



Threat detection and incident response using cloud-native services



Dzung Le
Solutions Architect
CMC Telecom

Agenda

The incident response lifecycle

Let's look into the phases

- Preparation
- Detection
- Triage – Collection and containment
- Remediation, recovery, and post-incident activity

Summary and conclusion

Incident response lifecycle



Preparation



Configure core services



Identity and access management

AWS Identity and Access Management (IAM)
AWS Single Sign-On
AWS Organizations
AWS Directory Service
Amazon Cognito
AWS Resource Access Manager



Threat detection

AWS Security Hub
Amazon GuardDuty
Amazon Inspector
Amazon CloudWatch
AWS Config
AWS CloudTrail
VPC Flow Logs
AWS IoT Device Defender



Infrastructure protection

AWS Firewall Manager
AWS Network Firewall
AWS Shield
AWS WAF
Amazon VPC
AWS PrivateLink
AWS Systems Manager



Data protection

Amazon Macie
AWS Key Management Service (KMS)
AWS CloudHSM
AWS Certificate Manager
AWS Secrets Manager
AWS VPN
Server-Side Encryption



Incident response

Amazon Detective
Amazon EventBridge
AWS Backup
AWS Security Hub
AWS Elastic Disaster Recovery



Governance

AWS Artifact
AWS Audit Manager
Amazon CloudWatch
AWS CloudTrail
AWS Config
AWS Security Hub
AWS Systems Manager

Detection

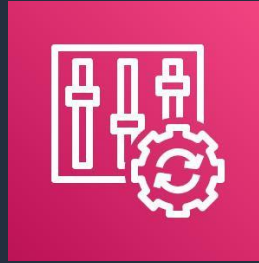


Detection using AWS services



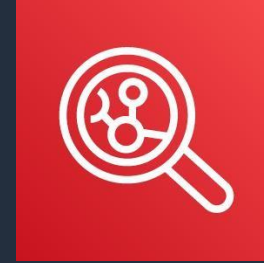
GuardDuty

Analyze log data
for anomalies and
malicious behavior



AWS Config

Check configuration
status and rule
compliance

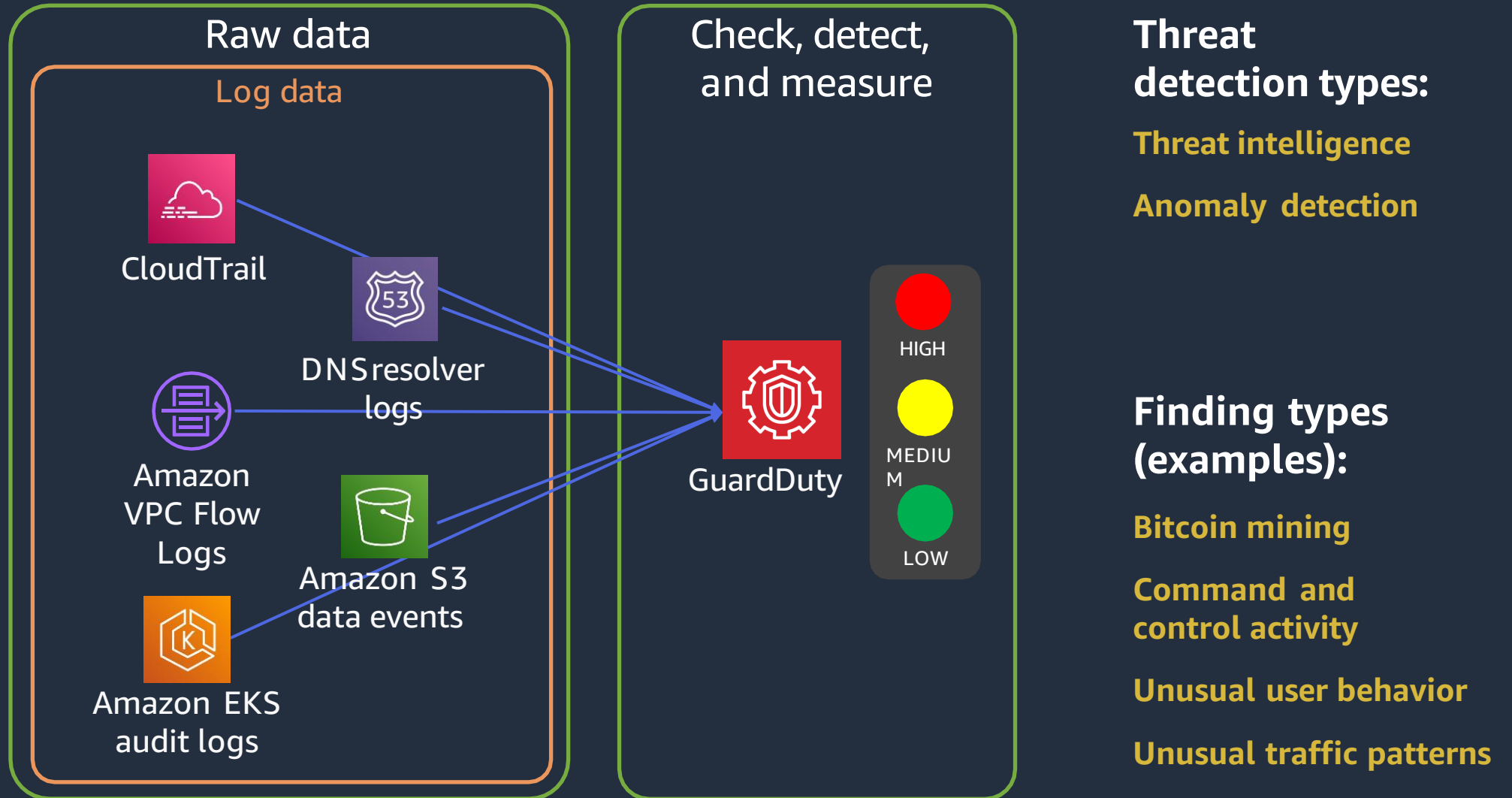


**Amazon
Inspector**

Check for software
vulnerabilities

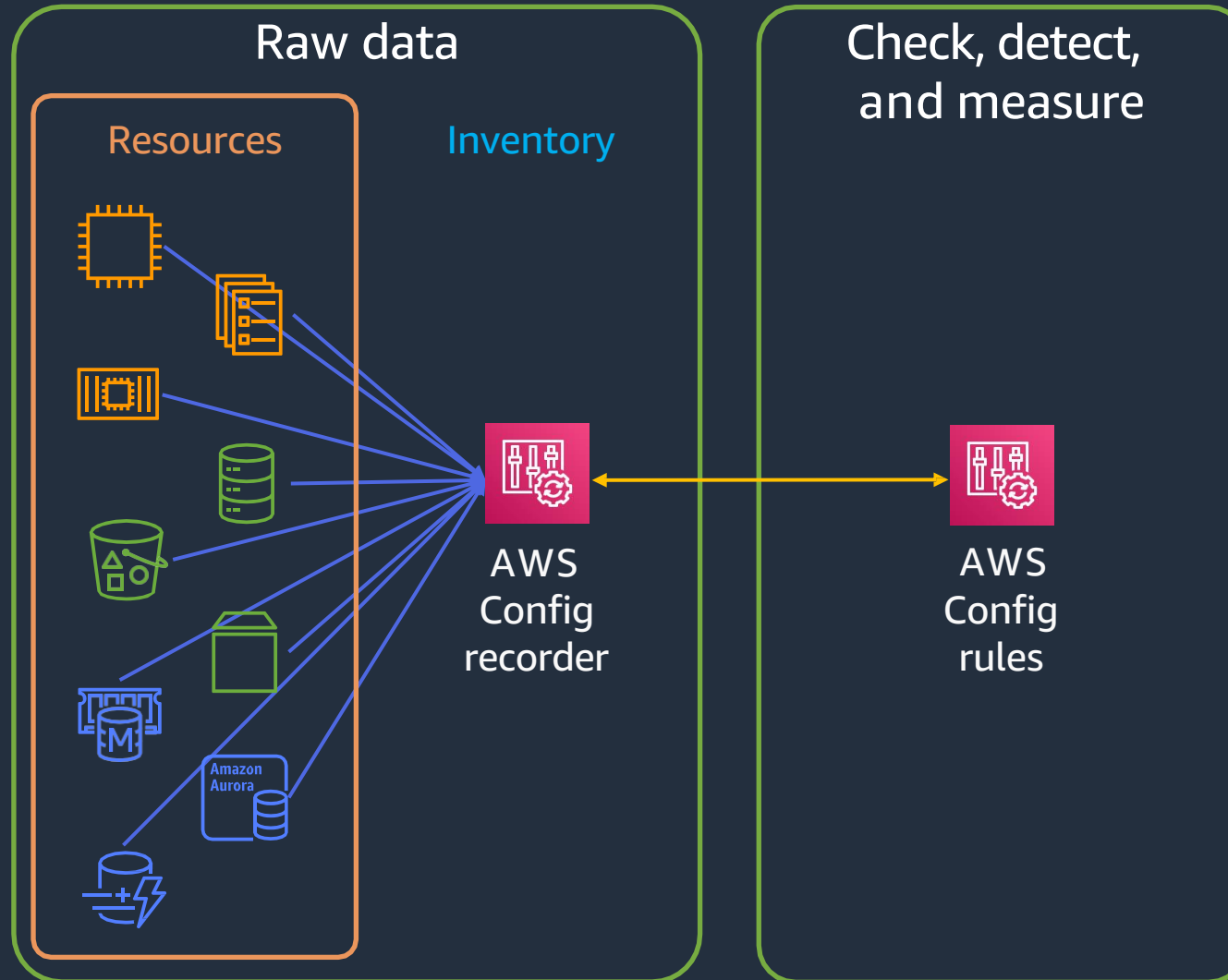
GuardDuty

No configuration needed for this log source



AWS Config

Rules are mostly triggered based on changes



Config rules:

Managed rules to show if resources comply with common best practices

Build custom rules while using guard custom policy or AWS Lambda functions

Conformance packs (CP):

Sample CPs, based on industry recommendations, or custom CPs can be used to group rules into a general-purpose compliance framework

AWS Config resources

Resource Inventory

Search existing or deleted resources recorded by AWS Config. For a specific resource, view the resource details, configuration timeline, or compliance timeline. The resource configuration timeline allows you to view all the configuration items captured over time for a specific resource. The resource compliance timeline allows you to view compliance status changes. To query your resource configurations, use the [advanced SQL query editor](#).

