COALFIRE PERSPECTIVE SERIES | JULY 1, 2016

SUMO LOGIC LOG ANALYTICS SERVICE (SAAS) AND PCI DSS 3.2

SUITABILITY FOR SUPPORTING COMPLIANCE

A COALFIRE OPINION
FINAL VERSION 1.0

sumologic

COALFIRE

North America | Latin America | EMEA
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

INTRODUCING THE PCI DSS LOGGING REQUIREMENT

The Payment Card Industry Data Security Standard version 3.2 (PCI DSS v3.2) is a proprietary information security standard that was created to reduce credit card fraud by stipulating a series of controls regulating the use of information systems that handle cardholder data (CHD) and sensitive account data (SAD). PCI DSS is not an optional standard. As stated, all entities who process, store, or transmit CHD and/or SAD must comply with the standard, or they can be fined and refused access to the card brand's payment systems.

The PCI DSS standard is comprised of six "control objectives" with twelve "requirements" that comprise the detail of the standard. The fifth control objective to "Regularly monitor and test networks" contains a requirement, number 10, to "Track and monitor all access to network resources and cardholder data". It is incumbent upon the entity, in order to be compliant with PCI DSS, to select and implement a particular technical approach to satisfying this requirement.

The traditional approach to comply with Requirement 10, has been to use an internal network systems logging resource, typically part of an internal security infrastructure, which can receive the (syslog) streams of event data, originating from key components in the system. These key components, typically servers, network devices, firewalls, intruder detection/prevention systems, etc., have been previously configured to generate streams of event information which may be monitored (for active alerts and alarms) and recorded (for subsequent inquiry). It is desirable for the information in this stream to contain sufficient details from the systems and devices, to create an "audit trail" of critical and ordinary events to satisfy the sub-requirements of Requirement 10, which call for specific user and system events to be tracked.

Although low-level event information, such as what is contained in a thorough (and properly configured) audit trail, does encompass enough detail to potentially satisfy the after-the-fact analysis of virtually everything the system may have done, the sub-requirements for daily review (10.6.1) and for post-review follow-up (10.6.3), make this requirement very hard to satisfy when manual methods are used by the customer. It is typical that raw event data is generated at a prodigious rate, often accumulating many megabytes per hour. For these reasons, most logging systems process the event data to correlate, summarize, and scan for critical (alerting and alarming) patterns of activity. Requirement 10.6.1 (daily review of all security events and logs) is usually met by the combination of correlation, summarization and then scanning for bona-fide security events – events that have usually been "confirmed" by automatic processing of two or (often many) more security events from the audit trail. Systems that historically perform this type of logging and analysis are collectively known as Security Incident and Event Monitoring (SIEM) systems. But with the increasing numbers of workloads moving to the cloud, and the explosive growth in the volume, variety, and velocity of data being generated, a new category is emerging to address, referred to as Advanced Security Analytics. It has been a long-standing tradition that systems were selected from SIEM vendors, but now more often from newer, cloud-native Security Analytics vendors entering the marketplace, who craft specific software and sell them to PCI DSS entities who deploy them internally, alongside their CHD processing infrastructure in their data centers.

SUMO LOGIC'S SOLUTION FOR PCI DSS REQUIREMENT 10

Sumo Logic provides an innovative Software as a Service (SaaS) solution to the traditional SIEM mission by using the Amazon Web Services (AWS) public cloud infrastructure to deliver a comprehensive solution for logging, analysis, and monitoring requirements used by PCI DSS and other regulations (HIPAA, FedRAMP, Sarbanes Oxley, CJIS, FISMA, etc.). This SaaS-based offering (referred to as Sumo Logic, or "the service," in this document) is provided to subscribers as a monthly service, with pricing based upon logging volume and retention period. Sumo Logic has the following features:

- On-site Collection Agents (Collectors) for Windows and Linux hosts. These agents collect and ship the raw log information up to the Sumo Logic AWS SaaS.
- Hosted Collector. Sumo Logic hosts the Collector in AWS. With a Hosted Collector, one can configure Amazon S3 Sources, allowing the movement of data from an S3 bucket directly into Sumo Logic, or HTTP Sources, generic collector endpoints that can be configured to operate with many other systems.
- In-the-cloud storage of ingested data
- Dynamically scaled capacity and rate adjustment for subscribers, placing more storage and processing into service on-the-fly
- Analysis and reporting services via the web, also dynamically scaled to fit the size and scope of the customer's needs and requests
- Comprehensive role-based access control and user management system to grant access to the Sumo Logic services and reports
- Access to web services, connectivity for collectors, via HTTPS secure connections
- A PCI DSS v3.1 Attestation of Compliance (AoC) for internal architecture, policies and procedures as an approved (requirement 10, and requirement 12.9) Service Provider
- Packaged analysis "Sumo Apps" for common log sources, such as Windows Event Logging, Linux Syslogging, Cisco/HP/Palo Alto routers and firewalls, etc.

