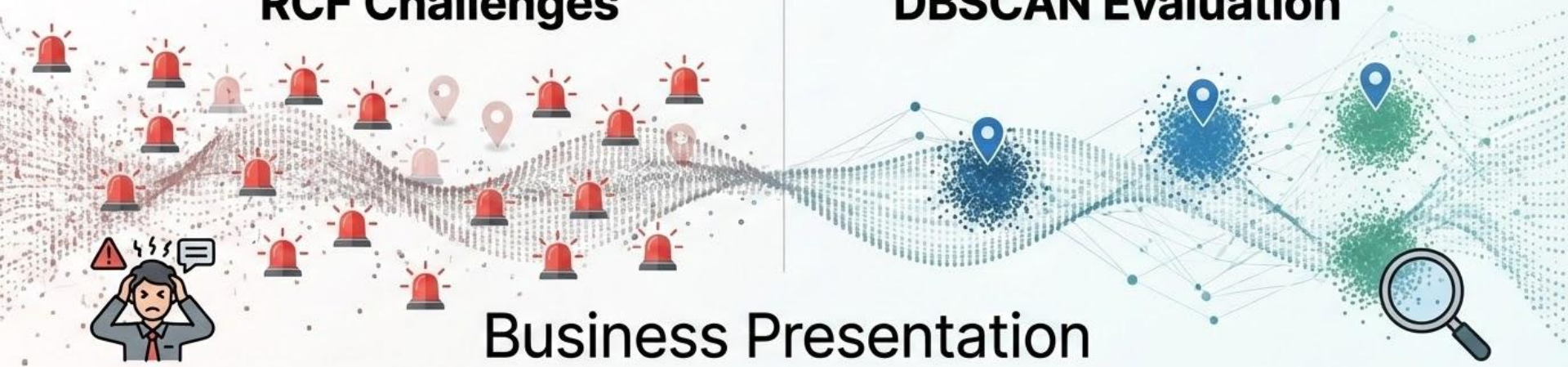
Time Series Anomaly Detection using DBSCAN

Business Presentation

Increased Alert Fatigue & Missed Critical Alerts

Current State: **RCF Challenges**

Proposed Solution: **DBSCAN Evaluation**



Business Presentation

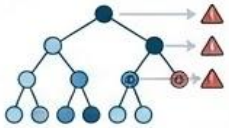
- Random Cut Forest (RCF) with high false discovery rate (~40%).
- Increased operational overhead, no reliability improvement.
- Alert desensitization leading to missed critical incidents.

- Evaluate Density-Based Spatial Clustering (DBSCAN).
- **Goal:** Increase alerting precision without sacrificing recall.
- Filter noise, surface true anomalies.

