

TECHNICAL ASSESSMENT

Overview

Prepared for:



EXECUTIVE SUMMARY

LogRhythm (The Company) engaged Coalfire Systems Inc. (Coalfire), as a respected Payment Card Industry (PCI) Qualified Security Assessor (QSA) company, to provide an independent compliance validation of LogRhythm's log and event management system. The Company's technology encompasses key control areas for PCI compliance.

The scope of the assessment is focused on validating the products ability to meet specific PCI controls and the augmentation of others. The scope of the PCI DSS controls selected for validation was derived through collaboration with LogRhythm solution architects and Coalfire test engineers. This review generated two types of control classes. The first is a class where the LogRhythm solution can directly fulfill the requirement when properly deployed as a control. The second class is where the control can partially fulfill the control requirement or augment other control procedures to assist a customer in meeting the requirement.

The audience for this validation report is merchants or service providers evaluating technical solutions for log and event management to meet their PCI compliance and IT security requirements. Additionally QSA's or other auditors reviewing a deployed LogRhythm solution in a PCI environment can use this report to support their verification efforts.

Methodology

Coalfire conducted this validation through rigorous technical testing in our compliance validation labs using common PCI environmental scenarios. The outcome of this testing provides verification that customers implementing the LogRhythm solution will be able to meet these specific PCI control requirements in their real world environments. Each PCI requirement was assessed by validating the output or state of the LogRhythm solution as deployed in our lab scenario. A broad spectrum of network, system and application scenarios was used in our validation testing. Test results and lab configurations are summarized in the technical section of the white paper. Any additional detail of test procedures, test results or lab configuration are available upon request.

Summary of Validation Findings

Coalfire has completed our validation testing of the LogRhythm log and event management solution and can confirm the following summary findings;

- I. The LogRhythm log and event management solution’s architecture and implementation requirements can be deployed in a PCI environment allowing a customer to adhere to all PCI requirements for the solution.
- II. Implementation and operational documentation provide customers with appropriate guidance for operating the solution in a PCI compliant manner
- III. When properly deployed and configured the LogRhythm solution either fully meets or augments the following PCI DSS requirements:

PCI REQUIREMENT	DIRECTLY MEETS REQUIREMENTS	AUGMENTS CONTROL PROCESS
1.1.5 & 1.1.6	☑	☑
1.2.1 & 1.2.2		☑
1.3.2, 1.3.3 & 1.3.5		☑
2.1	☑	
2.3		☑
3.6.7		☑
4.1		☑
5.2	☑	
6.1	☑	
6.3		☑
6.4.2		☑
6.5		☑
6.6		☑
7.1		☑
8.1		☑
8.5.1, 8.5.4, 8.5.5, 8.5.6, 8.5.8 & 8.5.9		☑
10.2, 10.2.2 & 10.2.4	☑	
10.3	☑	
10.4	☑	
10.5.1, 10.5.2, 10.5.3, 10.5.4 & 10.5.5	☑	
10.6		☑
10.7	☑	
11.4		☑
11.5	☑	
12.9		☑

