# sumologic

A Sumo Logic White Paper

Harnessing Continuous Intelligence to Enable the Modern DevOps Team

As organizations embrace the DevOps approach to application development they face new challenges that can't be met with legacy monitoring tools. DevOps requires a new breed of log analytics tools that runs at cloud-scale, employs predictive algorithms, and can be integrated with a host of DevOps tools across the entire pipeline, not just server data.

Sumo Logic is an advanced log analytics tool that brings these unique capabilities to DevOps teams. Regardless of whether an organization has a head-start in DevOps adoption or is just getting started, an advanced log analytics tool like Sumo Logic can make the difference between success and failure.

DevOps Changes Everything - Monitoring Too

We are witnessing a mass migration to DevOps. In a report by CA Technologies, DevOps adoption is accelerating year-on-year, with 88% of respondents saying that they have already adopted or have plans to adopt DevOps practices within five years.
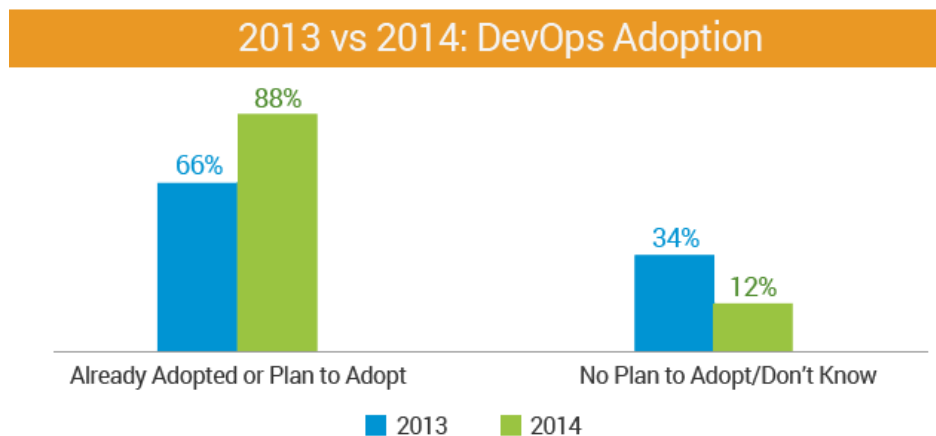
However, with the move to DevOps, traditional monitoring tools and processes can't be ported over. They were built for postmortem-style troubleshooting, whereas DevOps requires a more dynamic, real-time monitoring system.

According to *Puppet Labs' 2015 State of DevOps Report*, "High-performing IT organizations deploy 30x more frequently with 200x shorter lead times; they have 60x fewer failures and recover 168x faster." The key characteristic that defines high-performing organizations is how quickly they detect and recover from failures.

Figure 1

Comparison of IT performance metrics between high[1] and low performers

	2015 *(Super High vs. Low)*	2014 *(High vs. Low)*
Deployment Frequency	**30x**	**30x**
Deployment Lead Time	**200x**	**200x**
Mean Time to Recover (MTTR)	**168x**	**48x**
Change Success Rate	**60x**	**3x**

To detect and recover from failures, organizations that adopt DevOps practices require a new breed of monitoring tools. The modern dev shop needs real-time monitoring, and beyond that, it demands predictive analytics to prevent unexpected or unwanted incidents from happening. DevOps needs monitoring that brings greater visibility across the entire pipeline, and unifies people, processes, and tools. Log analysis enables Dev, QA, and Ops teams to be more proactive than reactive to changes and failures.

