Threat Detection

Mukhtar Kabir, CISSP

Associate Solutions Architect
Amazon Web Services

08-26-2021

AWS Security Hub

What is AWS Security Hub?

AWS Security Hub gives you a comprehensive view of your high-priority security alerts and security posture across your AWS accounts.

It provides a single place for aggregating, organizing, and prioritizing security alerts or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS IAM Access Analyzer, AWS Firewall Manager, as well as from AWS Partner solutions.

Key benefits of Security Hub?

- Reduces effort in collecting and prioritizing security findings across accounts, AWS services, and AWS partner tools.

- Improve security by running automated, continuous security checks based on industry standards and best practices, such as the Center for Internet Security (CIS) AWS Foundations Benchmark and Payment Card Industry Data Security Standard (PCI DSS).

- Quickly take actions with integrated dashboards that shows you the current security and compliance status.

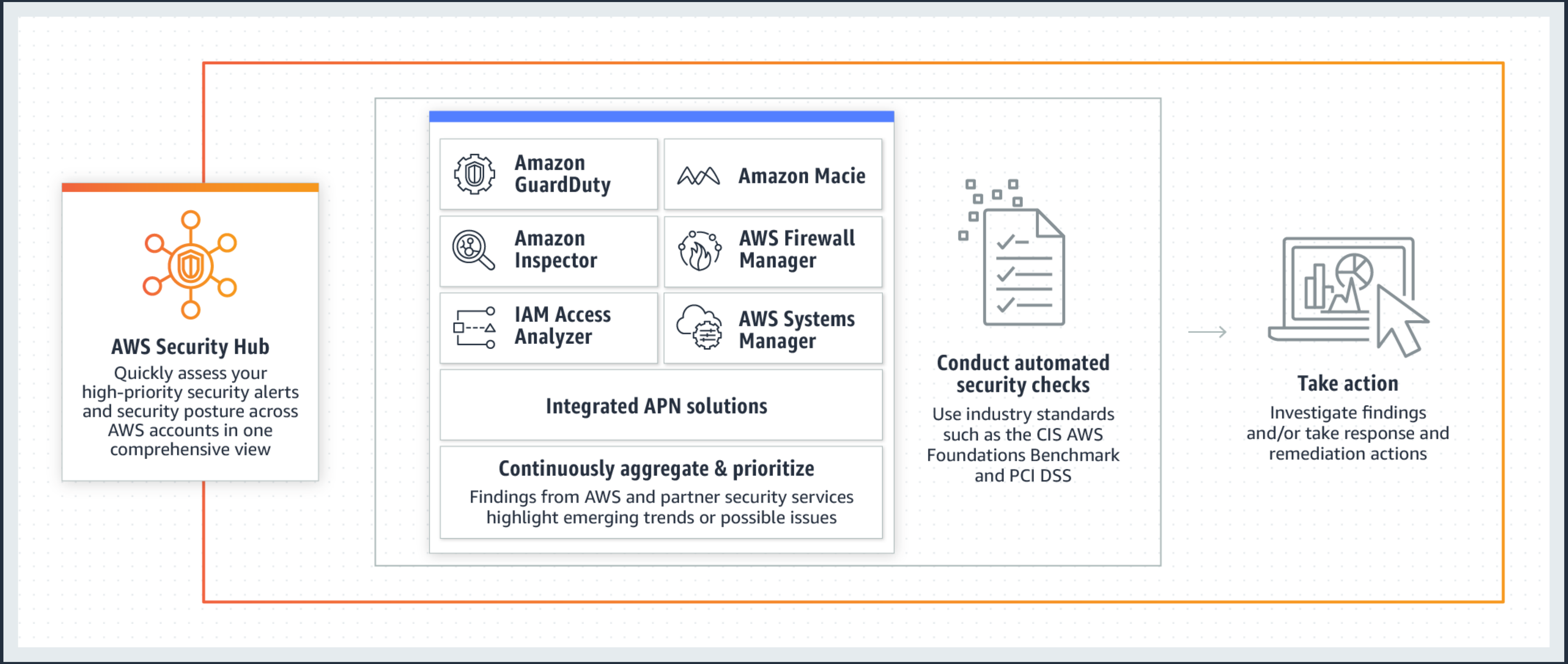
- Integration with EventBridge for custom actions or building remediation workflows

What’s new - Recent updates

- Security Hub now offers integrations with Caveonix Cloud and Forcepoint Cloud Security Gateway. Both integrations send findings to Security Hub – August 10, 2021.

- Added new controls for Amazon API Gateway (APIGateway.5), Amazon EC2 (EC2.19), Amazon ECS (ECS.2), Elastic Load Balancing (ELB.7), Amazon Elasticsearch Service (ES.5 through ES.8), Amazon RDS (RDS.16 through RDS.23), Amazon Redshift (Redshift.4), and Amazon SQS (SQS.1) – July 20, 2021.

How Security Hub works



AWS Security Hub

Quickly assess your high-priority security alerts and security posture across AWS accounts in one comprehensive view

Amazon GuardDuty

Amazon Macie

Amazon Inspector

AWS Firewall Manager

IAM Access Analyzer

AWS Systems Manager

Integrated APN solutions

Continuously aggregate & prioritize

Findings from AWS and partner security services highlight emerging trends or possible issues

Conduct automated security checks

Use industry standards such as the CIS AWS Foundations Benchmark and PCI DSS

Take action

Investigate findings and/or take response and remediation actions

Security Hub Terminologies

- Insights: A collection of related findings.

- Custom Actions: A Security Hub mechanism for sending selected findings to EventBridge.

