Threat Detection and Containment: A malicious actor compromises an EC2 instance

and initiates unauthorized data exfiltration.

1. Detection: Amazon VPC Flow Logs reveal abnormal outbound traffic. A SageMaker machine learning modelidentifies this behavior as anomalous

A screenshot of a computer

Description automatically generated

A black screen with white text

Description automatically generated

1. Sagemaker notebook creation

A screenshot of a computer

Description automatically generated

3 . Sagemaker Training via jupytor notebook

A screenshot of a computer

Description automatically generated

3.Sagemaker deployed

A screenshot of a computer

Description automatically generated

4.Anomaly detection and isolation

A screenshot of a computer

Description automatically generated

Step 5: Measure the Response Time

1. In CloudTrail, check:
   * Time when the user accessed AWS resources

"creationDate": "2025-07-06T20:05:01Z UTC

* + Time when Lambda triggered and blocked the access

2025-07-06T20:05:04Z UTC

A screenshot of a computer

Description automatically generated

Subtract timestamps to calculate response time (goal: under 2 seconds)

2025-07-06T20:05:09.016 -2025-07-06T20:05:04Z = 3 miliseconds