WHY EVENT NOISE REDUCTION AND PREDICTIVE ALERTING ARE CRITICAL FOR AIOPS

In recent months, there's been a significant amount of press and analyst coverage on AIOps. Is AIOps being over-hyped? While the market is in its early days, that doesn't mean there's nothing behind the buzz. In fact, the reality is that organizations are seeing significant benefits from AIOps today.

This is the second in a series of posts I'm publishing on use cases that offer opportunities for harnessing the benefits of AIOps in the near term. In this post, we'll look in more detail at how AIOps enables teams to reduce event noise and predictively alert.

Before we jump in, some definitions:

What is Event Noise Reduction?

Event noise is the term used to describe the hundreds of hourly and daily notifications and alarms (eg: CPU utilization, memory utilization, end user response time) delivered by monitoring systems to IT Ops teams to show the health and performance of infrastructure and applications across their IT environment.

Event noise reduction involves applying machine learning to historical and real-time operational data to identify patterns and suppress events that fall within bands of normalcy while surfacing the most critical alarms and events for prioritized triage and remediation.

What is Predictive Alerting?

Predictive alerting refers to the ability to use machine learning, pattern identification and log analytics to identify abnormalities in operational data and predictively alert IT Ops on these abnormalities that could potentially impact an application or service. By highlighting activity that falls out of operational norms, IT Ops can proactively remediate issues before any service impact to meet SLAs, optimize customer experience and increase productivity.

The IT Operations Complexity Challenge

While you could argue the job of IT operations has long been demanding, you could also make a strong case that the job has never been tougher than it is today. IT teams are being tasked with ensuring optimized service levels in a climate that's increasingly unforgiving of even short amounts of downtime. Further, these teams are tasked with managing environments that are introducing unprecedented complexity, dynamism, and interrelatedness.

Not all that long ago, monolithic, relatively static, on-premises computing stacks were the norm. Now, teams have to manage these legacy environments, plus a lot more. This typically includes implementations in dynamic microservices and container-based deployments and multiple cloud environments. Further, the expanded adoption of agile, continuous integration and continuous delivery, and DevOps approaches continues to fuel a massive acceleration in application release cycles and infrastructure changes.

While these modern environments present a number of challenges, one of the most urgent issues is the deluge of event volumes teams are being forced to sift through on an ongoing basis. Over the course of any given week, operations staff are overwhelmed by hundreds, if not thousands of alarms. Beyond the sheer scale, what compounds matters is that a significant percentage of alarms are redundant or false. Further, a single outage can often be responsible for triggering alarm storms, or massive spikes in alarms.

This overwhelming event noise creates several problems. Most fundamentally, it's a drain on resources, it saps staff energy, and it erodes morale. Further, the more teams are overwhelmed by event volumes, the more likely it is that significant incidents will be missed or spotted too late, which means service levels are at risk on a constant basis.

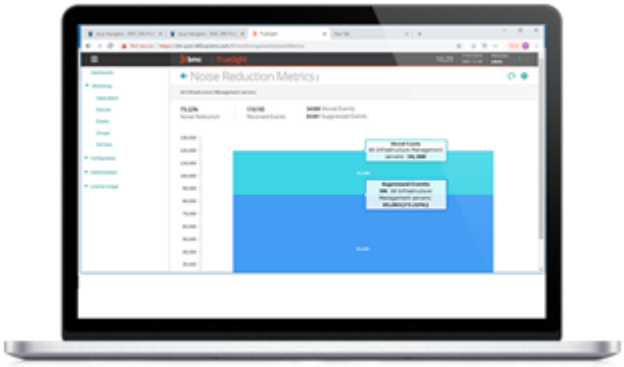
How AIOps Can Help

By establishing robust AIOps capabilities, IT operations teams can address the challenges outlined above to reduce event noise in their environments. It starts with ingesting data from diverse sources and technologies, and aggregating a variety of data types, including events, logs, metrics and end user experience monitoring data in a single consolidated data repository.

IT Ops teams can then employ policy-based rules that start to filter and suppress events. To be effective, teams need an engine that can group events, apply rules, enforce policies, and enable filtering by a range of attributes—including location, monitoring source, application tier, severity, and more. This sets the foundation for significant event noise reduction.

Machine learning is at the heart of an effective event noise reduction strategy and must be applied to historical and real-time data to study behavior and identify patterns. Based on this pattern identification, dynamic baselines can be established, reducing the overhead and inaccuracy

associated with static thresholds and associated event noise. Ultimately, event suppression is achieved by distinguishing between those arising within bands of normalcy versus those arising due to true abnormalities that could impact users.



Using AIOps for Predictive Alerting

The pattern identification and anomaly detection enabled by machine learning enables the valuable AIOps use case of predictive alerting. Machine learning, anomaly detection and log analytics enable IT Ops teams to spot potential issues, prioritize them for triage and diagnosis and address them before any impact on business services. TrueSight customers have been able to receive warnings 3 hours before a baseline is breached to proactively remediate. Predictive alerting is a valuable use case applied to capacity management as well – applying machine learning and analytics to capacity data enables potential capacity constraints to be identified ahead of time and corrective action taken. Since capacity outages are some of the most difficult to resolve, this type of insight is hugely valuable to IT Ops and capacity teams.

The Benefits of Event Noise Reduction and Predictive Alerting

When organizations employ AIOps to reduce event noise and establish predictive alerting, they can realize a range of significant benefits:

- **Harness more targeted intelligence.** IT Ops teams can better understand how specific issues affect business services, so they can more quickly identify and prioritize the most business-critical issues.
- **Boost staff productivity.** Reduce event volume levels by up to 90% to avoid the massive costs and inefficiency associated with managing thousands of redundant and inaccurate alerts.
- **Enhance service levels.** Receive warnings up to three hours before baselines are breached to remediate issues before services are affected. As a result, teams can enhance SLA compliance and improve the user experience.
- **Avoid outages and continuously optimize cost.** Use machine learning and automation to identify inefficiencies in IT infrastructure usage to prevent resource shortages and identify cost reduction opportunities

Recently, BMC worked with a large U.S. based insurer that deployed AIOps to reduce the event noise that the IT operations team had to contend with. Every month, the IT Ops team would have to sift through more than 15,000 events to diagnose, prioritize and triage. Now, by leveraging machine learning and establishing dynamic baselines, the team has been able to reduce this down to 1,500 events per month, all of which are 'meaningful' events which need to be actioned. This is a huge

boost to efficiency and cost reduction across IT Ops processes.

Achieving a balance between the competing demands of supporting business innovation and optimizing service levels can be difficult in today's complex, fast-moving environments. With the right AIOps platform, IT Ops can significantly reduce event noise and gain predictive insights, so they can optimize staff productivity and service levels and avoid downtime across their environment.

Be sure to keep an eye out for our next blog post in this series, which will provide a more detailed look at the AIOps use case of probable cause analysis. In the meantime, to learn more about our AIOps offerings, visit the TrueSight AIOps page.