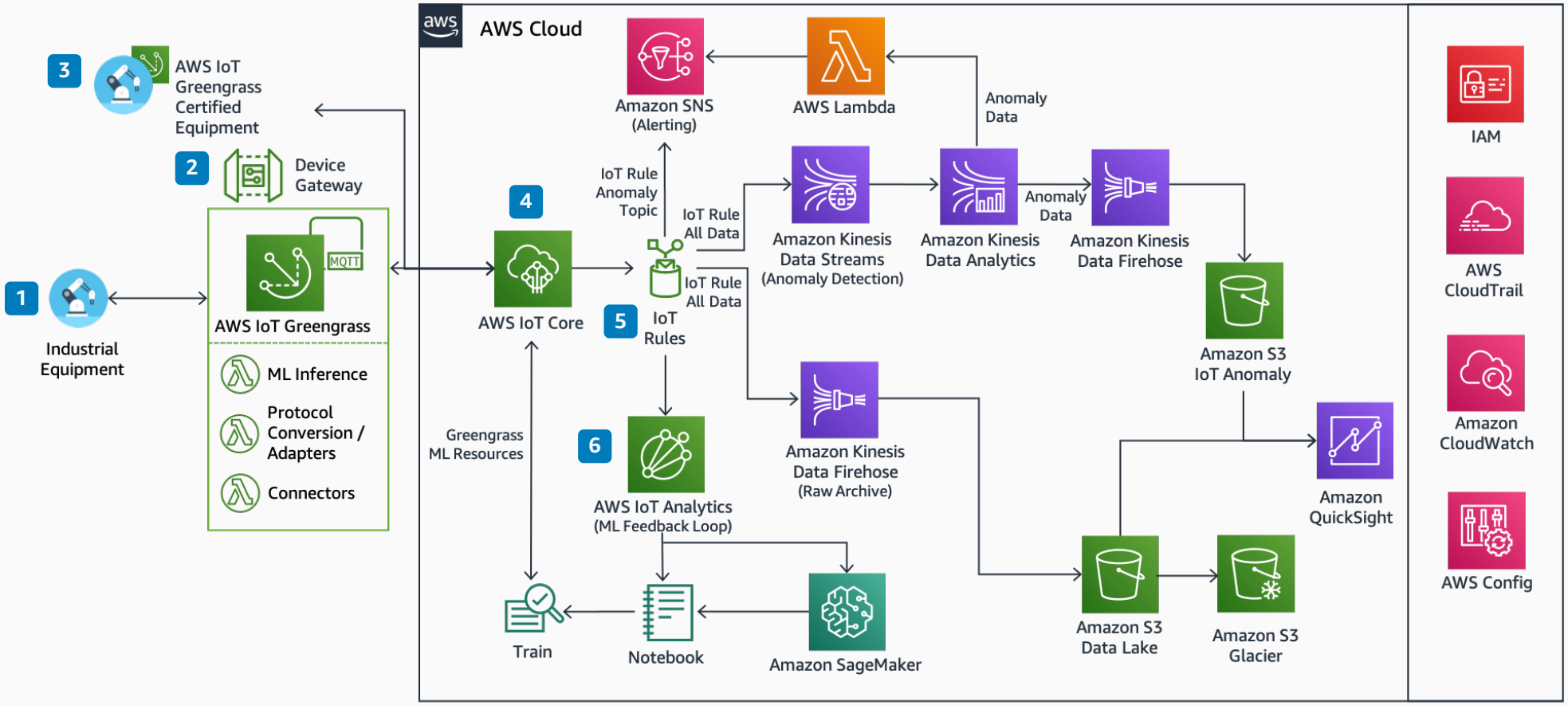
AWS Industrial

Anomaly Detection using AWS IoT (Part 1 of 2)

Create an anomaly detection notification workflow with a machine learning feedback loop using AWS IoT services, Amazon Simple Notification Service (Amazon SNS), Amazon SageMaker, and Amazon Kinesis Data Analytics.



1. Legacy **industrial equipment** uses a variety of lightweight, domain-specific protocols for intra-network communication. The equipment does not support direct connectivity and resides behind a **Device Gateway** located in the facility.

2. The **Device Gateway** translates protocols to create standardized communication capabilities to the connected IoT environment. **AWS IoT Greengrass** enabled gateway devices uses protocol conversation and protocol adapters to support translation between devices and the **Device Gateway**.

3. **AWS IoT Greengrass Certified Equipment** connect directly to the **AWS IoT Core**.

4. **AWS IoT Core** multiple protocol support enables devices to communicate with each other when using different protocols. **AWS IoT Core** endpoints allow devices/gateways to stream data to **AWS IoT Core** that can be acted upon for anomaly detection, archival, analytics, and machine learning feedback loops.

5. **IoT rules** query messages traversing **AWS IoT Core**, filters messages that match rules, and passes messages or subset of values to AWS service or third-party endpoint.