Resources

[View details](#)[Resource Timeline](#)

Resource category

AWS resources

Resource type

Multiple Selected

Compliance

Any compliance status

AWS EC2 SecurityGroup X

Resource identifier - optional

Q Enter resource identifier

 Include deleted resources

< 1 > ⚙

Resource identifier	Type	Compliance
<input type="radio"/> sg-019e071a23df05718	EC2 SecurityGroup	⚠ Noncompliant
<input type="radio"/> sg-04113ea6e68c26d4b	EC2 SecurityGroup	⚠ Noncompliant
<input type="radio"/> sg-048d5ac026fe26139	EC2 SecurityGroup	✅ Compliant
<input type="radio"/> sg-0cd88dd079707cd4b	EC2 SecurityGroup	⚠ Noncompliant
<input type="radio"/> sg-addaf3f3	EC2 SecurityGroup	⚠ Noncompliant

AWS Config resources timeline

Timeline

General details

Resource ID
sg-019e071a23df05718

Resource type
AWS::EC2::SecurityGroup

Resource name
SEC-TOOLING-SSH-LIMITED

Events

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

Start date

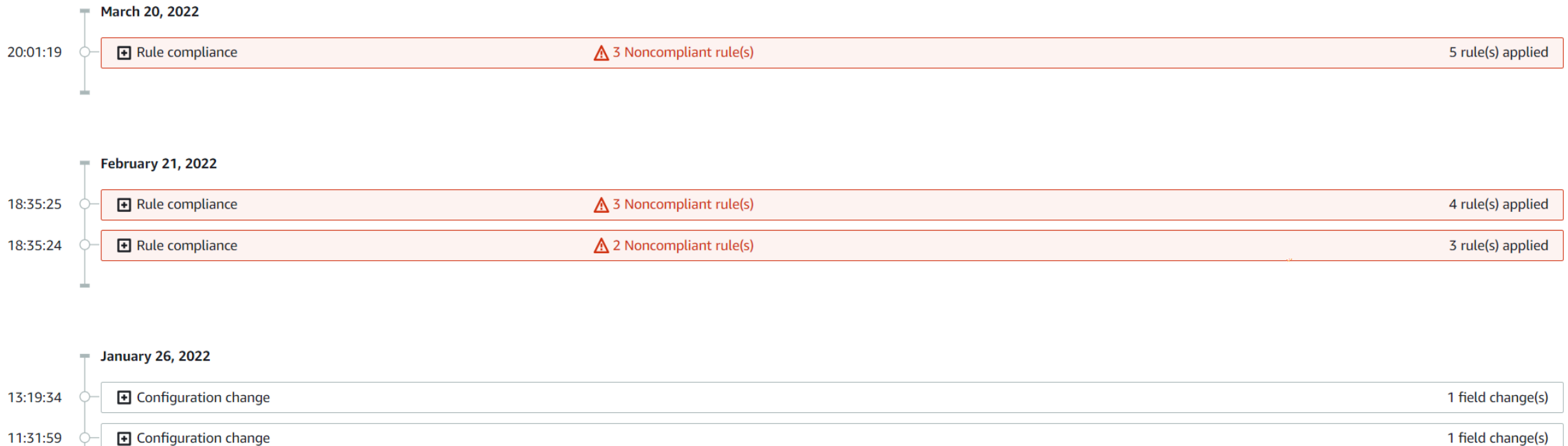
2022/06/23



Event type

Now

All event types



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	View details	Edit rule	Actions ▾	Add rule			
Any status ▾	<	1	2	3	...	>	⚙️
Name	Remediation action	Type	Compliance				
● EmrMasterNoPublicIp-conformance-pack-uqghya0wp	Not set	AWS managed	-				
● EfsEncryptedCheck-conformance-pack-uqghya0wp	Not set	AWS managed	-				
● CloudTrailLogFileValidationEnabled-conformance-pack-vieezssqt	Not set	AWS managed	✔️ Compliant				
● CMKBackingKeyRotationEnabled-conformance-pack-vieezssqt	Not set	AWS managed	⚠️ 4 Noncompliant resource(s)				
● Ec2SecurityGroupAttachedToEni-conformance-pack-uqghya0wp	Not set	AWS managed	⚠️ 11 Noncompliant resource(s)				
● CloudwatchLogGroupEncrypted-conformance-pack-uqghya0wp	Not set	AWS managed	⚠️ 24 Noncompliant resource(s)				
● Ec2ManagedInstanceAssociationCompliance-conformance-pack-uqghya0wp	Not set	AWS managed	✔️ Compliant				
● AcmCertificateExpirationCheck-conformance-pack-uqghya0wp	Not set	AWS managed	⚠️ 2 Noncompliant resource(s)				
● IAMPasswordPolicyCheck-conformance-pack-vieezssqt	Not set	AWS managed	⚠️ 1 Noncompliant resource(s)				
● CloudTrailCloudWatchLogsEnabled-conformance-pack-vieezssqt	Not set	AWS managed	⚠️ 1 Noncompliant resource(s)				

AWS Config rules details

CMKBackingKeyRotationEnabled-conformance-pack-vieezssqt

Actions ▾

▼ Rule details

Edit

Description

Checks that key rotation is enabled for each key and matches to the key ID of the customer created customer master key (CMK). The rule is compliant, if the key rotation is enabled for specific key object.

Config rule ARN

arn:aws:config:eu-west-1:██████████:config-rule/aws-service-rule/config-conforms.amazonaws.com/config-rule-siz3qq

Trigger type

Periodic: 12 hours

Scope of changes

-

Last successful evaluation

✔ September 19, 2022 6:12 AM

▼ Resources in scope

View details

Remediate



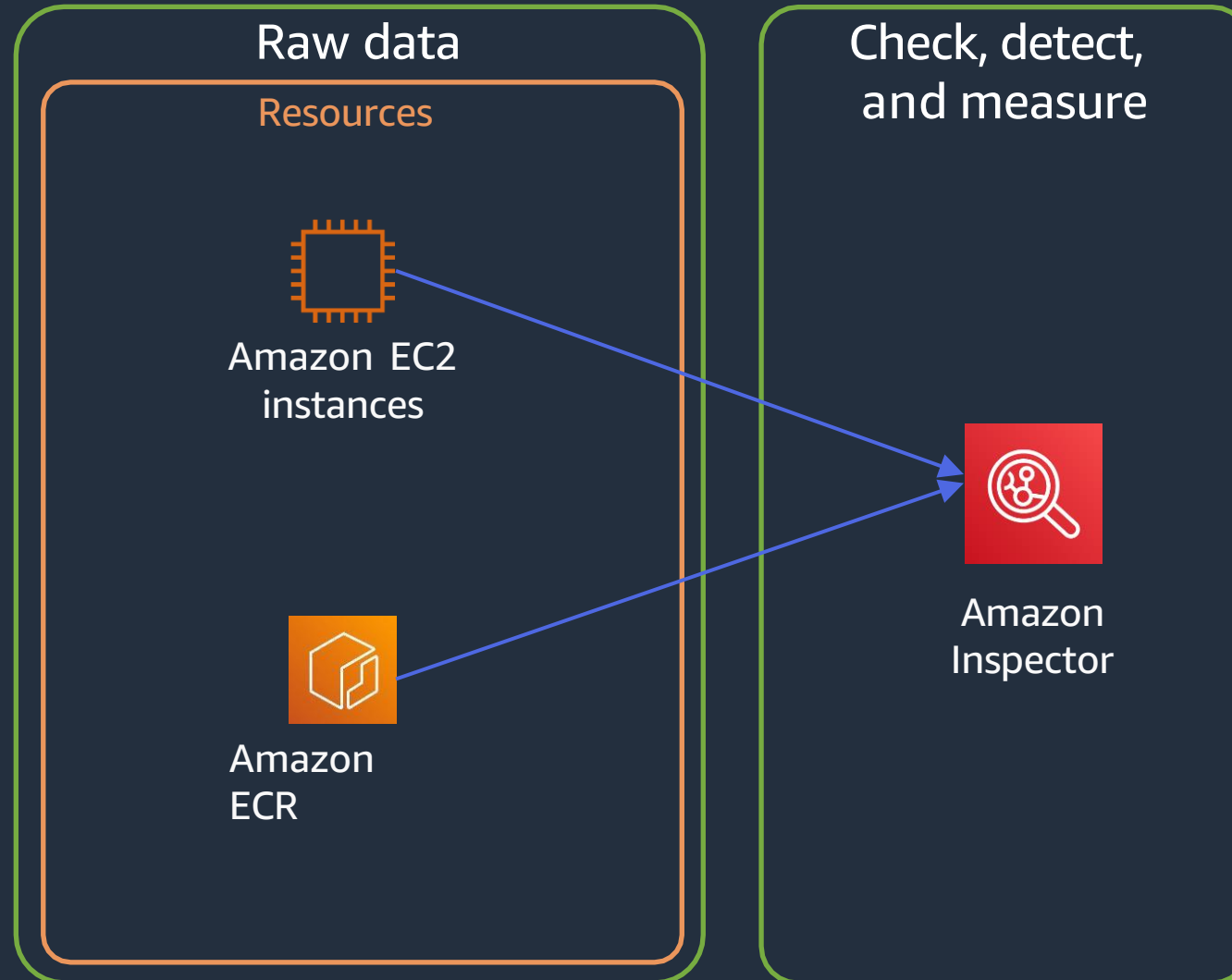
Noncompliant ▾

< 1 > ⚙

ID	Type	Status	Annotation	Compliance
b9e77947-1283-4406-ba37-c0199928f998	KMS Key	-	-	⚠ Noncompliant
bc7ee0d3-72ae-4e90-be7a-46f4f01f1d5b	KMS Key	-	-	⚠ Noncompliant
cb9d2583-ba15-4bee-9be3-48d65f45708a	KMS Key	-	-	⚠ Noncompliant
d128e4a1-9864-43c0-b2d1-468c50183f48	KMS Key	-	-	⚠ Noncompliant

Amazon Inspector

Continuous scans based on software changes and new or updated vulnerability intelligence



Vulnerability assessment:

Automatically discover vulnerabilities in near real time
Identify zero-day vulnerabilities quickly by using more than 50 intelligence sources

Network accessibility analysis:

Prioritize findings using context-based risk scores

Amazon Inspector summary

Summary Info

Viewing data from all accounts

Environment coverage

Your accounts, instances, and repositories that are enabled with Inspector.

