AWS Security Series

Part 6
AWS Security: Logging & Monitoring Best Practices

Nitin Sharma
CyberSecurity and DevSecOps Engineer
LinkedIn: linkedin.com/in/nitins87
Quora: quora.com/profile/NitinS-1
Blog: 4hathacker.in

Contents

$ whoami

$ Why Logging and Monitoring significant ?

$ AWS Logging and Monitoring Scenarios

$ AWS Cloud Security Ecosystem

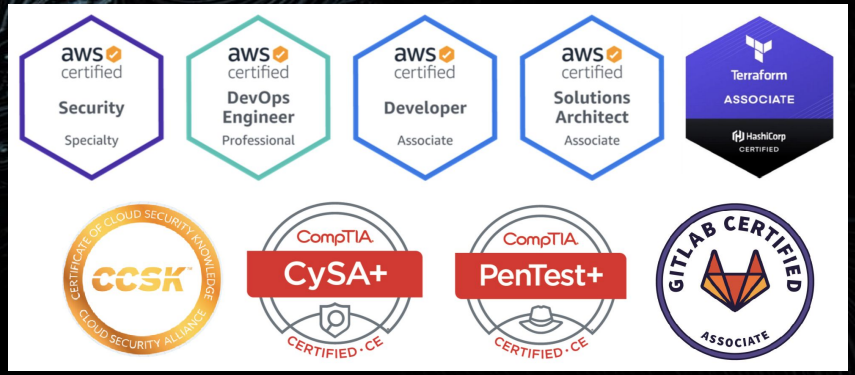
$ AWS Logging/Monitoring: Typical Architecture

$ AWS CloudTrail & Demo

$ AWS CloudWatch & Demo

$ whoami

- Cybersecurity and DevSecOps professional experienced in Cloud Security, Container Security and DevOps Research
- Certifications:



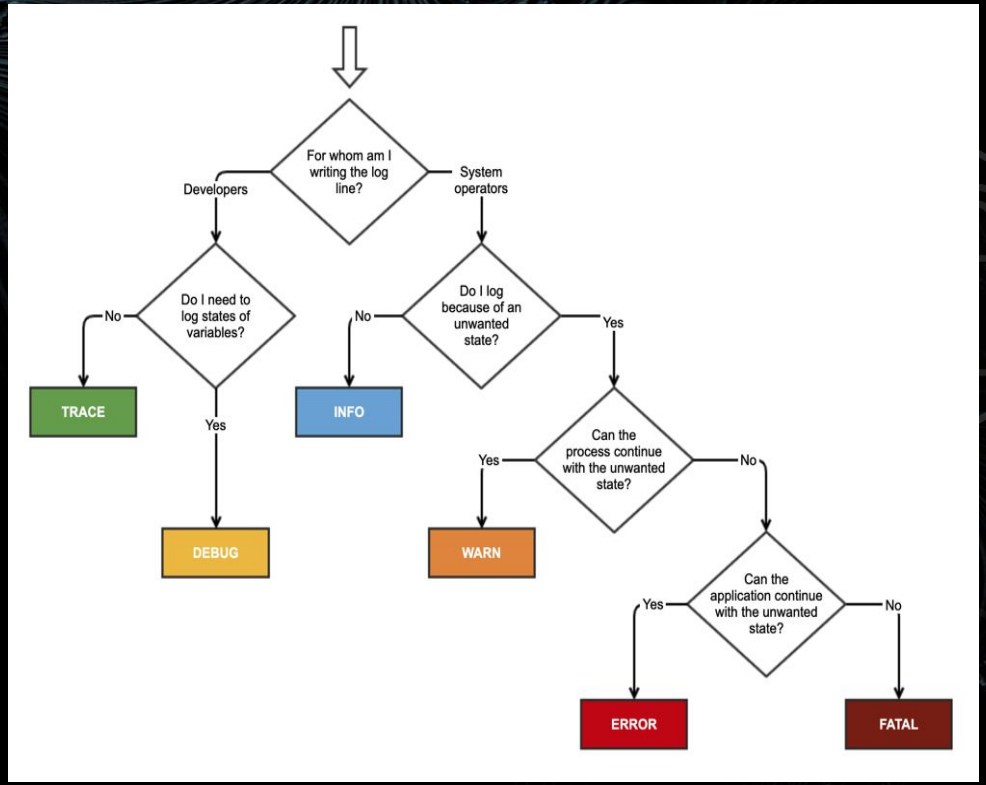
- Published author for "Securing Docker - The Attack & Defense Ways" book under CyberSecrets Publication
- Half Marathon runner, Cyclist and Fitness Enthusiast
- Helping out beginners in Cloud, DevOps and CyberSec at Quora

