Assumptions:

1. System is only used by Agency Officers, not public users.
2. Data is not sensitive and can be stored in the cloud
3. Existing perimeter tier that we can leverage on
4. System access will be via WOG only.
5. Sensor data is sent over Internet
6. Raw video data is stored short-term (e.g. 3 days), processed data needs to be stored long term.
7. Visualisation platform is available for re-use
8. Dashboards displays data snapshot, not real-time. Visuals are updated through refreshing the Dashboard.
9. There is an an existing CIAM, (e.g. Azure Entra ID, OKTA, AWS Congnito), that can be integrated to Data and Visualisation Platform
10. Access control is managed at CIAM, Fine Grained Access Control is managed at Data Platform
11. Centralised SIEM and log storage available to leverage on
12. HA SLA: 99.95%
13. RTO / RPO: 4 hrs, 5min
14. AI/ML capabilities are optional, not mandatory

Queries:

1. Is there a technology stack that the customer prefers?
2. Are there any existing licenses that we can reuse?
3. What are the expected performance benchmarks for:
    a. Raw data processing
    b. Data transformation pipelines
    c. Data query

Design objectives

- A robust and resilient data platform to process and store video data from edge for analytics and AI/ML workloads

Design Principles

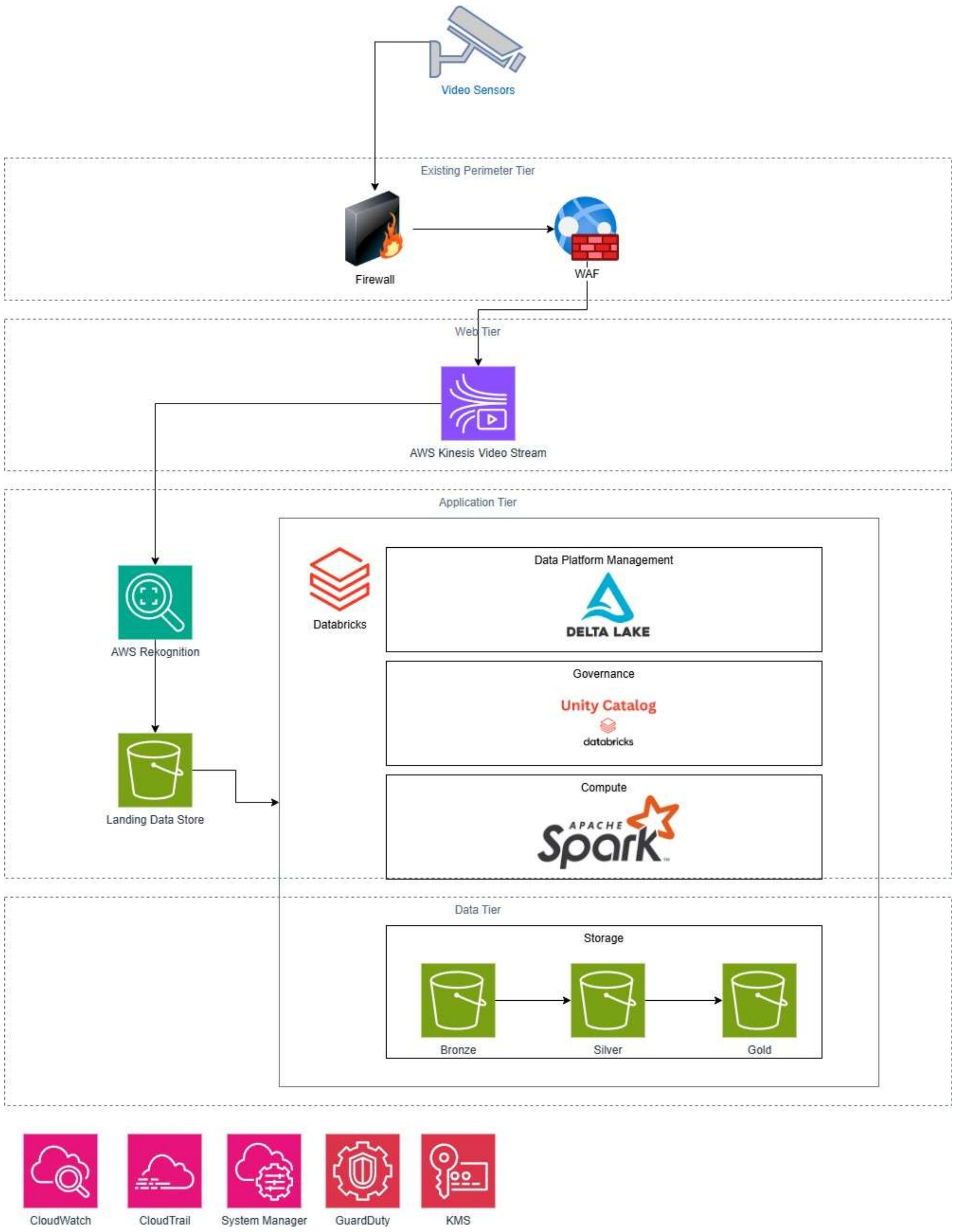
1. Security – Security is always a priority. Security features must be robust to meet the stringent requirements of IM8 and other agency security requirements.
2. Maintainability – System should be highly maintainable with low complexity. Solution to leverage on managed services where ever possible
3. Reliability – System has a high HA SLA, RTO and RPO benchmarks. All components must meet be able to meet the SLA requirements