Accounts

100%

27 / 27 accounts

Instances

16%

4 / 24 instances

Repositories

66%

2 / 3 repositories

Critical findings

All active critical findings in your environment.

ECR container

0 Critical

0 total findings

EC2 instance

21 Critical

700 total findings

Network reachability

0 Critical

2 total findings

Risk based remediations

Vulnerabilities impacting the most instances and images.

Package name	Critical	All
expat	15	47
python-pillow	4	14
httpd-tools	1	10
httpd-filesystem	1	10
httpd	1	10

[View all vulnerabilities](#)

AWS accounts with most critical findings

Accounts with the most critical findings.

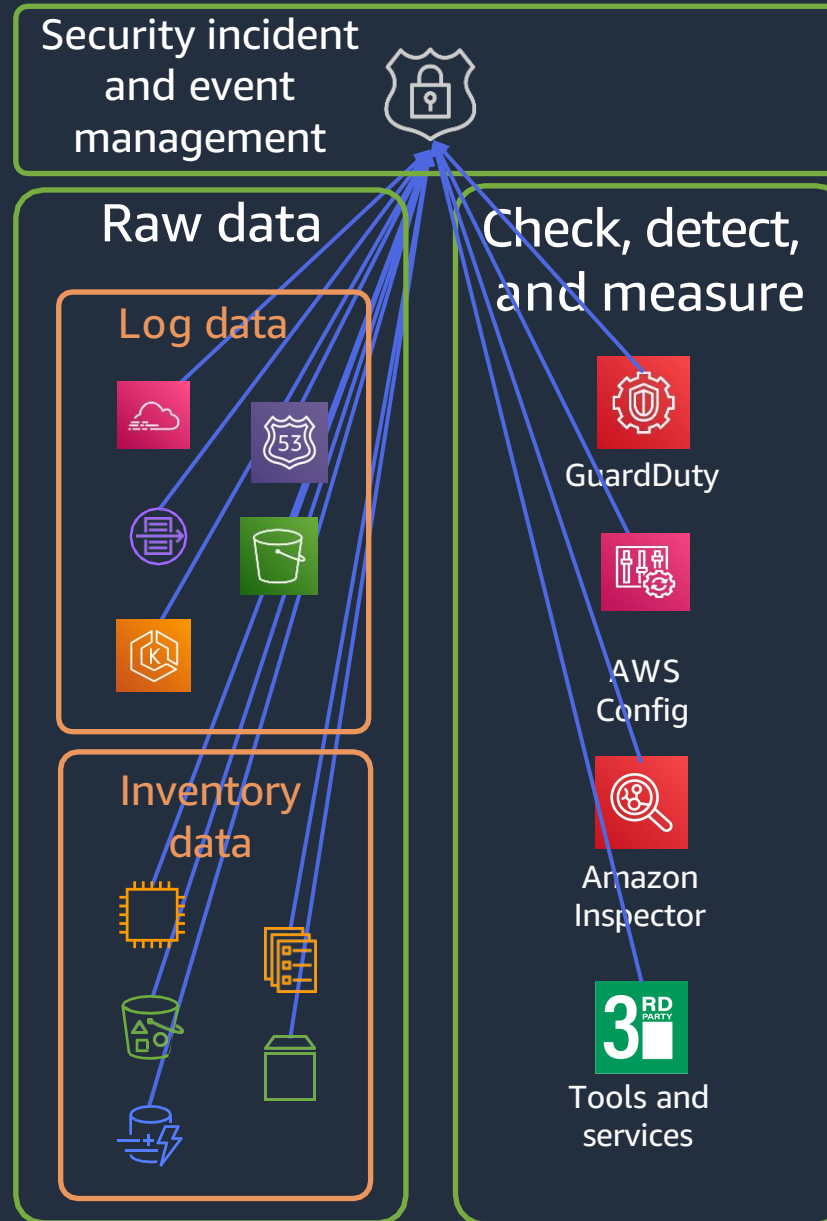
AWS account	Critical	All
SignFast-Play	10	277
Networking Account	6	187
Logging Account	3	76
Forensic Account	2	83
Shared Services Account	0	38

Collection Containme nt



Triage and collection – What do we have so far?

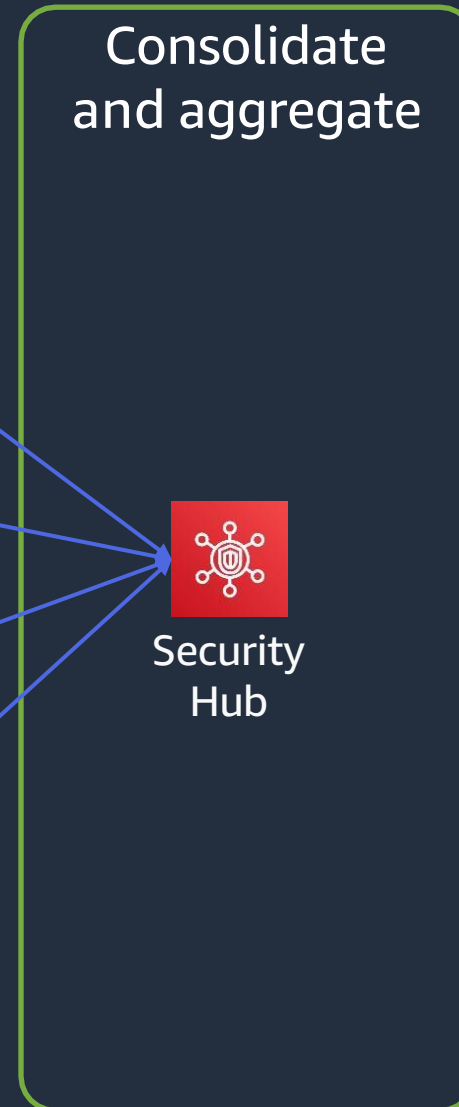
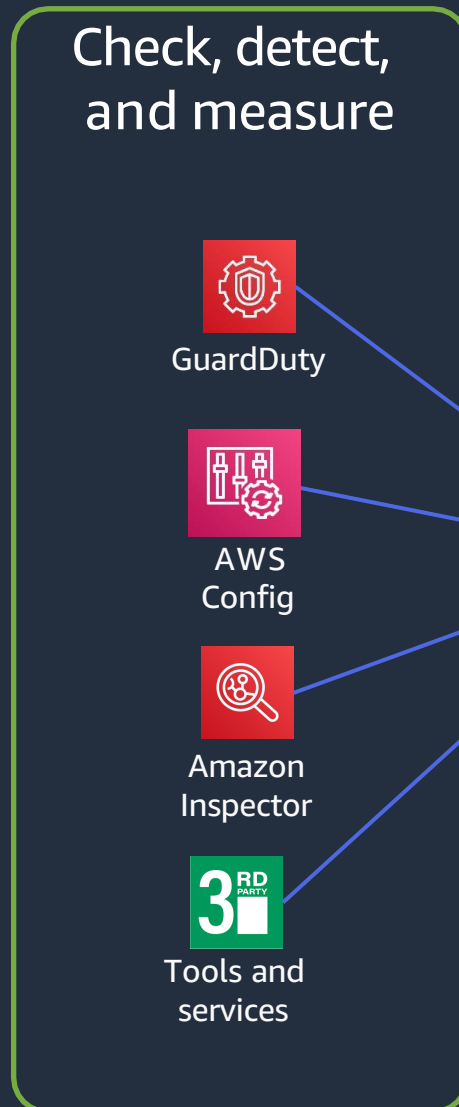
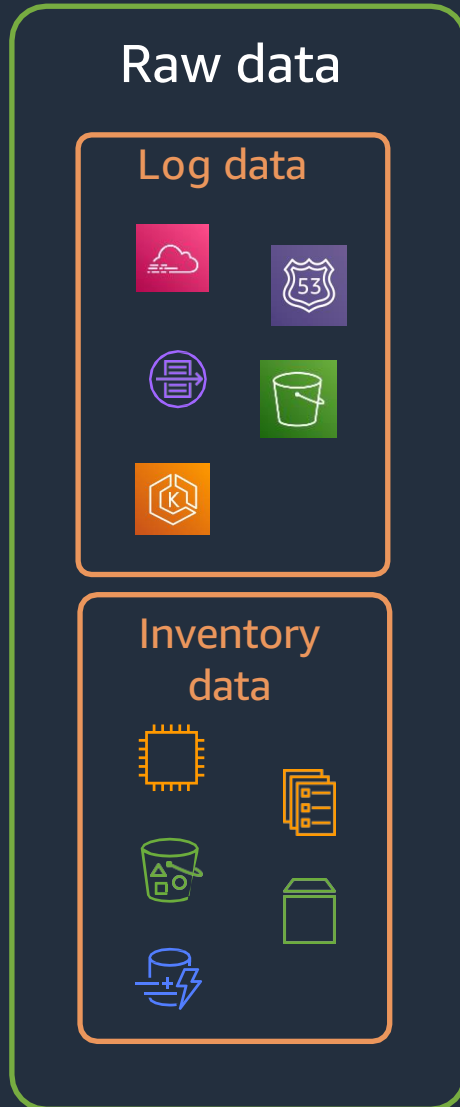
Data that isn't measured or weighted