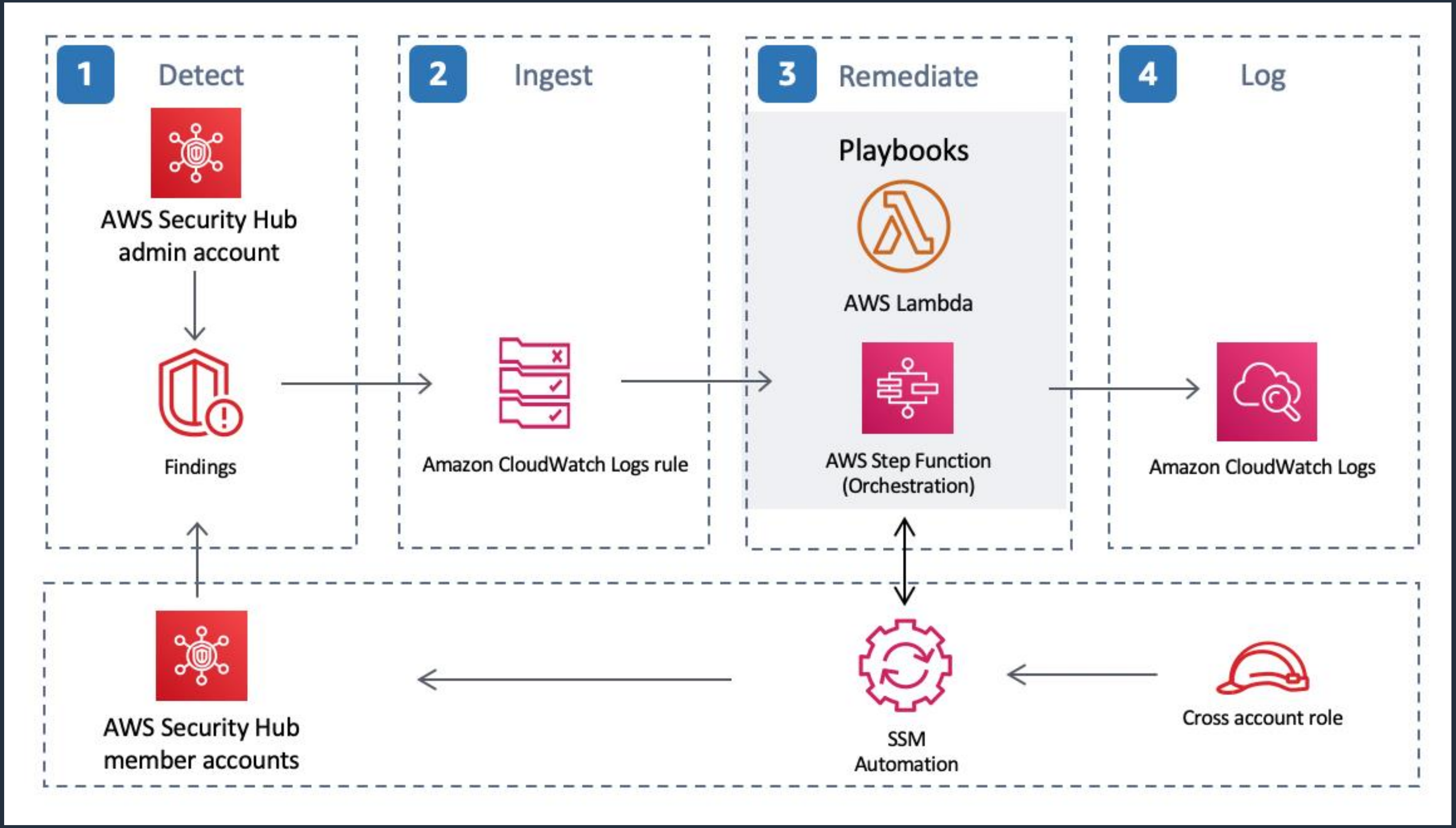
- AWS Security Finding Format (ASFF): A standardized format for the contents of findings that Security Hub aggregates or generates.

- Severity Labels: Information, Low, Medium, High and Critical.

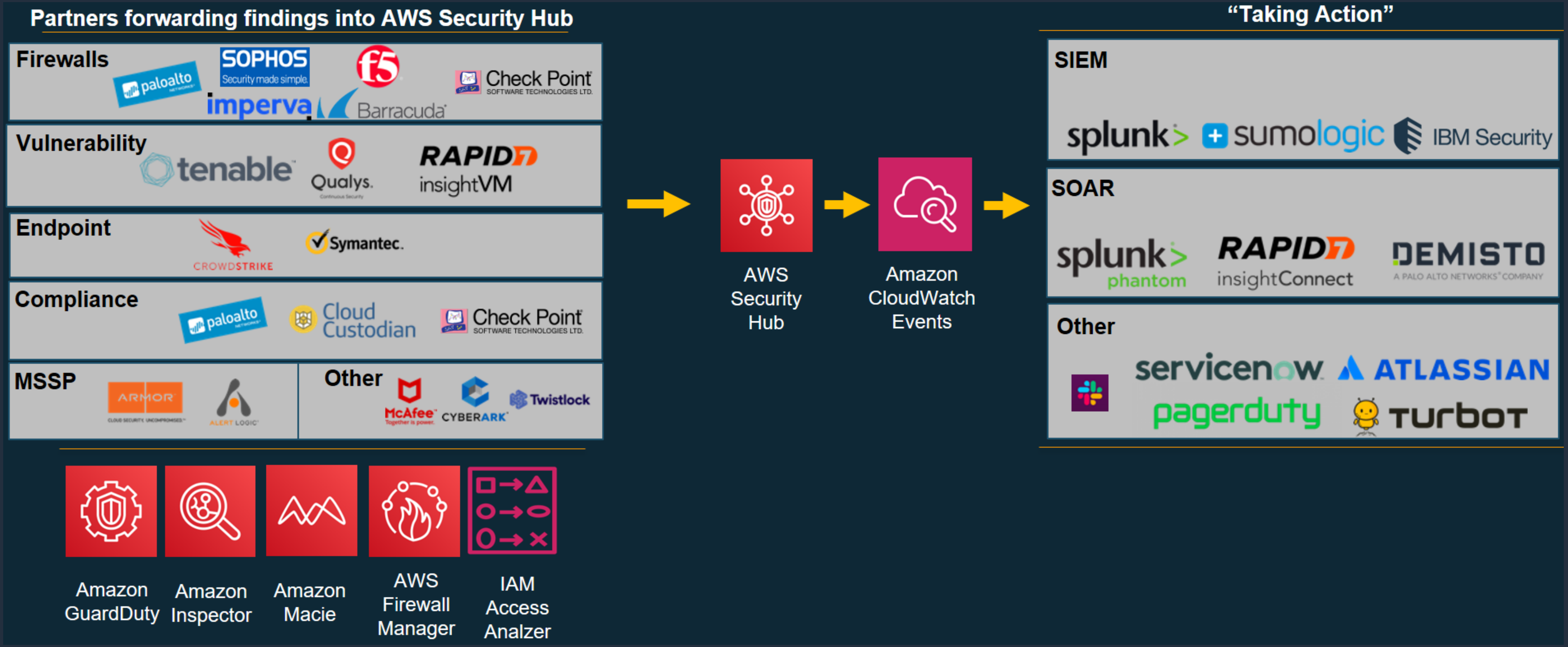
Security Hub Standards

- CIS AWS Foundations
- Payment Card Industry Data Security Standard (PCI DSS)
- AWS Foundational Security Best Practices