AWSUGNCR
aws
AWS USER GROUP NCR

$ whoami (To change the generic philosophy)

And then →

$ Why Logging and Monitoring significant ?



(Source: StackOverflow)

- **Scenario 1**: To see for the performance and troubleshooting concerns. (The Developer Picture)

- **Scenario 2**: To see for the infra issues like Memory/CPU utilization, ASG requirements, etc. (The SysOps Picture)

$ Why Logging and Monitoring significant ?

- Scenario 3: The Security Perspective

  [Use Case 1: Threat Detection and Incident Response]

(Source: Medium Blog)

$ Why Logging and Monitoring significant ?

- Scenario 3: The Security Perspective

  [Use Case 2: Security Audit and Compliance]

PCI DSS Requirement 10: Track and monitor all access to network resources and cardholder data

"Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimising the impac
thorough tracking, ale
compromise is very d

What do HIPAA regulations say about system logging? What are HIPAA compliant system logs?

Event, audit, and access logging are required for HIPAA compliance. HIPAA requires you to keep logs for at least six years. These three HIPAA requirements apply to logging and log monitoring:

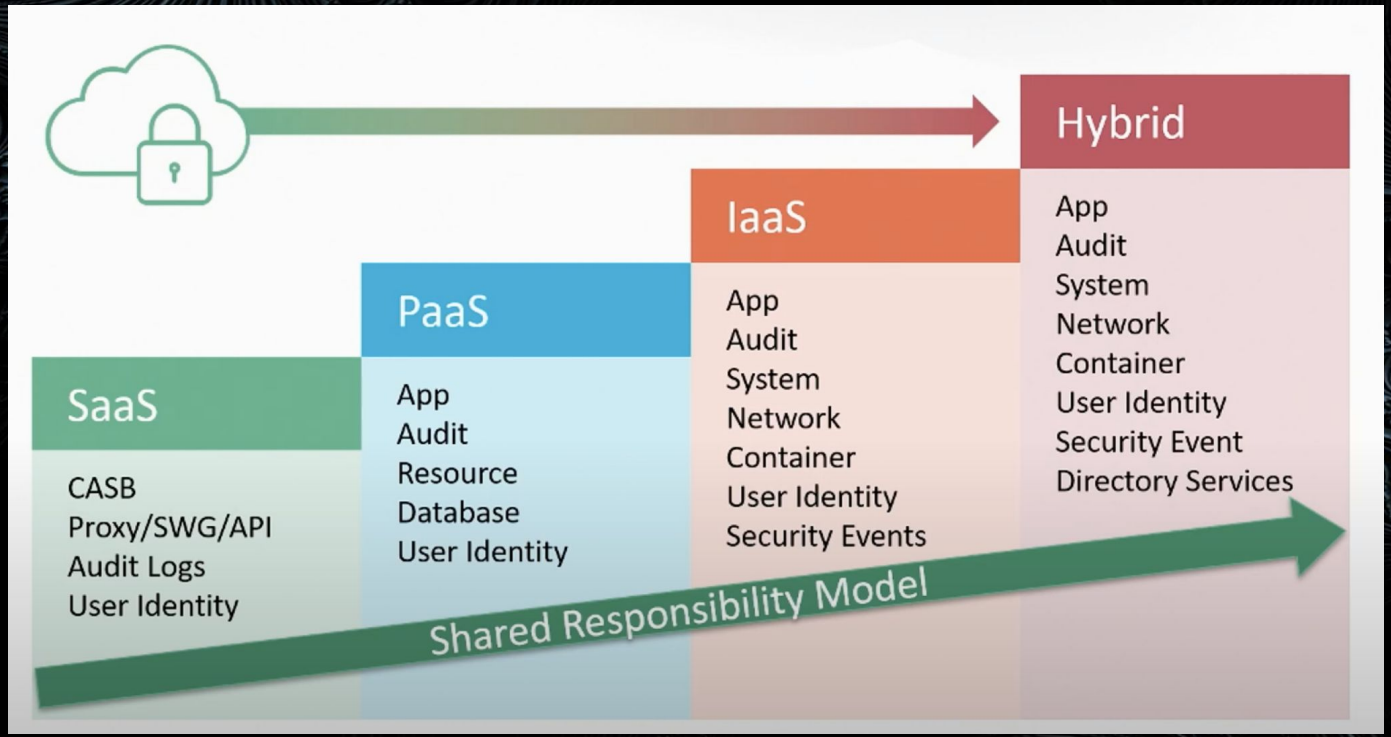
- § 164.308(a)(5)(ii)(C): Log-in monitoring (Addressable). [Implement procedures] for monitoring log-in attempts and reporting discrepancies.
- § 164.312(b): Audit controls (Required). Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
- § 164.308(a)(1)(ii)(D): Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