Results or findings based on rules and patterns

Security Hub

A single, standardized data format for all of your findings



Cloud security posture management:

Automated, continuous security checks based on industry and vendor best practices

Consolidated findings:

Aggregates security findings generated by AWS security services and partners across accounts and Regions

Security Hub summary

Security Hub ×

Summary

Security standards

Insights

Findings

Integrations

Settings

What's new

Security standards

51%
Security score

Standard	Passed	Failed	Score ▲
CIS AWS Foundations Benchmark v1.2.0	5	23	18%
CIS AWS Foundations Benchmark v1.4.0	8	19	30%
PCI DSS v3.2.1	24	20	55%
AWS Foundational Security Best Practices v1.0.0	104	71	59%

[View all standards](#)

Resources with the most failed security checks

	Failed checks
arn:aws:s3::: [redacted]	12
arn:aws:s3::: [redacted]	12
arn:aws:es:eu-west-1: [redacted]:domain/[redacted]	11
arn:aws:s3:::secure-cabbage-[redacted]	11
arn:aws:s3:::athena-[redacted]	10

Findings by Region

Findings from all linked Regions are visible from the aggregation Region.

All linked Regions (6)
Linked Regions with findings (3)

Region	Critical	High	Medium	Low
Europe (Ireland) [Current Region]	125	1141	2588	598
Europe (Frankfurt)	7	9	69	24
US East (N. Virginia)	2	1	11	7

Security Hub findings

Security Hub

Summary
Security standards
Insights
Findings
Integrations
Settings
What's new 4

A finding is a security issue or a failed security check.

Product name is GuardDuty X Workflow status is NEW X Workflow status is NOTIFIED X Record state is ACTIVE X Add filters

<input type="checkbox"/>	Severity	Workflow status	Record State	Region	Account Id	Company	Product	Title	Resource
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance i-098f302ff7851db51
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance i-098f302ff7851db51
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance i-098f302ff7851db51
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance i-098f302ff7851db51
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance i-098f302ff7851db51
<input type="checkbox"/>	HIGH	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Data exfiltration through DNS queries from EC2 instance i-08d0c7a9c27319c16.	EC2 Instance i-08d0c7a9c27319c16
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance i-098f302ff7851db51
<input type="checkbox"/>	HIGH	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Command and Control server domain name queried by EC2 instance i-08d0c7a9c27319c16.	EC2 Instance i-08d0c7a9c27319c16
<input type="checkbox"/>	LOW	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Amazon S3 Block Public Access was disabled for account.	IAM Access Key ASIAZ5I6Y5OV2R7FGLXI
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance i-098f302ff7851db51
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Reconnaissance API ListInstanceAssociations was invoked from an IP address on a custom threat list.	EC2 Instance i-098f302ff7851db51
<input type="checkbox"/>	MEDIUM	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	EC2 instance i-08d0c7a9c27319c16 communicating with disallowed IP address.	EC2 Instance i-08d0c7a9c27319c16
<input type="checkbox"/>	HIGH	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	2 security risk(s) detected including EICAR-Test-File (not a virus) on EC2 instance i-07a954a1fbc76df2e.	EC2 Instance i-07a954a1fbc76df2e
<input type="checkbox"/>	HIGH	NEW	ACTIVE	eu-west-1		Amazon	GuardDuty	Command and Control server domain name queried by EC2 instance i-0569ee2fd39c70828.	EC2 Instance i-0569ee2fd39c70828

Security Hub finding details

Command and Control server domain name queried by EC2 instance i-0569ee2fd39c70828. ✕

Finding ID: `arn:aws:guardduty:eu-west-1: [redacted]:detector/c2bc8ca87a1c16a25de44cd8a700d912/finding/66c1226d26db6adc7a231a31e11136d5`

HIGH
EC2 instance i-0569ee2fd39c70828 is querying a domain name associated with a known Command & Control server.

Workflow status: **New** (dropdown)

RECORD STATE: **ACTIVE**
Set by the finding provider

AWS account ID: [redacted]

Created at: 2022-07-28T12:48:53.686Z

Product name: GuardDuty

Company name: Amazon

Severity (original): 8

Updated at: 2022-07-28T13:10:20.259Z

Severity label: **HIGH**

Source URL: `https://eu-west-1.console.aws.amazon.com/guardduty/home?region=eu-west-1#/findings?macros=current&fld=66c1226d26db6adc7a231a31e11136d5`

- Types and Related Findings
- Resources
- Investigate in Amazon Detective
- Finding Provider Fields

Types and Related Findings

Types: TTPs/Command and Control/Backdoor:EC2-C&CAActivity.BIDNS

Resources

Resources detail: `arn:aws:ec2:eu-west-1:[redacted]:instance/i-0569ee2fd39c70828`

Resource type: AwsEc2Instance

Resource ID: `arn:aws:ec2:eu-west-1:[redacted]:instance/i-0569ee2fd39c70828`

EC2 instance image ID: ami-01efa4023f0f3a042

EC2 instance launched at: 2022-07-28T11:42:31.000Z

Resource region: eu-west-1

EC2 instance type: t2.large

EC2 instance subnet ID: subnet-07007d1b8f78afb20

Investigate in Amazon Detective


Finding Provider Fields

Finding Provider Fields detail: Finding Provider Field


Provider severity label: **HIGH**

Types: TTPs/Command and Control/Backdoor:EC2-C&CAActivity.BIDNS


Continuous containment in the cloud




Amazon VPC



Security group



Network ACL



Network Firewall

Network
isolation



AWS Organizations



Organizational units




Accounts




Service control policies


Logical
isolation




Systems Manager



Amazon EBS snapshots



AWS Step Functions



Amazon EventBridge

Forensic automation
using service and
features

Remediation Post-incident activity



Challenges



Auditors
and
regulators

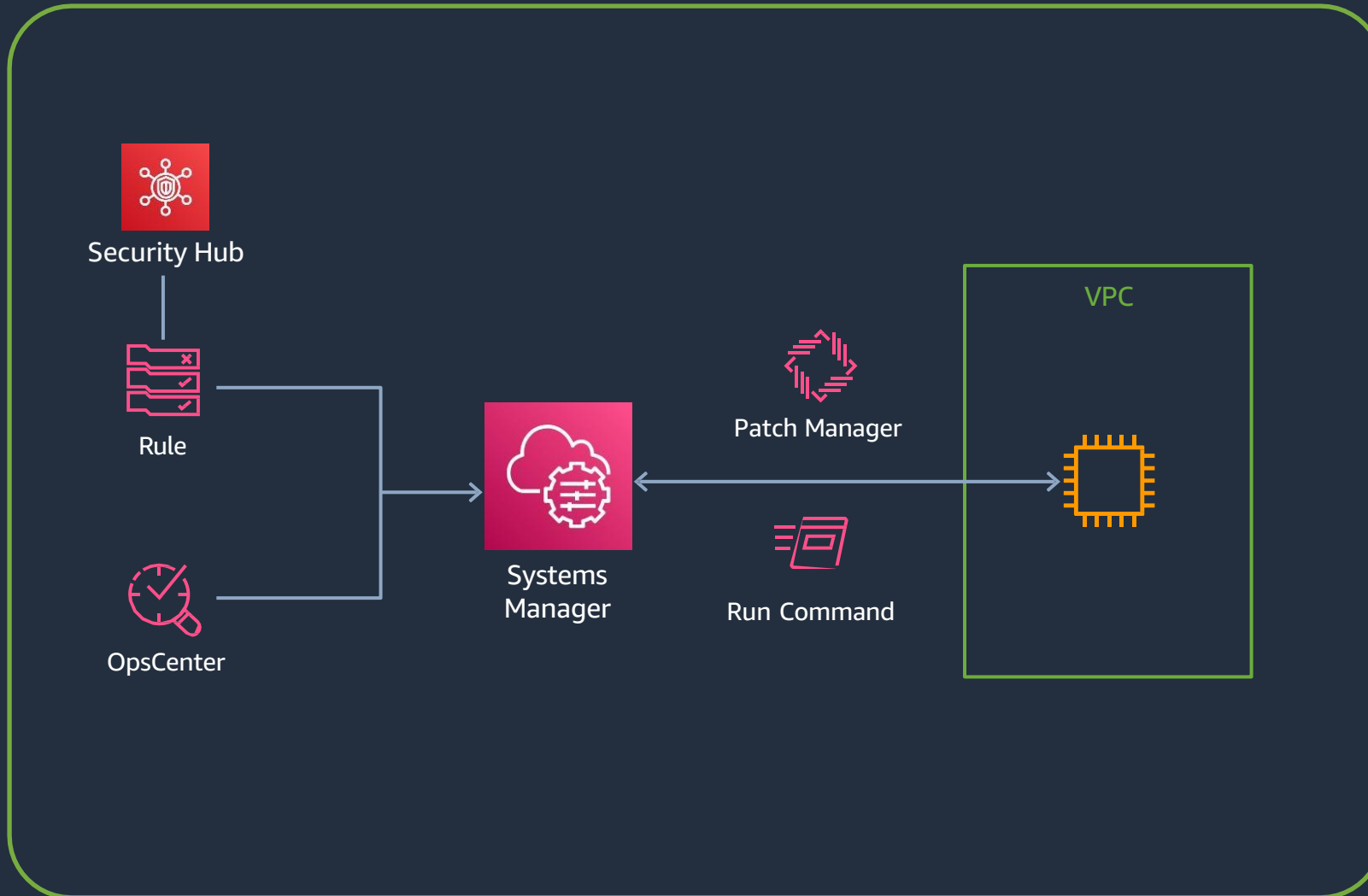


Customers



“What happened?
At what time?”