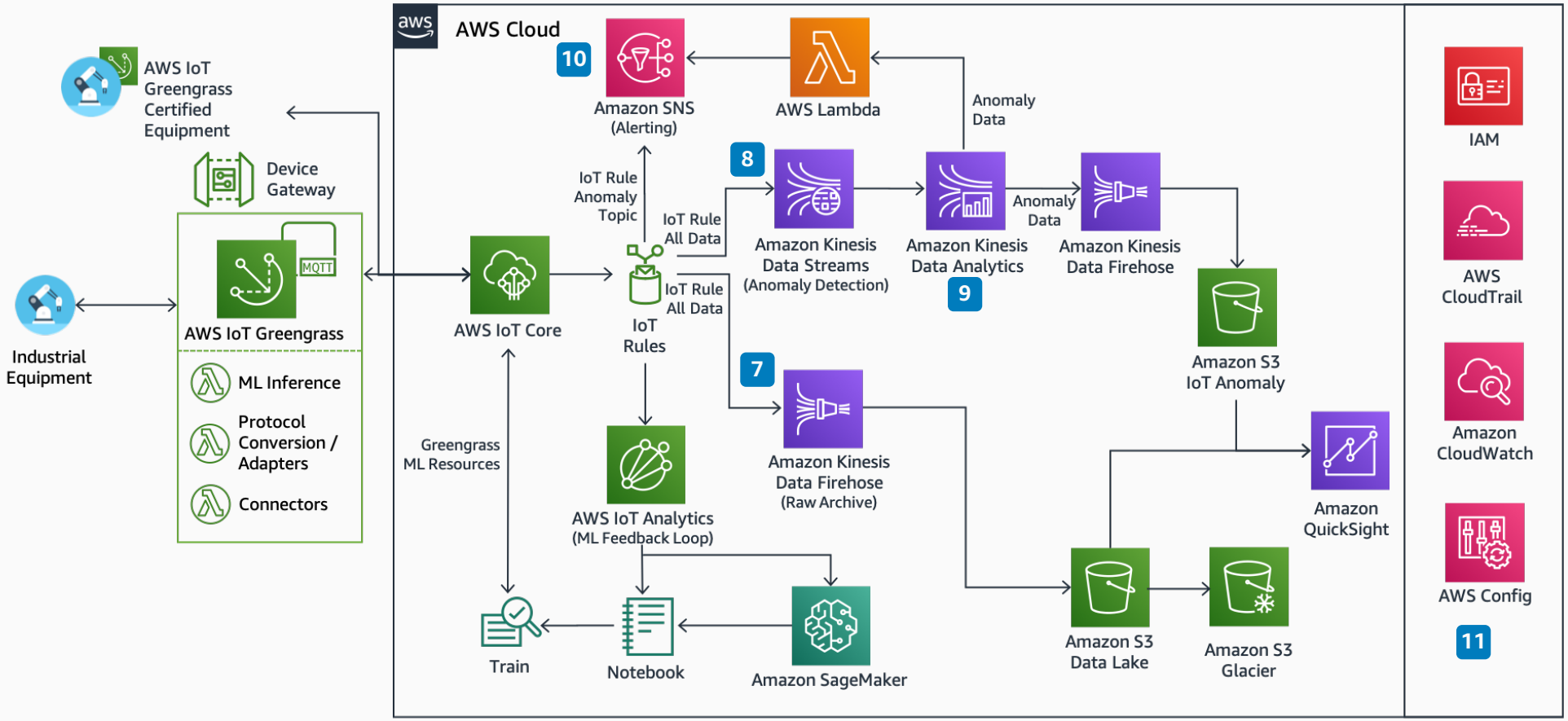
6. Messages that meet IoT rule filter criteria are routed to **AWS IoT Analytics** for a machine learning feedback loop using **Amazon SageMaker** hosted notebook. Data scientists can apply changes to the model and run training passes using **AWS IoT Analytics** data sets. Trained models are deployed using **AWS IoT Greengrass** groups.

AWS Reference Architecture

AWS Industrial

Anomaly Detection using AWS IoT (Part 2 of 2)

Create an anomaly detection notification workflow with a machine learning feedback loop using AWS IoT services, Amazon Simple Notification Service (Amazon SNS), Amazon SageMaker, and Amazon Kinesis Data Analytics.



7 Raw device messages that meet IoT rule filter criteria are routed to an **Amazon Kinesis Data Firehose** stream, then onward to **Amazon S3** for storage. **Amazon QuickSight** provides dashboard visualizations of raw data. **Amazon S3 bucket lifecycle policies** move raw data to **Amazon S3 Glacier** for archiving.

8 Raw device messages that meet IoT rule filter criteria are routed to an **Amazon Kinesis Data Stream** where **Amazon Kinesis Data Analytics** runs queries to determine anomalistic behavior in data set. Anomalous data is pushed to **Amazon Kinesis Data Firehose** and streamed to **Amazon S3** as verified anomaly. **Amazon QuickSight** provides dashboard visualizations of anomalous data.

9 **Amazon Kinesis Data Analytics** invokes an **AWS Lambda** function containing message data and sends **Amazon SNS** alert to individuals or to start a new workflow.

10 **Amazon SNS** sends notifications of anomalies to teams or starts automated response workflow to other systems.

11 Security and monitoring provided by **AWS Identity and Access Management** policies and roles, **AWS CloudTrail**, **Amazon CloudWatch**, and **AWS Config**.

AWS Reference Architecture