$ Why Logging and Monitoring significant ?

- Scenario 3: The Security Perspective

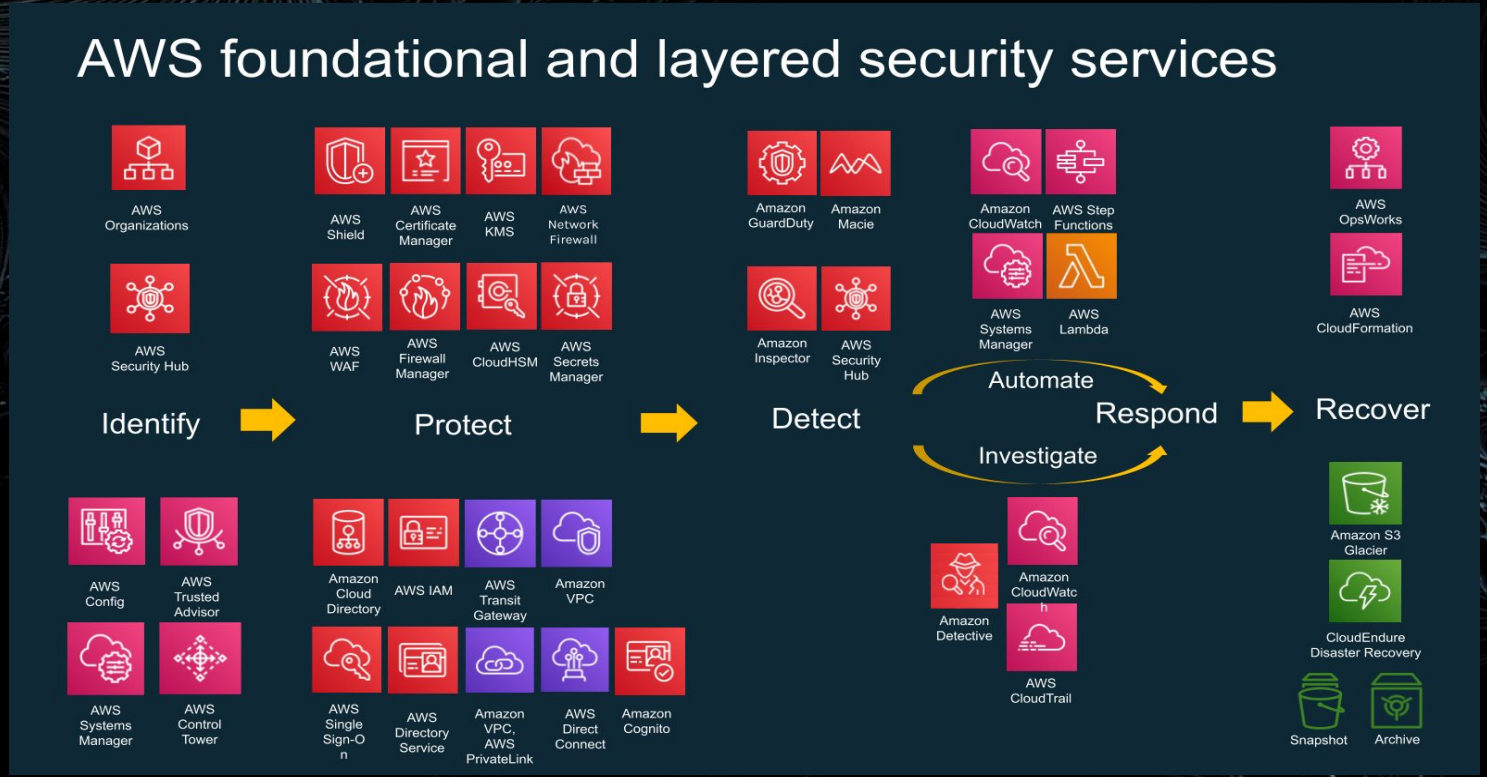
  [Use Case 3: Visibility and Governance]