Sample Architecture


1
Detect
AWS Security Hub admin account
Findings
2
Ingest
Amazon CloudWatch Logs rule
3
Remediate
Playbooks
AWS Lambda
AWS Step Function (Orchestration)
4
Log
Amazon CloudWatch Logs
AWS Security Hub member accounts
SSM Automation
Cross account role

Partners



Partners forwarding findings into AWS Security Hub

Firewalls
paloalto NETWORKS
SOPHOS Security made simple.
f5
Check Point SOFTWARE TECHNOLOGIES LTD.
imperva
Barracuda

Vulnerability
tenable
Qualys.
RAPID7 insightVM

Endpoint
CROWDSTRIKE
Symantec.

Compliance
paloalto NETWORKS
Cloud Custodian
Check Point SOFTWARE TECHNOLOGIES LTD.

MSSP
ARMOR CLOUD SECURITY. UNCOMPROMISED.
ALERT LOGIC

Other
McAfee Together is power.
CYBERARK
Twistlock

Amazon GuardDuty

Amazon Inspector

Amazon Macie

AWS Firewall Manager

IAM Access Analzer

AWS Security Hub

Amazon CloudWatch Events

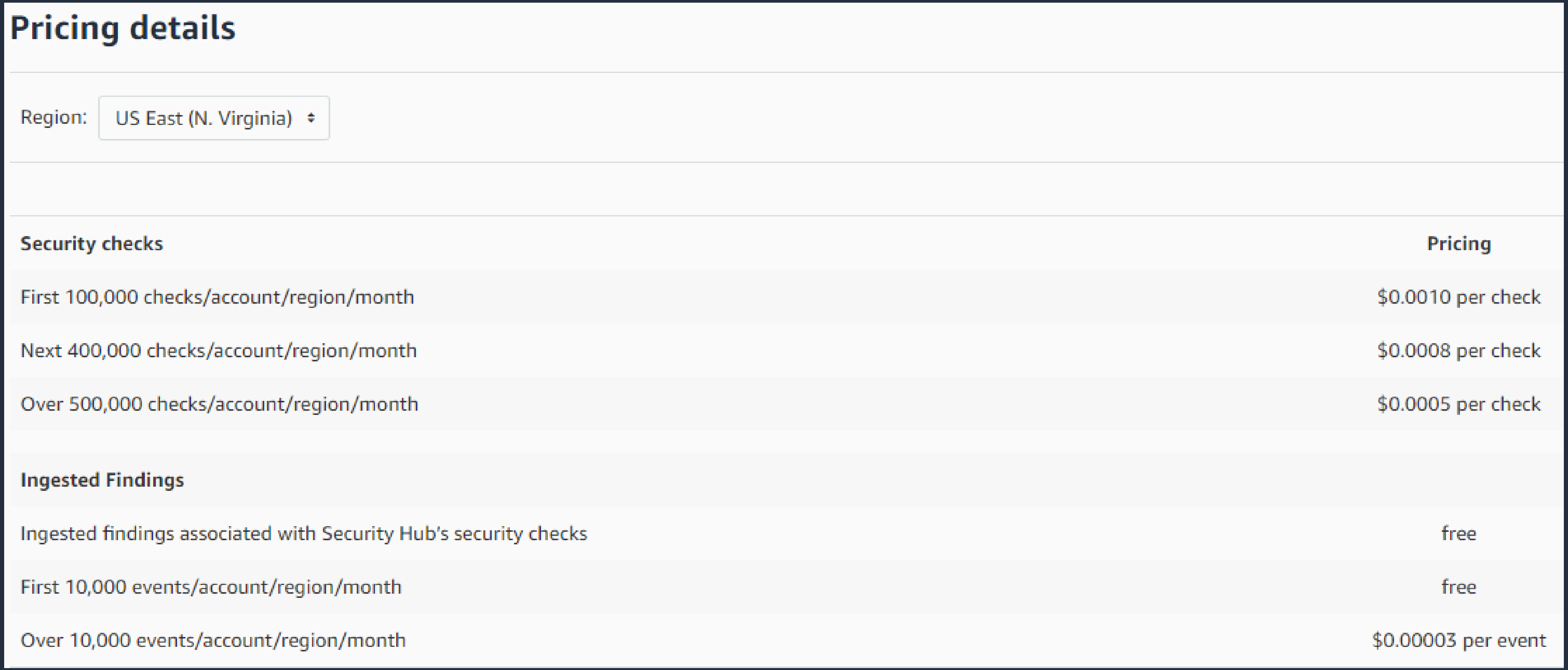
"Taking Action"

SIEM
splunk>
sumologic
IBM Security

SOAR
splunk> phantom
RAPID7 insightConnect
DEMISTO A PALO ALTO NETWORKS COMPANY

Other
servicenow
ATLASSIAN
pagerduty
turbot

Pricing



Pricing details

Region: US East (N. Virginia)

Security checks	Pricing
First 100,000 checks/account/region/month	$0.0010 per check
Next 400,000 checks/account/region/month	$0.0008 per check
Over 500,000 checks/account/region/month	$0.0005 per check
Ingested Findings	
Ingested findings associated with Security Hub's security checks	free
First 10,000 events/account/region/month	free
Over 10,000 events/account/region/month	$0.00003 per event

Key Takeaways

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

Security Hub Best Practices

- Enable in all regions using the provided lambda scripts
- Principles of least privilege: Use IAM policies
- Enable AWS Config in all AWS accounts and regions
- Leave the AWS CIS Foundations standard check enabled
- Communicate findings e.g. Send high severity to Sec Team
- Integrate with third party tools you may already be using
- Take action: Automate via Lambda or notify via SNS
- Add findings procedures to your runbook

Amazon GuardDuty

What is Amazon GuardDuty?