Evaluation Approach

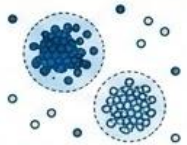
1. Find Appropriate Dataset

Find appropriate Dataset behaving logging scenarios



2. Demonstrate RRCF Baseline

Demonstrate current baseline by implementing RRCF



3. Implement DBSCAN Alternative

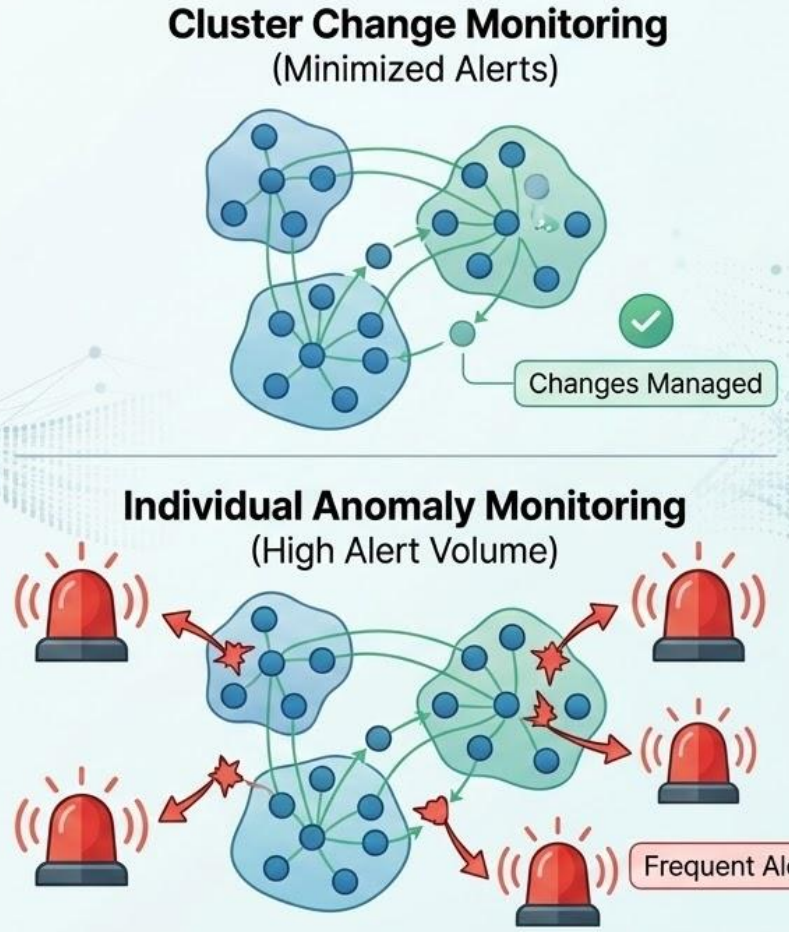
Implement DBSCAN alternative

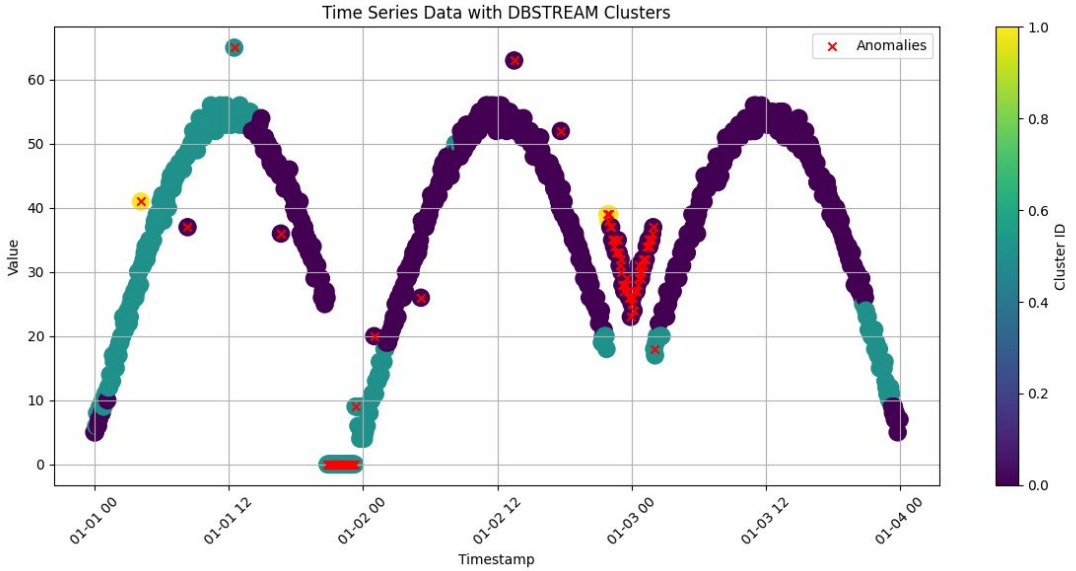
4. Measure Results

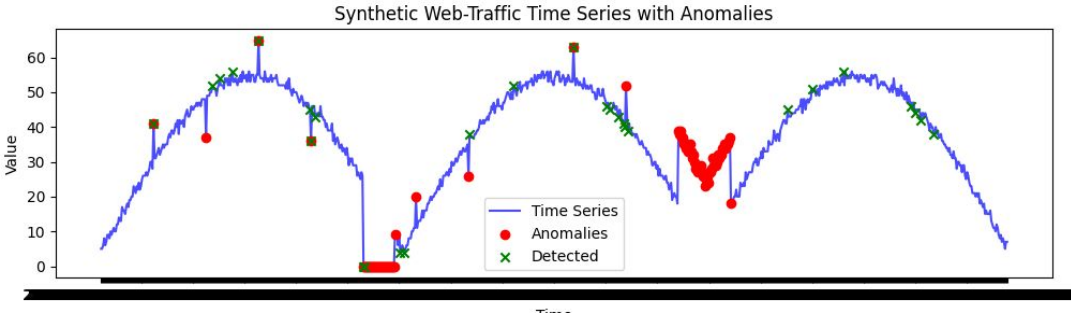
Measure results

Key Findings

Monitoring cluster changes minimize alerting compared to anomaly monitoring.




Time Series Data with DBSTREAM Clusters
Anomalies
Value
Timestamp
Cluster ID
01-01 00
01-01 12
01-02 00
01-02 12
01-03 00
01-03 12
01-04 00


Synthetic Web-Traffic Time Series with Anomalies
Value
Time Series
Anomalies
Detected

Recommendation

1. Proof-of-Concept Scope

Our proof-of-concept is just a fraction of what the tools is advertising.

2. Soft-Transition Pilot

We recommend to pilot a soft-transition to the new tool.

Risk & Considerations

Cost

Initial investment and ongoing operational expenses.

Migration Complexity

Challenges in data transfer and system integration.

Learning Curve

Time and training required for team adoption.