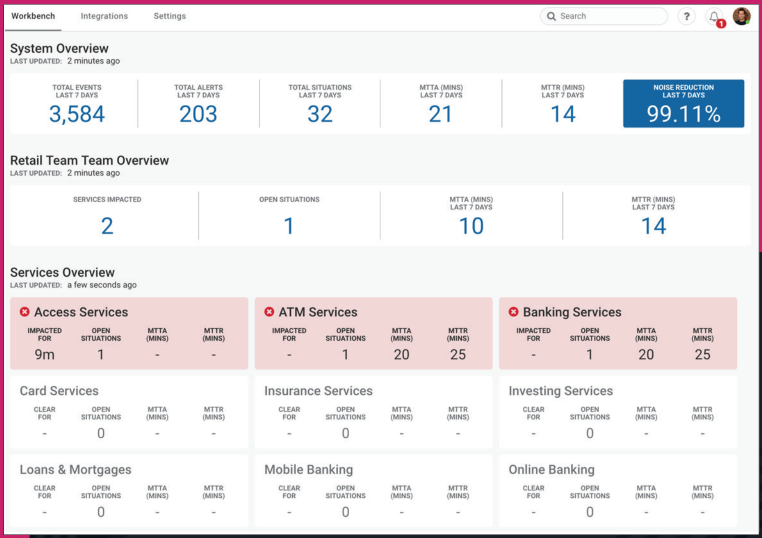
Moogsoft®

AT A GLANCE
ALERT CORRELATION

Controlling the Chaos with AI-Driven Alert Correlation

Today's digital businesses run on complex technology stacks to deliver an amazing customer experience. Moogsoft AIOps correlation is about making connections between data from multiple IT systems from different parts of the enterprise. Alert Correlation allows operators to see patterns across the systems that make up technology stacks to ensure applications and microservices are at peak performance. Moogsoft AIOps correlation algorithms analyze alerts to identify clusters of similarity across service-affecting incidents, problems or changes. The result of this correlation and aggregation is a massive reduction in the number of alerts bombarding IT Operations, NOC centers, and application delivery.

Moogsoft AIOps Summary Dashboard - Alert Correlation



System Overview
LAST UPDATED: 2 minutes ago

TOTAL EVENTS LAST 7 DAYS	TOTAL ALERTS LAST 7 DAYS	TOTAL SITUATIONS LAST 7 DAYS	MTTA (MINS) LAST 7 DAYS	MTTR (MINS) LAST 7 DAYS	NOISE REDUCTION LAST 7 DAYS
3,584	203	32	21	14	99.11%

Retail Team Team Overview
LAST UPDATED: 2 minutes ago

SERVICES IMPACTED	OPEN SITUATIONS	MTTA (MINS) LAST 7 DAYS	MTTR (MINS) LAST 7 DAYS
2	1	10	14

Services Overview
LAST UPDATED: a few seconds ago

Access Services			
IMPACTED FOR	OPEN SITUATIONS	MTTA (MINS)	MTTR (MINS)
9m	1	-	-

ATM Services			
IMPACTED FOR	OPEN SITUATIONS	MTTA (MINS)	MTTR (MINS)
-	1	20	25

Banking Services			
IMPACTED FOR	OPEN SITUATIONS	MTTA (MINS)	MTTR (MINS)
-	1	20	25

Card Services			
CLEAR FOR	OPEN SITUATIONS	MTTA (MINS)	MTTR (MINS)
-	0	-	-

Insurance Services			
CLEAR FOR	OPEN SITUATIONS	MTTA (MINS)	MTTR (MINS)
-	0	-	-

Investing Services			
CLEAR FOR	OPEN SITUATIONS	MTTA (MINS)	MTTR (MINS)
-	0	-	-

Loans & Mortgages			
CLEAR FOR	OPEN SITUATIONS	MTTA (MINS)	MTTR (MINS)
-	0	-	-

Mobile Banking			
CLEAR FOR	OPEN SITUATIONS	MTTA (MINS)	MTTR (MINS)
-	0	-	-

Online Banking			
CLEAR FOR	OPEN SITUATIONS	MTTA (MINS)	MTTR (MINS)
-	0	-	-

Alert Correlation offers the following benefits:

- Shared context for faster incident, problem and change management
- 99% fewer events hitting IT Ops and DevOps teams
- 60% faster Mean Time To Detect (MTTD)
- 40% faster Mean Time To Resolve (MTTR)

Agile Moogsoft Recipes Deliver Precise Results

Cookbook is a Moogsoft AIOps algorithm that provides out-of-the-box recipes to define the relationships, or similarities, between alerts. Cookbook runs multiple recipes concurrently. That way, it can precisely correlate incoming data and create Situations with contextual information derived from the clustered alerts to enable rapid Mean Time To Resolution (MTTR).