DevOps Brings an Explosion in Machine Data

DevOps is not about making the agile development cycle faster or improving on existing ITIL practices. It's about making development, test, and release cycles smaller, iterative, and more like non-events.
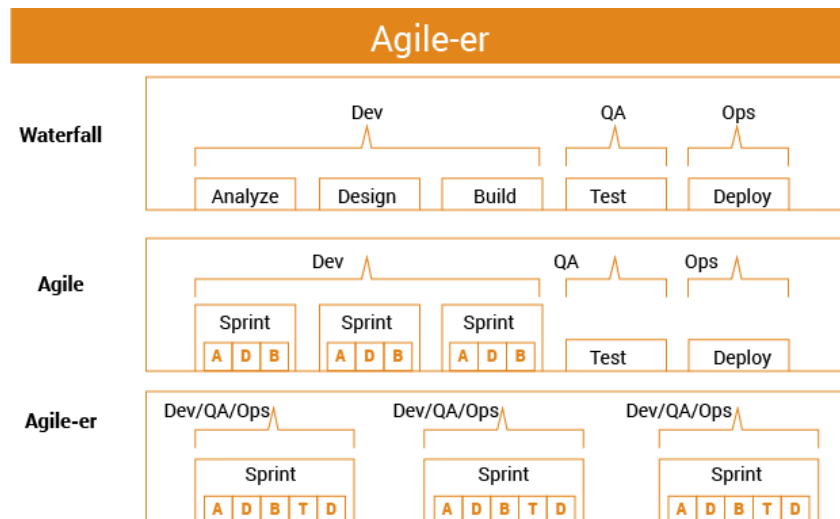
According to Webopedia, "DevOps is an enterprise software development phrase used to mean a type of agile relationship between Development and IT Operations. The goal of DevOps is to change and improve the relationship by advocating better communication and collaboration between the two business units." Beyond development, DevOps seeks to optimize the software lifecycle by focusing on the seemingly peripheral aspects that constitute Ops.

DevOps makes release cycles shorter and more frequent than its predecessors, Agile and Waterfall. It is driven by two underlying processes – Continuous Integration (CI) and Continuous Delivery (CD). CI is the process of committing code to a repository in small, iterative steps, several times a day. CD is its counterpart for release management. CD enables CI builds to be tested and deployed to production in small iterations.

> " DevOps needs monitoring that brings greater visibility across the entire pipeline.

This results in more moving parts, and a continuous exchange of information between Dev, QA, and Ops. DevOps breaks down the barriers between these three functions that make up the modern development shop. This means the software development pipeline is not just faster, it's also more dynamic. There are more people communicating with each other, processes that depend on other processes, and tools that are integrated with each other. All this complexity means that DevOps teams deal with exponentially larger volumes of machine data than they were used to with agile.

DevOps Doesn't Play Well with Traditional Monitoring

Change of culture is the defining characteristic of the DevOps movement. One key factor that enables organizations to usher in this change is by altering the way they monitor their pipeline. You can't change what you don't monitor. Any attempt to move to DevOps and change culture requires taking a closer look at the metrics from your pipeline that matter to you. This is where many organizations fail.

Fast – Too Fast?

DevOps adoption may be easy to get started, but many organizations find it soon becomes overwhelming to maintain quality and speed of development. DevOps accelerates software delivery to such an extent that today companies like Etsy deploy 50 times per day, and companies like Netflix and Amazon deploy code thousands of times a day. At this pace, there is no time to do deliberate manual check-ins, and the release process has to be automated. Mobile apps aren't updated as frequently as web apps, but the top mobile apps are updated every 10 days on average. Users have come to expect that frantic pace of fixing and updating their apps. Apps that tolerate bugs for more than a couple of weeks risk losing users to competitors.

While the 'unicorn' companies can sustain this pace, for many mid-market organizations, quality is compromised when they try to bolt DevOps onto their existing culture. For example, they may cling to rigid QA standards and compliance controls, and pressure their Dev teams to just do faster Waterfall-style development. The faster you move, the more important monitoring becomes.

Disconnected Stakeholders

Modern dev shops take the form of globally distributed teams with differing priorities and agendas. Architects have one system for prototyping, Developers use a CI system to compile source code, QA has their test automation platform, and Ops manages the infrastructure underlying all other systems. Developers, Operations and QA staff effectively speak different professional languages. This makes communicating even basic issues and desires difficult.