$ Why Logging and Monitoring significant (in cloud) ?



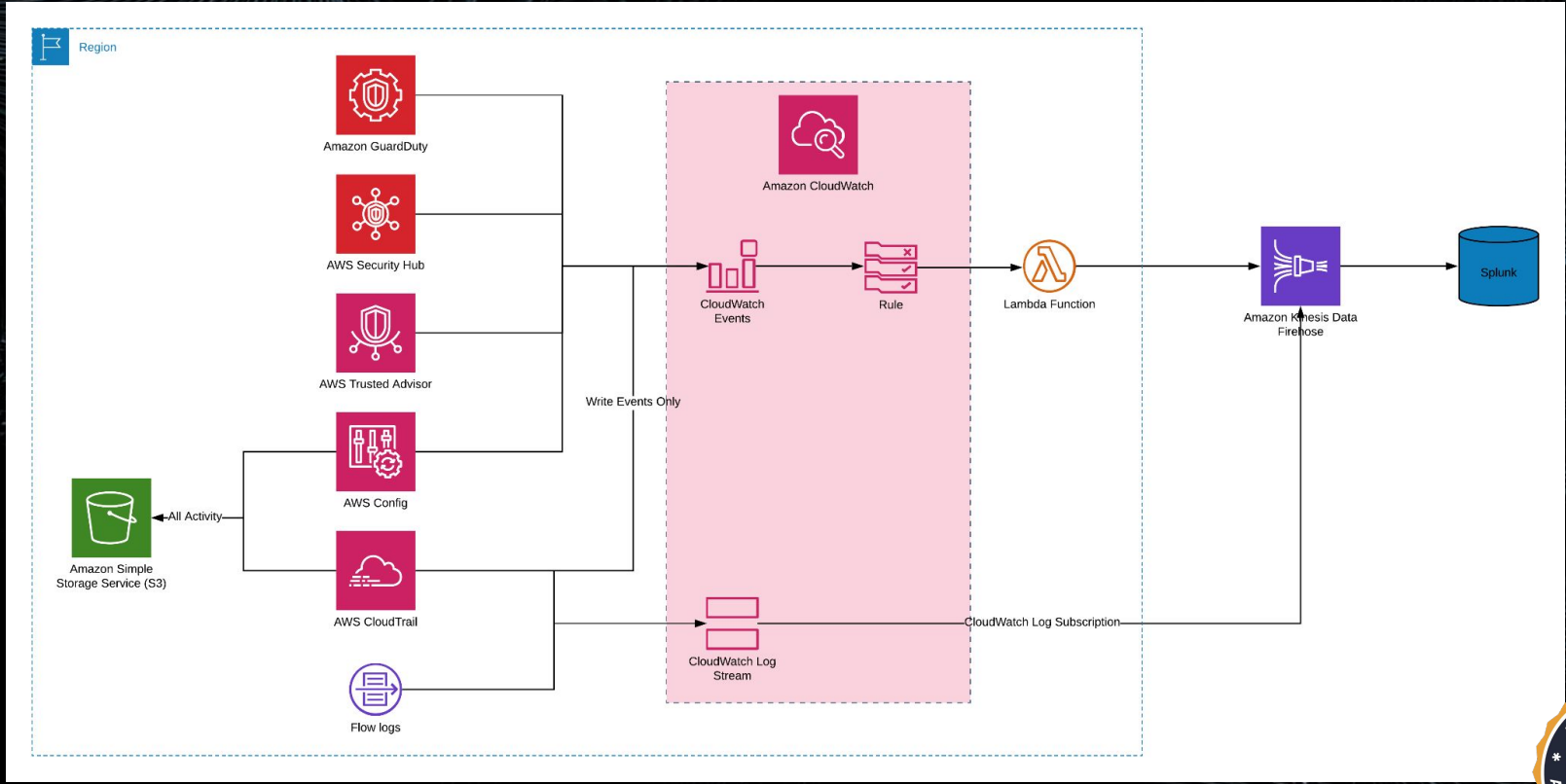
(Source: The Fog of Cloud Security Logging, RSA Conference 2020)

