305 Main Street
Redwood City, CA 94063

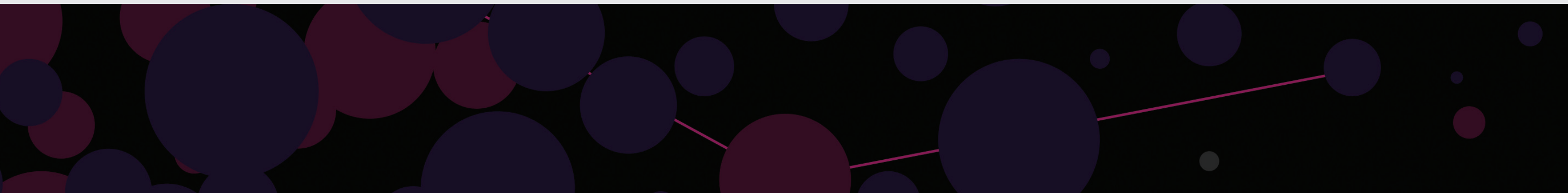
Toll-Free 1 855-LOG-SUMO +
Int'l 1 650 810 8700 +
www.sumologic.com +

sumologic

The Sumo Logic Solution: Security and Compliance

Introduction

With the number of security threats on the rise and the sophistication of attacks evolving, the inability to analyze terabytes of logs using home-grown tools or aging on-premise SIEM and log managements system has become an insurmountable barrier for enterprise security teams. As a result, organizations are more vulnerable to malware, external attacks, insider threats, data breaches, advanced persistent threats (APT) and other security threats. Retaining, reviewing and reporting on activity recorded within an ever-growing log data sets gets harder and more expensive every day, thus making it nearly impossible to stay compliant.



> "Ability to quickly uncover evidence of security incidents is essential in preventing large-scale security breaches. With Sumo Logic, the most recent log data is available instantly so that you can investigate and analyze network, system and user behavior immediately."

To make matters worse, the adoption of physical, virtual and cloud (PVC) computing infrastructures is resulting in blurring enterprise boundaries. Gaining visibility into activity within the PVC is critically important to ensure enterprises can leverage and drive benefit from these new computing paradigms. Today's enterprises require a far more powerful and a fundamentally different approach to log management and analytics. Next generation log management and analytic solution must:

1. Be easy to adopt and deploy across data centers and the cloud
2. Scale to collect, manage, and analyze exponentially more log data
3. Be able to automatically detect and flag potentially malicious activity
4. Enable low cost retention and easy reporting for compliance

Existing commercial solutions and home grown tools can't keep up with modern enterprise security and compliance requirements for log management and analytics. Modern enterprises relying on legacy tools have inherent blind-spots and are vulnerable to large scale data breaches seen across industries in the last few years.

Sumo Logic's Log Management and Analytics Service

Sumo Logic's next-generation log management and analytics service changes this equation, delivering actionable insights into security and compliance while dramatically reducing complexity and cost.

As a massively scalable, multi-tenant service, Sumo Logic performs log data collection, processing, storage and analysis within a centralized and highly secure cloud-based platform. It effortlessly handles all of your log data, regardless of volume, type or location enabling IT teams to uncover security insights buried under terabytes of logs in seconds. As a result, log data is emerging as one of the most strategic business assets within the enterprise.

Sumo Logic is designed from the ground up to handle Big Data-scale environments. Among Sumo Logic's breakthroughs is its near-zero latency Real-Time Forensics engine that delivers real-time search results from terabytes of logs. Real-Time Forensics makes critical new events occurring within IT infrastructure instantly available for analysis. Anomalous conditions can be spotted as they occur, enabling security teams to respond immediately to uncover security incidents, detect compliance issues, proactively uncover intrusions and prevent data breaches. In short, Sumo Logic reduces security and compliance investigation and resolution time dramatically.

Sumo Logic also scales to support orders of magnitude more data than legacy premise-based SIEM and log management systems. Its patented Elastic Log Processing™ engine scales each component of the service independently to meet every customer's compute, storage and data processing requirements on demand.

