DOCUMENTATION

Anomaly Detection (AD)

HEAL Software Inc.

Table of Contents

Anomaly detection is the automated identification of patterns in the operational data that deviate significantly from expected behavior.

In HEAL infrastructure, services, microservices, and components generate massive volumes of logs, metrics, and traces: making manual inspection difficult without anomaly detection.

Hence, HEAL’s anomaly detection engine supports both real-time streaming data and historical batch analyses, giving you the flexibility to detect issues as they happen and before they cause outage.

An anomaly detection capability helps the platform with the benefits below:

- Continuously sets the baselines.
- Automatically generates anomaly when there is a breach in real-time.
- Reduce noise and false detections.
- Send the alert before the outage.

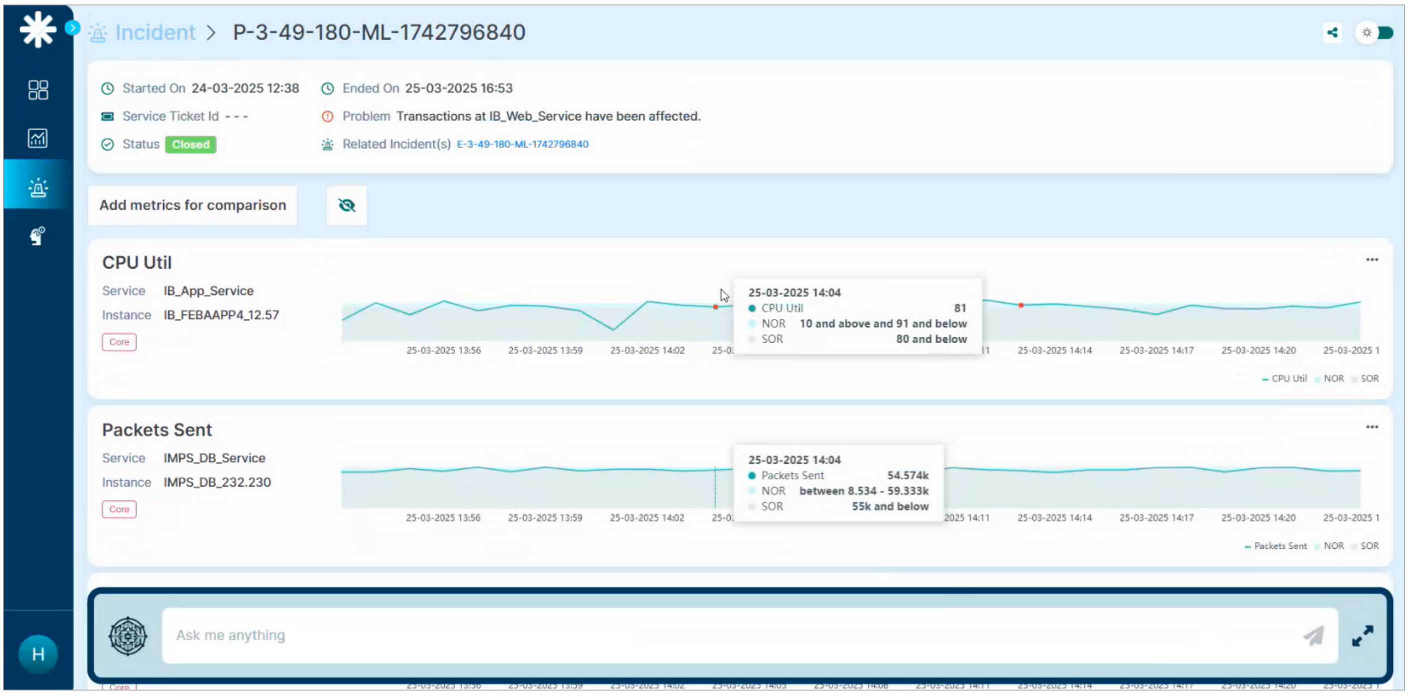
When you navigate to an incident page in the HEAL UI:

1. Scroll down to the metrics section to view graphs of impacted metrics.

For example: CPU Util , Packets Sent

2. Red dots on the graphs indicate anomalies (i.e., events detected by the AD engine).
3. Hover over a red dot to view detailed anomaly context, including:

- NOR (Normal Operating Range)
- SOR (Safe Operating Range)



Incident > P-3-49-180-ML-1742796840

Started On 24-03-2025 12:38

Ended On 25-03-2025 16:53

Service Ticket Id - - -

Problem Transactions at IB_Web_Service have been affected.