$ AWS Cloud Security Ecosystem



(Source: AWS Security Panel Summary, AllCloud.io)

$ AWS Logging and Monitoring: Typical Arch.



(Source: DisruptOps Blog)

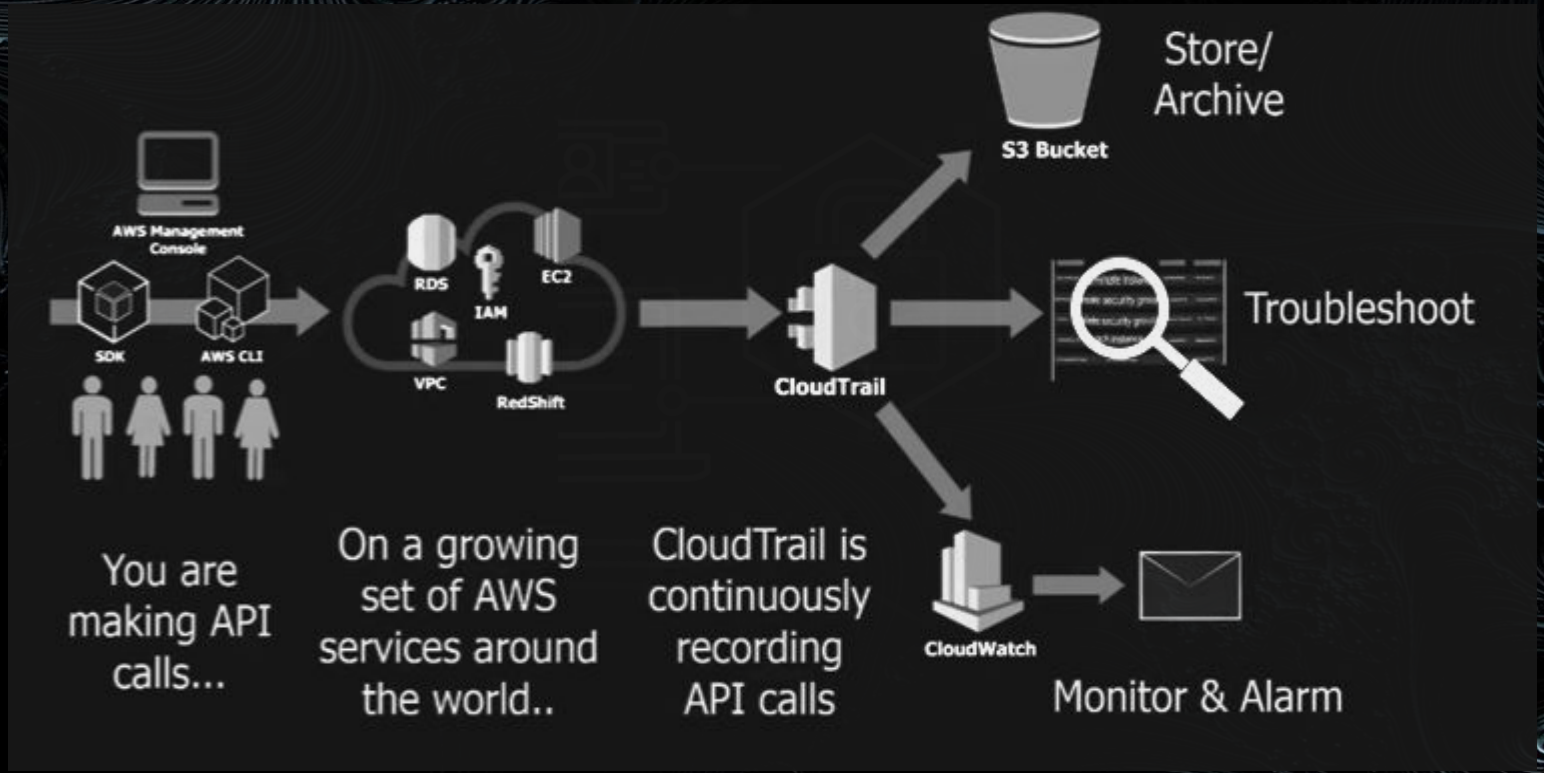
$ AWS CloudTrail

CloudTrail provides event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history (90 days) can be leveraged for security analysis, resource change tracking, and troubleshooting. In addition, CloudTrail can be used to detect unusual activity in your AWS accounts.

SERVICE	WHAT IT COLLECTS	SECURITY VALUE	S3	CloudWatch Logs	CloudWatch Events
CloudTrail	Nearly all API calls, which includes console activity and AWS internal activity on your resources	High	Yes	Yes	Write activity only, and only when CloudWatch Logs enabled

Recommendation: Use S3 and CloudWatch for storage/collection, and CloudWatch Events for alerting.

$ AWS CloudTrail



$ AWS CloudTrail: Event History

Log	CloudTrail Event History
Content	Last 90 days of AWS API call details. It's enabled by default and cannot be disabled. Included events types: Read and Write Management event (control plane). Formerly known as API Activity History.
Format	JSON
Delivery	15 min
Output	Must be queried (API or Console)
Custom/Filter	apply only one filter at a time
Scope	Account
ID	None
Sharing	No
Regional	Yes. IAM Service events in us-east-1 only
Cost	Free
Availability	API Activity History: Mars 2015 (last 7 days on limited services and regions). Event History: August 2017 (GA, all regions), June 2018 (All Management events and last 90 days)

(Source: AWS Logs Overview)

$ AWS CloudTrail: Trail

Log	CloudTrail trail
Content	AWS API call details. Included events types: Read/Write Management event (control plane), Data events (data plane) of S3 bucket and/or Lambda functions, Insights (unusual activity of write management events volume)
Format	JSON
Delivery	15 min
Output	at least to a S3 bucket and optionnaly to a CloudWatch Logs log group.
Custom/Filter	Event type (Management, Data, Insight), Action type (Read, Write) and region (Current, All). KMS events can be excluded. A Organization trail can be created on the Master Account applied on all Accounts and regions .
Scope	Trail per Account or per Organization (current and future Accounts)
Regional	Yes. IAM Service events in us-east-1 only
ID	ARN: `arn:aws:cloudtrail:<region>:<accountID>:trail/<trailName>`
Sharing	No
Cost	The first trail of Management events is free, the following are paying as well as other events types: Data and Insights. Indirect charges: CloudWatch/S3 charges
Availability	November 2013 (GA) November 2016 (S3 Data Events) November 2019 (Insights)