The key challenge with the security incident and monitoring mission is to make sense of all the data. By converting unmanageable data into information, and cleverly drawing working insights from the deluge of log data, intelligence can be extracted from the security analytics systems enabling the actuality of Requirement 10, to "Track and monitor all access to network resources and cardholder data." Sumo Logic purports to be such a tool.

In this document, we present an "auditor's perspective" on Sumo Logic's approach to the fulfillment of Requirement 10, and state our opinion of the product's applicability to satisfy the specifics of each sub-requirement of the PCI DSS, and further declare whether we believe it is suitable, in whole or in part, to assist in securing cardholder data and secure account data.

SCOPE OF REVIEW

Our review of Sumo Logic's product primarily focused on what the PCI DSS Qualified Security Assessor (QSA) might review, when they are following the Council's Testing Procedure during the in-depth assessment around requirement 10. For this reason, our primary scope is directed towards satisfaction of the elements of requirement 10.

In a true assessment, there would be an actual cardholder data environment at the heart of the examination of a particular PCI DSS entity. In our review, no such PCI DSS CHD/SAD application was in play and therefore we used three methods to compensate for this absence:

First, we conducted a pair of customer interviews, to inquire into true CHD use cases, with the intent of following elements of how these Sumo Logic customers approached the tasks of deployment, integration, analysis and reporting in their particular PCI DSS environment. This being only an anecdotal sample, we added subject matter expert insights from the Sumo Logic sales engineers to get a more complete picture of how customers used the product to address their compliance objectives.

Second, using the information collected during method one, we constructed a small test environment at Coalfire Labs, where we could install and exercise Sumo Logic and observe through first-hand experience, the processes more closely. A hands-on experience is usually the best way to validate and understand the nuances involved in deploying and leveraging a security analytics solution, something customer interviews can't adequately convey. Using this lab test site as a reference, we could then walk the PCI DSS requirement 10 matrices, line by line, and create a control mapping that reviews the service accurately.

Third and finally, we conducted an additional subject matter expert (SME) deep dive on the aspects of using Sumo Logic with newer all-cloud and other SaaS architectures. Emerging cloud services are becoming more attractive to PCI DSS required entities, and we are seeing increased activity in developing under Amazon Web Services (AWS), Microsoft Azure and other cloud providers. These implementations use collector-less configurations, where native cloud services are leveraged for data ingest into Sumo Logic (e.g. VPC Flow Logs writes to Amazon CloudWatch and the CloudWatch API, Kinesis or Lambda functions are leveraged to obtain the data).

Sumo Logic is a cloud-native logging and analytics service, and targets multiple use cases – DevOps and IT Operations - not solely Security and PCI DSS compliance. However, the primary focus of our process, was to leverage the particular methodology used by customers for PCI DSS. We put particular emphasis on understanding the Data Ingest, Search, Live and Interactive Dashboards, and other features used to simulate real-time and forensic analysis during our review. We were not looking to become experts in the use of Sumo Logic, just to fulfill the Requirement 10 mapping, and to get enough "feel" for what a customer would do to satisfy our QSA assessment activity in the real-world.

Although requirement 10 is the primary focus of our review, revisions in PCI DSS released since 2015 have emphasized the importance of service provider relationships, under goal five, "Maintain an Information Security Policy." Specifically, sub-requirement 12.8 ("Maintain and implement policies … to manage service providers … that could affect the security of the cardholder data…"), and sub-requirement 12.9 ("Additional requirement for service providers only: Service providers acknowledge in writing that they are responsible for the security of cardholder data … to the extent that they could impact the security of the customer's cardholder data environment"). We will briefly touch on these elements in our Conclusion and Opinion summary.