Status Closed

Related Incident(s) E-3-49-180-ML-1742796840

Add metrics for comparison

CPU Util

Service IB_App_Service

Instance IB_FEBAAPP4_12.57

Core

25-03-2025 14:04

CPU Util 81

NOR 10 and above and 91 and below

SOR 80 and below

Packets Sent

Service IMPS_DB_Service

Instance IMPS_DB_232.230

Core

25-03-2025 14:04

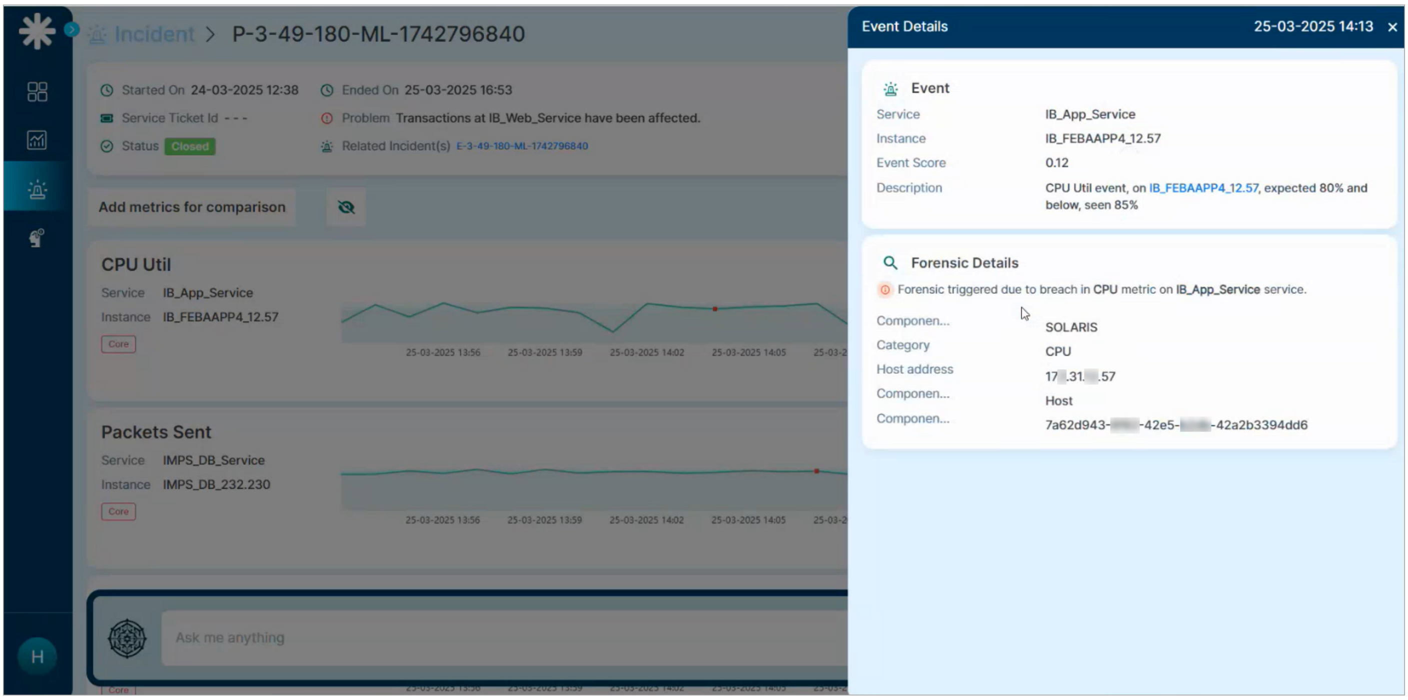
Packets Sent 54.574k

NOR between 8.534 - 59.333k

SOR 55k and below

Ask me anything

4. Click on the red dot (anomaly); the Event Details page will pop-up with the Forensic Details



Event Details 25-03-2025 14:13

Event

Service IB_App_Service

Instance IB_FEBAAPP4_12.57

Event Score 0.12

Description CPU Util event, on IB_FEBAAPP4_12.57, expected 80% and below, seen 85%

Forensic Details

Forensic triggered due to breach in CPU metric on IB_App_Service service.

Componen... SOLARIS

Category CPU

Host address 17[redacted].31.[redacted].57

Componen... Host

Componen... 7a62d943-[redacted]-42e5-[redacted]-42a2b3394dd6

Incident > P-3-49-180-ML-1742796840
Started On 24-03-2025 12:38
Ended On 25-03-2025 16:53
Service Ticket Id - - -
Problem Transactions at IB_Web_Service have been affected.
Status Closed
Related Incident(s) E-3-49-180-ML-1742796840
Add metrics for comparison
CPU Util
Service IB_App_Service
Instance IB_FEBAAPP4_12.57
Packets Sent
Service IMPS_DB_Service
Instance IMPS_DB_232.230
Ask me anything