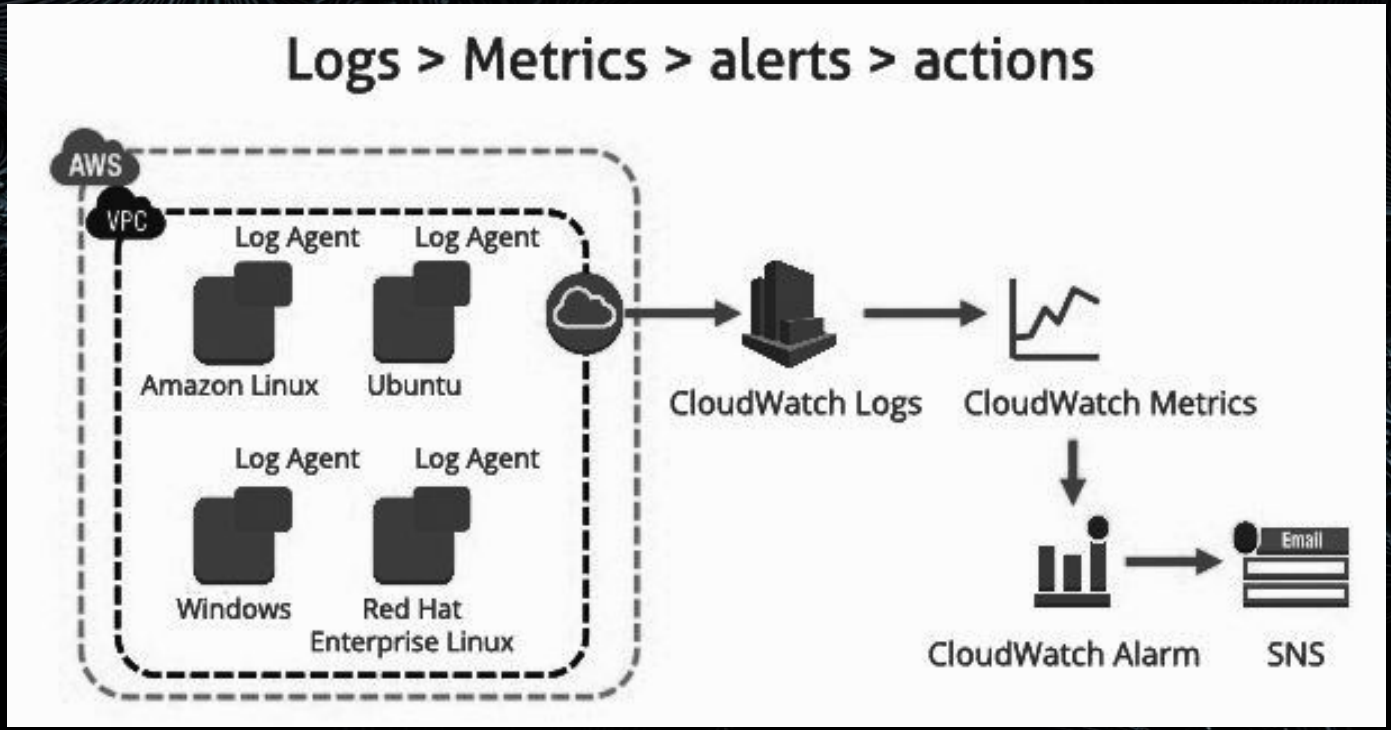
(Source: AWS Logs Overview)

$ AWS CloudWatch:

CloudWatch is a **monitoring and observability service** that provides data and actionable insights to monitor applications, systems, optimize resource utilization, and get a unified view of operational health.

It collects monitoring and operational data in the form of logs, metrics, and events, and visualizes it using **automated dashboards** to provide a unified view of resources, applications, and services. CloudWatch can also be used to **create alarms based on custom metric value thresholds**, or can watch for anomalous metric behavior based on machine learning algorithms. CloudWatch Logs can be manually exported to S3 for long-term storage, or streamed to subscriptions such as Lambda, a Kinesis Data Stream, or Kinesis Data Firehose Stream.

$ AWS CloudWatch:



$ AWS CloudWatch: EventBridge

Log	EventBridge default bus
Content	AWS API call details (recorded by CloudTrail) can be catch in the EventBridge default bus of the Account. Only Write Management event (control plane) are available. Formerly known as 'CloudWatch Events' (same API).
Format	JSON
Delivery	near-real time (1 sec)
Output	EventBridge Rule
Custom/Filter	Service or/and action
Scope	Account
ID	ARN: `arn:aws:events:<region>:<accountID>:rule/<ruleName>`
Sharing	Yes by using another Account bus as Rule target
Regional	Yes. IAM Service events in us-east-1 only
Cost	Free. Indirect: EventBridge rule target charges
Availability	January 2016

(Source: AWS Logs Overview)

$ AWS CloudTrail and CloudWatch

Demo Time…

- Creating a multi-region CloudTrail
- Analysing logs in Event History
- Analysing CloudWatch Logs in Log Group
- Creating Metric Filter for Log Group

Assignment:

- Create Alarm for Metric Filter
- Check Prowler from previous sessions to create Security controls/checks

Thank You...

For queries feel free to connect with AWS Delhi User Group at:

1. **AWS Delhi User Group (MeetUp) - Learn Together, Grow Together**
2. **AWS User Group Delhi NCR (Follow us on LinkedIn Page)**