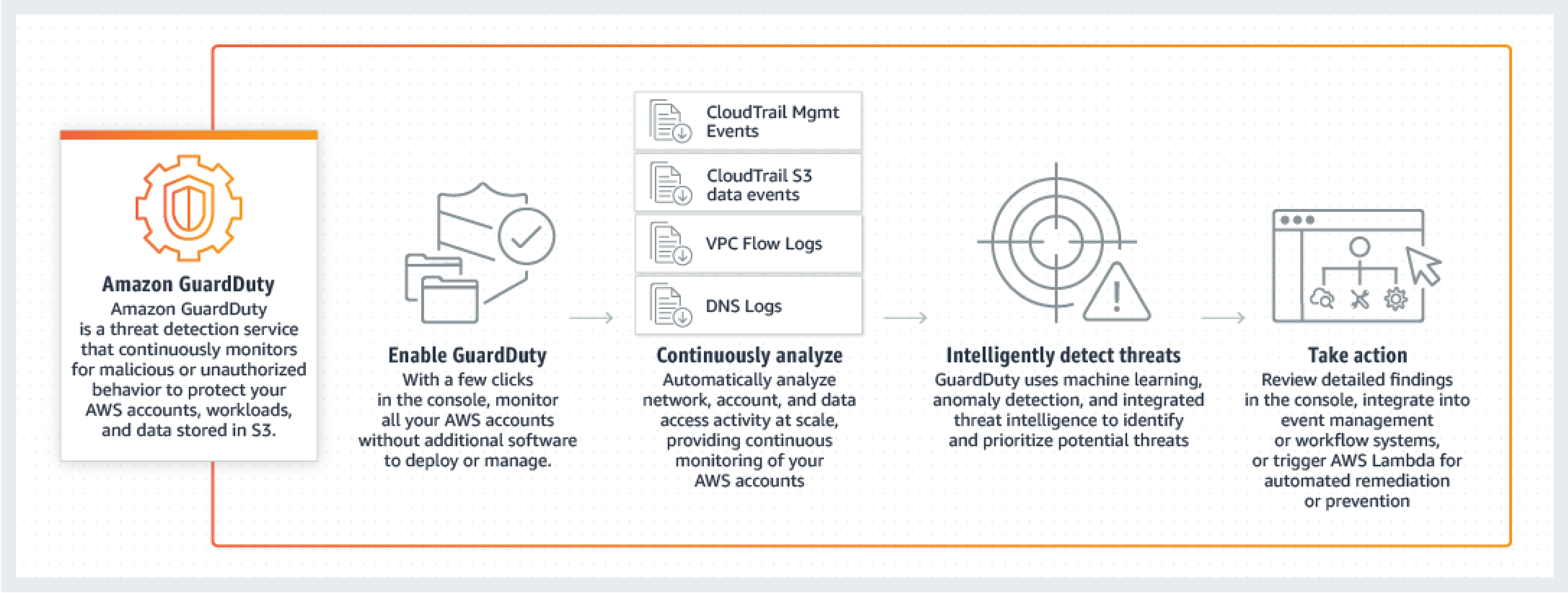
Amazon GuardDuty is a threat detection service that provides you with a more accurate and easy way to continuously monitor and protect your AWS accounts and workloads.

With just a few clicks, GuardDuty analyzes events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs.

Key benefits of GuardDuty?

- Continuous monitoring and threat detection
- Broad Coverage - Account compromise, user behavior
- Security at scale – No resources to manage
- Severity levels for easy prioritization
- Intelligence feeds from AWS, CrowdStrike, and Proofpoint.
- GuardDuty API available for developers

How GuardDuty works



Amazon GuardDuty
Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to protect your AWS accounts, workloads, and data stored in S3.

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

- CloudTrail Mgmt Events
- CloudTrail S3 data events
- VPC Flow Logs
- DNS Logs

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

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

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

GuardDuty Finding Types

- A finding is a notification that contains the details about a potential security issue
- Currently 70+ finding types and counting
- Finding types are divided into 12 categories e.g. Backdoor, Behavior, CryptoCurrency, Policy finding types etc.

Backdoor Finding Types:

- Backdoor:EC2/Spambot: EC2 might be compromised and sending out spam

Behavior Finding Types

- Behavior:EC2/NetworkPortUnusual: EC2 is sending large traffic to remote host on an unusual port

CryptoCurrency Finding Types:

- CryptoCurrency:EC2/BitcoinTool.B!DNS: EC2 is querying a domain name that is associated with Bitcoin

