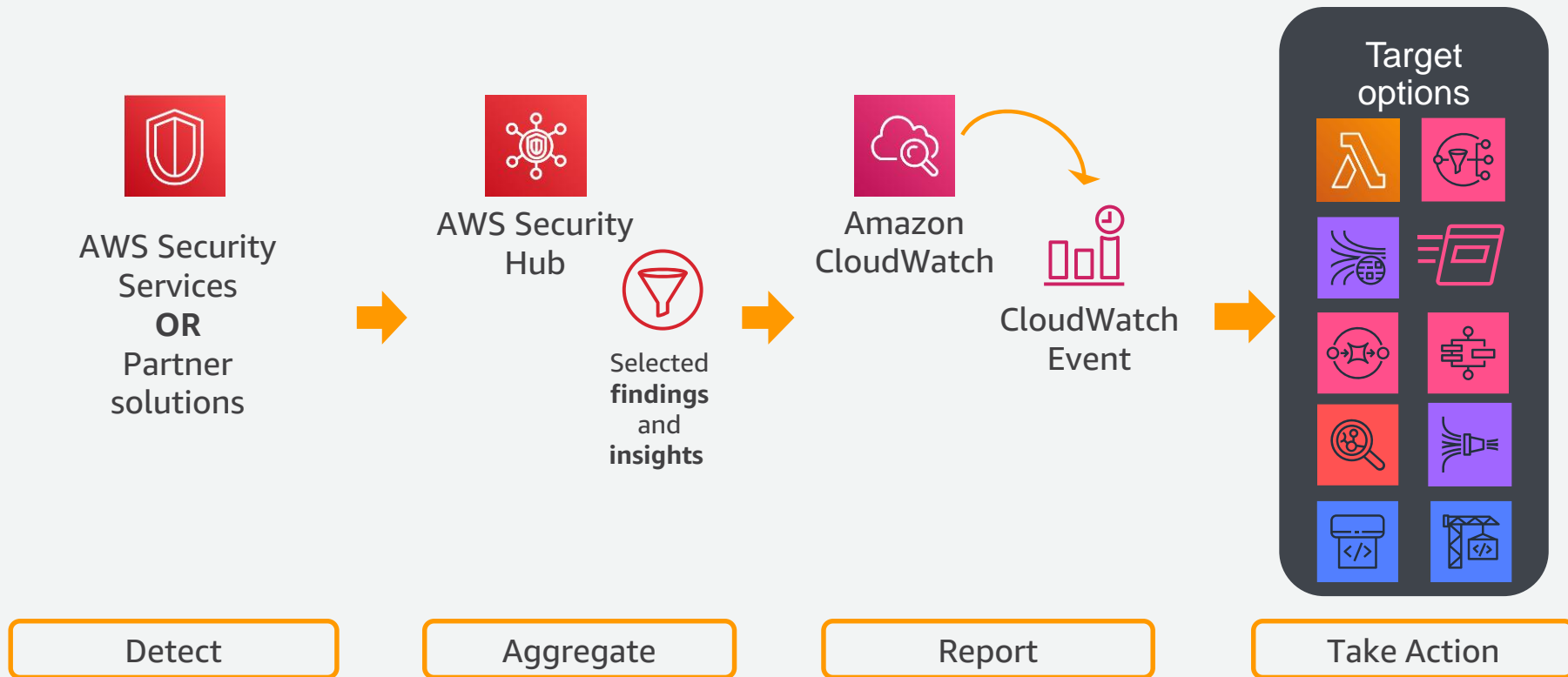
AWS Security Hub - Benefits

Compliance standards

Aggregated findings

Insights

aws professional services

AWS Security Hub - Automated compliance checks

43 fully automated, nearly continuous checks
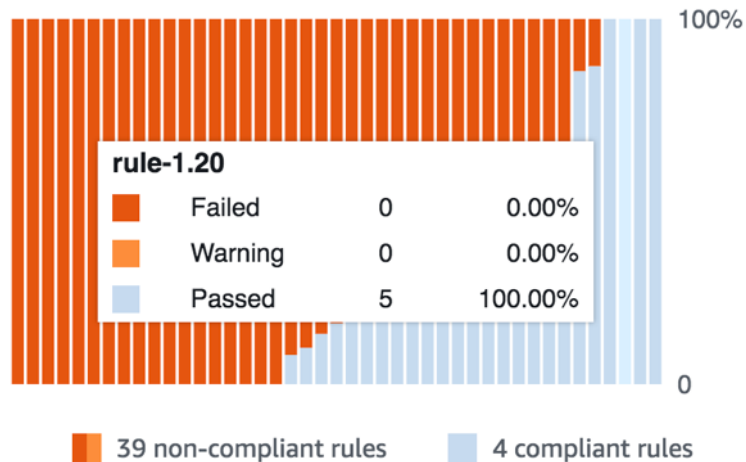
AWS Security Hub – Compliance Standards

CIS AWS Foundations rules
AWS Security Hub conducts 43 automated checks against the CIS AWS Foundations Benchmark rules.

🔍 Filter rules

< 1 2 3 >

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

Custom Actions in Security Hub

Custom Actions in Security Hub
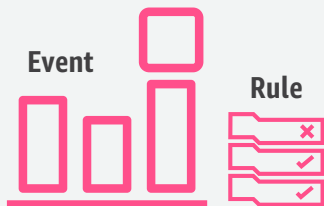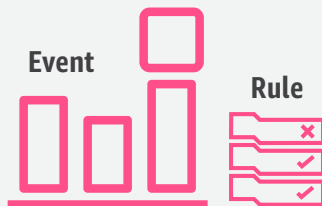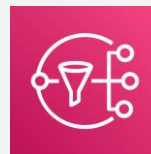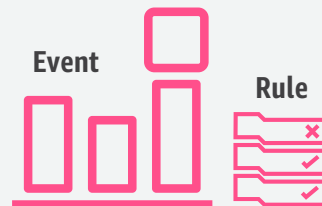
Accounts   **Custom actions**   **Usage**   **General**