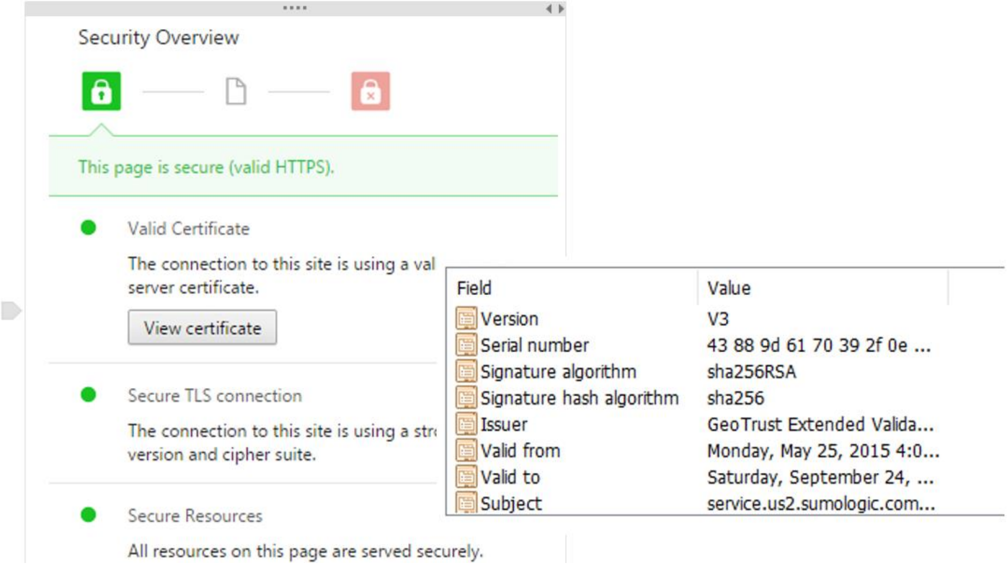
METHODOLOGY AND FINDINGS

We began with product familiarization and initial introductions with the assistance of a Sumo Logic sales engineer who gave us a quick start with the product. Sumo set up a group account with the following parameters for our lab testing:

Your **Free Trial** account has the following limits:

- 1.5 TB per month (50.0 GB / day average)
- 30 days of retention
- 20 users

We further confirmed that the connection to their service provided strong TLS 1.2 cryptography for any HTTPS sessions. Although not a specific requirement, since CHD/SAD is not typically in transit, we interpret that all control and InfoSec management traffic should abide by the strong encryption provisions as a best practice. We observed:



Security Overview

This page is secure (valid HTTPS).

Valid Certificate

The connection to this site is using a val
server certificate.

View certificate

Secure TLS connection

The connection to this site is using a str
version and cipher suite.

Secure Resources

All resources on this page are served securely.

Field	Value
Version	V3
Serial number	43 88 9d 61 70 39 2f 0e ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	GeoTrust Extended Valida...
Valid from	Monday, May 25, 2015 4:0...
Valid to	Saturday, September 24, ...
Subject	service.us2.sumologic.com...

Figure 1 - Chrome Security Overview of https://service.us2.sumologic.com/...

The certificate used to sign the TLS session was generated using the latest version of the X.509 standard (V3), and all interactions are authenticated using a strong hashing algorithm (sha256) including initial connectivity, subsequent collector interactions, and even general, non-user connections with their website.

We moved to enrollment and account set-up, confirming that sufficient user roles were available to meet PCI DSS requirement 10.5.1 that users may be granted view access based on “job-related need”. Availability of both “administrator” and “auditor” roles confirmed this role requirement. For our testing, we were provided with a 20 user accounts, which permitted us to positively verify both roles, and specifically that the “auditor” role could only view data and analyses, but not make configuration changes. Furthermore, we confirmed that unprivileged users (visitors) are unable to view audit data.

COLLECTOR INTEGRATION

By this point, we were ready to download and install collectors. We did so, and used a lab configuration that sampled Windows Server, Windows workstation, network switch, network perimeter firewall, VMware hypervisor, and power control devices, through two collectors. This test lab selection of assets was representative of likely and typical system components we would find “in scope” (components that store, process and/or transmit CHD/SAD) during a routine assessment by a QSA.

Our lab configuration had the following topology, which was also typical for “in scope” implementation and following best practices to secure “in scope” CHD networks using segmentation (not a requirement but widely adopted):