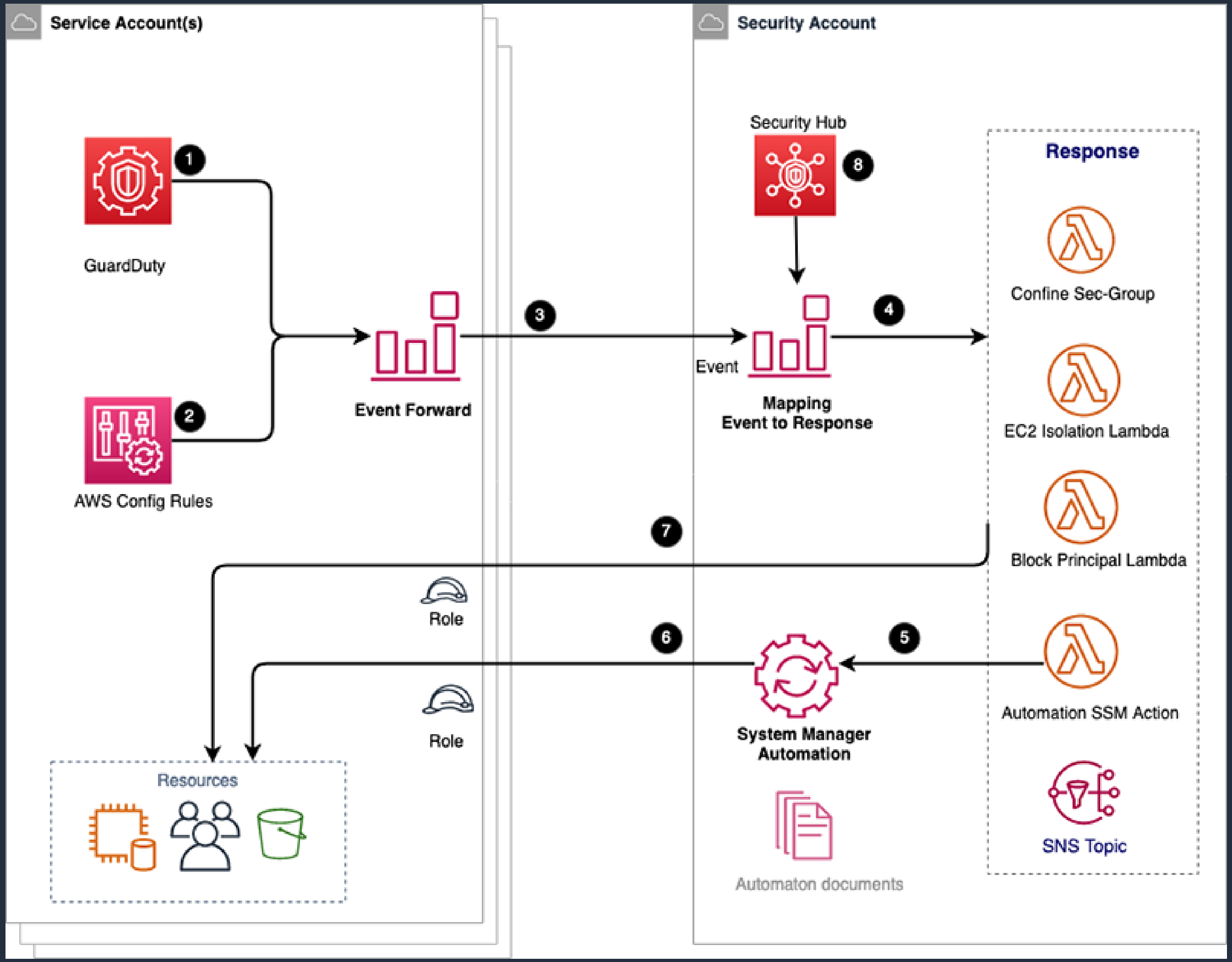
Policy Finding Types:

- Policy:S3/BlockPublicAccessDisabled: S3 block public access was disabled for an S3 bucket.

Severity Levels

- Values 0 and 9.0 to 10.0 - Reserved for future use
- High (7.0 to 8.9): E.g. EC2 Compromise
- Medium (4.0 to 6.9): E.g. Unusual activity by our EC2
- Low (1.0 to 3.9): E.g. A port scan

Sample Architecture

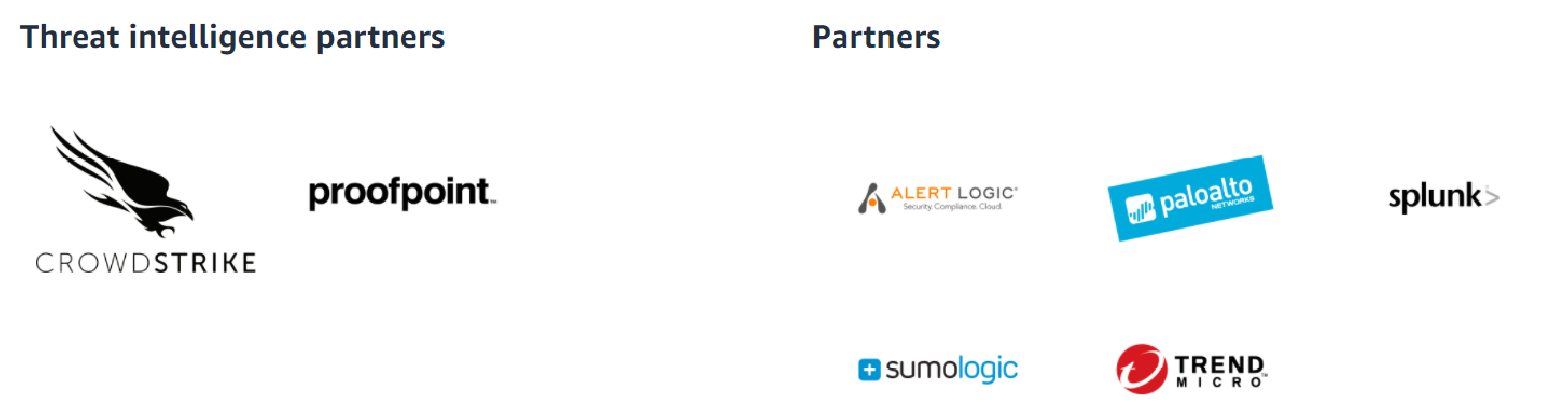


What’s new - Recent updates 2021

- New machine learning techniques - discerning potentially malicious user activity from anomalous, but benign operational behavior.

- Integration with Amazon Detective - jump from a GuardDuty security finding into a pre-populated Amazon Detective investigation experience.

Partners



Threat intelligence partners

Partners

Pricing

AWS CloudTrail Management Event Analysis	
Per 1 million events / month	$4.00 per 1 million events

AWS CloudTrail S3 Data Event Analysis	
First 500 million events / month	$0.80 per 1 million events

VPC Flow Log and DNS Log Analysis	
First 500 GB / month	$1.00 per GB

Guard Duty Best Practices!

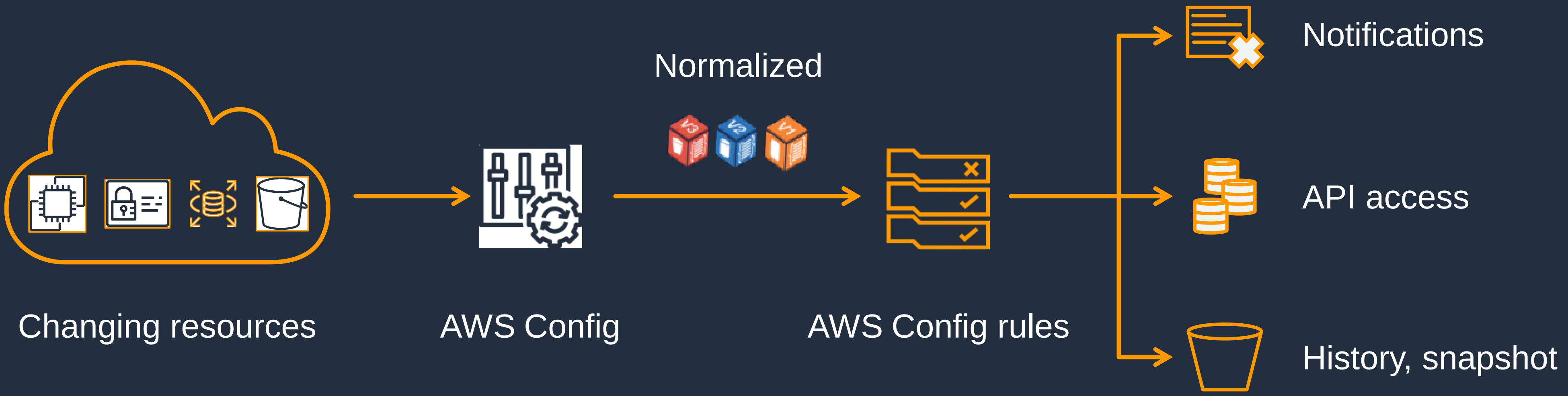
- Enable in all regions
- Principles of least privilege: Use IAM policies.
- Communicate findings e.g. Send high severity to Sec Team
- Take action: Automate via Lambda or notify via SNS
- Integrate with third party tools you may already be using
- Add findings procedures to your runbook

