Enterprise Centralized Logging and Observability Architecture on AWS.

1. Problem Statement

An organization operating multiple AWS accounts lacked centralized visibility into logs and security findings. Logs were dispersed across accounts, limiting detection capabilities. A unified logging and SIEM integration architecture was required.

I implemented this solution to ensure that critical logs from distributed workloads are consistently collected, securely stored, retained according to compliance requirements, and analyzed through a centralized SIEM platform.

2. Objectives

The primary objectives of this implementation were to:

- Centralize AWS service and application logs
- Improve security monitoring and incident investigation
- Support regulatory and compliance requirements
- Enable real-time detection and alerting
- Ensure secure and durable log storage
- Reduce operational blind spots

3. Logging Architecture Overview

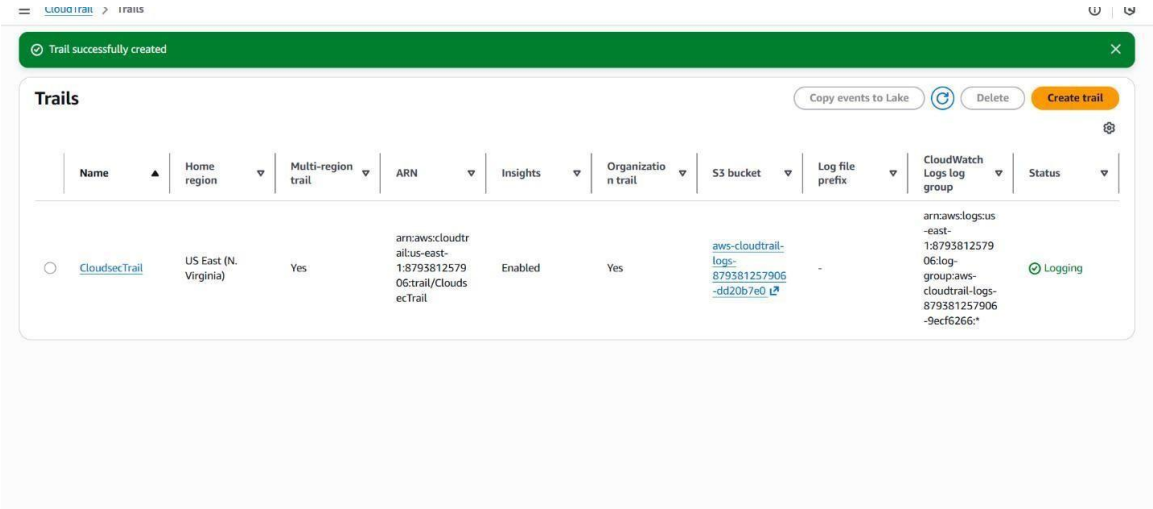
The centralized logging platform was built using:

- AWS CloudTrail
- Amazon CloudWatch Logs
- Amazon Kinesis Data Firehose
- AWS Lambda
- Amazon OpenSearch
- Amazon S3

All service and application logs are routed through CloudWatch and streamed into a secure analytics platform.

4. CloudTrail Configuration

CloudTrail was configured as a multi-region, organization-level trail.



The configuration includes:

- Management event logging
- CloudTrail Insights for anomaly detection
- Centralized S3 storage
- Streaming to CloudWatch Logs

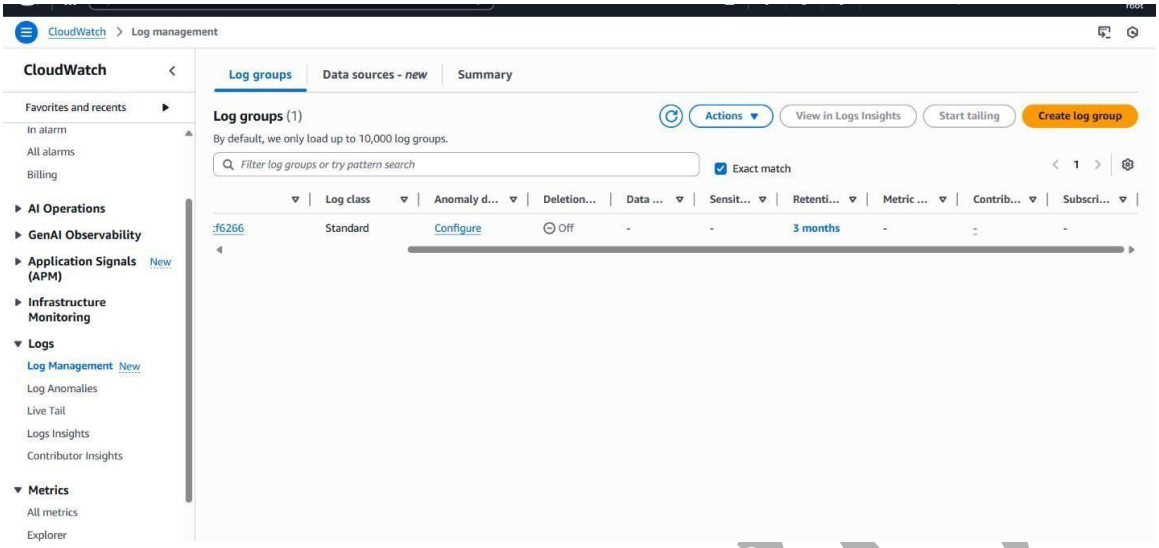
This ensured full visibility into account activity across regions.

