

1. Objective This report presents an analysis of hourly transaction data from two checkout points. The goal was to identify anomaly patterns in sales behavior using statistical and SQL-based methods, with a focus on operational integrity and security monitoring.

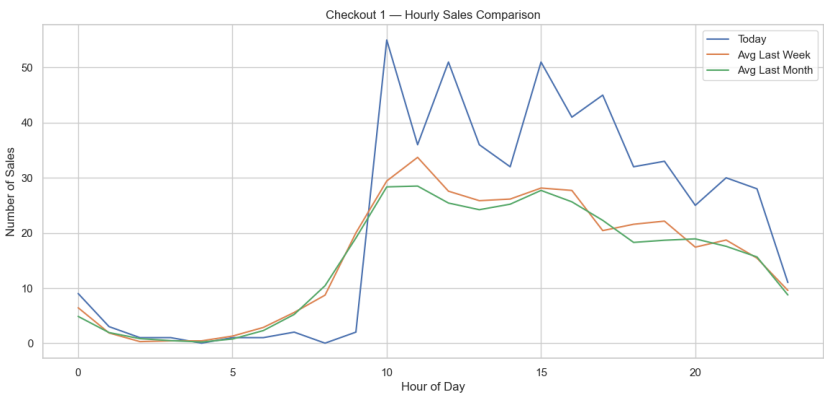
---

2. Methodology

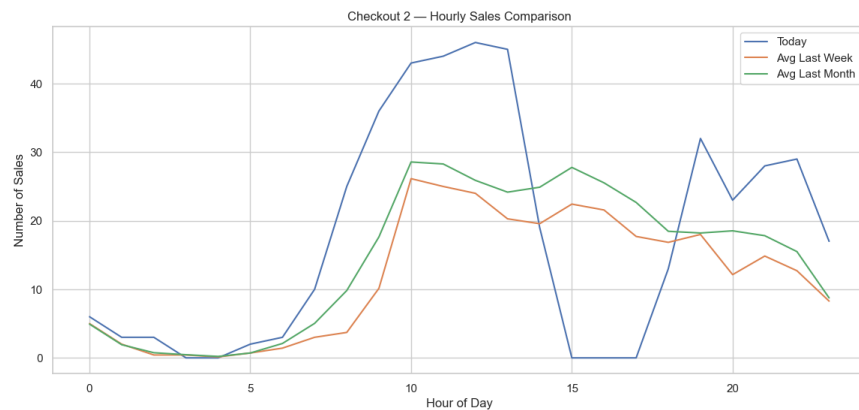
- Data Sources: checkout\_1.csv and checkout\_2.csv
  - Tools Used: Python (Pandas, Seaborn, Matplotlib), SQLite (in-memory)
  - Approach:
    - Visual comparison of today's sales vs. historical benchmarks
    - Anomaly detection using standard deviation thresholds
    - SQL query simulation to validate suspicious time windows
    - Security-oriented interpretation of anomalies
- 

3. Summary of Findings

- Checkout 1
  - Transaction spikes at 10h, 12h, and 15h exceeded historical averages by more than 2 standard deviations.
  - These patterns may indicate unauthorized batch processing, promotional abuse, or scripted transaction injections.



- Checkout 2
  - A complete drop to zero transactions between 15h and 17h, while historical averages remained above 20.
  - This behavior suggests a critical failure in the checkout system, potentially linked to infrastructure outage or denial-of-service conditions.



- 
4. SQL-Based Validation An SQL query was executed to identify hours where today's volume exceeded twice the weekly average:

```
SELECT time, today, avg_last_week
FROM checkout1
WHERE today > (avg_last_week * 2)
ORDER BY time;
```

The results confirmed the same anomaly windows detected via statistical methods, reinforcing the reliability of the findings.

---

## 5. Security Implications

- Checkout 1: High-volume spikes may reflect fraud attempts or misuse of transaction systems.
  - Checkout 2: The outage window represents a high-severity incident with direct impact on transaction integrity.
- 

## 6. Recommended Actions

- Flag affected time windows for immediate alerting and escalation.

- Integrate anomaly thresholds into real-time monitoring pipelines.
- Ensure audit logs and system traces are preserved for forensic validation.
- Apply containment protocols for suspected abuse patterns.