

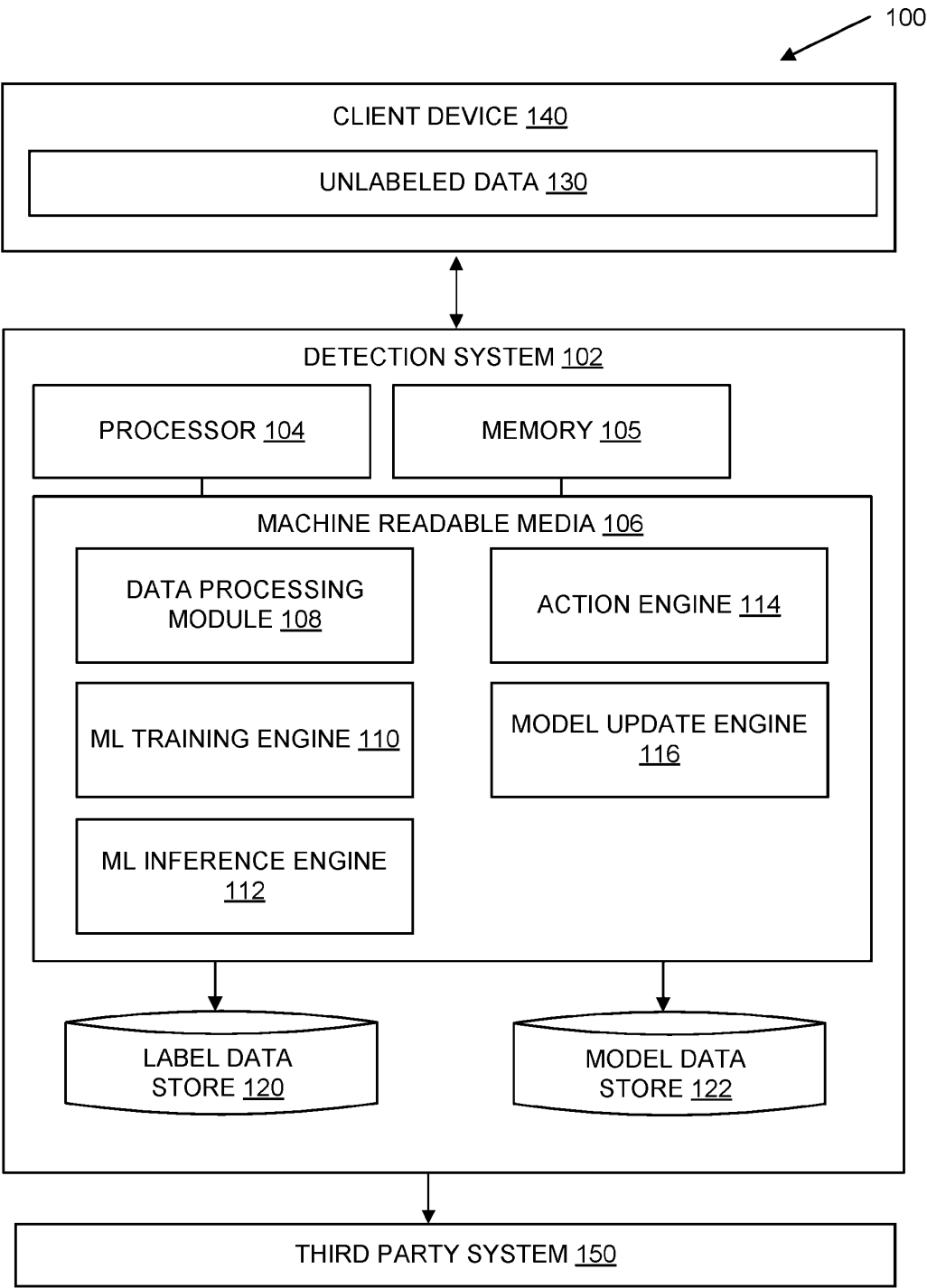


FIG. 1

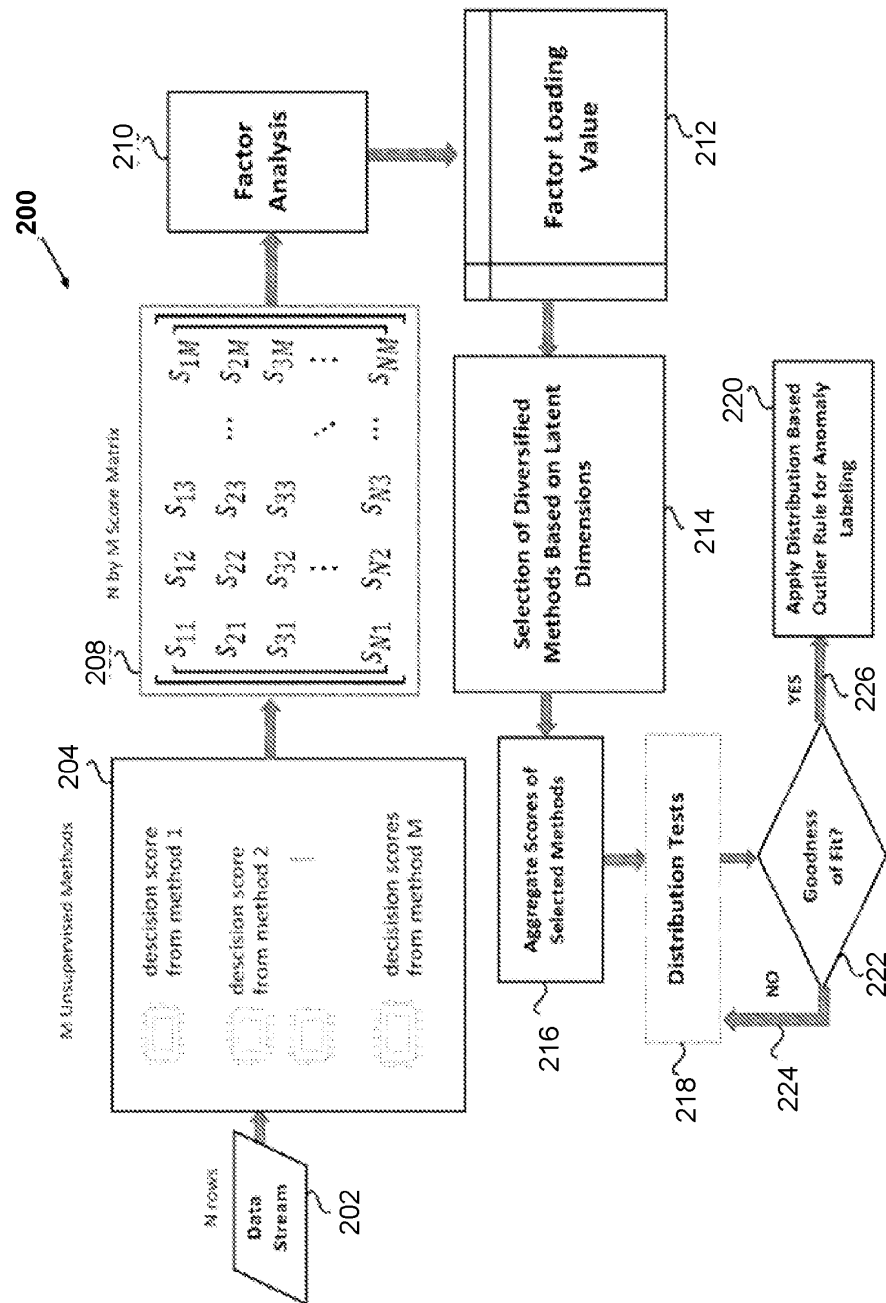


FIG. 2

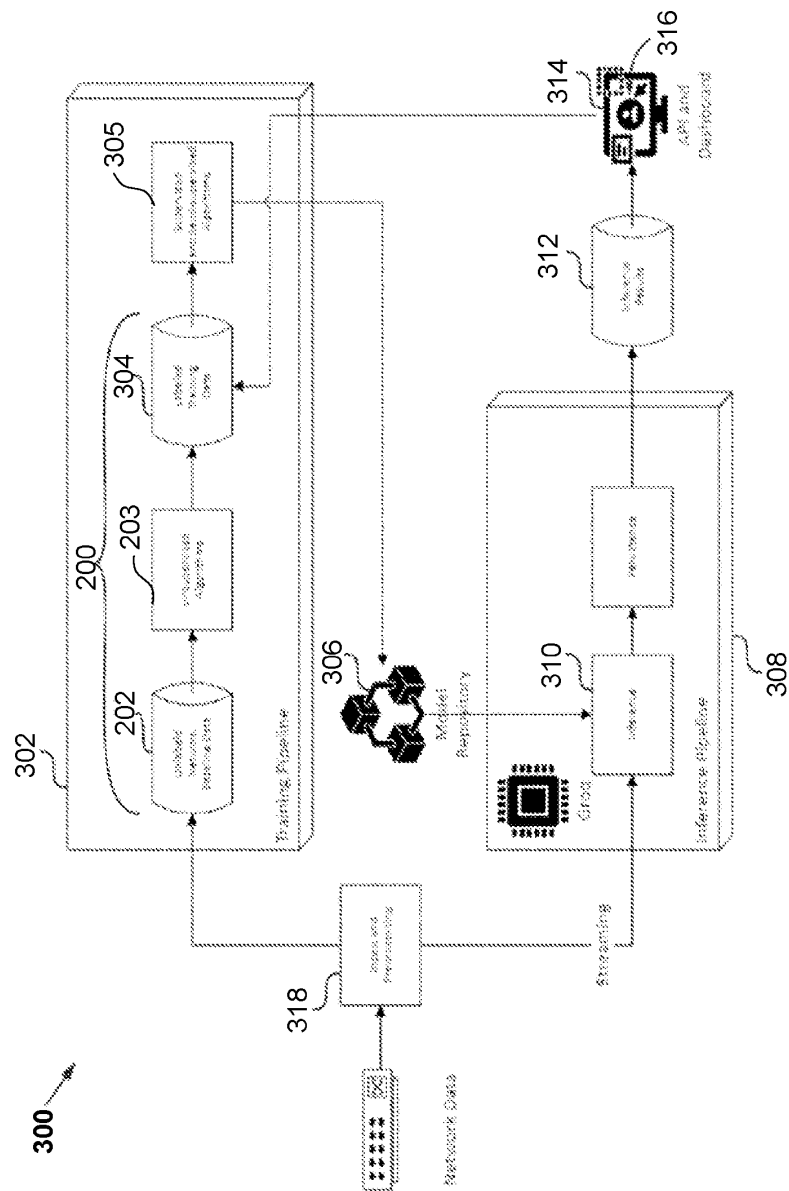


FIG. 3

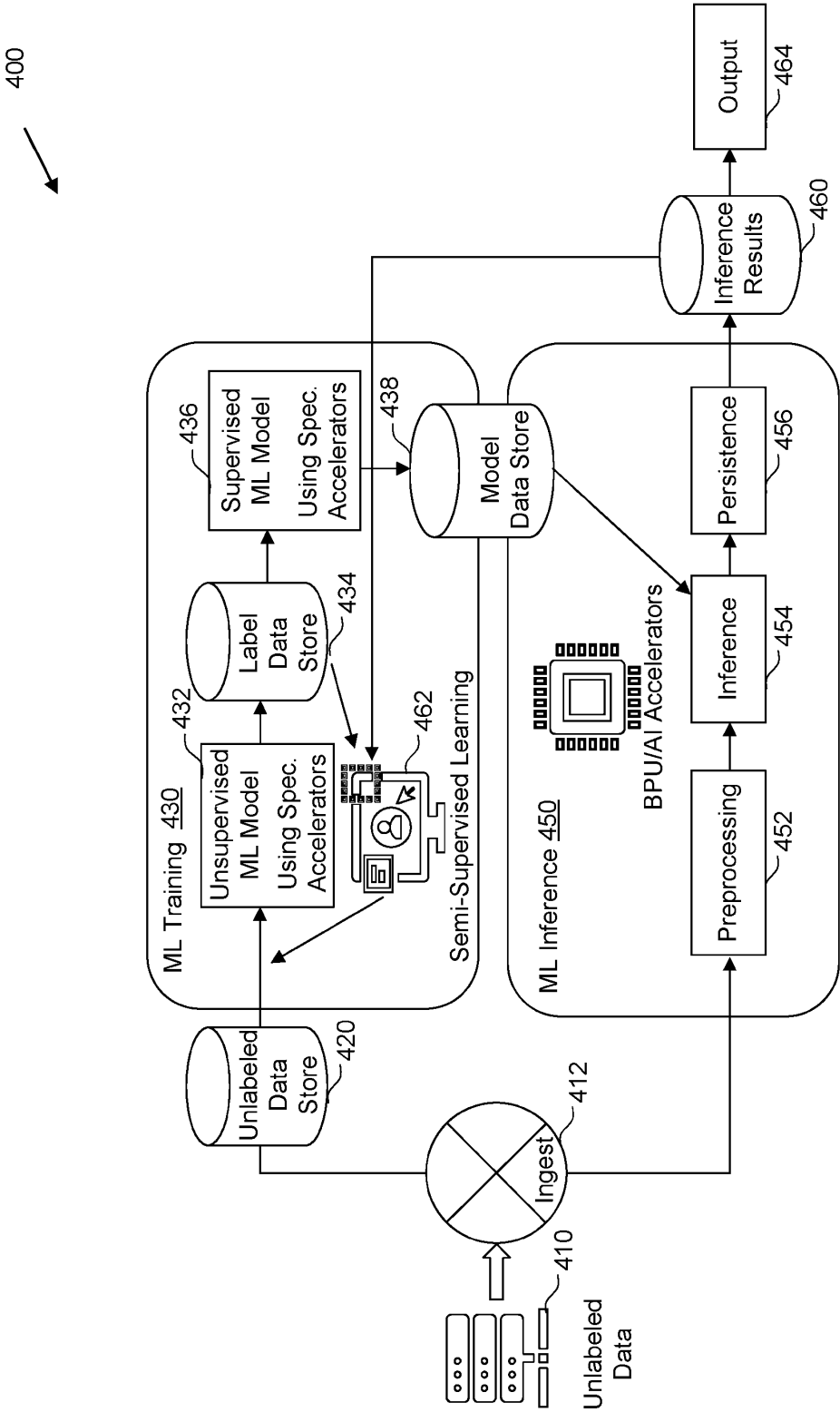


FIG. 4

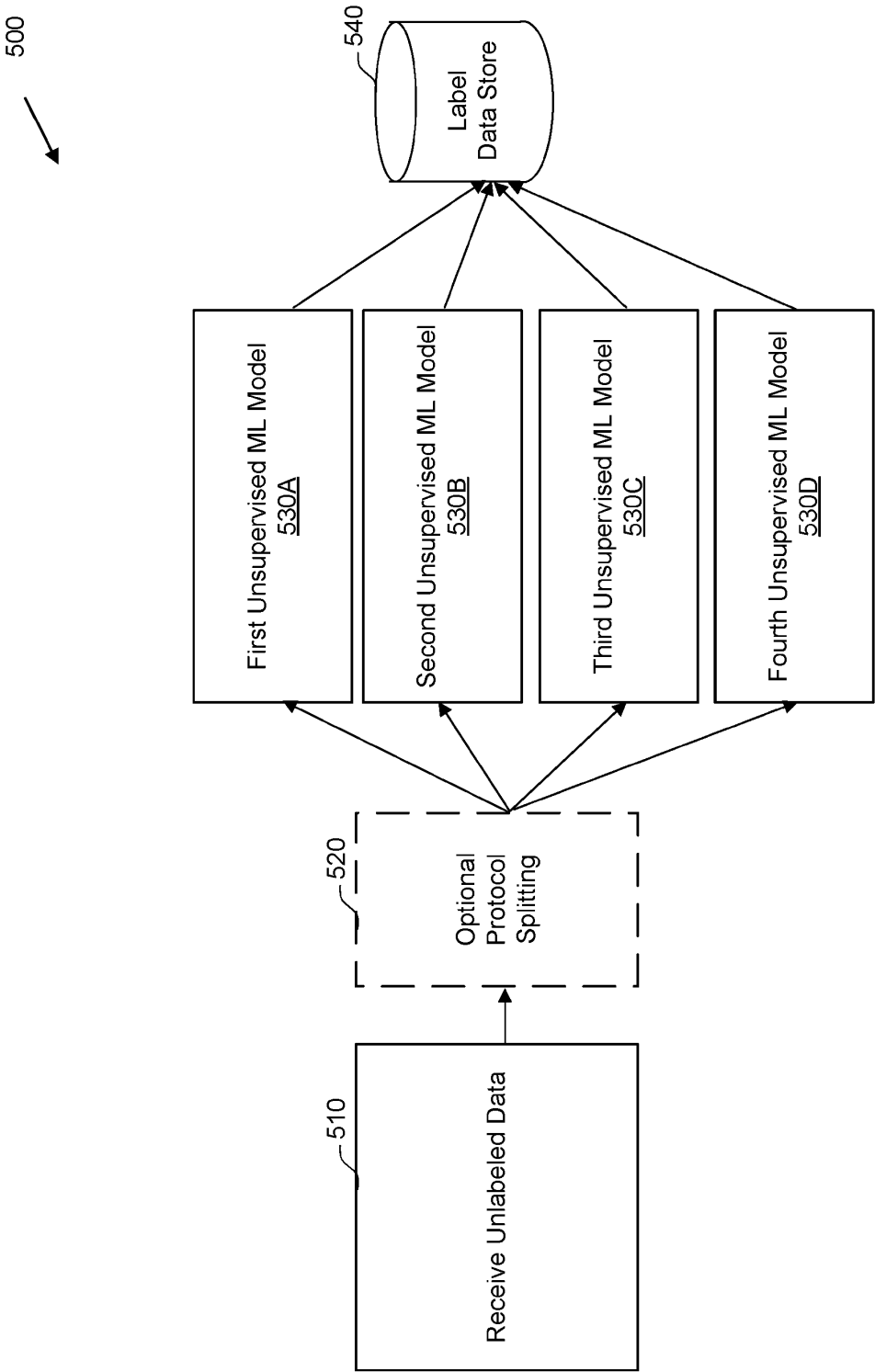


FIG. 5

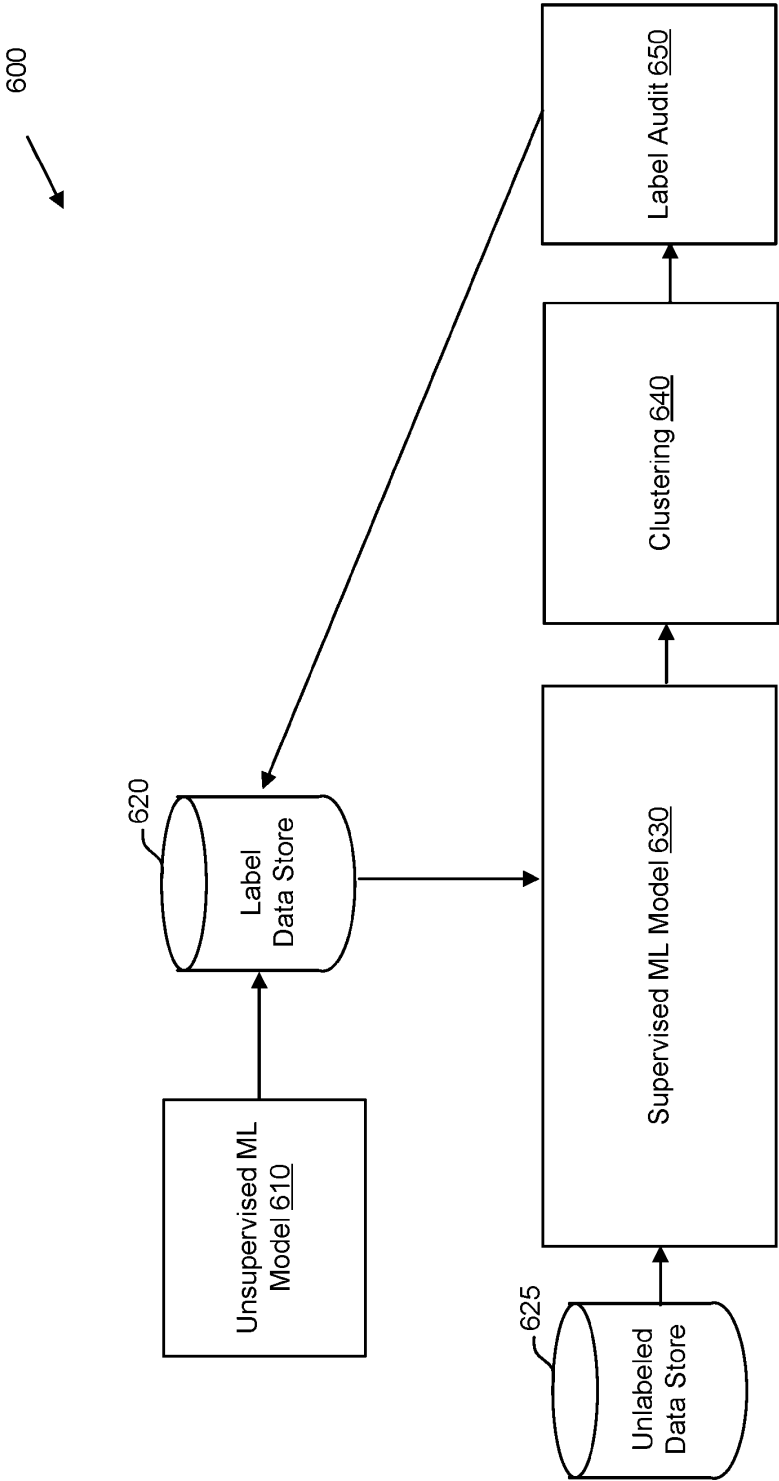


FIG. 6

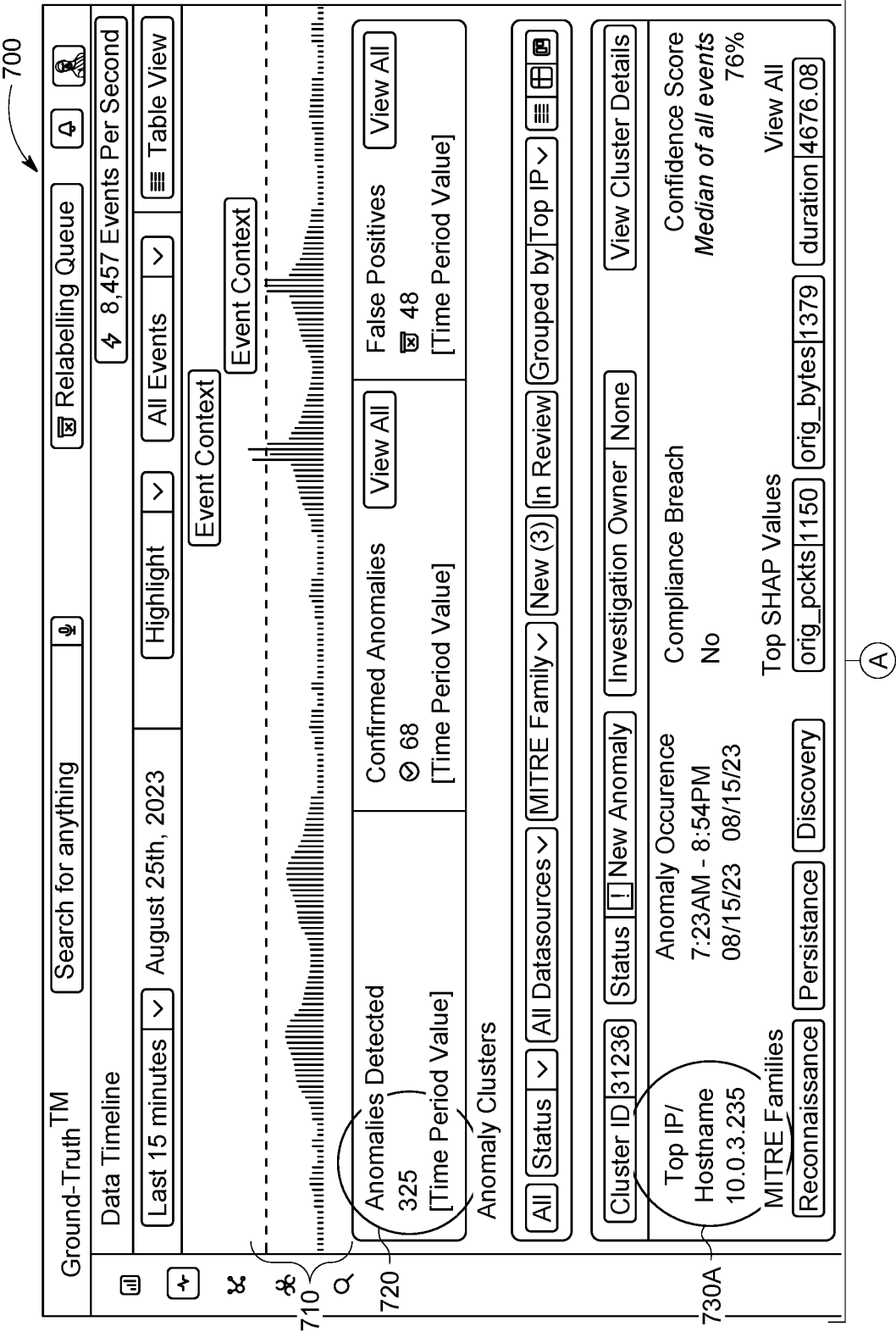


FIG. 7

A

730B