Now teams have a powerful tool to match alert information based on time, class or type, geographic location, topology proximity, and server priority. By correlating millions of alerts with any mix of these criteria, Moogsoft AIOps reduces the number of tickets that IT Ops and DevOps teams receive by 40%, while teaching the algorithms to deliver highly accurate, recommended Probable Root Cause (PRC) and resolving steps for recurring incidents. As the teams develop trust in the accuracy of the recommendations, auto-ticketing further streamlines the process for faster fixes.

© 2019 Moogsoft Inc. All rights reserved.

Fine-tuning Alert Correlation

Situation Visualization provides a powerful visual tool for understanding the similarity of the alerts within a Situation. Utilizing the tool's rich view into the AIOps algorithms, teams can fine-tune algorithm recipes to focus on the data sets that deliver the most insight for resolving Situations.

Moogsoft Alert Correlation

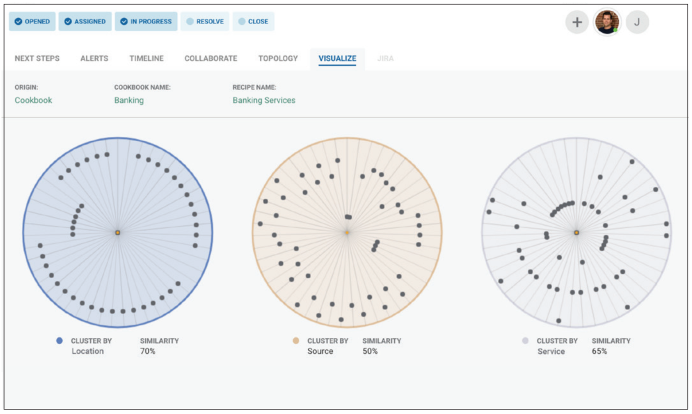
There is no one-size-fits-all algorithms. Moogsoft provides a number of machine learning algorithms that are used to cluster alerts into Situations. The clusters are made more precise through recipes that contain identifying characteristics such as:

- event arrival times,
- network topological-proximity, and
- contextual similarity

These algorithms cluster alerts with enrichment information from CMDBs, or other systems of record. This additional information adds to the contextual relevance, presents Operation teams with situational awareness, and recommends Probable Root Cause identification.

Cookbook Algorithm

Cookbook is a deterministic clustering algorithm that creates Situations defined by the relationships between alerts. Cookbook clusters alerts into Situations based on: time, topological proximity, class or type, description, server priority, geographical location, or environment classification. A Cookbook can run multiple recipes concurrently to correlate the incoming event stream and dramatically reduce the total number of alerts sent to IT Ops and DevOps teams. For example, a Cookbook recipe could match the same service and application, or the same host and location, or indicate the critical nodes within your network and their tendency to produce important events using Vertex Entropy.



ORIGIN: Cookbook

COOKBOOK NAME: Banking

RECIPE NAME: Banking Services

● CLUSTER BY Location SIMILARITY 70%

● CLUSTER BY Source SIMILARITY 50%

● CLUSTER BY Service SIMILARITY 65%

Visualization Screen

Vertex Entropy

Vertex Entropy ingests topology data from sources such as Application Performance Monitoring (APM), Network Performance Monitoring (NPM) systems, or CMDBs and uses advanced graph theory-based AI to quickly and efficiently identify the critical nodes within your network topology and their topological importance. Working hand-in-hand with Vertex Entropy, Situation Topology Visualization displays the application and infrastructure topology map with Probable Root Cause, highlighting the root cause node(s) of any customer-impacting problem.

Tempus Algorithm

Tempus is a time-based algorithm that clusters alerts based on the similarity of event arrival patterns. For example, it clusters alerts in real time for availability-related failure scenarios, in which different parts of the technology stack are sending failure events and are likely to be coincident in time. This can be visualized in a timeline to pinpoint the original cause from the cascading downstream alerts.

VISIT WWW.MOOGSOFT.COM TO LEARN MORE

© 2019 Moogsoft Inc. All rights reserved.