With so many stakeholders needed for a product to come in on time and under budget, they need unified systems, a common language, and common metrics. The DevOps culture is designed to break down silos, put departments in close contact with one another, and focus them all on the same goal. It starts with a monitoring system that delivers value to teams at every stage of the pipeline.

Disjointed Processes and Tools

The software development pipeline is becoming more complex. With DevOps, organizations look to use best of breed tools for specific needs as they arise rather than looking for a single do-it-all platform. This means new components are being added constantly. Applications are becoming increasingly distributed, with requests crossing several service or container boundaries. This suite of tools and infrastructure types may not always be integrated with each other. As a byproduct, different data sources from the various systems can't be correlated. This makes compliance and troubleshooting even more difficult than it already is. The basic challenge behind DevOps is to stay in sync when every part is moving.

> DevOps adoption may be easy to get started, but many organizations find it soon becomes overwhelming to maintain quality and speed of development.

DevOps needs a monitoring solution that is automated, and covers the entire pipeline. It should be usable by Dev, QA, and Ops. To keep up with the pace of DevOps, it should naturally enable real-time analytics, and predictive capabilities. Log analysis is the ideal solution for today's demanding DevOps monitoring requirements.

DevOps Requires the Visibility & Control that Log Analysis Brings

Log Analysis Impacts the Entire Pipeline

Log analysis impacts the pipeline end-to-end. For Developers, log analysis gives insight into failed GitHub commits, CI infrastructure, developer machines, the ebb and flow of volume in backlog systems, and release management tools. And none of these steps live in an abyss. By correlating with production data Developers can get a complete picture of the entire development environment.

For QA, log analysis enables monitoring of test runs, including the start, stop, script names, and failures. This allows Ops to optimize the test infrastructure. For example, every time a test script fails Ops can load balance, or increase performance because the disk IO is a hurdle. This enables QA to run more tests on a slow Selenium grid, and increases the efficiency of the pipeline.

For Ops, being proactive about risk management, availability, and performance issues is possible. If a new release reduces performance, Dev, QA and Ops have visibility across the entire pipeline and can identify the root cause easily.

Log Analysis Quickens Troubleshooting

Log analysis enables precise, proactive analytics that quickly uncovers hidden root causes across all layers of the application and infrastructure stack. Powerful log search capabilities enable you to quickly isolate the application node or module where the root cause of the problem hides to troubleshoot bugs and performance issues.

However, log search alone isn't enough, with the volume of log data to be analyzed, DevOps requires advanced log analytics. Advanced log analytics features include predictive algorithms, and highly-scalable infrastructure that leverages the power of the cloud. The ability of a log analytics tool to integrate with other tools in the DevOps ecosystem is a key factor. This can be in the form of APIs, or apps for other platforms. A log analysis tool that doesn't integrate with other systems is less useful. Not all tools are created equal, and many tools in the market may not enable the advanced log analysis that DevOps requires.

Sumo Logic - Advanced Log Analysis for DevOps Teams

Sumo Logic is a cloud-based log analytics platform ideal for DevOps teams that need Continuous Intelligence to complement their Continuous Integration, and Continuous Delivery workflows. Sumo Logic brings you the following advantages over legacy monitoring tools\ and other log analytic tools:

### Sumo Logic - Advanced Log Analysis for DevOps Teams

Sumo Logic is a cloud-based log analytics platform ideal for DevOps teams that need Continuous Intelligence to complement their Continuous Integration, and Continuous Delivery workflows. Sumo Logic brings you the following advantages over legacy monitoring tools\ and other log analytic tools:

LogReduce for High-Volume Log Data

Analyzing log data is a daunting task because of the high volumes of data to be analyzed, and most of the data being unstructured. However, the interesting thing about log data is that it is very repetitive. This means a single line of log code can generate thousands of lines of log data. Using this principle, Sumo Logic reverse-engineers log data to find the underlying patterns that have generated them.