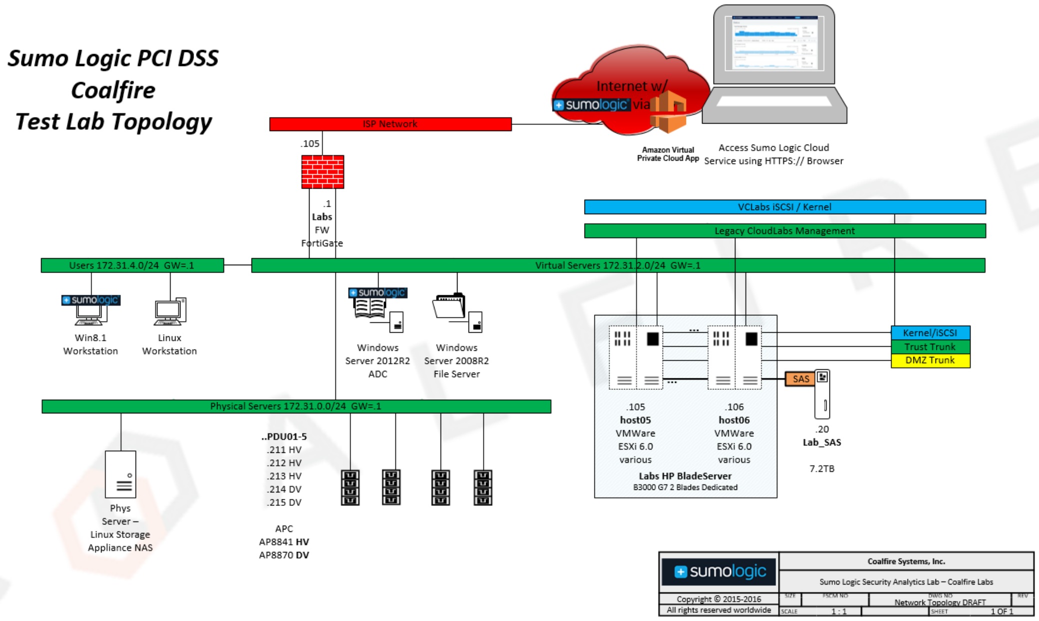


Figure 2 - Sumo Logic PCI DSS Coalfire Test Lab Topology

In the above diagram, Windows Server 2012R2 and Win8.1 Workstation were the installed collector instances. The Labs FW, a perimeter security device, acted as the default router for the Users, Virtual Servers, and Physical Servers networks, and could inspect traffic – simulating the “segmented CHD” reference architecture we see ideally at assessment customer sites. All servers and networking devices behind the firewall would be in the CHD segmented and protected sub-network.

On the right side of the diagram, we show the Hypervisors (.105 and .106) and a portion of the virtualization network used to supply all servers and workstations. *(Note: Not shown in this depiction is the network switch, the vCenter management server, and other supporting infrastructure which supports multiple roles besides this test lab. In a typical customer environment these networks and assets would be in the scope of the assessment because they can manipulate and affect CHD/SAD.)*

Sumo collectors communicate directly with the Sumo Logic service over the internet, and traverse Labs FW for secure access. HTTPS with secure TLS was observed for these transactions.

The Sumo collectors were configured with unique “names” identifying the collector logically, and a series of “source(s)” that permit the collector to collect multiple similar types of logging information.

OBSERVATION OF CUSTOMER USE CASES

We performed two customer interviews, one with Scholastic and one with Twitter, to get real-world customer perspectives and refined use cases in our Requirement 10 review.

DIRECT CLOUD LOG MONITORING

Another key strength of the Sumo Logic SaaS platform is the capacity to leverage “collector-less” Direct Cloud Logging which can deliver similar insights for Public Cloud infrastructure to what a Sumo Collector does for on-premise assets. We interviewed SME resources to understand this dimension of the Sumo Logic offering and specifically observed the **AWS Config** which is designed to deliver real-time interactive visualizations that track configuration changes to Amazon Web Services infrastructure.

An example of Cloud Log Monitoring of the AWS Config changes follows here in figure 3:

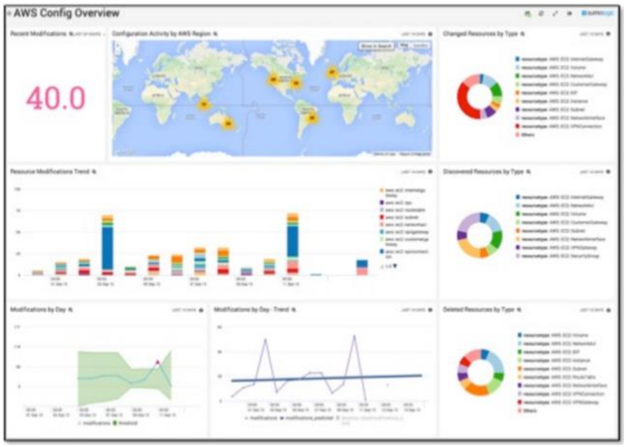

AWS Config Overview
Recent Modifications
40.0
Configuration Activity by AWS Region
Changed Resources by Type
Resource Modifications Trend
Discovered Resources by Type
Modifications by Day
Modifications by Day - Trend
Deleted Resources by Type

Figure 3 - Sumo Logic AWS Config Sample Screen

SUMO LOGIC APPS

A powerful aspect of the Sumo Logic technology is integration of the analysis and reporting functions via the Sumo Apps. The process of continuous monitoring in an actual PCI DSS entity, per requirement 10.6.1, has mandated vigilance with a 24-hour response window to “Review at least daily…” Sumo Logic Apps assist in the sifting and categorization of information collected at the raw level, providing “at a glance” review tools, which show near-real-time status and forensic information.

