

## CASE STUDY

Unified Communications  
Provider

### Domain

- Cloud-based Communications Solutions

### Key Challenges

- 2hr Mean-Time-To-Detect
- 2hr Mean-Time-To-Restore
- Too many disparate tools and event sources
- Lack of event correlation across application, network and infrastructure
- 1000's of email alerts/day
- 300-400 tickets each week
- 70% of tickets closed with no action
- Bridge calls were all hands

### Business Impact

- 70% of incidents detected by customers
- Frequent service impacting incidents that lasted 2-4 hours
- Significant productivity burn across multiple teams

### Moogsoft AIOps Business

#### Benefits

- >90% reduction in daily alert volumes
- 75% reduction in MTTD
- 25% reduction in MTTR
- 30% reduction in customer identified incidents
- Dramatic increase in level-1 operator productivity

#### Integrations

- SCOM
- Solarwinds
- Splunk
- Cacti
- Various homegrown solutions

**"I bought Moogsoft AIOps to gain insight into our alerts so that I can sleep better at night"**

—Director of Technology



# Communications Provider Drops MTTD by 75% with Moogsoft AIOps

This company is a leading outsourcer of communications and collaboration solutions for large enterprises. Their services runs on a cloud-based delivery model. They have been developing custom solutions across a wide range of products and services for over 10 years.

## Key Challenges

This organization was using tools like SCOM, Splunk, Solarwinds, Cacti and various homegrown solutions that would create email notifications for their operations teams to view. With roughly 15 people across the NOC, Systems Operations, Infrastructure and Applications teams, managing incidents proactively was an absolute challenge.

Through SCOM, operations teams has visibility into roughly 40% of the total alert volume. The rest was turned off to avoid further alert storming. Of these email alerts, 300 to 400 tickets were created each week for the NOC team to manage. 70% of these tickets were closed without any action taken. Furthermore, when a P1/P2 incident did occur, all-hands bridge calls were conducted.

It was taking the operations teams roughly 2 hours to detect incidents and 2 hours to resolve incidents. They were operating reactively, as over 70% of incidents were detected by customers first.

According to the NOC Manager, "Because there was such a high volume of alerts, we could only look at critical alerts when things were breaking. The 'Lows' and 'Mediums' that could be leading to problems would always be missed. It was like firefighting" Furthermore, "Because of SCOM's server-level focus, it was very difficult to determine whether a larger part of the environment was being effected as a whole, since we were just concentrating on alerts coming in from one server. After years of challenges, they decided to evaluate Moogsoft AIOps.

## Moogsoft AIOps Solution

Today, all data from across their toolsets, including SCOM, are feeding into Moogsoft AIOps, which is now a direct interface into their ticketing system.

According to NOC Manager, "We are using the same tools but the way in which we are using them has completely changed. We have turned on all alerts and are sending everything to Moogsoft AIOps for full visibility."

Moogsoft AIOps has helped this organization achieve a 90% reduction in workload, a 30% reduction in customer identified incidents, a 75% reduction in Mean-Time-To Detect Incidents, and a 25% reduction in Mean-Time-To-Resolve Incidents.