5. Log Retention and Lifecycle Management

CloudWatch Log Groups were configured with defined retention periods to prevent indefinite storage.

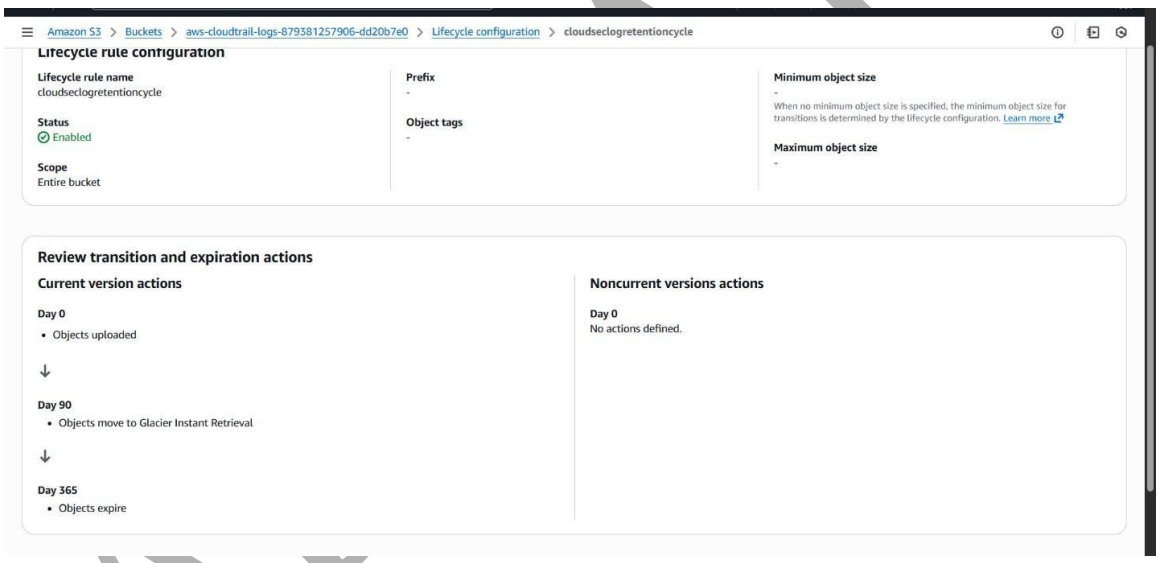
CloudTrail logs stored in S3 are managed using lifecycle policies that:

- Retain logs in S3 Standard for 90 days



- Archive older logs to S3 Glacier

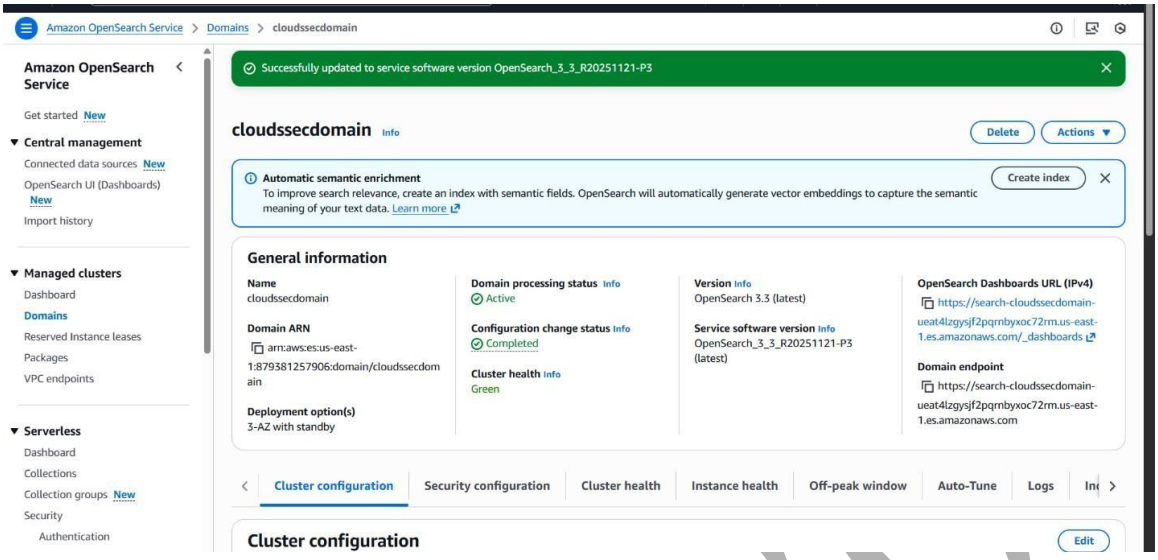
- Delete logs after one year



This approach aligns with common compliance standards such as PCI-DSS while controlling storage costs.

6. Centralized SIEM Platform (Amazon OpenSearch)

Amazon OpenSearch was deployed as the centralized log analytics and SIEM platform.



The domain was configured with:

- No public internet exposure
- VPC-based deployment
- Fine-grained access control
- IAM-based authentication
- Encrypted storage
- Node-to-node encryption

Access was restricted using security groups to authorized ingestion services.

7. Secure Log Ingestion Pipeline

7.1 CloudWatch Subscription Filters

Subscription filters were created to forward all CloudTrail events to Kinesis Data Firehose.

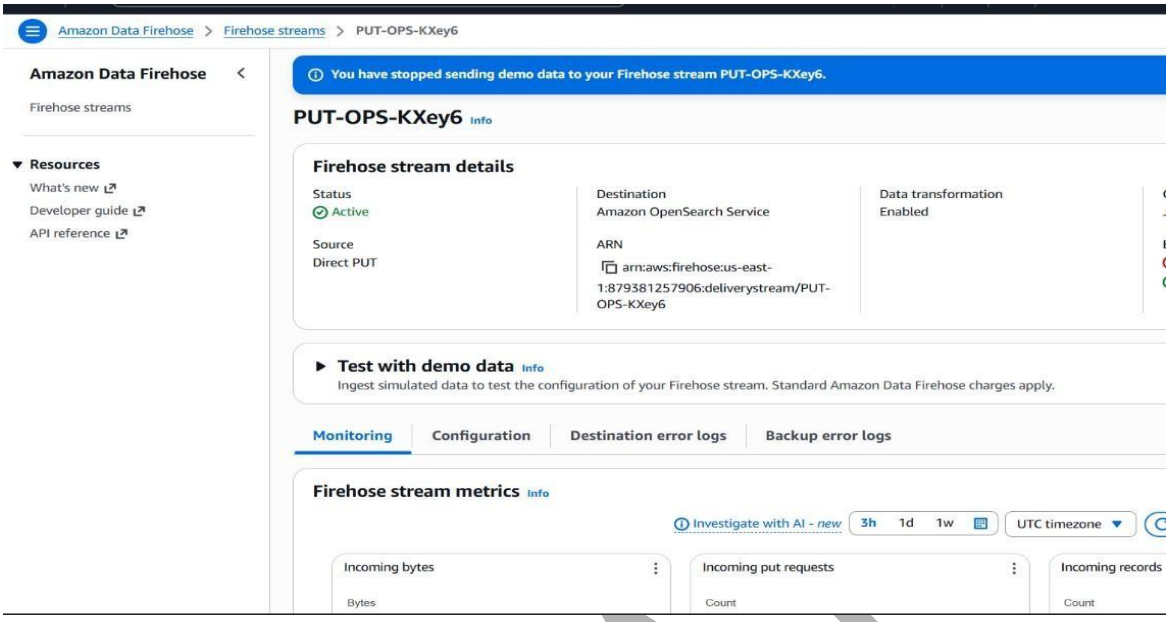
No filtering was applied to ensure complete audit coverage.