Sumo Logic also takes a unique approach to log data collection. Data is securely and reliably collected through either local collection (via Sumo Logic Collectors) or through hosted collection (via https or directly from Amazon S3). All data is collected in raw, or unstructured format with no need to parse or understand the data upfront; all data processing and parsing is handled in the cloud. By separating collection from processing and parsing, which occur entirely in the Sumo Logic service, there is no need to update complex parsing logic. Consequently performance is significantly improved and management overhead significantly reduced.

To help enterprises manage exploding volumes of log data, Sumo Logic is built around a globally distributed data retention architecture featuring built-in data redundancy. Sumo Logic eliminates the need for costly SAN and NAS infrastructures and removes the complexity of data archiving, backups and restores.

Another major breakthrough is Sumo Logic's patent-pending LogReduce™ technology that eliminate the time-consuming and tedious tasks of manually reading log records, writing scripts and handcrafting queries. LogReduce technology reduces millions of log lines into a handful of human digestible patterns that enable IT security teams to get to insights without having to manually writing queries to slice and dice the data. This enables our customers to quickly find important and emerging security issues that would otherwise require days of analysis. Sumo Logic's patent-pending Push Analytics™ leverages LogReduce technology to automatically uncover insights and it then pushes those insights proactively to IT security teams in order to facilitate immediate investigations.

Sumo Logic at Work

Sumo Logic plays a key role in ensuring optimal security and compliance for today's enterprises through its Real-Time Forensics, Push Analytics, and retention of all relevant log data that is critical for auditing purposes.

Security incidents vary greatly and so does the degree of difficulty of uncovering their evidence. Lets start with a few examples of security incidents:

- A brute force attack on a system succeeds after hundreds of attempts because of a failure to change a default username and password on a system or application.
- Insider downloads far more source code from a repository than is typical for a single user.
- An insider performs a "low-and-slow" attack by testing for vulnerabilities over a long period of time and gains access to a sensitive system.
- A malware gains access to a server and turns it into a SPAM mail server.
- A sophisticated group succeeds in taking control of a single system and sets up an APT with Command & Control server that sits dormant for months.

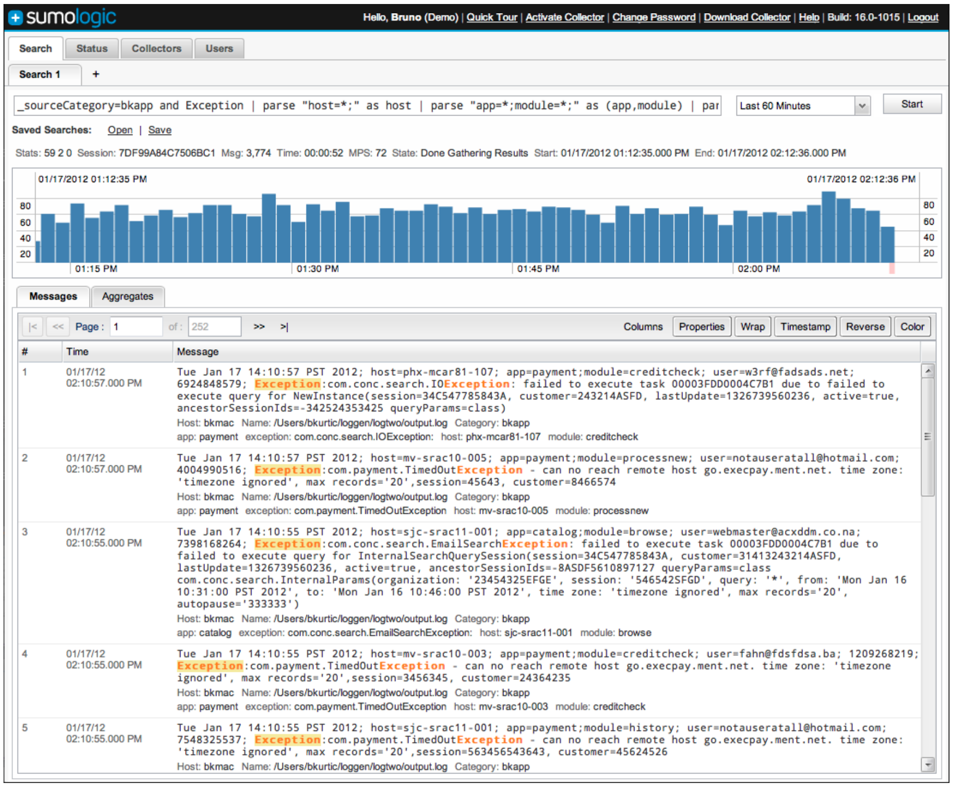
All of these hypothetical security incidents leave different traces inside infrastructure logs. Some record large amounts of activity such as SMTP traffic or a stream of unsuccessful login messages, others record tiny amounts of IRC traffic used by C&C or 2-3 failed login attempts into a sensitive system per day.

