Leading European Fashion Brand Turns Alert Noise into Actionable Incidents with CloudFabrix AIOps

Situation

The client expanded its data center and used multiple monitoring tools to analyze andprevent incidents. This resulted in the IT team receiving false alerts in the ticketing system,causing delays in attending real alerts

Impact

The delay in resolving real alerts caused SLA breaches and end customer churn in the company. The IT team's productivity levels were also hampered.

Resolution

CloudFabrix offered a comprehensive solution including an incident room, asset optimization advisor and asset dependency mapping apps, helping the team automatically separate real alerts from the false ones

The client is one of the largest fashion and personal care brands in Europe. With 15+ data centers, 10+ monitoring and log analytic tools to measure key metrics and events from IT assets, the company has an expanding footprint across multiple markets in the retail industry.

The Need

As a market leader, the fashion and personal care brand needed to continue expanding its data center to grow into multiple markets. At the same time, they wanted to ensure efficient IT functioning. But using multiple tools resulted in alert noise, with too many false alerts coming into their ticketing and support system.

The IT team had to spend time manually differentiating between real and false alerts. They then had to manually classify and route tickets, resulting in a lengthy incident response process. The high incident volume and complexity, along with a lack of historical knowledge base, made the team inefficient at reactive measures.

The Solution

The solution offered by CloudFabrix included Incent Room, Asset Optimization Advisor, and Asset Dependency Mapping Apps. The existing monitoring and log analytics tools were configured to send alerts to the Incident Room directly, instead of logging them as a ticket in the system.

The solution resulted in alerts being analyzed first, identifying false alerts and suppressing those using alert correlation, classification and noise reduction algorithms. The real alerts were now logged as an incident using a built-in bi-directly ticketing system integration. CloudFabrix also integrated the different data sources for ingestion and analysis to let its advanced artificial intelligence and machine learning algorithms identify optimization opportunities. Right from finding assets suitable for dynamic thresholds, identifying the time of the day hotspots, predicting capacity overrun issues and more, the insights helped the company induce preventive actions. The prioritization and hardening of operations helped them reduce false alerts drastically.

Key Success Metrics	Before CFX	After CFX
# of Tools Used	8	1
# of Alerts Generated per Month	367000	367000
# of False Alerts Reduced per Month	3200	256900
# of Incidents Raised per Month	125080	8170
# Capacity related outages/month	100	0

Benefits

The company noticed an improvement in the IT team's productivity, service availability, and reliability. The solution also minimized SLA breach, reduced customer churn and optimized all IT operations. The following were the measured success metrics:

- Alert de-duplication and grouping of alerts to a single incident
- Suppressing and/or auto closure of false alerts freeing up the IT team's time
- Forecasting and anomaly detection based alerting users before impacting service
- Understanding alert dependencies, improving the collaboration among teams