7.2 Kinesis Data Firehose Configuration

Firehose was configured with:

- OpenSearch as primary destination

- S3 backup destination
- VPC delivery enabled

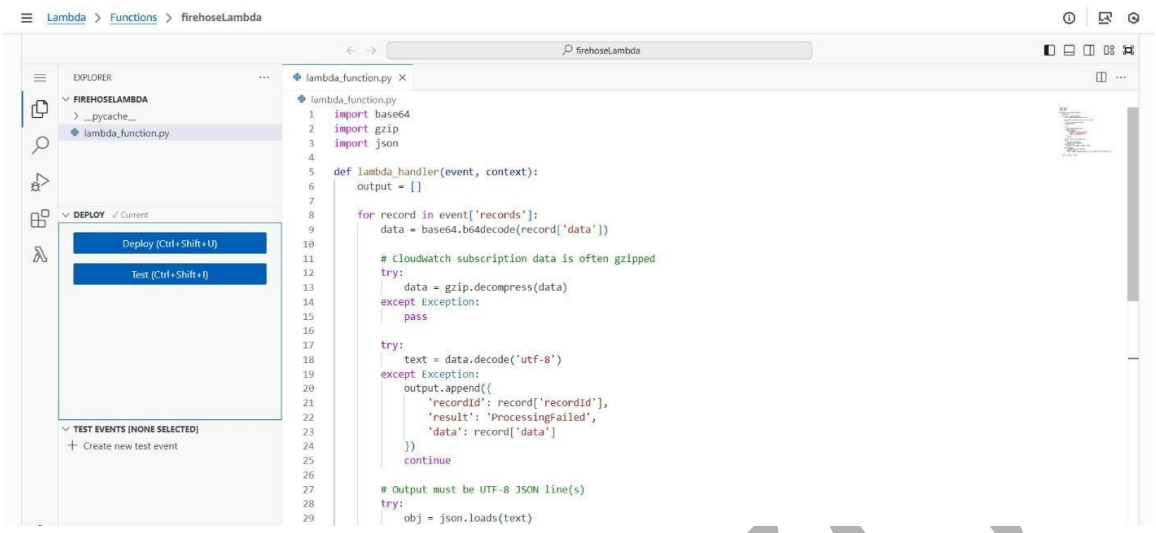


An IAM role was created with permissions for:

- Writing to OpenSearch
- Delivering data to S3
- Managing network interfaces

7.3 Lambda Log Transformation

A Lambda function was integrated into Firehose to perform log transformation.



Functions included:

- Normalizing log formats
- Adding metadata
- Ensuring indexing compatibility

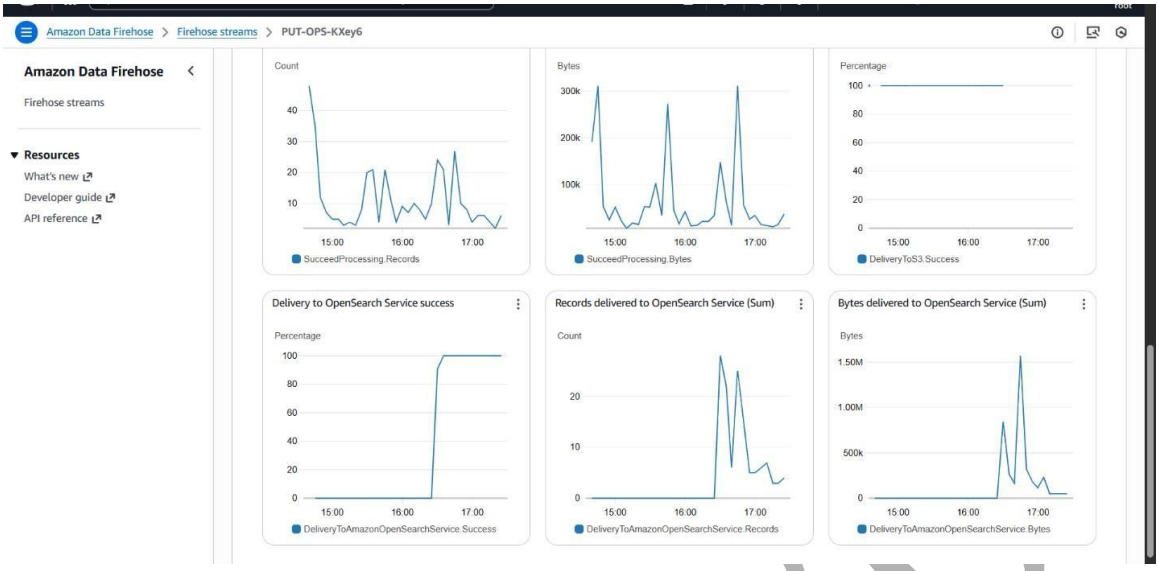
This improved searchability and consistency.