Most PCI DSS compliance candidates use firewalls as a key security element for in-scope control of CHD data, and to establish known perimeters to what is in-scope. An example App for Cisco components with a view of ASA firewalls is depicted here in figure 4:

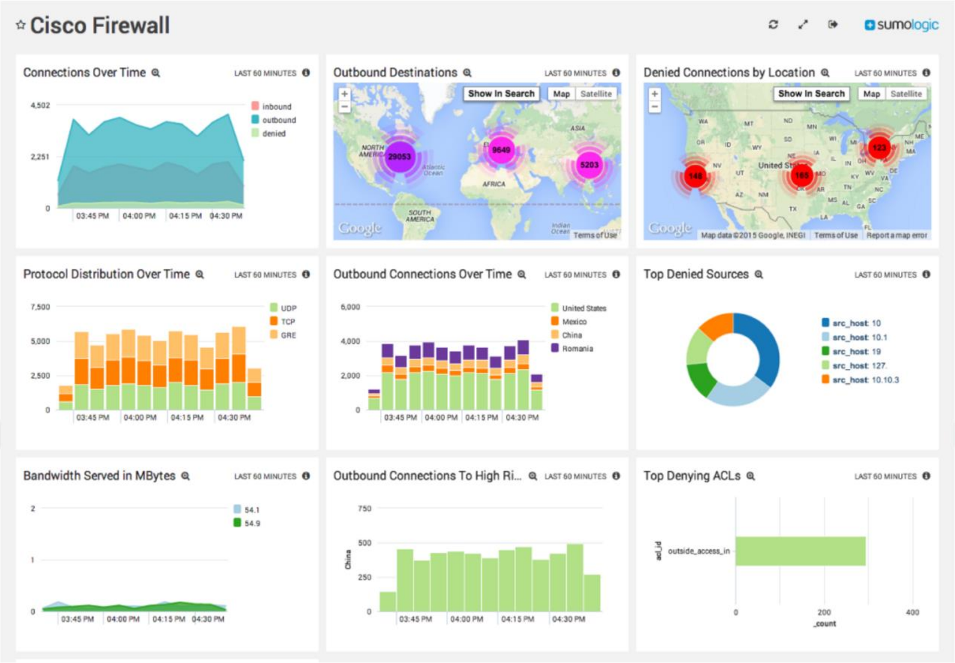


Figure 4 - Sumo Logic App for Cisco (Firewall view)

Figure 4 represents the Sumo Logic App for Cisco Firewall. General services for other Cisco products, switches, routers, IDS/IPS are also available with the same capacity for visualizations as shown above.

SUMO LOGIC DASHBOARDS

Sumo Logic uses the concept of Dashboards to provide a graphical representation of data and information gleaned from it. Dashboards rapidly communicate insights into the current state of the systems being monitored. To relieve the user from running queries and then interpreting the response from them, a dashboard takes the routine searches, runs them, and visualizes the results as part of the named and reproducible measurement. The prime mover of this concept is the Data Panel, which contains the reproducible measurement and may be used to create a Panel in Sumo Dashboards.

Live Dashboards update data as it arrives, providing near real-time views of the systems being monitored and may display a previously created Data Panel in their view. Live Dashboards are intended for real-time missions at the PCI DSS entity and are useful in the 10.6.1 “Daily…” obligation for compliance used most often by the Operations team at the entity.

Interactive Dashboards are the forensic tool that may be constructed, saved, and then routinely used for follow-up activity arising from detection of security anomalies and indicators of compromise (IOC) during daily operation.

Figures 5 and 6 depict examples of the two Dashboards and representative Cisco data which was taken from Sumo’s product overview webpage(s):

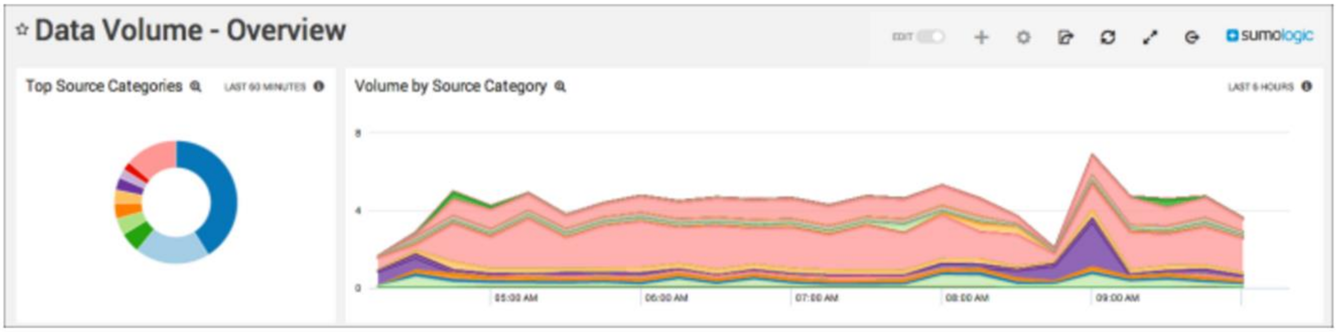
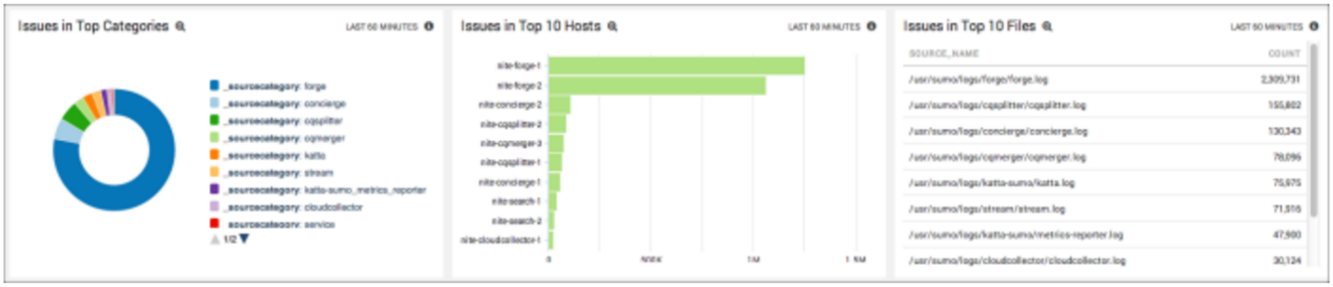


