Created by: Gil Klainert FP NYC

Date: 2025-06-09

Investigation Risk Assessment Report

Investigation Summary

Investigation ID:	TEST-ALL-FOR-DEVICE-f394742f39214c908476c01623bf4bcd
Device ID:	f394742f39214c908476c01623bf4bcd
Time Range:	120d
Overall Risk Score:	0.10
Status:	Unknown
Generated:	2025-06-09 13:57:44

Module Analysis Summary

Module	Risk Score	Records	Status
Device Analysis	0.00	0	Low Risk
Location Analysis	0.00	0	Low Risk
Network Analysis	0.00	0	Low Risk
Logs Analysis	0.00	0	Low Risk

Detailed Module Analysis

Device Analysis (Risk Score: 0.00)

Risk Level: LOW RISK

Records Analyzed: 0

Analysis:

No detailed analysis available for this module.

Location Analysis (Risk Score: 0.00)

Risk Level: LOW RISK

Records Analyzed: 0

Analysis:

No device location data is available, and the official address country is also unknown. With zero device location entries and no OII country information, no anomalies can be detected at this time.

Network Analysis (Risk Score: 0.00)

Risk Level: LOW RISK

Records Analyzed: 0

Analysis:

Without any network signal data, there is no basis for identifying geographic inconsistencies or device ID anomalies. As a result, the risk level is assigned as very low, and the confidence in this assessment is also low due to insufficient data.

Logs Analysis (Risk Score: 0.00)

Risk Level: LOW RISK

Records Analyzed: 0

Analysis:

No authentication logs found for this user.

Key Risk Factors:

- No logins found

Overall Risk Assessment

Final Risk Score: 0.10 (LOW RISK)

Final Assessment:

After reviewing the available data from device, location, and network domains, we have determined that the risk score for the user is 0.1. This relatively low value reflects minimal detected suspicion across multiple domains, although the absence of device signals, location data, and network information reduces our overall confidence in the assessment. Because we lack critical data points (such as country of address, network location, or detailed device telemetry), it is challenging to identify patterns of activity that might otherwise indicate higher levels of risk. Nonetheless, no meaningful anomalies or location conflicts have been detected, which supports maintaining a lower level of concern.

A key consideration is the limited data available. The implications of having very little to no information are twofold: on the one hand, there is no evidence of malicious activity or suspicious behaviors. On the other, the absence of data means we cannot fully confirm legitimate usage patterns or user whereabouts. This gap in visibility may warrant additional checks or verifications to improve confidence in the overall assessment. When signals are insufficient, even innocuous risk factors can remain unnoticed.

Given the risk score for the user, the recommended next steps include diligent gathering of more robust facts and signals, such as device fingerprints, network metadata, and location confirmations, to enhance decision-making. Further investigation into the user’s typical behaviors—if available—may help confirm consistency over time. By supplementing the current data set, we can be more certain about future risk evaluations and better address any emerging red flags should they arise. Overall, careful monitoring, improved data collection, and continued vigilance remain the most effective strategies for maintaining a secure environment in this scenario.

Report generated on 2025-06-09 at 13:57:58

This report contains sensitive security information - handle with care