4. Performance – System must meet the performance benchmarks at the 95th percentile
5. Scalability – The proposed solution must demonstrate elastic scalability to uphold performance benchmarks under abrupt or high-volume spikes in incoming data.
6. Resource-Cost Optimised – the proposed solution should keep idle resources to a minimum. Options should also be provided for cost-optimised pre-emptive scaling.
7. Observability – all activities performed within the data platform must be auditable

Design Overview

- Data Lakehouse architecture for unified data management, flexibility storage of data lake and structure, performance and management features of data warehouse
- Medallion Architecture to organise data into layers where each layer incrementally improves data quality and structure
- Cloud-Native services to sink and process raw data from source.

Proposed Solution



1. The solution will be deployed in an N-Tier architecture to support a strong security posture.
2. Video Sensor data will be sent through the Internet via the Perimeter Tier to AWS Kinesis Video Stream

3. AWS Rekognition will process the data in Kinesis Video Stream to extract Event Data in the format of Dataset A and store them in .parquet format in a temporary landing store in AWS S3.
4. Databricks use AutoLoader to continuously ingest data into bronze schema from Landing S3 bucket. Data retention policy in AWS Kinesis Video Streams and Landing S3 bucket will be configure for 3 days.
5. Bronze schema is monitored and will trigger ELT pipelines for downstream data transformations into silver schema. As TopXItemByGeographicalLocation addresses the issues and concerns that the users raised regarding data quality, will be updated to write the output into silver schema. Visualisation platform consume data from silver schema to produce the required dashboards.
6. The gold schema contains models of the highest quality and can be shared commercially. As there is no requirement at the moment for this, there will be no pipelines to be setup.
7. All data processed within Databricks is tracked and catalogues through Databricks Unity Catalogue. Unity catalog stores all the metadata on all objects (schema, tables, even AI / ML models) and provides capabilities to manage access control to the data. Dashboards will connect to Databricks through a connection string, similar to most data sources. Access credentials are managed by WOG AD and access controls are managed in Unity Catalog. Unity Catalog also provide data lineage for traceability of data flows.
8. All logs from the solution are logged to CloudWatch Logs. We can configure CloudWatch to send alert if any of the monitored matrix are breached, e.g. compute utilisation, job duration etc.
9. Perimeter Security is provided through existing perimeter tier. Additionally we can attach AWS WAF to scan all traffic passing from Perimeter Tier into the solution.
10. All data in transit is secure using TLS only traffic. TLS should be 1.2 and above.
11. All data at rest is encrypted with AWS KMS.
12. All outbound data will past through the firewall in the perimeter tier. If the downstream system is also hosted on AWS, we can integrate the 2 systems using private links to restrict the traffic within AWS network.
13. We will also enable GuardDuty to continuously detect any threats to the system.