Systems Manager



Patch Manager,
a capability of
Systems Manager:

**Maintain instance
compliance against your
patch, configuration, and
custom policies**

OpsCenter,
a capability of
Systems Manager:

**Central location to view,
investigate, and resolve
operational items**

Systems Manager

AWS Systems Manager

- Quick Setup
- Operations Management
 - Explorer
 - OpsCenter
 - CloudWatch Dashboard
 - Incident Manager
- Application Management
 - Application Manager
 - AppConfig
 - Parameter Store
- Change Management
 - Change Manager
 - Automation
 - Change Calendar
 - Maintenance Windows
- Node Management
 - Fleet Manager
 - Compliance
 - Inventory
 - Hybrid Activations
 - Session Manager
 - Run Command
 - State Manager
 - Patch Manager
 - Distributor

Explorer

Dashboard actions Settings Create resource data sync

OpsData Filter

Select a resource data sync Region

Filter by OpsItem source, tag keys, or tag values

Q

OpsItem by status

Actions

277 Unresolved 277 Open

Non-compliant instances for patching

Actions

Age Group	Critical	Total
Under 15 days	4	4
15-90 days	0	0
Over 90 days	0	0

Under 15 days: Total non-compliant resources: 4, Critical non-compliant resources: 0
15-90 days: Total non-compliant resources: 0, Critical non-compliant resources: 0
Over 90 days: Total non-compliant resources: 0, Critical non-compliant resources: 0

Desired state compliance status

Actions

Compliance status of Quick Setup associations.

Association name	Total compliant resources	Total non-compliant resources	Compliance percentage
AWS-QuickSetup-SSMHostMgmt-ScanForPatches-tzrpw	1	5	17%
AWS-QuickSetup-SSMHostMgmt-CollectInventory-tzrpw	6	0	100%
AWS-QuickSetup-SSMHostMgmt-UpdateSSMAgent-tzrpw	6	0	100%
AWS-PatchNowAssociation	5	0	100%

OpsItem by severity

Actions

18 Critical 259 High 0 Medium 0 Low 0 Unspecified

Patch Manager

AWS Systems Manager

- Quick Setup
- Operations Management
 - Explorer
 - OpsCenter
 - CloudWatch Dashboard
 - Incident Manager
- Application Management
 - Application Manager
 - AppConfig
 - Parameter Store
- Change Management
 - Change Manager
 - Automation
 - Change Calendar
 - Maintenance Windows
- Node Management
 - Fleet Manager
 - Compliance
 - Inventory
 - Hybrid Activations
 - Session Manager
 - Run Command
 - State Manager
 - Patch Manager**
 - Distributor

AWS Systems Manager > Patch Manager

Patch Manager

[Dashboard](#) | [Compliance reporting](#) | [Patch baselines](#) | [Patches](#) | [Patch groups](#) | [Settings](#)

[Configure patching](#) [Patch now](#)

Amazon EC2 instance management

Snapshot of EC2 instances in your AWS account that are and are not managed by Systems Manager.

Reporting not enabled

To view the EC2 instance snapshot, enable the Amazon EC2 OpsData source in Explorer and set up recording in AWS Config. [Learn more](#)

[Enable Explorer](#)

Compliance summary

Summary of compliance status for managed nodes that have previously reported patch data.

■ Compliant: 1 ■ Critical noncompliant: 0
■ High noncompliant: 0 ■ Other noncompliant: 4

Noncompliance counts

The number of noncompliant nodes for each of the most common reasons for being out of compliance.

Nodes with missing patches: 4

Nodes with failed patches: 0

Nodes pending reboot: 0

Compliance reports

Count of instances based on the age of their most recent patching compliance reports.

■ Compliance reported within the past 7 days: 4
■ Compliance not reported within the past 7 days: 0
■ Compliance never reported: 0

Patch operations history (4)

This summary of recent patching operations indicates whether an operation was started manually, or started by a maintenance window or State Manager association. Choose an operation link to view the command output.

< 1 >

Patch operation	Started by	Document name	End time	Status	Targets
Scan	Association	AWS-RunPatchBaseline	September 22, 2022 at 5:07 PM GMT+2	Success	InstanceIds: *
Scan	Association	AWS-RunPatchBaselineAssociation	September 22, 2022 at 5:04 PM GMT+2	Success	InstanceIds: 4
Scan	Association	AWS-RunPatchBaselineAssociation	September 19, 2022 at 3:47 PM GMT+2	Success	InstanceIds: i-08d0c7a9c27319c16
Scan	Association	AWS-RunPatchBaselineAssociation	September 19, 2022 at 9:41 AM GMT+2	Success	InstanceIds: i-08d0c7a9c27319c16

Recurring patching tasks (2)

The following is a list of State Manager associations and maintenance windows that run any patching-related task. Choose a task name to view its details

Patch Manager

AWS Systems Manager ×

Quick Setup

▼ **Operations Management**

- Explorer
- OpsCenter
- CloudWatch Dashboard
- Incident Manager

▼ **Application Management**

- Application Manager
- AppConfig
- Parameter Store

▼ **Change Management**

- Change Manager
- Automation
- Change Calendar
- Maintenance Windows

▼ **Node Management**

- Fleet Manager
- Compliance
- Inventory
- Hybrid Activations
- Session Manager
- Run Command
- State Manager
- Patch Manager**
- Distributor

AWS Systems Manager > Patch Manager > Patch now

New Features ×

We listened to your concerns and now we provide a way to orchestrate complex patch operations in a way that does not compromise your fleet's availability. The Patch Lifecycle Hooks feature is available under advanced options below.

Patch instances now [Info](#)

Basic configuration

Scan for missing patches or install patches, with or without rebooting. For more patching options, use the [Configure patching](#) page.

Patching operation

Scan

Scan and install

Reboot option

Specify whether Patch Manager should reboot your instances, or reboot on a schedule

Reboot if needed

Do not reboot my instances

Schedule a reboot time New

Instances to patch

Choose whether to patch all instances or only the instances you specify

Patch all instances

Patch only the target instances I specify

Target selection

Choose a method for selecting targets.

Specify instance tags
Specify one or more tag key-value pairs to select instances that share those tags.

Choose instances manually
Manually select the instances you want to register as targets.

Choose a resource group
Choose a resource group that includes the resources you want to target.

Specify instance tags

Specify one or more instance tag key-value pairs to identify the instances where the tasks will run.

Enter a tag key and optional value applied to the instances you want to target, and then choose Add.

Patching log storage New

Select or create an S3 bucket for storing patching operation logs. Select **Do not store logs** if you don't require log information.

AWS Backup



AWS
Backup

A fully managed, policy-based backup service that makes it easy to centrally manage and automate the backup of data across AWS services