LogReduce Example
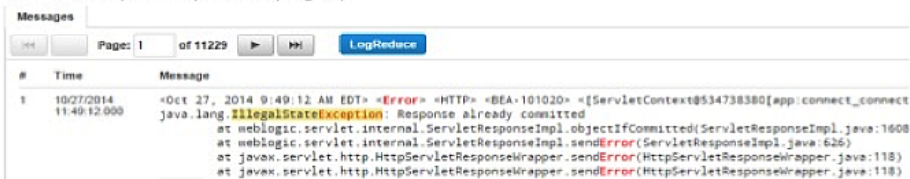
Outlier and Anomaly Detection

Often, analysis and troubleshooting is centered around known data in systems. However, most errors and security breaches stem from unknown data or data that is new to a system. Analyzing this data requires highly-scalable infrastructure and advanced algorithms to process the data. This is what Sumo Logic enables with its Anomaly Detection feature.
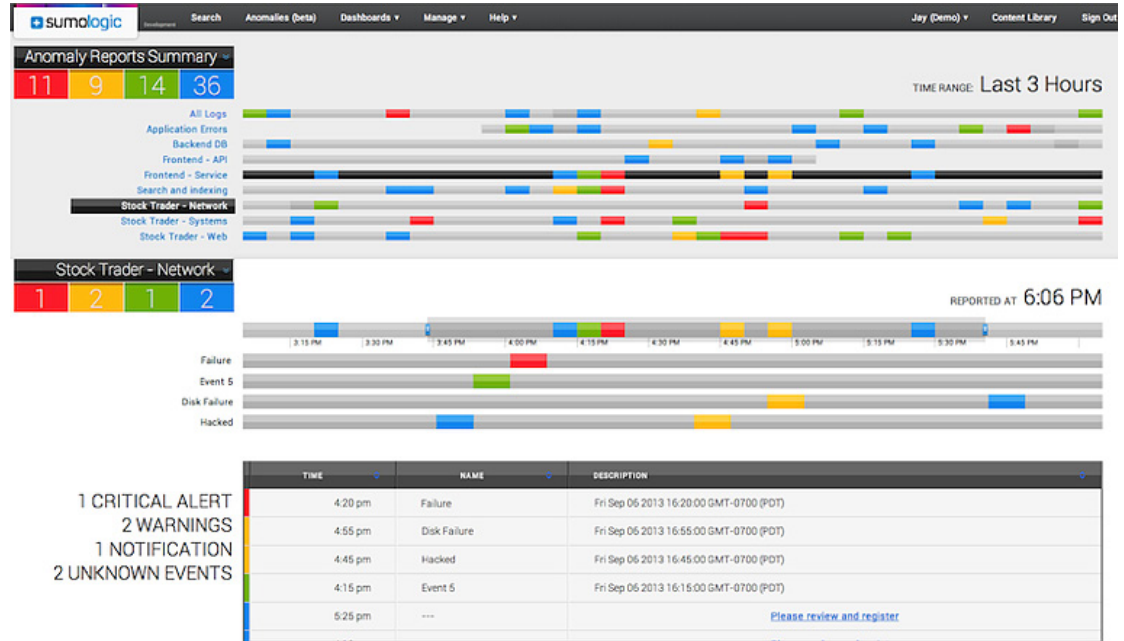
APIs for Greater Extensibility

The Search API exposed by Sumo Logic can be used to access resources and log data within the service by third-party scripts and applications. Similarly, there is a Collector Management API which allows you to configure multiple Collectors and Sources using a script, without needing to use the Sumo Logic Web Application UI. The APIs make the Sumo Logic platform extremely extensible.

Apps for Wider Coverage

Sumo Logic provides out-of-the-box support for everything from AWS to Docker, Linux, Apache, Box, Active Directory, Artifactory, and many more apps. This enables you to monitor and troubleshoot performance in these apps by leveraging the power of Sumo Logic.