Technology Stack

Component	Product	Reason
Data Platform	Databricks	Databricks is a unified analytics platform for data science, machine learning, and AI, built on an open lakehouse architecture. It allows organizations to process and analyze large volumes of data by combining the best features of data lakes and data warehouses. The platform offers a collaborative environment for data teams and is a managed service

		that simplifies infrastructure management for tasks like building, deploying, and managing data and AI applications.
Video Streaming	AWS Kinesis Video Streams	Amazon Kinesis Video Streams is a managed service that securely streams video from connected devices to Amazon Web Services for storage, playback, and analytics. It allows you to ingest video and other time-series data from sources like security cameras, smartphones, and drones, then use APIs and SDKs to process, analyze, and store the data. The service automatically handles the infrastructure for ingestion and scaling, making it easier to build applications for tasks like real-time computer vision and machine learning.
Video Analytics	AWS Rekognition	AWS Rekognition is a cloud-based service that uses deep learning to analyze images and videos, making it easy to add powerful visual analysis capabilities to applications without needing machine learning expertise. Its key features include detecting objects, scenes, and text in images, recognizing faces for verification and comparison, and identifying unsafe content. It will be used to extract event information through video analysis to be stored on the data platform. It can also query videos by providing an image as input.
Object Store	AWS S3	AWS S3, or Amazon Simple Storage Service, is an object storage service provided by Amazon Web Services (AWS) that is built to store and retrieve any amount of data from anywhere on the web. It offers industry-leading scalability, availability, security, and performance for a wide range of use cases like backups, cloud-native applications, and data lakes.
Monitoring and Observability	AWS CloudWatch	AWS CloudWatch is a monitoring and observability service for AWS cloud resources and applications. It collects and tracks metrics, logs, and events to provide a unified view of operational health. Users can set alarms to trigger automated actions, such as scaling resources, and gain system-wide visibility to optimize performance, detect anomalies, and reduce downtime.
Governance	AWS CloudTrail	AWS CloudTrail is a service that enables operational auditing, risk auditing, governance, and compliance for an AWS account by logging all user activity and API calls as events. It provides a record of "who did what, where, and when" within an AWS environment, including actions taken through the AWS Management Console, command-line interface (CLI), SDKs, and other AWS services. These events can be used for security

		monitoring, troubleshooting, and meeting compliance requirements.
Resource Management	AWS System Manager	AWS Systems Manager is a management service that provides a central hub for operating AWS and hybrid cloud environments. It enables you to automate operational tasks, view and control your nodes at scale, and maintain security and compliance by applying patches, collecting inventory, and managing configurations. Key features include Patch Manager, Session Manager for secure access without SSH keys, and Run Command for remote task execution.
Intelligent Threat Detection	AWS GuardDuty	AWS GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious or unauthorized activity. It uses machine learning, anomaly detection, and threat intelligence feeds to analyze data sources like VPC Flow Logs, CloudTrail event logs, and DNS logs to identify threats such as malware, credential compromise, and communication with malicious IP addresses.
Key Management	AWS KMS	AWS KMS is a managed service that creates and controls cryptographic keys used to encrypt and protect data across AWS services and in your applications. It provides a centralized and secure way to manage keys, with operations protected by FIPS 140-3 validated hardware security modules (HSMs). With AWS KMS, you can encrypt data, perform digital signing, and use asymmetric or symmetric keys for your data protection needs.