AWS Config

AWS Config

- ✓ Native, agent-less AWS capability to discover resources in your account
- ✓ Tracks configuration changes and maintains a history (up to 7 years)
- ✓ Evaluates configuration changes against compliance policies (using AWS Config rules)
- ✓ Provides aggregated view of resource configuration and compliance status across accounts and regions
- ✓ Integrates with AWS Security Hub and AWS Audit Manager
- ✓ Integrates with your own ITSM/CMDBs (such as ServiceNow, Jira Service Desk)

AWS Config = Continuous Configuration Auditor



Benefits

Continuous monitoring

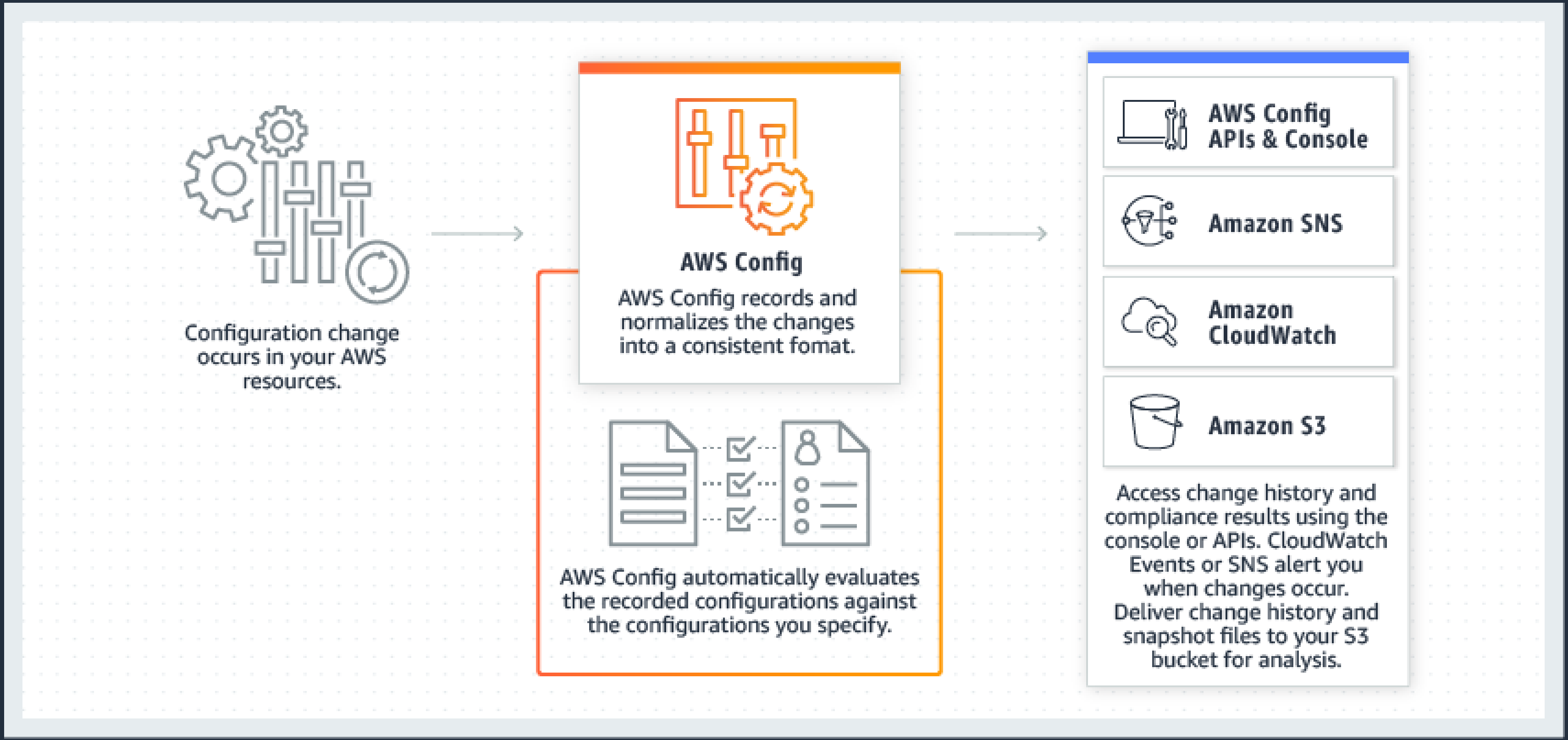
Continuous assessment

Change management

Operational troubleshooting

Enterprise-wide compliance monitoring including third-party resources

How it works



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 Config features

Resource relationship tracking

Discovers, maps, and tracks AWS resource relationships in your account

Conformance packs

Packages a collection of AWS Config rules and remediation actions into a single entity and deploy it in a single account or across an entire organization.