Cluster ID31236

StatusUnder Investigation

Investigation OwnerP Byrne

View Cluster Details

Top IP/ Hostname
10.0.3.235

MITRE Families

Reconnaissance

Anomaly Occurrence
7:23AM - 8:54PM
08/15/23 08/15/23

Persistence

Discovery

Compliance Breach
No

Top SHAP Values
orig_pkts1150 orig_bytes1379

View All
duration4676.08

Confidence Score
Median of all events
95%

730C

Cluster ID31236

StatusUnder Investigation

Investigation OwnerR Hennig

View Cluster Details

Top IP/ Hostname
10.0.3.235

MITRE Families

Reconnaissance

Anomaly Occurrence
7:23AM - 8:54PM
08/15/23 08/15/23

Persistence

Discovery

Compliance Breach
No

Top SHAP Values
orig_pkts1150 orig_bytes1379

View All
duration4676.08

Confidence Score
Median of all events
88%

730D

Cluster ID31236

StatusNew Anomaly

Investigation OwnerNone

View Cluster Details

Top IP/ Hostname
10.0.3.235

MITRE Families

Reconnaissance

Anomaly Occurrence
7:23AM - 8:54PM
08/15/23 08/15/23

Persistence

Discovery

Compliance Breach
No

Top SHAP Values
orig_pkts1150 orig_bytes1379

View All
duration4676.08

Confidence Score
Median of all events
41%

⊗

⚙

FIG. 7 (Cont'd)