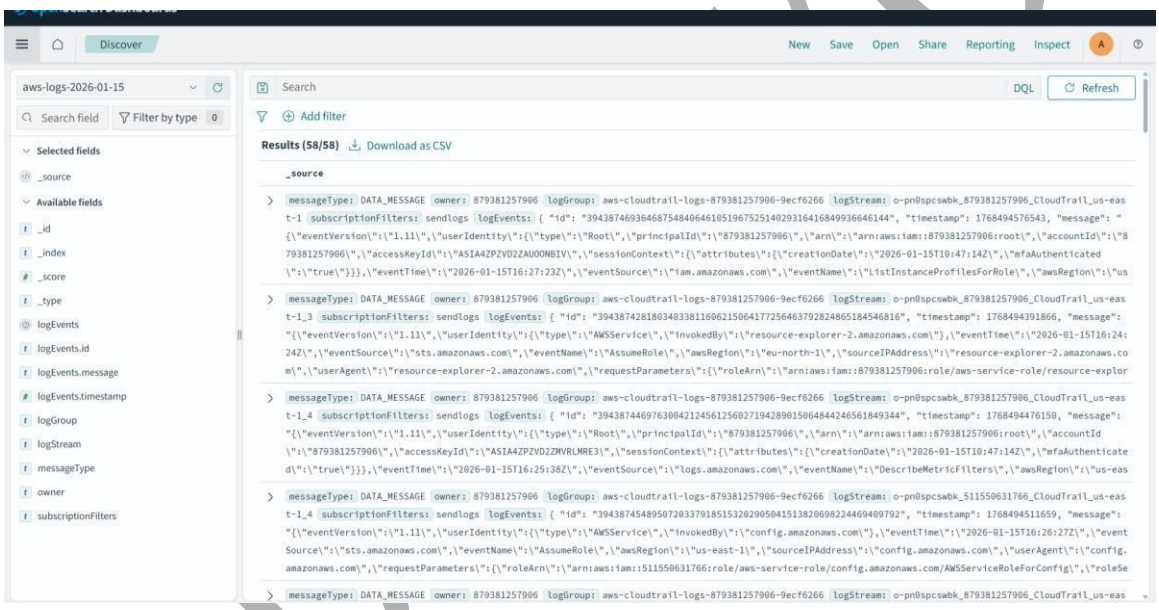
8. Pipeline Validation and Testing

The logging pipeline was validated end-to-end.

After resolving VPC network restrictions, log ingestion was confirmed in OpenSearch.

Indexed records were verified to be searchable and complete.