Automated Compliance

Sumo Logic delivers a simple, proactive and automated process to audit and investigate operational, security and regulatory compliance incidents. All data is centralized, secured, and easily analyzed in real-time through a single, highly scalable solution. You can automatically generate audit ready compliance reports from your event logs. Demonstrating compliance for PCI and other audits is a breeze with pre-built searches, real-time dashboards, and pre-defined reports.

Taking your First Steps in DevOps with Log Analytics & Metrics

Get a Budget

A traditional mindset that restricts monitoring to bare minimum team sizes and legacy testing tools is inadequate for the modern DevOps team. Change starts with recognizing the value that monitoring can bring to your DevOps team and organization. But importantly, it should be followed up with executive buy-in and an approved budget.

Get Infrastructure Out of the Way

One concern with monitoring may be that you have to deal with infrastructure because currently your Ops team provides you with infrastructure. However, with a cloud vendor like Sumo Logic you won't have to worry about infrastructure. Infrastructure is provided and managed for you, and monitoring automatically scales with your usage. This can go a long way in ensuring a smooth migration to DevOps.

> All data is centralized, secured, and easily analyzed in real-time through a single, highly scalable solution. You can automatically generate audit ready compliance reports from your event logs.

Adopt Continuous Documentation

Documentation is a powerful counterpart to monitoring. While log analysis captures machine data, documentation operates one layer above by recording design decisions, comments, and other abstracted information that can't be captured by logs. Documentation isn't fun for most DevOps folk. However, if it's continuous documentation, it becomes an automatic collection of the processes in your application. Coupled with log analysis, continuous documentation can give your DevOps pilot project the right foundation to scale quickly.

Monitor Something, then Monitor Something Else

The key to taking the first step in DevOps is to start somewhere and start small. You could start with monitoring just the CI server, and work your way down the pipeline to testing, and release management. You eventually want to be measuring every part of the pipeline, but starting small will ensure your efforts aren't overwhelmed with the sheer volume of data you'll need to deal with.

Deliver Quick Wins

Log analysis enables you to measure results of your move to DevOps. This is an effective way to evangelize DevOps internally to stakeholders. Point out monitoring wins to the rest of the team. These could be metrics like average time to resolve bugs in the past quarter, or how the number of releases had increased in the last month. You could share this data with the team in a standup meeting and gain support across the board. Delivering quick wins is key to working your way up to bigger and bigger wins.

Key Takeaways

+ The move to DevOps requires unifying people, processes and tools, but you can't change what you don't measure.

+ Log analysis brings deep visibility across every step of the pipeline, and thus unifies people, processes, and tools that constitute DevOps.

+ Log analysis delivers real-time data and powerful log search capabilities. However, DevOps needs advanced log analytics features like predictive analytics, highly-scalable cloud infrastructure, and a number of extensions to other platforms.

+ With the plethora of options available it's important to choose the right platform to enable log analytics for your DevOps team. Sumo Logic is an advanced log analytics platform built for modern DevOps teams.

+ Sumo Logic brings you unique features like LogReduce, Outlier and Anomaly Detection, and powerful APIs.

+ If you already have a functioning DevOps team in your organization, you have a lot to gain from the advanced functionality of Sumo Logic.

+ If you're taking your first steps in DevOps, you could start by securing a budget for your plans, starting small, and delivering quick wins.

Sumo Logic

Sumo Logic is the industry's leading, secure cloud-based log management, monitoring and analytics service. With more than 700 customers around the globe, the Sumo Logic platform helps organizations derive continuous intelligence from their machine data for real-time operational, business and customer insights. Founded in 2010, Sumo Logic is a privately held company based in Redwood City, CA and is backed by Greylock Partners, Sutter Hill Ventures, Accel Partners and Sequoia Capital. For more information, visit www.sumologic.com.