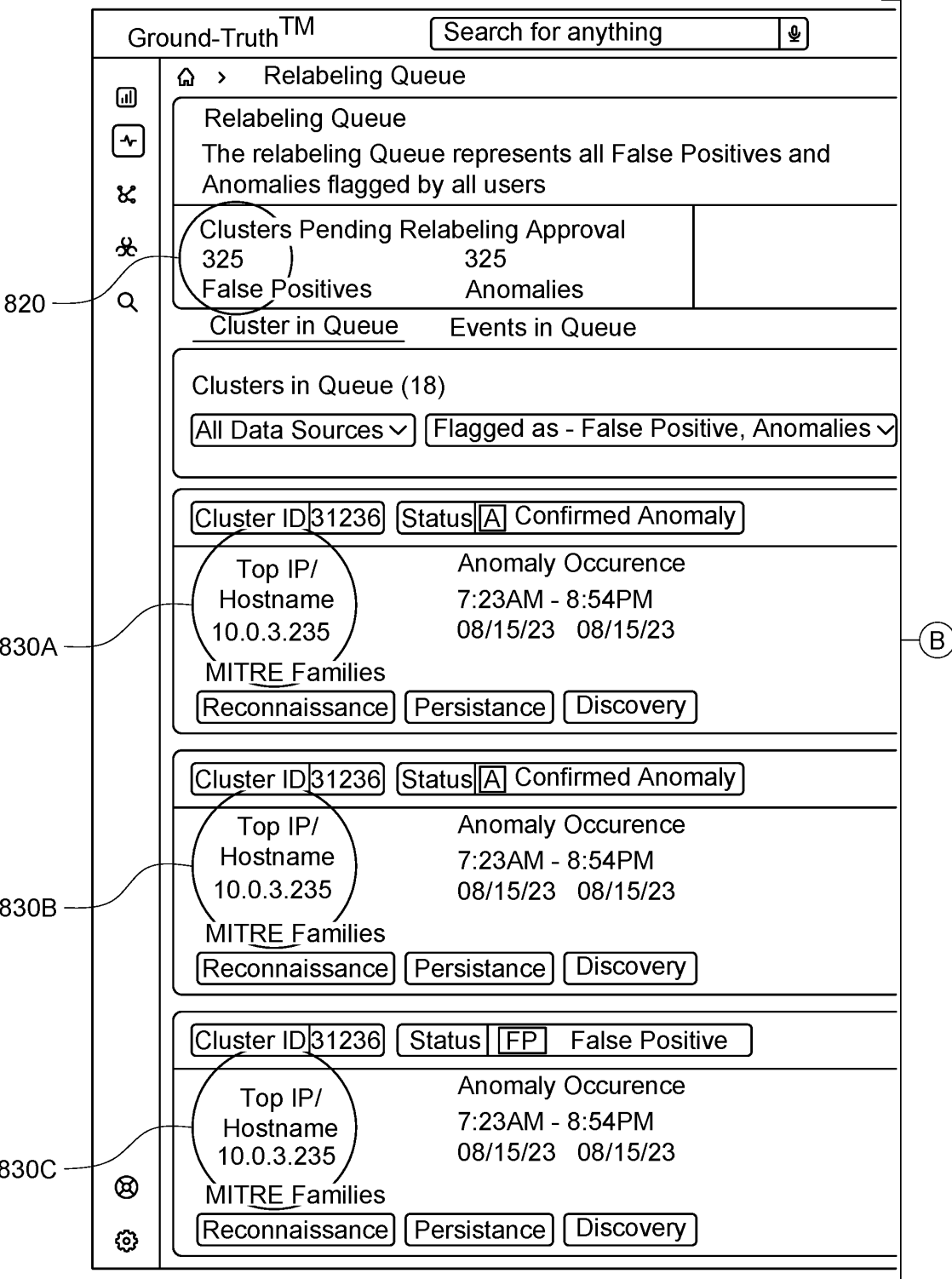


FIG. 8

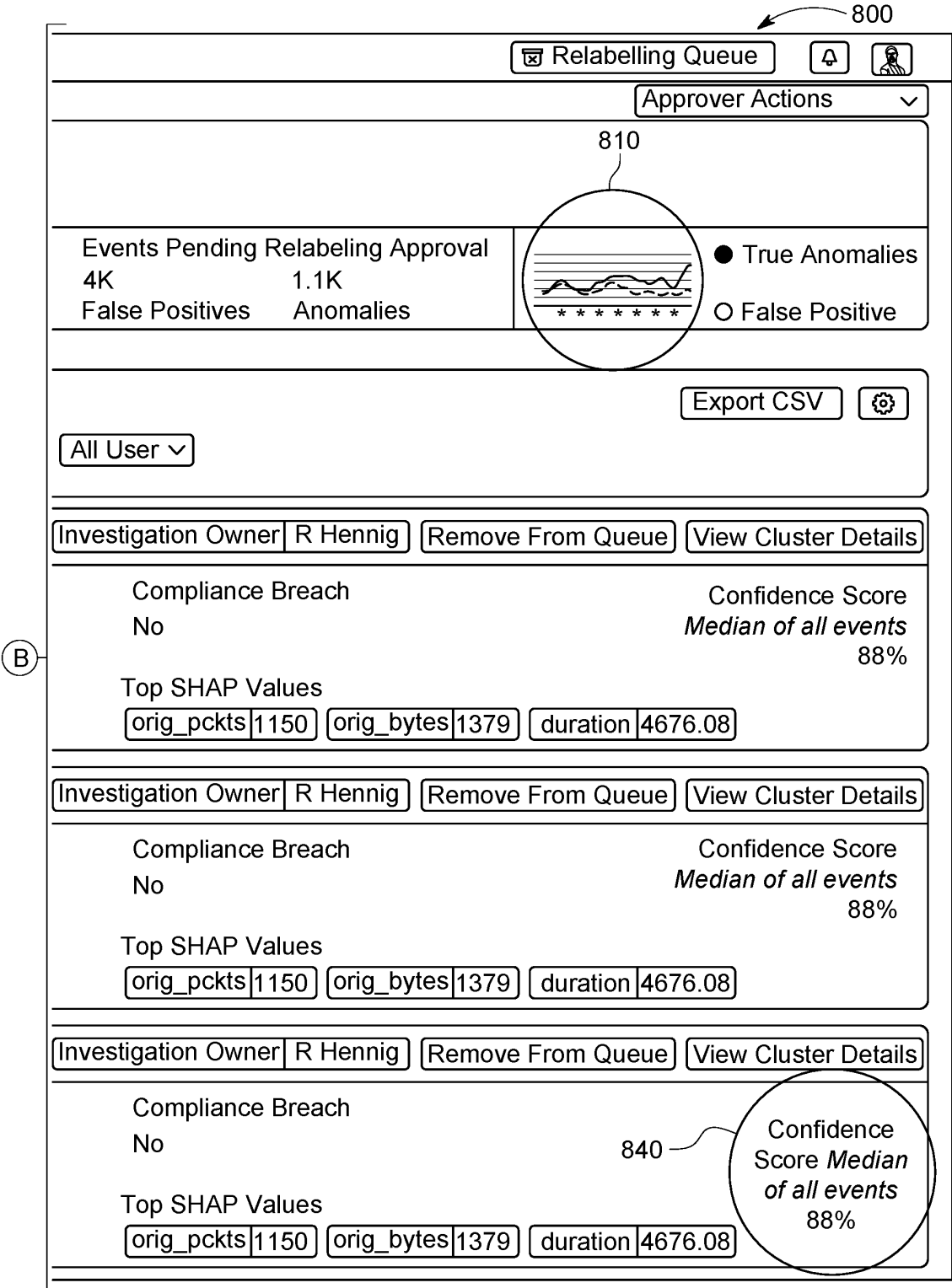


FIG. 8 (Cont'd)