Custom actions

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

Delete   **Create 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

aws professional services

Auditing – IAM Credential Report

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.
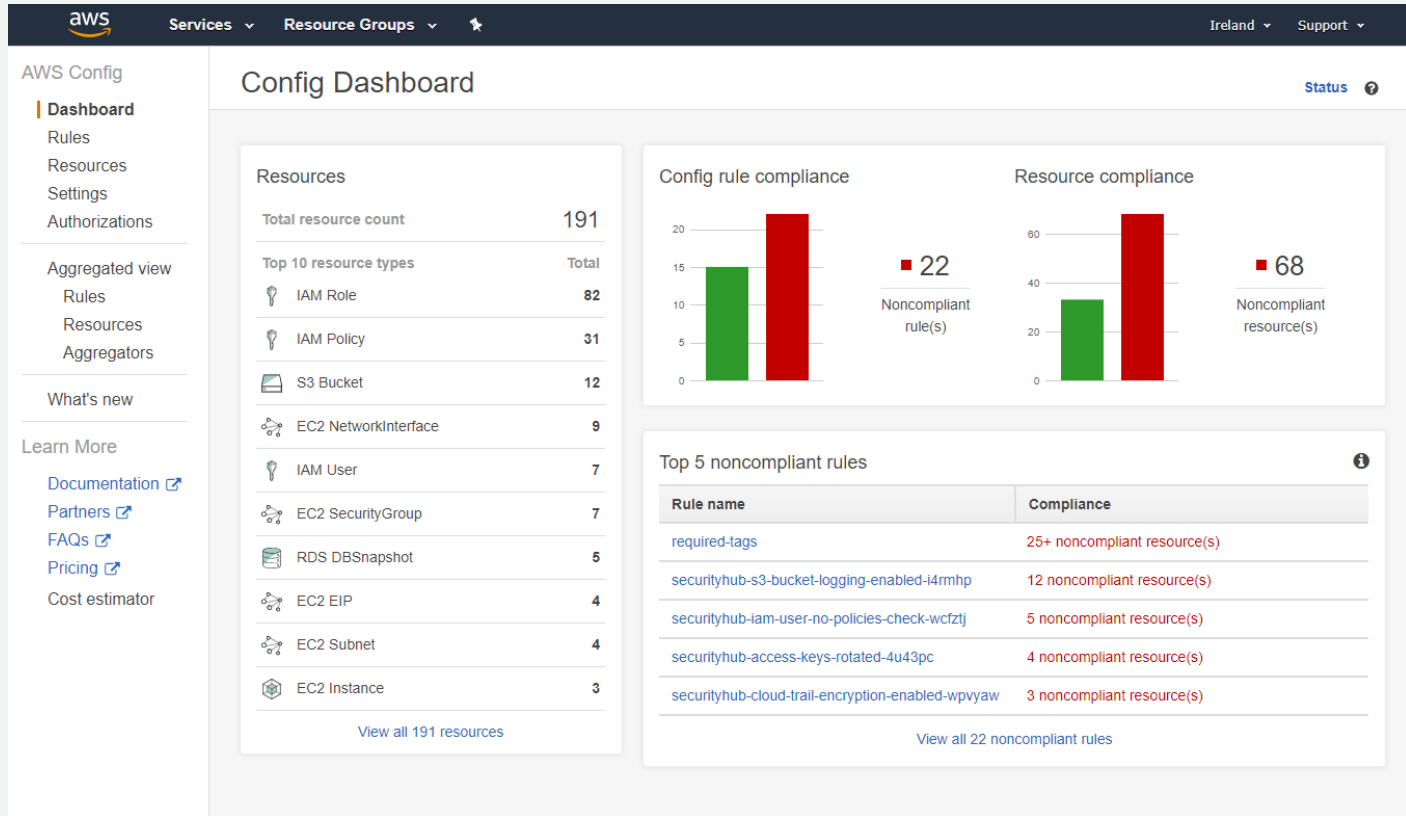
AWS Config APIs & Console

Amazon SNS

Amazon CloudWatch

Amazon S3

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.

aws professional services

Auditing – AWS Config

Auditing – AWS Config

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

aws professional services

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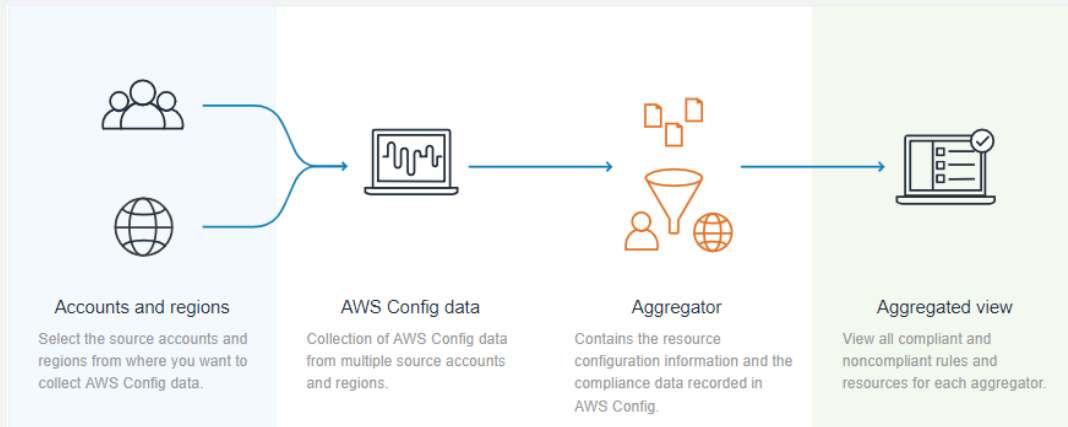
cloudformation-stack-drift-detection-c...

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?

aws professional services