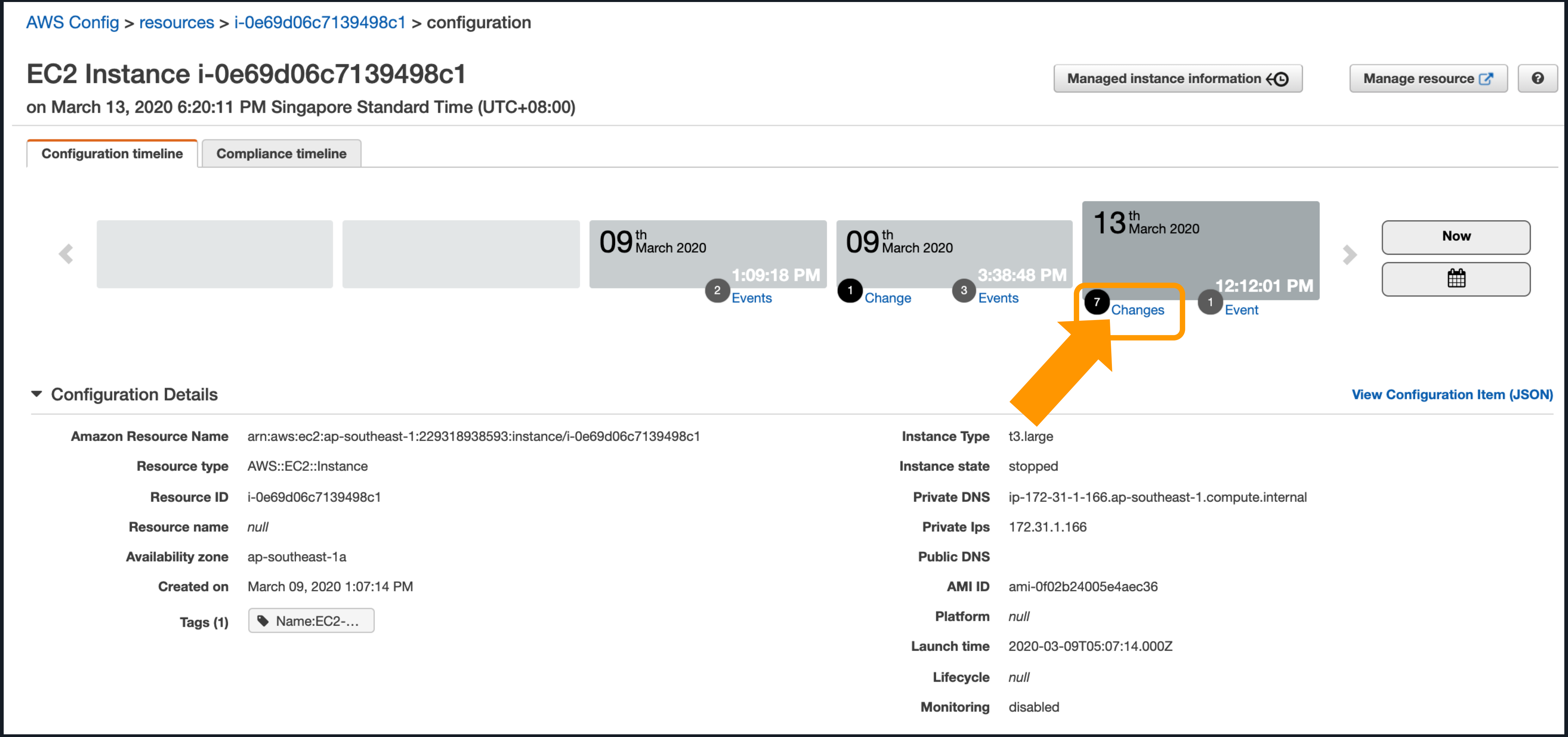
Multi-account, multi-region data aggregation

Enables centralized auditing and governance by providing an enterprise-wide view of your resources and Config rule compliance status

Cloud governance dashboard

Provides a visual dashboard to help you quickly spot non-compliant resources and take appropriate action

Resource Timeline



AWS Config > resources > i-0e69d06c7139498c1 > configuration

EC2 Instance i-0e69d06c7139498c1

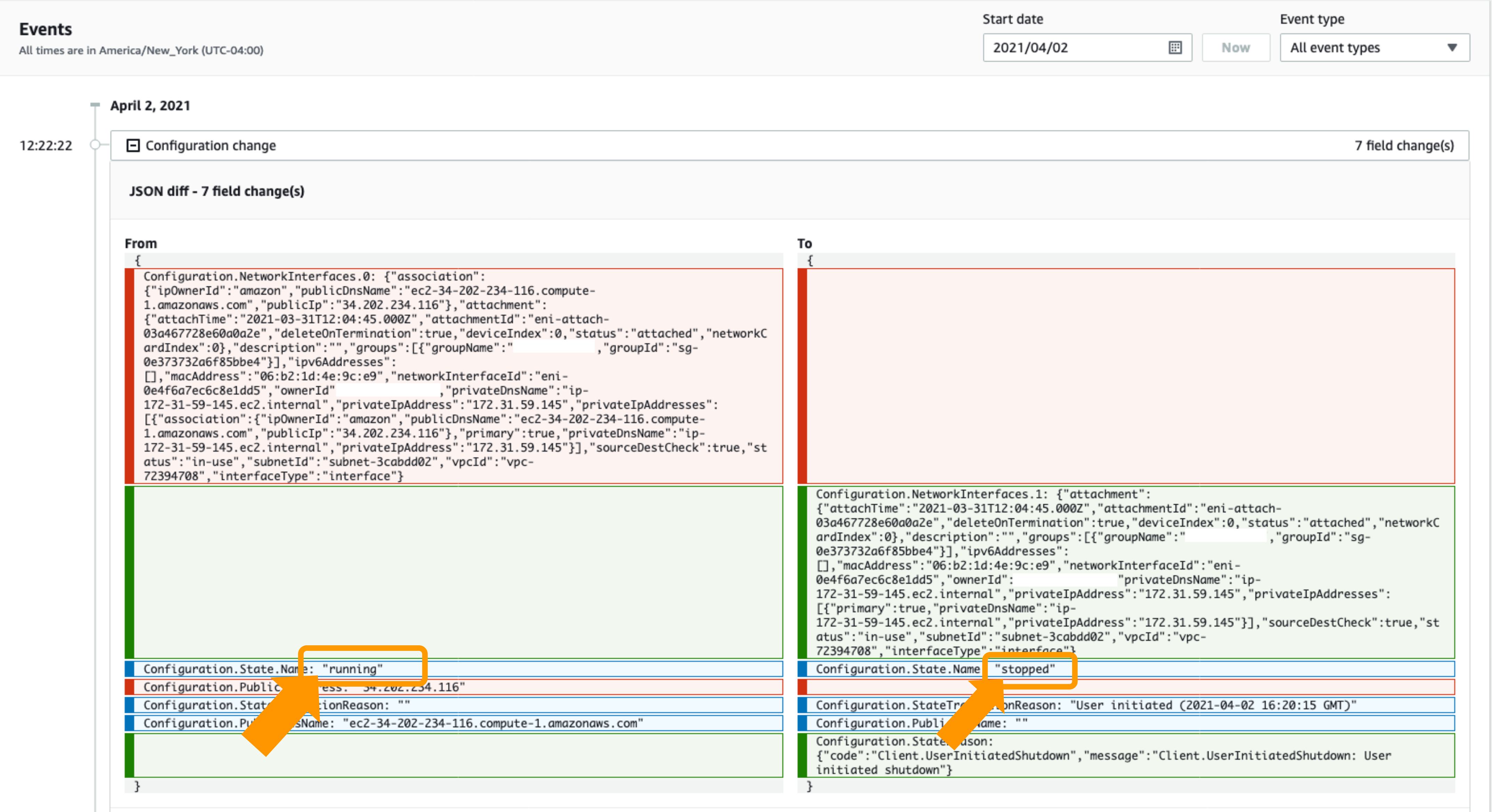
on March 13, 2020 6:20:11 PM Singapore Standard Time (UTC+08:00)