Forensic Analysis

Ability to quickly uncover evidence of security incidents is essential in preventing large-scale security breaches. However, uncovering that evidence is getting more and more difficult with the ever-growing log volumes, new computing paradigms exposing new attack vectors, and increasing sophistication of those attacks. Sumo Logic helps our customers overcome all three of these obstacles.

First, Sumo Logic Elastic Log Processing Engine is able to process orders of magnitude more logs than an aging on-premise log management system. New logs are collected, processed and available for analysis with near-zero latency. This means that our customers can perform security forensics on all relevant logs that could contain evidence of security incidents.

Second, Sumo Logic makes it easier to adopt new computing paradigms like Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) by allowing our customers to extend their security posture into all cloud environments. Inability to collect data from off-premise assets exposes blind-spots for enterprises and as such presents a barrier to adoption of these new business-enabling technologies. Sumo Logic removes those barriers, and is designed to effortlessly handle all of your log data, regardless of volume, type or location.



```
_sourceCategory=bkapp and Exception | parse "host=*;" as host | parse "app=*;module=*;" as (app,module) | par
```

Stats: 59 2 0 Session: 7DF99A84C7506BC1 Msg: 3,774 Time: 00:00:52 MPS: 72 State: Done Gathering Results Start: 01/17/2012 01:12:35.000 PM End: 01/17/2012 02:12:36.000 PM

```
#   Time                Message
1   01/17/12            Tue Jan 17 14:10:57 PST 2012; host=phx-mcar81-107; app=payment;module=creditcheck; user=w3rf@fadsads.net;
    02:10:57.000 PM     6924848579; Exception:com.conc.search.IOException: failed to execute task 00003FDD0004C7B1 due to failed to
                        execute query for NewInstance(session=34C547785843A, customer=243214ASFD, lastUpdate=1326739560236, active=true,
                        ancestorSessionIds=-342524353425 queryParams=class)
                        Host: bkmac  Name: /Users/bkurtic/loggen/logtwo/output.log  Category: bkapp
                        app: payment  exception: com.conc.search.IOException:  host: phx-mcar81-107  module: creditcheck
2   01/17/12            Tue Jan 17 14:10:57 PST 2012; host=mv-srac10-005; app=payment;module=processnew; user=notauseratall@hotmail.com;
    02:10:57.000 PM     4004990516; Exception:com.payment.TimedOutException - can no reach remote host go.execpay.ment.net. time zone:
                        'timezone ignored', max records='20',session=45643, customer=8466574
                        Host: bkmac  Name: /Users/bkurtic/loggen/logtwo/output.log  Category: bkapp
                        app: payment  exception: com.payment.TimedOutException  host: mv-srac10-005  module: processnew
3   01/17/12            Tue Jan 17 14:10:55 PST 2012; host=sjc-srac11-001; app=catalog;module=browse; user=webmaster@acxddm.co.na;
    02:10:55.000 PM     7398168264; Exception:com.conc.search.EmailSearchException: failed to execute task 00003FDD0004C7B1 due to
                        failed to execute query for InternalSearchQuerySession(session=34C547785843A, customer=31413243214ASFD,
                        lastUpdate=1326739560236, active=true, ancestorSessionIds=-8ASDF5610897127 queryParams=class
                        com.conc.search.InternalParams(organization: '23454325EFGE', session: '546542SFGD', query: '*', from: 'Mon Jan 16
                        10:31:00 PST 2012', to: 'Mon Jan 16 10:46:00 PST 2012', time zone: 'timezone ignored', max records='20',
                        autopause='333333')
                        Host: bkmac  Name: /Users/bkurtic/loggen/logtwo/output.log  Category: bkapp
                        app: catalog  exception: com.conc.search.EmailSearchException:  host: sjc-srac11-001  module: browse
4   01/17/12            Tue Jan 17 14:10:55 PST 2012; host=mv-srac10-003; app=payment;module=creditcheck; user=fahn@fdsfdsa.ba; 1209268219;
    02:10:55.000 PM     Exception:com.payment.TimedOutException - can no reach remote host go.execpay.ment.net. time zone: 'timezone
                        ignored', max records='20',session=3456345, customer=24364235
                        Host: bkmac  Name: /Users/bkurtic/loggen/logtwo/output.log  Category: bkapp
                        app: payment  exception: com.payment.TimedOutException  host: mv-srac10-003  module: creditcheck
5   01/17/12            Tue Jan 17 14:10:55 PST 2012; host=sjc-srac11-001; app=payment;module=history; user=notauseratall@hotmail.com;
    02:10:55.000 PM     7548325537; Exception:com.payment.TimedOutException - can no reach remote host go.execpay.ment.net. time zone:
                        'timezone ignored', max records='20',session=563456543643, customer=45624526
                        Host: bkmac  Name: /Users/bkurtic/loggen/logtwo/output.log  Category: bkapp
```