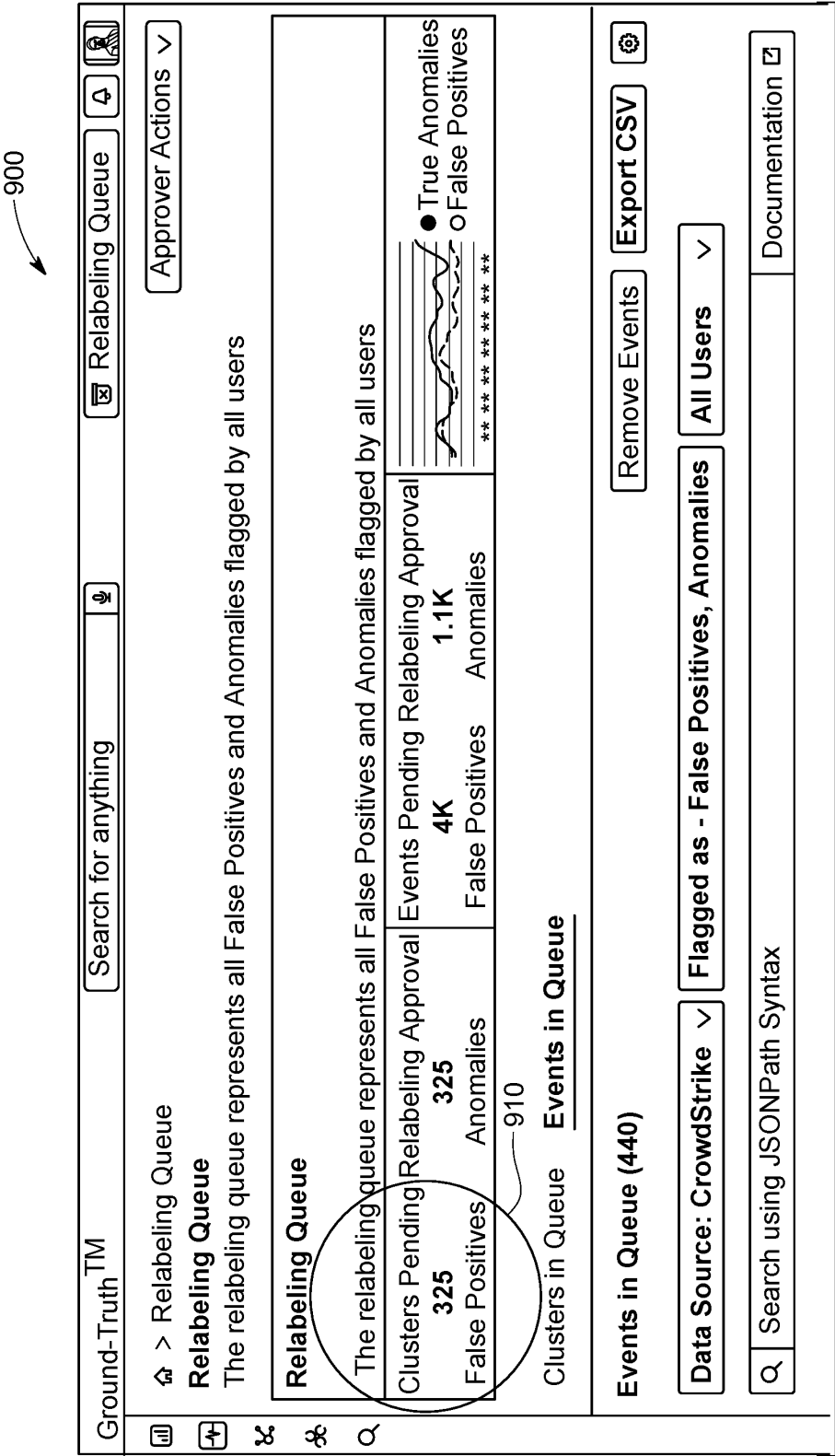


FIG. 9

C

☐	Status↓	Confidence↓	MITRE↓	User↓	Timestamp↓	Asset Name↓	Criticality↓	Source IP↓	Destination IP↓
☐	☐ A	Not Processed	☐ 88%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ A	Not Processed	☐ 88%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ A	Not Processed	☐ 88%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ A	Not Processed	☐ 88%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ A	Not Processed	☐ 88%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ FP	Not Processed	☐ 30%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ FP	Not Processed	☐ 30%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ FP	Not Processed	☐ 30%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ FP	Not Processed	☐ 30%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ FP	Not Processed	☐ 30%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ FP	Not Processed	☐ 30%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ FP	Not Processed	☐ 30%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ FP	Not Processed	☐ 30%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ FP	Not Processed	☐ 30%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ FP	Not Processed	☐ 30%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ FP	Not Processed	☐ 30%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24
☐	☐ FP	Not Processed	☐ 30%	oReconn. Rhennig	10:47:22 AM MDT 8/9/2023	groq1-server.com	High	10.0.3.235	47.24

920

⊗ ⚙

FIG. 9 (Cont'd)

