# **Guidance for Connecting Automated Inputs to Contact Centers on AWS**

This architecture diagram shows how to enable real-time error, anomaly detection, automated incident resolution, and seamless contact center integration for IoT-connected systems. This servers to reduce downtime and optimize issue resolution through AI-driven workflows. Steps 1-7 are shown below; steps 8-11 are shown on the next slide.



loT

2

3

5

6

′7b

#### IoT devices publish to AWS IoT Core.

Errors or alerts generated by devices are published to designated IoT topics, such as an "error topic" or "basic ingest topic". These inputs are then routed to an **AWS Lambda** function based on the defined IoT rule.

Devices publish standard telemetry data to an IoT topic. This real-time data can be acted on, while a copy is also routed to a data store for the purposes of analytics and anomaly detection.

4 The Lambda function transmits the error code, device ID, and any additional relevant information to Amazon Bedrock Agents.

The data is streamed through Amazon Data Firehose and ingested into an Amazon Simple Storage Service (Amazon S3) data store.

An Amazon EventBridge rule invokes a Lambda function at a schedule frequency specified by the user using a cron expression. If anomaly is detected in the stored data using Amazon SageMaker Canvas, it sends relevant information including device ID(s) to the Lambda function.

Amazon Bedrock Agents reviews the received input and takes appropriate action by triggering the right action group.

The agent queries the QnABot on AWS knowledge base to retrieve any relevant supplementary information or policies, including remediation procedures. This is appended to the ticket if required in step 7b.

The agent creates a ticket within the contact center and enriches the message with any data from step 7a.



### **AWS Reference Architecture**

## **Guidance for Connecting Automated Inputs to Call Centers on AWS**

This architecture diagram shows how to enable real-time error, anomaly detection, automated incident resolution, and seamless contact center integration for IoT-connected systems. This servers to reduce downtime and optimize issue resolution through Aldriven workflows. Steps 1-7 are shown below; steps 8-11 are shown on the next slide.



If the automated remediation policy is enabled, the system will automatically remediate the IoT device by executing an AWS IoT Job.

8

9

The site operator, owner, or customer is notified of the incident and any actions taken.

**10** The site operator engages with the QnABot on AWS solution along with the ability to request additional information or access historical data as needed.

11 The company's manuals, standard operating procedures (SOPs), and engineering specifications are ingested into an Amazon S3 bucket, which the knowledge base then references.



### **AWS Reference Architecture**