Configuration Details

View Configuration Item (JSON)

Amazon Resource Name	arn:aws:ec2:ap-southeast-1:229318938593:instance/i-0e69d06c7139498c1	Instance Type	t3.large
Resource type	AWS::EC2::Instance	Instance state	stopped
Resource ID	i-0e69d06c7139498c1	Private DNS	ip-172-31-1-166.ap-southeast-1.compute.internal
Resource name	*null*	Private Ips	172.31.1.166
Availability zone	ap-southeast-1a	Public DNS	
Created on	March 09, 2020 1:07:14 PM	AMI ID	ami-0f02b24005e4aec36
Tags (1)	Name:EC2-...	Platform	*null*
		Launch time	2020-03-09T05:07:14.000Z
		Lifecycle	*null*
		Monitoring	disabled

Configuration Changes



Events

All times are in America/New_York (UTC-04:00)

Start date: 2021/04/02

Event type: All event types

April 2, 2021

12:22:22 Configuration change — 7 field change(s)

JSON diff - 7 field change(s)

From

```
{
Configuration.NetworkInterfaces.0: {"association":
{"ipOwnerId":"amazon","publicDnsName":"ec2-34-202-234-116.compute-
1.amazonaws.com","publicIp":"34.202.234.116"},"attachment":
{"attachTime":"2021-03-31T12:04:45.000Z","attachmentId":"eni-attach-
03a467728e60a0a2e","deleteOnTermination":true,"deviceIndex":0,"status":"attached","networkC
ardIndex":0},"description":"","groups":[{"groupName":"[redacted],"groupId":"sg-
0e373732a6f85bbe4"}],"ipv6Addresses":
[],"macAddress":"06:b2:1d:4e:9c:e9","networkInterfaceId":"eni-
0e4f6a7ec6c8e1dd5","ownerId"[redacted],"privateDnsName":"ip-
172-31-59-145.ec2.internal","privateIpAddress":"172.31.59.145","privateIpAddresses":
[{"association":{"ipOwnerId":"amazon","publicDnsName":"ec2-34-202-234-116.compute-
1.amazonaws.com","publicIp":"34.202.234.116"},"primary":true,"privateDnsName":"ip-
172-31-59-145.ec2.internal","privateIpAddress":"172.31.59.145"}],"sourceDestCheck":true,"st
atus":"in-use","subnetId":"subnet-3cabdd02","vpcId":"vpc-
72394708","interfaceType":"interface"}
Configuration.State.Na e: "running"
Configuration.Public    ess:  34.202.234.116"
Configuration.Stat    ionReason: ""
Configuration.Pu     sName: "ec2-34-202-234-116.compute-1.amazonaws.com"
}
```

To

```
{
Configuration.NetworkInterfaces.1: {"attachment":
{"attachTime":"2021-03-31T12:04:45.000Z","attachmentId":"eni-attach-
03a467728e60a0a2e","deleteOnTermination":true,"deviceIndex":0,"status":"attached","networkC
ardIndex":0},"description":"","groups":[{"groupName":"[redacted],"groupId":"sg-
0e373732a6f85bbe4"}],"ipv6Addresses":
[],"macAddress":"06:b2:1d:4e:9c:e9","networkInterfaceId":"eni-
0e4f6a7ec6c8e1dd5","ownerId":[redacted]"privateDnsName":"ip-
172-31-59-145.ec2.internal","privateIpAddress":"172.31.59.145","privateIpAddresses":
[{"primary":true,"privateDnsName":"ip-
172-31-59-145.ec2.internal","privateIpAddress":"172.31.59.145"}],"sourceDestCheck":true,"st
atus":"in-use","subnetId":"subnet-3cabdd02","vpcId":"vpc-
72394708","interfaceType":"interface"}
Configuration.State.Name  "stopped"

Configuration.StateTr    onReason: "User initiated (2021-04-02 16:20:15 GMT)"
Configuration.Publi    ame: ""
Configuration.State   ason:
{"code":"Client.UserInitiatedShutdown","message":"Client.UserInitiatedShutdown: User
initiated shutdown"}
}
```

Pricing

AWS Config rules evaluations	Price
First 100,000 rule evaluations	$0.001 per rule evaluation per region
Next 400,000 rule evaluations (100,001-500,000)	$0.0008 per rule evaluation per region
500,001 and more rule evaluations	$0.0005 per rule evaluation per region

Conformance pack evaluations	Price
First 1,000,000 conformance pack evaluations	$0.0012 per conformance pack evaluation per Region
1,000,001- 25,000,000 conformance pack evaluations	$0.001 per conformance pack evaluation per Region
25,000,001 and more	$0.0008 per conformance pack evaluation per Region

AWS Config Best Practices!

- Enable AWS Config in all accounts and Regions.
- Principles of least privilege: Use IAM policies.
- Select “All resources” when setting up the service
- Record global resources (such as IAM resources) only in one Region.
- Turn on periodic snapshots with a minimum frequency of once per day.

Thank you!