Third, once all the data from all corners of enterprise infrastructure is collected and processed, the equally hard task of uncovering evidence of malicious activity begins. Sumo Logic Real-time Forensics engine dramatically increases the speed of analysis and makes it possible to performs analysis on logs as they are generated or on logs that were generated months ago. Sumo Logic LogReduce™ technology helps dramatically improve the quality of that analysis by boiling down hundreds of thousands of logs into actual patterns of activity within logs. For example, it can help automatically detect when a particular user behavior deviates from regular patters, or when a device begins to communicate on a new protocol or with an external IP addresses. Furthermore, our Push Analytics proactively notifies security teams when it uncovers these and other types of anomalies within log data.

Maintaining Regulatory Compliance

Maintaining regulatory compliance with ever-more stringent new or evolving regulations is more challenging then ever. PCI DSS, HIPPA, SOX, FISMA and other regulations require log data retention, routine reviews, and reporting on specific activity within your infrastructure. In order to comply, not only must you securely retain an ever-larger volume of activity logs, but you must also adapt to evolving regulation. In addition, you must satisfy individual external auditors with their own subjective views of compliance reporting for whom vendor canned reports simply won't do. All of this requires a system that is flexible, scalable, and enables you to adapt to individual regulations and auditors.

> "With Sumo Logic, we've brought a powerful log management and analytics capability online that we weren't able to do with other third party solutions."

Sumo Logic Elastic Log Processing engine collects, processes and retains all your log data without requiring you to scale your hardware, provision expensive long-term storage, or ever deal with backups and restores of log data. Sumo Logic Real-time Forensics powered data analysis and reporting enables you to quickly and easily demonstrate that you retain all relevant activity logs and perform routine analysis.

To maximize system flexibility, Sumo Logic enables security and compliance officers to easily tag and categorize sources of log data to facilitate regulation-specific investigations and reporting. In case of PCI, as an example, you can easily tag systems that hold Primary Account Number(PAN) and subsequently quickly produce reports on how many failed logins occurred only on those systems. These reports can be customized easily to satisfy specific needs of individual auditors. Reports can also be scheduled for automated review and are then stored as evidence of routine activity analysis.

Summary

Enterprises can now offload the collection and management of all their security log data into a highly secure cloud-based platform that scales effortlessly and transparently. With Sumo Logic, organizations can analyze their log data in real time, interactively, or by automating the analysis of a large portion of their log data. At the same time, they can leverage Sumo Logic's ability to detect anomalous network, system and user behavior to augment in-house security expertise.

Finally, Sumo Logic helps enterprises become more compliant by storing and managing all security log data related to regulatory compliance and enabling more targeted and customizable analysis and reporting required by today's auditors.