Amazon
RDS



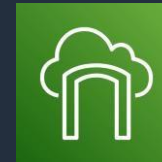
Amazon
EBS



Amazon
EFS



Amazon EC2



AWS
Storage
Gateway



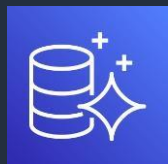
Amazon
DynamoDB



Amazon
FSx for
Lustre



Amazon FSx for
Windows File Server



Amazon
Aurora

How AWS Backup works



Operators



IAM



Admin



AWS Backup: compliance reporting

Automate the restore processes

Restore using AWS cloud-native services or third-party services such as

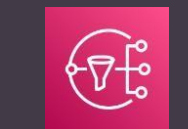
- AWS CDK
- AWS CloudFormation

Or third-party services like Terraform

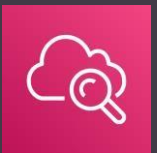
Scale through AWS Organizations

Automate backups across accounts and organizational units

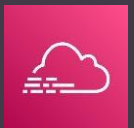
Restrict access to backup plans



Amazon SNS

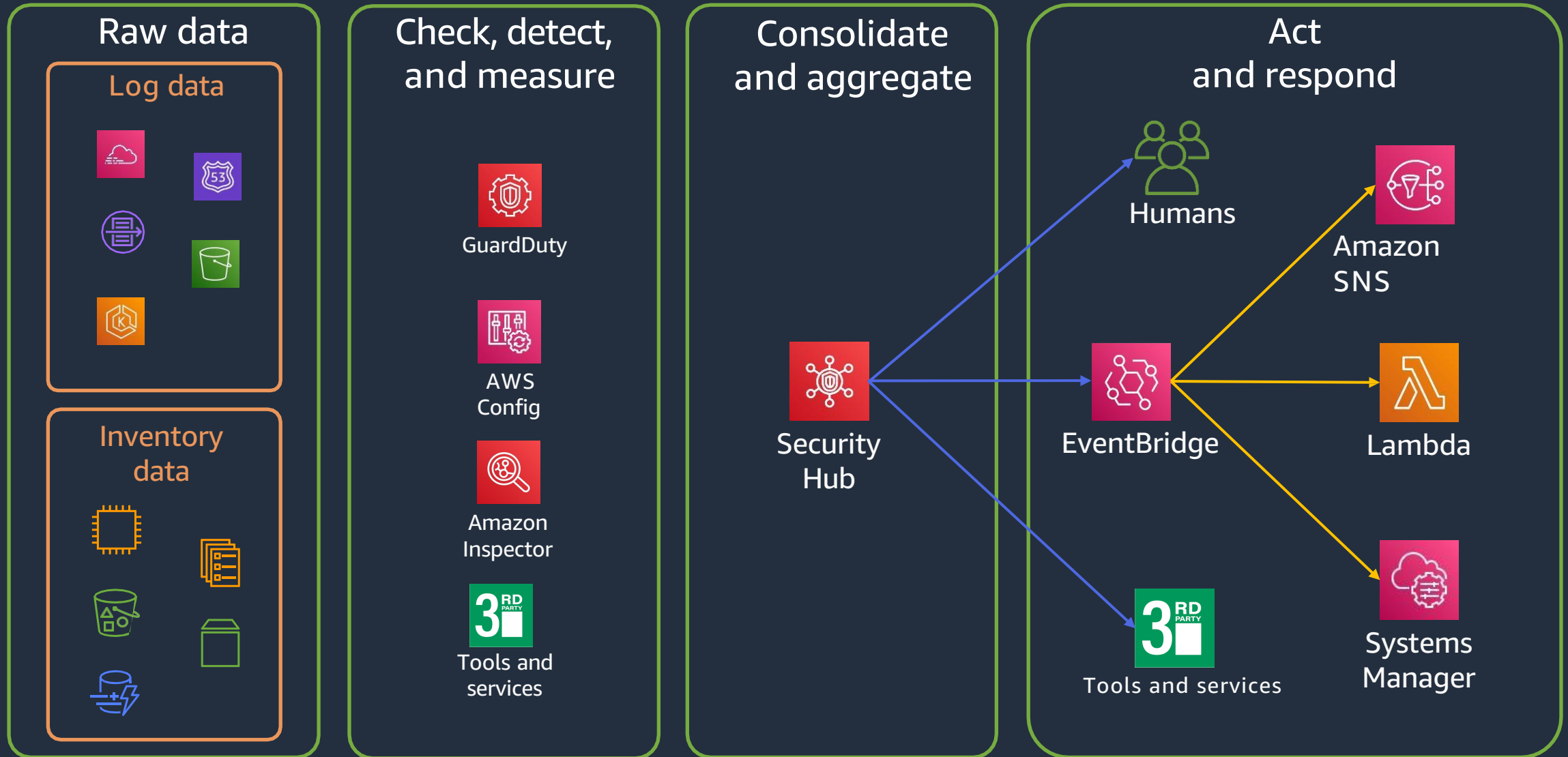


CloudWatch

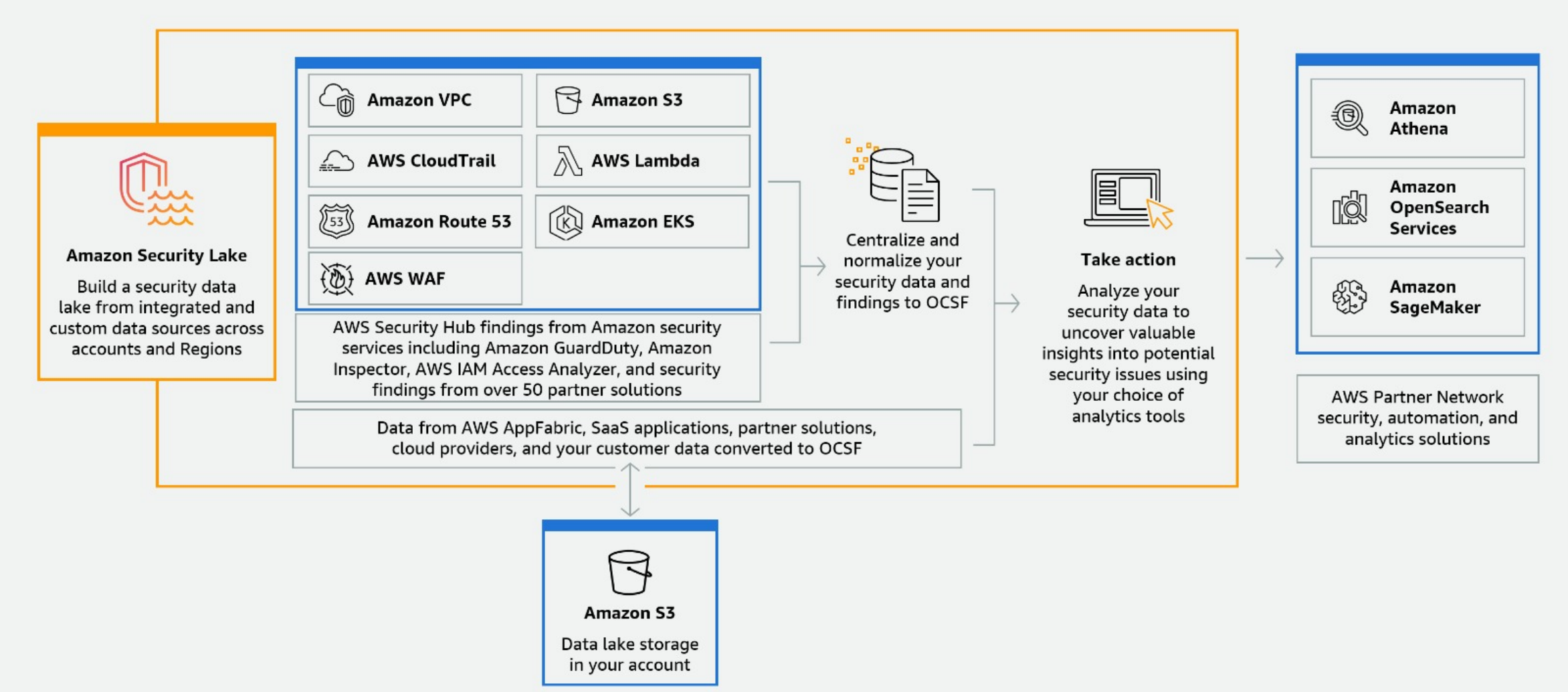


CloudTrail

Incident lifecycle on AWS



Security Lake



Security Lake



Step 1
Define collection objective

Step 2
Define target objective

Step 3
Review and create

Define collection objective

To enable Security Lake, start by selecting which data sources, Regions, and accounts you want to include in your data lake.

Sources to ingest [Info](#)

Security Lake ingests selected data sources. Data is encrypted with Amazon S3 managed keys.

Ingest the AWS default sources

Recommended

Ingest specific AWS sources

Specific sources

Enable ingestion for specific log and event sources.

Each account receives a 15-day free trial period when you enable log ingestion for the first time for that account.

Log and event sources (8)

< 1 >

<input type="checkbox"/>	Source	Description	Version
<input checked="" type="checkbox"/>	CloudTrail - Management events - <i>recommended</i>	Management operations that are performed on your AWS resources	2.0
<input checked="" type="checkbox"/>	CloudTrail - Lambda data events - <i>recommended</i>	Subset of API calls for Amazon Lambda captured by CloudTrail, including calls from the Lambda console and code calls to Lambda APIs	2.0
<input checked="" type="checkbox"/>	EKS Audit Logs - <i>recommended</i>	Activities performed on the Kubernetes resources running in your Elastic Kubernetes Service (EKS) clusters	2.0
<input checked="" type="checkbox"/>	Route 53 - <i>recommended</i>	DNS queries made by resources within your Amazon VPC	2.0
<input checked="" type="checkbox"/>	Security Hub - <i>recommended</i>	Security findings related to your AWS resources	2.0
<input checked="" type="checkbox"/>	VPC Flow Logs - <i>recommended</i>	Information about IP traffic going to and from network interfaces in your VPC	2.0
<input type="checkbox"/>	CloudTrail - S3 data events <i>High volume data</i>	Subset of API calls for Amazon S3 captured by CloudTrail, including calls from the S3 console and code calls to S3 APIs	2.0
<input type="checkbox"/>	AWS WAF - <i>new</i> <i>High volume data</i>	Monitor web requests sent to your applications and control access to your content	2.0

Demo

- Automating Incident Response
- Ransomware protection strategies with AWS Backup
- AWS Elastic Disaster Recovery for fast recovery

