# LC UI ID03 screen data

# Case Summary

A recent audit of warehouse inventory and security footage identified a suspected incident of inventory theft. On 2025/07/24, a staff member accessed the warehouse after standard operating hours with no authorized activities scheduled. This coincided with a recorded decrease of 50 units of Widget A from inventory, for which no sales, returns, or delivery documentation could be found. The convergence of these anomalies prompted a fraud investigation.

# Actors Involved

* Warehouse Staff Member: Observed entering the warehouse via the east entrance outside of operational hours.
* Fraud Detection Team: Conducted the audit, reviewed inventory records, and examined security footage.
* Warehouse Management: Responsible for inventory oversight and authorizing after-hours access (no such authorization recorded).

# Visual Timeline of Events

|  |  |
| --- | --- |
| Time | Event |
| 2025/07/24, 22:18 | Warehouse staff member accesses facility via east entrance (outside standard hours). |
| 2025/07/24, 22:18–22:47 | Staff member remains inside warehouse; no authorized activities scheduled or logged. |
| 2025/07/24, post-22:47 | Inventory review reveals a reduction of 50 units of Widget A with no supporting sales, return, or delivery documentation. |
| Following days | Fraud detection team audits records, reviews CCTV, and confirms the timeline aligns with the unexplained inventory reduction. |

# Risk Explanation

The case highlights significant risks to operational integrity within the warehouse environment:

* Unauthorized Access Risk: Staff entry outside authorized hours increases the likelihood of unsupervised activities and potential misconduct.
* Inventory Control Weakness: Lack of real-time reconciliation and documentation for inventory movements exposes the organization to stock losses and theft.
* Process Gap: The absence of controls to monitor after-hours access and tie it directly to inventory movements enabled unauthorized removal to occur undetected in real time.
* Potential Insider Threat: The evidence suggests possible involvement of internal personnel, underlining the importance of robust segregation of duties and access controls.

Mitigating these risks requires tighter control measures, improved surveillance integration, and prompt documentation of all inventory activities, particularly those occurring outside regular operations.