1000

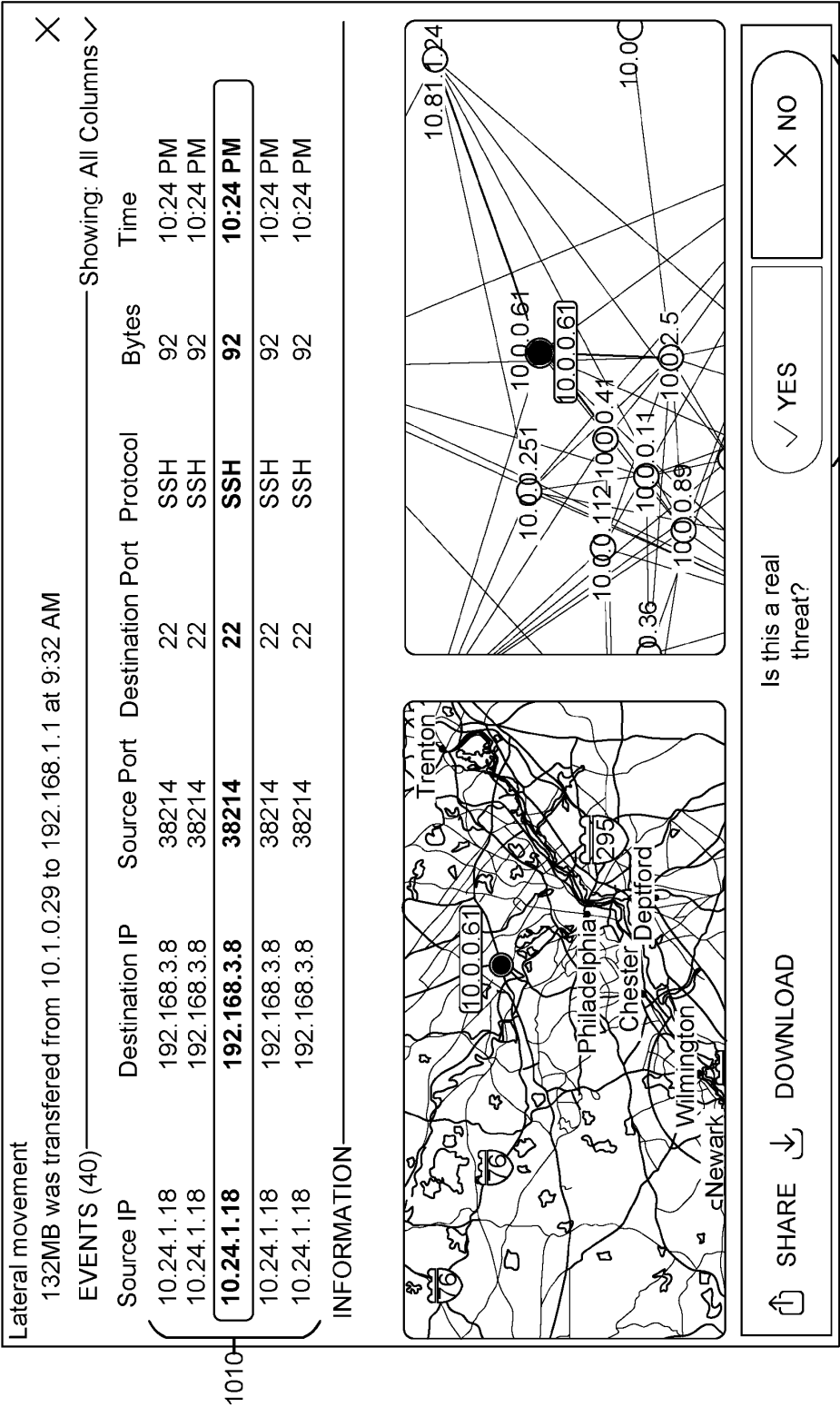


FIG. 10

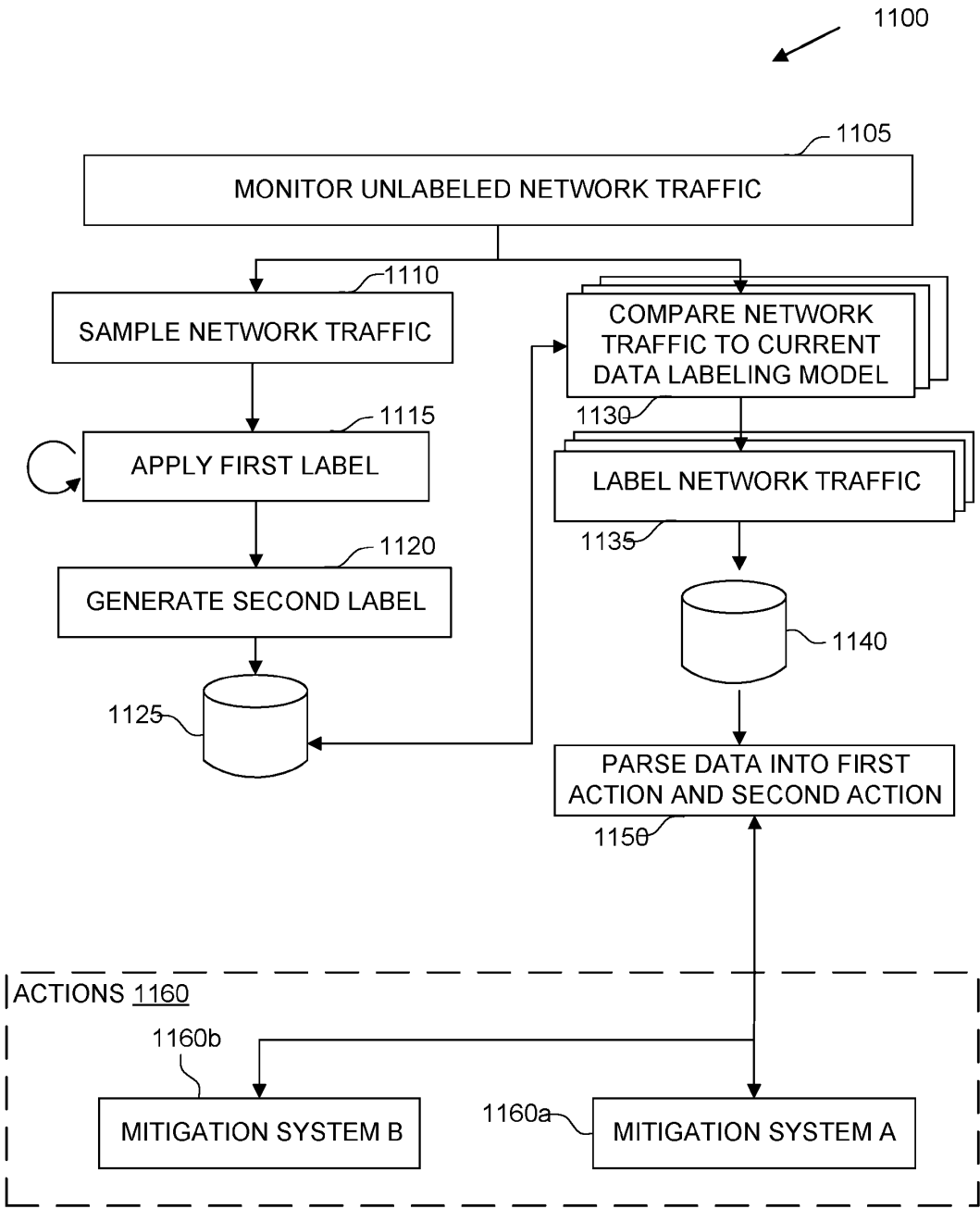