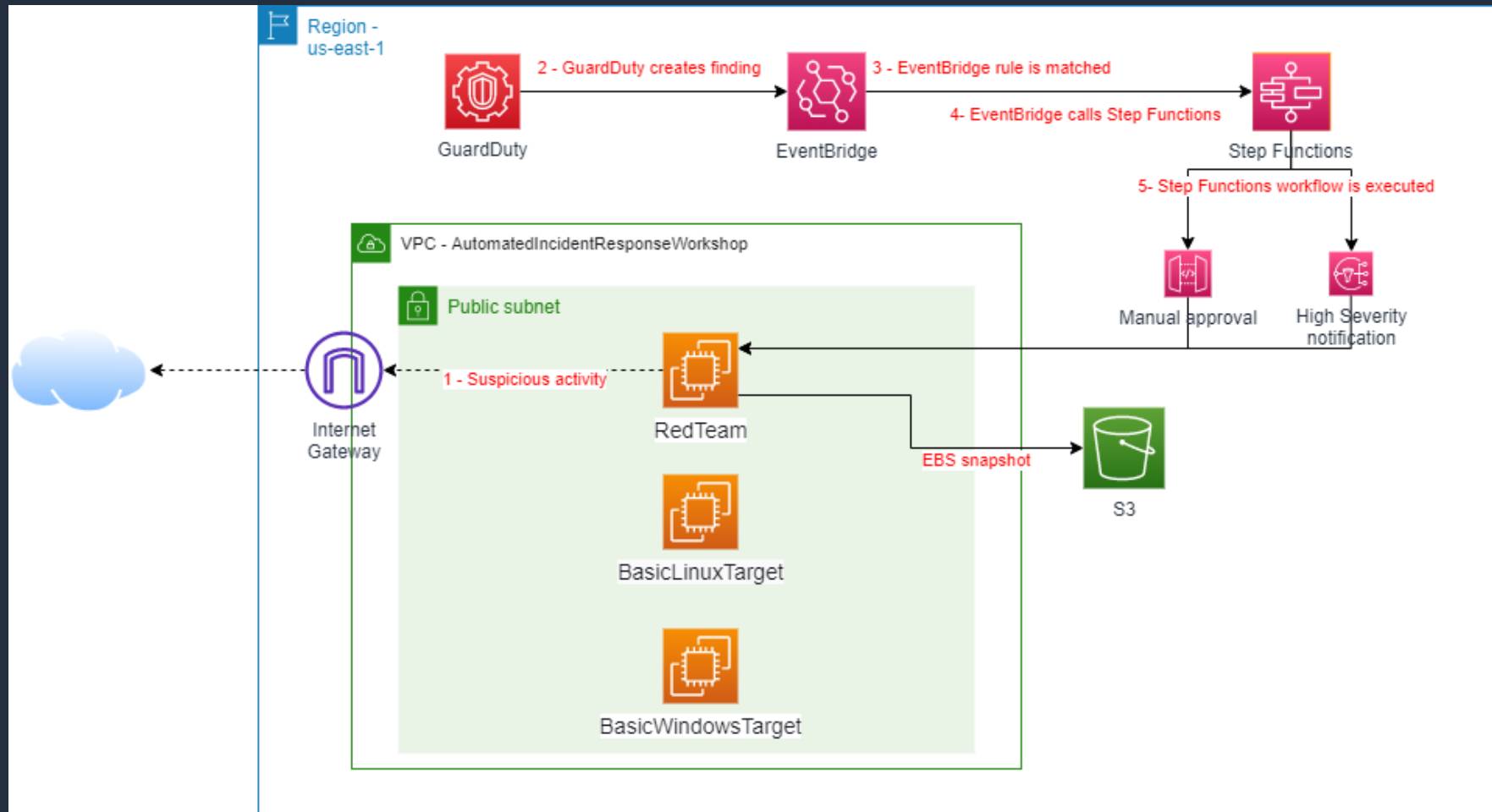
Thanh Nguyen

Solutions Architect

CMC Telecom

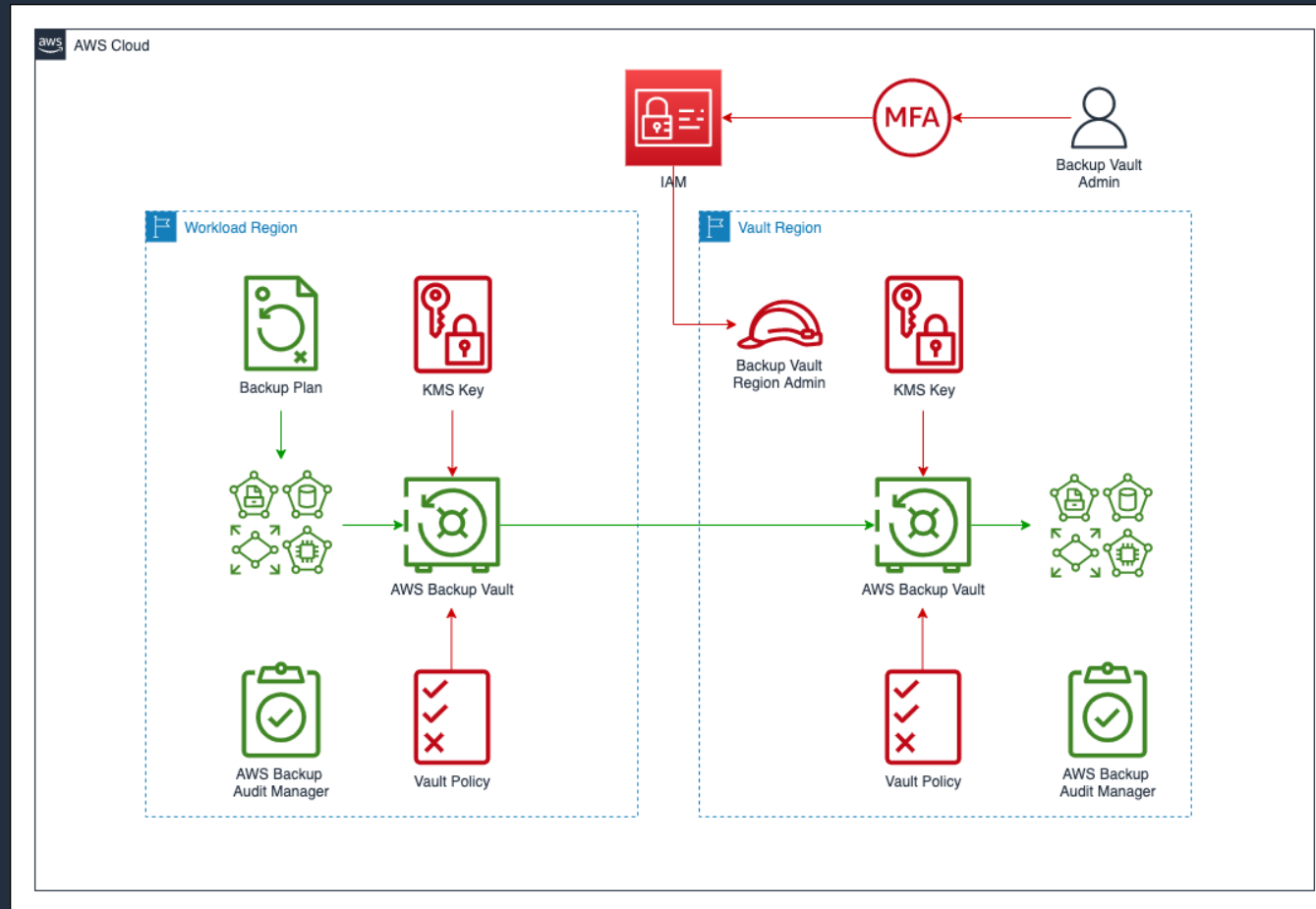
Automating Incident Response

Demos: use Amazon GuardDuty to detect threats, but the same security automations can be triggered on instances upon detection from an Antimalware solution or using other indicator of compromise.

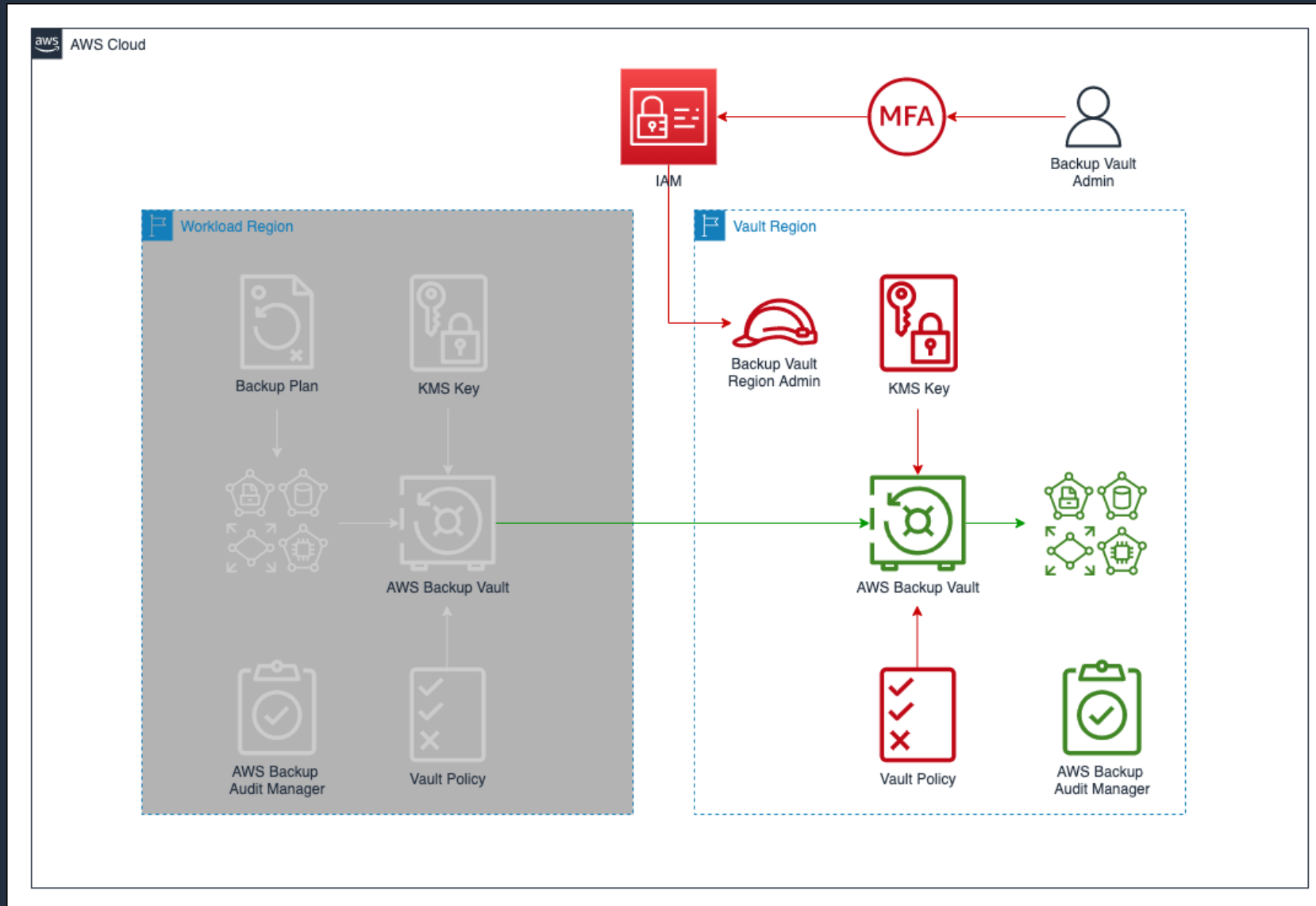


Ransomware protection with AWS Backup

Demos: we will design a backup strategy, setup immutable backup vaults, and configure cross-Region backups for maintaining logically separated copies of your data to meet your disaster recovery needs. We will setup data immutability to mitigate data exfiltration, protect against accidental or malicious deletion, and ransomware risks.