Figure 5 - Sumo Logic Data Volume Dashboard Example



SOURCE_NAME	COUNT
/usr/sumo/logs/forge/forge.log	2,309,731
/usr/sumo/logs/cqsplitter/cqsplitter.log	155,802
/usr/sumo/logs/concierge/concierge.log	130,343
/usr/sumo/logs/cqmerger/cqmerger.log	78,096
/usr/sumo/logs/katta-sumo/katta.log	75,975
/usr/sumo/logs/stream/stream.log	71,516
/usr/sumo/logs/katta-sumo/metrics-reporter.log	47,900
/usr/sumo/logs/cloudcollector/cloudcollector.log	30,124

Figure 6 - Sumo Logic Issues Dashboard Example

CONCLUSION

Sumo Logic represents a new approach to the PCI compliance and security mission – an approach that promises the economies of Public Cloud SaaS; the benefits of constant innovation and an “open systems” approach to the development and emerging science around logging and alerting; and a monthly subscription utility model to make the spend in this Requirement 10 portion of PCI DSS a combination of “sweat equity (the effort to configure and tune the IT enterprise)” and the recurring fees for service. All three of these promises are exciting and compelling to PCI DSS required entities.

We found Sumo Logic delivered these key values to their customers:

- Provides merchants with a unified platform to automate and demonstrate compliance with PCI DSS requirements 10.1-10.7
- Can deliver audit-ready compliance reporting
- For merchants with complex CHD environments, it assists in consolidating diverse and disparite logging sources into a single view, with a single and authoritative log
- Accomodates both legacy bare-metal, and modern cloud-based infrastructures as well as hybrids involving both
- Supports the ongoing Security Response Team missions required under PCI DSS 12.10 with a service to track alerts per requirement 12.10.5 and dashboards to expedite the activities typically required by those teams
- If used by a PCI DSS Service Provider (SP), can assist in complying with requirement 12.11, which will mandate (on Jan 31, 2018) daily log review, FW rule-set review, applied configuration standards to new systems, reponse to alerts, change management process logging, and quarterly review-process documentation

Sumo also addresses one of the challenge faced by PCI DSS Assessors who have been dealing with traditional SIEM systems and home-brew logging and analytics engines. The Sumo Logic service allows the QSA to assess requirement 10 compliance by reviewing the Service Provider’s Attestation of Compliance pertaining to the service approach and secure handling of systems impacting the entities’ security, followed by an in-depth review of the customer-sided configuration of Collectors, Cloud Native / Sumo Logic Apps, Dashboards, and how to best utilize the Sumo Logic SaaS service in the Cloud. Sumo Logic provides for support of sub-requirements 12.8.2, “Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data…”, and 12.9, “Additional requirement for service providers only: *Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the cardholder data environment.*”; and, will provide merchants with the necessary written confirmations to include in their Report on Compliance (ROC) or Self-assessment Questionnaire (SAQ).

COALFIRE OPINION

It is the opinion of the reviewer that the Sumo Logic SaaS service **is suitable** for sections that are open to the technical solution (non-policy and procedure) controls of Requirement 10 compliance with PCI DSS v3.2 with these caveats:

- Deployment and configuration of Collector and Cloud Native technologies have been completed by the Sumo Customer with particular and effective deployment of logging on all CHD, Security, and Critical (Cloud, Virtualization, Storage, Management Networks, etc.) infrastructure
- Appropriate Dashboards, typically available from the pre-built inventory of Sumo Dashboards, for the Customer's real-time and forensic alerting and analysis have been created, tested, and will be reviewed at least daily. No automated system can substitute for human review of audit logs to identify anomalous activity. Active use of dashboards and event response is subject to review and testing during a PCI DSS assessment
- Appropriate logging retention duration and capacities have been subscribed to by the Customer to align with the Risk Program as stated
- Role Based Access Control (RBAC) has been properly configured and is in force at the time of the assessment
- Other best practices not specifically stated that are customary to "in house" log management are also employed by the Entity and are aligned with the particulars of using the Sumo Logic service