FIG. 11

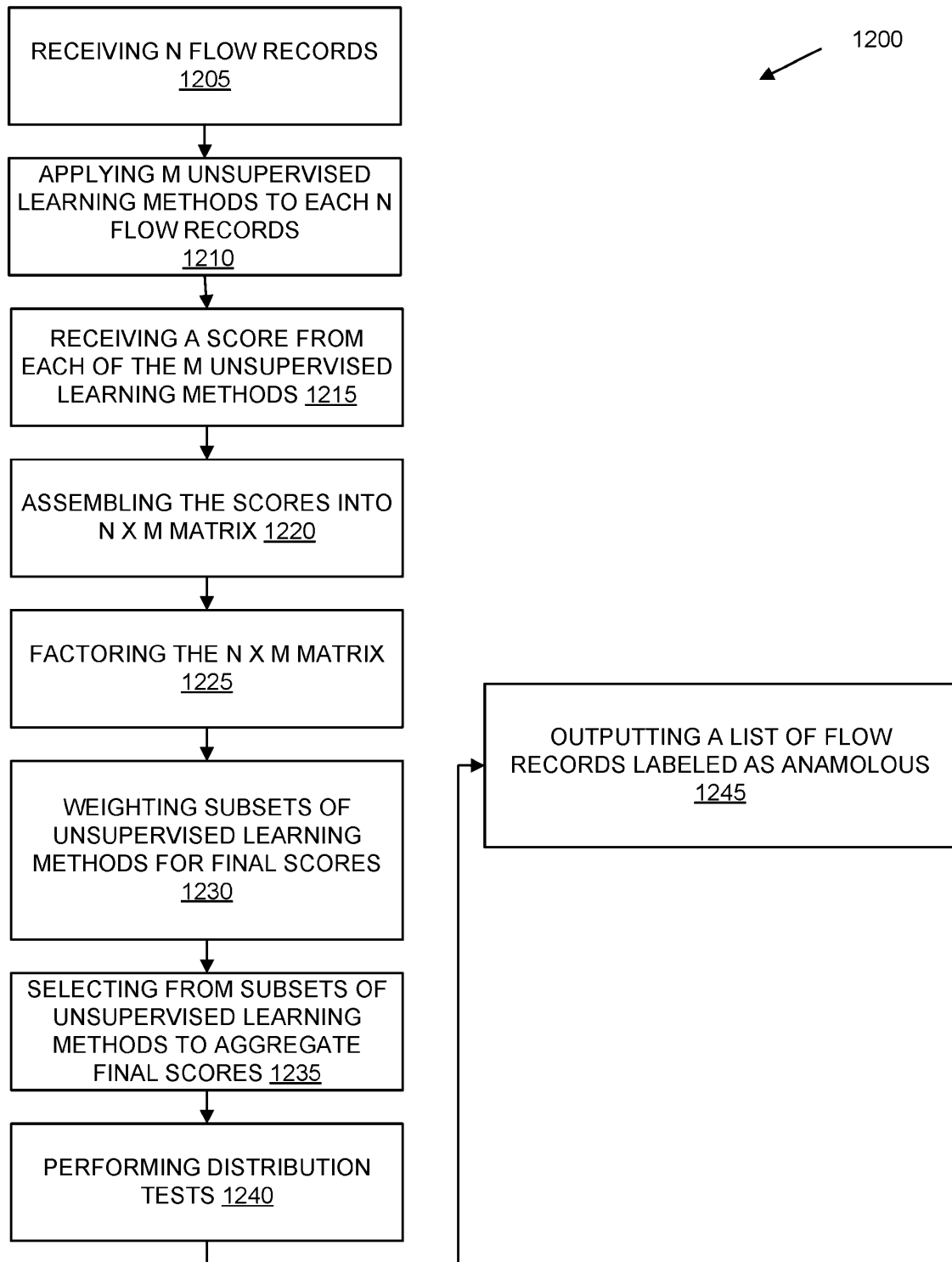


FIG. 12