Centralized Region Vault



AWS Backup Vault Lock

Backup vault locks [Info](#)

A vault lock helps protect backups from lifecycle changes, accidental deletion, or malicious activities.


▼ How AWS Backup Vault Lock works

Perform the following steps to help protect your backups from inadvertent or malicious actions by storing backups using a Write-Once-Read-Many (WORM) model.



AWS Backup Vault Lock


AWS Backup Vault Lock helps protect your vault from accidental or malicious deletion. You can add data retention policies on your vault for governance and compliance purposes.

[Learn more](#) 



Manage permissions

A vault lock can only be added or edited if you have specific permissions. To grant permissions or check for own permissions, click on "Manage permissions".

[Manage permissions](#) 



Create vault lock

To create a vault lock, click on "Create vault lock" button and configure the vault lock policy to your backup vault with a specific retention mode.

[Create vault lock](#)

Vault lock details

Protect your vault with your choice of retention mode.

Backup vault [Info](#)

The vault lock will apply to the contents of the selected vault.

RegionalAWSBackupVault

Vault lock mode [Info](#)

Governance mode

The lock can be managed or deleted by users with specific IAM permissions.

Compliance mode

The lock cannot be managed or deleted by any user, even by the root user (account owner) or AWS.



Backups cannot be deleted manually

All backups in this vault will be protected with a vault lock. They cannot be deleted manually. This vault can be managed or deleted by only those users with specific IAM permissions. [Learn more](#)

Retention period [Info](#)

Vault locks help protect backups within the minimum and maximum retention periods.

Minimum retention period - optional [Info](#)

Backups with retention period equal to or greater than the entered value will be protected. 1 day is the default.

1

Days

Maximum retention period - optional [Info](#)

Backups with a retention period equal to or less than the entered value will be protected.

Enter maximum retention period

Days

Backup vault [Info](#)

The vault lock will apply to the contents of the selected vault.

RegionalAWSBackupVault

Vault lock mode [Info](#)

Governance mode

The lock can be managed or deleted by users with specific IAM permissions.

Compliance mode

The lock cannot be managed or deleted by any user, even by the root user (account owner) or AWS.



Backups cannot be deleted manually

When locked in compliance mode, vaults cannot be managed or deleted by any user or by AWS. Backups within a locked vault cannot be deleted until their lifecycle completes. Compliance mode begins after the grace time ends. [Learn more](#)

Retention period [Info](#)

Vault locks help protect backups within the minimum and maximum retention periods.

Minimum retention period - optional [Info](#)

Backups with retention period equal to or greater than the entered value will be protected. 1 day is the default.

1

Days

Maximum retention period - optional [Info](#)

Backups with a retention period equal to or less than the entered value will be protected.

Enter maximum retention period

Days

Compliance mode start date [Info](#)

Specify the date when the vault will be permanently locked. Until that time, the configuration can be edited or removed. The minimum grace time is 3 days (72 hours).

2024/06/15



The vault will become immutable on **June 15, 2024, 16:34:40 (UTC+07:00)**. You have 3 days of grace time to manage or delete the vault lock before it becomes immutable. During this time, only those users with specific IAM permissions can make changes.

AWS Backup Audit Manager

Create framework [Info](#)

Choose controls to evaluate your backup activity.

Framework name and description

Framework name

Framework name must contain 1 to 256 alphanumeric and '_' characters.

Framework description - *optional*

Framework description can be up to 1024 characters.

Controls (9) [Info](#)

[Edit controls](#)

Control name

Resources are protected by a backup plan

Backup plan minimum frequency and minimum retention

Frequency: 1 day, retention: 1 month

Vaults prevent manual deletion of recovery points

Recovery points are encrypted

Vaults prevent manual deletion of recovery points [Info](#)

Evaluates if backup vaults do not allow manual deletion of recovery points with the exception of certain IAM roles.

Enter up to 5 IAM roles that may delete recovery points manually - *optional*

arn:aws:iam::[REDACTED]:role/Backup_Vault_Region_Admin

Remove

IAM role format: arn:aws:iam::**960959050653**:role/role-name, arn:aws:iam::**960959050653**:*

Add another role

You can add 4 more roles.

Choose backup vaults to evaluate

- All backup vaults
- Tagged backup vaults
- Single backup vault

Backup vault name

RegionalAWSBackupVault

Recovery points are encrypted [Info](#)

Evaluates if recovery points are encrypted.

Choose recovery points to evaluate

- All recovery points
 Tagged recovery points

Minimum retention established for recovery point [Info](#)

Evaluates if recovery point retention period is at least 3 days.

Retention period

Days ▼

Choose recovery points to evaluate

- All recovery points
 Tagged recovery points

Backups protected by AWS Backup Vault Lock [Info](#)

Evaluates if resources are configured to have backups in a locked backup vault.

Minimum retention period for the Backup Vault Lock - *optional*

Specify at least 1 day. If not specified, the control will not enforce a minimum retention period.

Days ▼

Must be a whole number.

Maximum retention period for the Backup Vault Lock - *optional*

Specify up to 100 years. If not specified, the control will not enforce a maximum retention period.

Days ▼

Must be a whole number.

Choose resources to evaluate

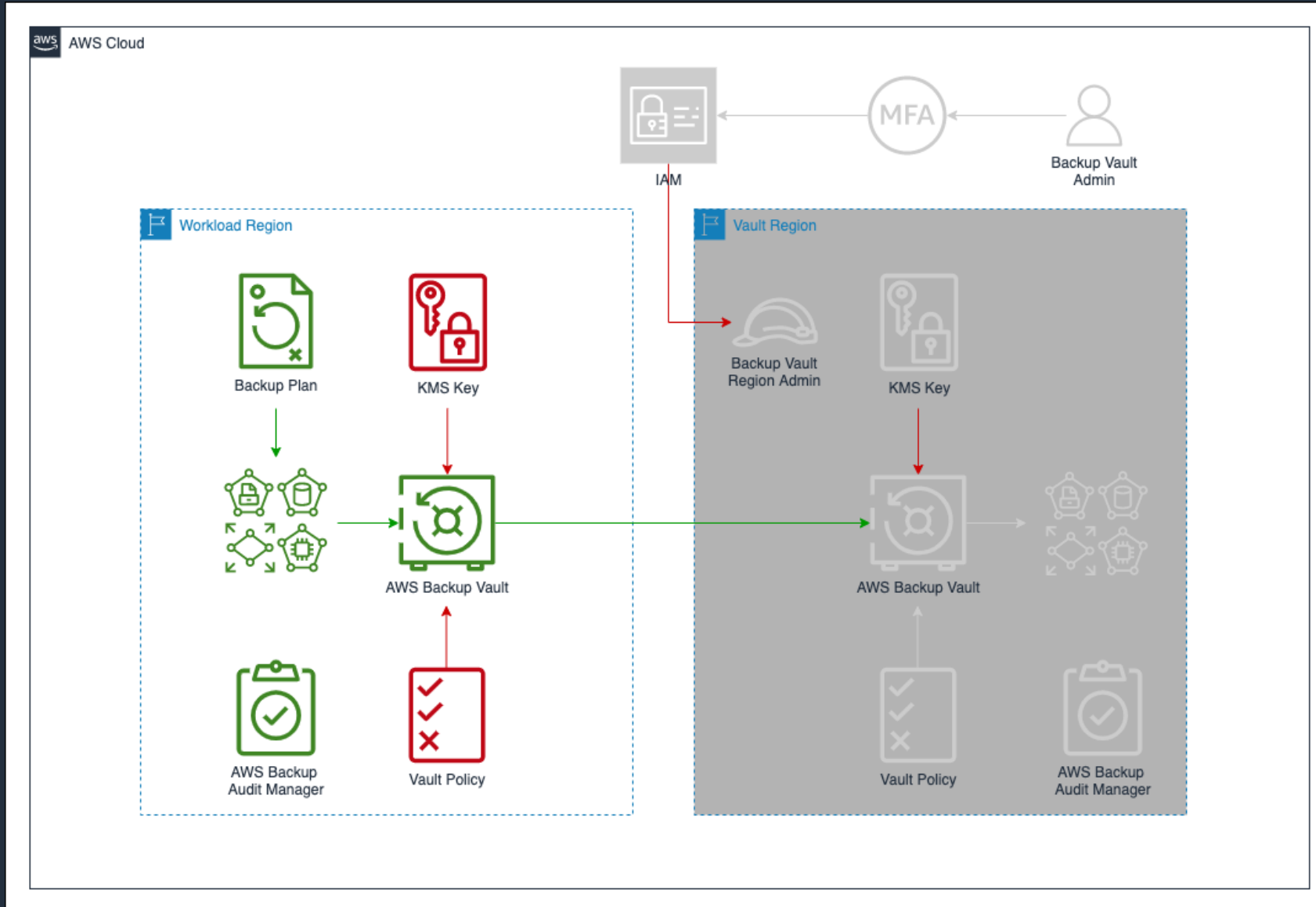
- Resources by type
- Tagged resources
- Single resource

Resource type

▼

EC2 × EFS ×

Workload Region



AWS Elastic Disaster Recovery for fast recovery

AWS Elastic Disaster Recovery – In-AWS Cross Region **Failover**