APPENDIX – DSS MAPPING REQUIREMENT 10

The detailed mapping that follows in Table 1, is derived from assessor analysis of the Sumo Logic product against the material contained in the Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 3.2, April 2016, available online at https://www.pcisecuritystandards.org/document_library. Coalfire Systems used the specific requirements/testing/guidance section on pages 88-95 titled, *Regularly Monitor and Test Networks, Requirement 10: Track and monitor all access to network resources and cardholder data*, to supply the detailed requirements and testing; and, added the **Compliance and Guidance** column to reflect the details of our opinion and insights into actual use by the required entity.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	COMPLIANCE AND GUIDANCE
10.1 Implement audit trails to link all access to system components to each individual user.	**10.1** Verify, through observation and interviewing the system administrator, that: · Audit trails are enabled and active for system components. · Access to system components is linked to individual users.	Sumo Logic fully supports individual user accounts and roles, which is necessary for compliance with this requirement.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following:	...
10.2.1 All individual user accesses to cardholder data	**10.2.1** Verify all individual access to cardholder data is logged.	Supported via coordinated systems and applications configuration. Can be facilitated through a variety of OS Specific access accounting features in DBMS and Operating Systems.
10.2.2 All actions taken by any individual with root or administrative privileges	**10.2.2** Verify all actions taken by any individual with root or administrative privileges are logged.	See 10.2.1
10.2.3 Access to all audit trails	**10.2.3** Verify access to all audit trails is logged.	Supported by inherent nature of the Sumo Cloud Application. Sumo Logic insulates direct access to the raw logs, unlike many on-premises systems.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	COMPLIANCE AND GUIDANCE
10.2.4 Invalid logical access attempts	**10.2.4** Verify invalid logical access attempts are logged.	Supported via enabling Sumo Logic Auditing and using a search source of _sourceCategory=account_management
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	**10.2.5.a** Verify use of identification and authentication mechanisms is logged.	Rely on authentication system to generate these logs. Sumo can handle that data.
	10.2.5.b Verify all elevation of privileges is logged.	Use of the sudo command on Linux systems or equivalent and modification of account status may be logged. Yes.
	10.2.5.c Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.	Reliant upon hosting OS and Authentication system. This control can be accomplished with Sumo.
10.2.6 Initialization, stopping, or pausing of the audit logs	**10.2.6** Verify the following are logged: · Initialization of audit logs · Stopping or pausing of audit logs.	Monitoring state change or configuration changes to the collector. Collector SaaS web controls generate start, stop and pause entries to the log. Yes.
10.2.7 Creation and deletion of system-level objects	**10.2.7** Verify creation and deletion of system level objects are logged.	OS dependent setting in Windows, DBMS, and Linux. Yes can be supported by Sumo.
10.3 Record at least the following audit trail entries for all system components for each event:	**10.3** Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following:	...

PCI DSS REQUIREMENTS	TESTING PROCEDURES	COMPLIANCE AND GUIDANCE
10.3.1 User identification	**10.3.1** Verify user identification is included in log entries.	Yes.
10.3.2 Type of event	**10.3.2** Verify type of event is included in log entries.	Should be available to customize within the OS. Yes.
10.3.3 Date and time	**10.3.3** Verify date and time stamp is included in log entries.	Supported.
10.3.4 Success or failure indication	**10.3.4** Verify success or failure indication is included in log entries.	If logging entity supports, Sumo would as well.
10.3.5 Origination of event	**10.3.5** Verify origination of event is included in log entries.	Yes, supported.
10.3.6 Identity or name of affected data, system component, or resource.	**10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries.	Also yes, if supported in hosting platform.
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).	**10.4** Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	...