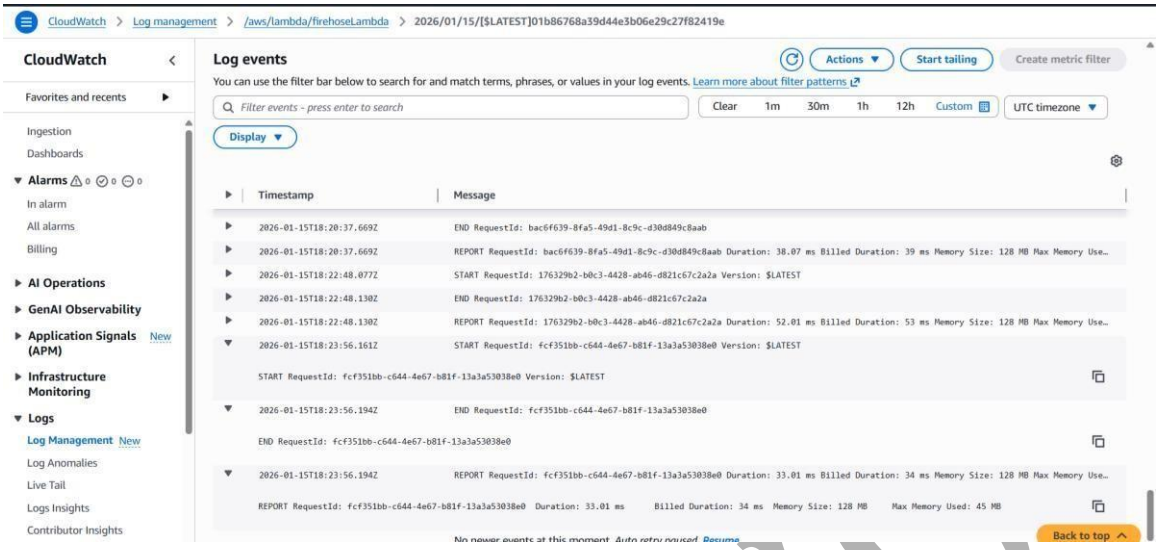


9. Workload Log Integration

9.1 AWS Lambda Logging

Lambda workloads were verified to emit logs to CloudWatch.

Test invocations confirmed correct log group and stream creation.

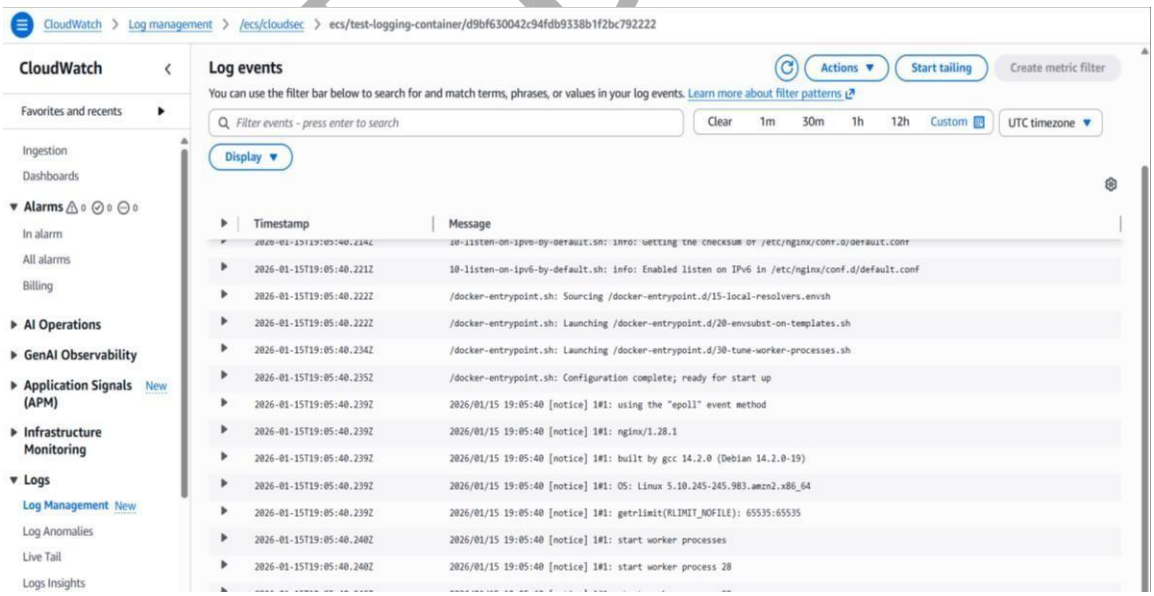


9.2 ECS Container Logging

ECS Fargate workloads were configured using the awslogs driver.

Application logs were verified in dedicated CloudWatch log groups.

This ensured container workloads were centrally monitored.



10. Durability and Backup Strategy

All logs delivered through Firehose are backed up to S3.

Lifecycle policies archive data to Glacier for long-term retention.

This provides durability, disaster recovery, and compliance support.

11. Governance and Documentation

All logging configurations, access policies, and retention standards were documented.

This supported:

- Audit reviews
- Compliance reporting
- Incident investigations
- Operational continuity

12. Outcomes and Impact

This implementation delivered:

- Centralized security visibility
- Improved incident response capability
- Compliance-aligned log retention
- Secure SIEM deployment
- Reliable log delivery
- Reduced operational blind spots

13. Conclusion

I designed and implemented a secure, scalable, and compliant centralized logging and observability platform on AWS.

Through automated log collection, secure analytics, and structured retention policies, this solution supports enterprise security monitoring, investigations, and regulatory requirements.