

Jump start your PCI DSS requirement 10 implementation

Address PCI log management, monitoring and data retention challenges with a free Sumo Logic Proof of Concept

What is the problem?

PCI is an essential part of any organization's IT strategy in relation to how credit card information is handled. However, meeting PCI requirements can be costly and complex since organizations must meet 12 stringent requirements with approximately 200 controls requirements. Merchants pay an average of \$225,000 per year for audits, with some bearing the costly expense of failing compliance audits.

A key element in PCI is to centralize logs for review, auditing and analysis, spelled out as PCI DSS Requirement 10. Requirement 10 strives to ensure safe and reliable transfer of major credit and payment card data via the monitoring and analysis of PCI system activity logs. However, a recent survey by the PCI Security Standards Council (SSC) Daily Log Monitoring Special Interest Group (SIG), showed that addressing PCI requirement 10 (Track and monitor all access to network resources and cardholder data) and 10.6 (Review logs and security events for all system components to identify anomalies or suspicious activity) were particularly challenging for the majority of respondents. This challenge is magnified as systems that fall within the scope of PCI generate data at an exponential rate and companies move from on-premises to cloud or hybrid environments.

PCI 10 as a service

AWS, Sumo Logic and Consulting Partners have partnered to help companies accelerate the implementation of PCI requirement 10 for key AWS services and operating systems. The joint solution includes these components:

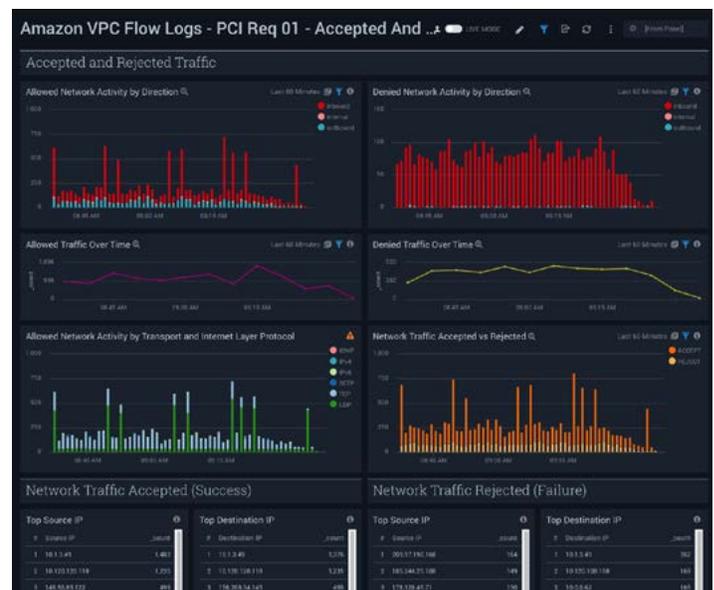
a) Sumo Logic as the platform to integrate log sources from different devices and systems into a unified reporting and monitoring layer to automate and demonstrate compliance with PCI DSS requirements 10.1-10.7.

b) A Consulting Partner engagement to configure AWS VPC Flow, AWS CloudFront, Linux and Windows servers to send logs to Sumo Logic and install Sumo Logic PCI Compliance Apps to monitor and quickly meet PCI DSS Requirement 10.

Details of the Sumo Logic Solution for PCI DSS Requirement 10 can be found in https://assets.sumologic.com/resources/brief/PCI_DSS_Compliance.pdf

Benefits for customers

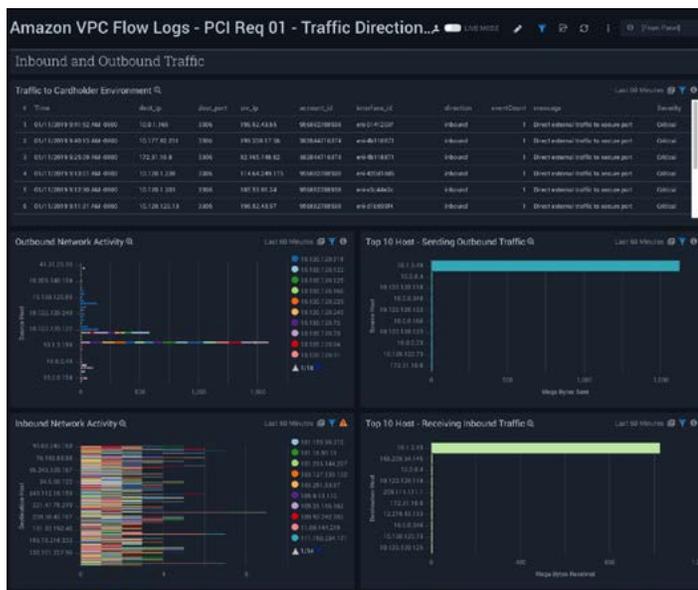
- Accelerated time to compliance. Automate and demonstrate compliance with PCI DSS Requirement 10
- Quick start on PCI delivered as part of the Sumo Logic free Proof of Concept
- Simplify compliance and shorten audit cycles
- Visibility across all systems by consolidating disparate logging sources from legacy bare-metal, modern cloud-based infrastructures as well as hybrid environments
- Support the ongoing Security Response Team missions required under PCI DSS 12.10 with a service to track alerts per requirement 12.10.5
- Secure by Design: Sumo Logic Platform is PCI DSS 3.0 Service Provider Level 1 Certified
- Reduced cost of ownership with a cloud-native, highly-scalable service
- Segmented, unalterable, and centralized repository for all your log data



Solution deliverables

During this engagement the Consulting Partner will provide the following services:

- Configure Sumo Logic account for customer
- Enable and collect VPC Flow Logs
- Collect logs for PCI compliance for CloudTrail, Linux and Windows
- Install and configure the PCI Compliance Apps for AWS VPC Flow Logs, AWS CloudTrail, and up to 5 Linux and Windows servers
- Setup fully managed alerting for a sampling of PCI-DSS Guidelines and CIS Benchmarks
- Test the dashboards included in each of the PCI Compliance Apps



Engagement duration: 3 days delivered remotely. At the end of the 3 days companies will have their free trial Sumo logic account configured with real-time PCI dashboard for VPC Flow, CloudTrail, Linux and Windows

To learn more, please contact your AWS Account Executive

About Sumo Logic

Sumo Logic is the leading cloud-native, machine data analytics platform that delivers continuous intelligence across the entire application lifecycle and stack. More than 2,000+ customers around the globe rely on Sumo Logic for the analytics and insights to build, run and secure their modern applications and cloud infrastructures. With Sumo Logic, customers gain a service-model advantage to accelerate their shift to continuous innovation, increasing competitive advantage, business value and growth. Founded in 2010, Sumo Logic is a privately held company based in Redwood City, Calif. and is backed by Accel Partners, Battery Ventures, DFJ, Franklin Templeton, Greylock Partners, IVP, Sapphire Ventures, Sequoia Capital, Sutter Hill Ventures and Tiger Global Management. For more information, visit www.sumologic.com



Toll-Free: 1.855.LOG.SUMO | Int'l: 1.650.810.8700
305 Main Street, Redwood City, CA 94603

www.sumologic.com

© Copyright 2019 Sumo Logic, Inc. All rights reserved. Sumo Logic, Elastic Log Processing, LogReduce, Push Analytics and Big Data for Real-Time IT are trademarks of Sumo Logic, Inc. All other company and product names mentioned herein may be trademarks of their respective owners. Updated 07/19