PCI DSS REQUIREMENTS	TESTING PROCEDURES	COMPLIANCE AND GUIDANCE
10.4.1 Critical systems have the correct and consistent time.	**10.4.1.a** Examine the process for acquiring, distributing and storing the correct time within the organization to verify that: · Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. · Where there is more than one designated time server, the time servers peer with one another to keep accurate time, · Systems receive time information only from designated central time server(s).	Sumo's SaaS solution utilizes NTP with GMT offset +0 correlation. Logs are time stamped by Sumo's service, and also contain the timestamps provided by the collector. (Note: additional Compliance and Guidance comments that follow are in the context of this GMT +0 master log timestamp provision. Also note: Log details often contain timestamps with differing GMT +/- and incorrect time server settings, which are corrected by this feature.)
	10.4.1.b Observe the time-related system-parameter settings for a sample of system components to verify: · Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. · Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. · Systems receive time only from designated central time server(s).	Yes supported. Not entirely a Sumo issue. Proper configuration of log contributors is desirable, too. See notes in 10.4.1 above.
10.4.2 Time data is protected.	**10.4.2.a** Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a	Yes, supported.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	COMPLIANCE AND GUIDANCE
	business need to access time data.	
10.4.2 Time data is protected.	**10.4.2.b** Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.	Is supported.
10.4.3 Time settings are received from industry-accepted time sources.	**10.4.3** Examine systems configurations to verify that the time server(s) accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).	Is supported.
10.5 Secure audit trails so they cannot be altered.	**10.5** Interview system administrators and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows:	...
10.5.1 Limit viewing of audit trails to those with a job-related need.	**10.5.1** Only individuals who have a job-related need can view audit trail files.	Administrator and Auditor configuration settings under User Setup support the SaaS part of this requirement. Systems must also be properly configured to prevent viewing, disabling, etc. by unauthorized users and/or changing target to point away from Collector(s).

PCI DSS REQUIREMENTS	TESTING PROCEDURES	COMPLIANCE AND GUIDANCE
10.5.2 Protect audit trail files from unauthorized modifications.	**10.5.2** Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	Insulated by SaaS architecture. Supported. Deletion of customer log data requires a specific request be made to Sumo Logic by an appropriately authorized customer.
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	**10.5.3** Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.	Near-realtime (delay of seconds) transmission of log data from collector agents to the central Sumo cloud service meets the intent and requirement of prompt backup to centralized location. Log alteration is not allowed, as mentioned in 10.5.2 above.
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	**10.5.4** Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media.	Supported.
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	**10.5.5** Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs.	Supported.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	**10.6** Perform the following:	...

PCI DSS REQUIREMENTS	TESTING PROCEDURES	COMPLIANCE AND GUIDANCE
10.6.1 Review the following at least daily: · All security events · Logs of all system components that store, process, or transmit CHD and/or SAD · Logs of all critical system components · Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	**10.6.1.a** Examine security policies and procedures to verify that procedures are defined for reviewing the following at least daily, either manually or via log tools: · All security events · Logs of all system components that store, process, or transmit CHD and/or SAD · Logs of all critical system components · Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	Dashboard for historical and near-real-time is supported. Very rich correlation functions. Apps exist for most major OS combinations and devices used in typical (and customer interviewed) use cases.
	10.6.1.b Observe processes and interview personnel to verify that the following are reviewed at least daily: · All security events · Logs of all system components that store, process, or transmit CHD and/or SAD · Logs of all critical system components · Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	Same as 10.6.1a

PCI DSS REQUIREMENTS	TESTING PROCEDURES	COMPLIANCE AND GUIDANCE
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	**10.6.2.a** Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization's policies and risk management strategy.	Sumo Logic supports this sub-requirement, and has helpful provisions for periodic summary emails and text messages to assist in automation of this activity.
	10.6.2.b Examine the organization's risk-assessment documentation and interview personnel to verify that reviews are performed in accordance with organization's policies and risk management strategy.	N/A
10.6.3 Follow up exceptions and anomalies identified during the review process.	**10.6.3.a** Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process.	N/A
	10.6.3.b Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed.	N/A
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	**10.7.a** Examine security policies and procedures to verify that they define the following: · Audit log retention policies · Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online.	Supported.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	COMPLIANCE AND GUIDANCE
	10.7.b Interview personnel and examine audit logs to verify that audit logs are retained for at least one year.	Yes, options exist for this retention period.
	10.7.c Interview personnel and observe processes to verify that at least the last three months' logs are immediately available for analysis.	Supported.
10.8 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	**10.8** Examine documentation and interview personnel to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are: · Documented, · In use, and · Known to all affected parties.	N/A

Table 1 - Sumo Logic DSS Requirement 10 Mapping

ABOUT THE AUTHOR AND REVIEWER

Chris Krueger | **Author** | Principal, Cloud and Virtualization, Coalfire Labs, Coalfire Systems
As Principal, Mr. Krueger contributes as an author and thought leader on information security and regulatory compliance topics for Coalfire's clientele in the "new and emerging" technical areas.

Mark Bloom | **Reviewer** | Director Product Marketing, Security and Compliance, Sumo Logic
Mr. Bloom is responsible for all security use case marketing and messaging for the Sumo Logic service.

THE NATION'S CYBER RISK MANAGEMENT AND COMPLIANCE LEADER

With more than 15 years in IT security and compliance and ASV-certified since inception, Coalfire is a leading provider of IT advisory services, helping organizations comply with global financial, government, industry, and healthcare mandates while helping build the IT infrastructure and security systems that will protect their businesses from security breaches and data theft.

Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; Neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.