ALERTLOGIC
Security. Compliance. Cloud.

WHITEPAPER

PCI DSS Reporting

CONTENTS

The Payment Card Industry Data Security Standard (PCI DSS) Requirements 6, 10 and 11 can be costly and resource intensive to meet as they require proof that you have log management, vulnerability assessment, intrusion detection and web application protection in place.

The purpose of this white paper is to illustrate key data and reports that are generated from Alert Logic's security & compliance services and solutions that help you maintain and demonstrate PCI DSS compliance.

Alert Logic is the leading provider Security-as-a-Service solutions for the cloud. Built for enterprises that have IT infrastructure in-house, off-site, or in the cloud, Alert Logic provides advanced security tools that are coupled with expert security services from a 24x7 Security Operations Center (SOC) to help customers address the most pressing security threats and challenging compliance mandates. By leveraging an "as-a-Service" delivery model, Alert Logic solutions include day-to-day management of security infrastructure, security experts that translate complex data into actionable insight, and flexible deployment options to address customer security needs anywhere they have IT infrastructure.

1776 Yorktown, 7th Floor, Houston, TX 77056 | 877.484.838 | info@alertlogic.com | www.alertlogic.com

Executive Summary

With large data breaches affecting retailers in 2013 and the PCI DSS 3.0 January 1, 2015 deadline approaching, the Payment Card Industry Data Security Standard (PCI DSS) is an important topic for many organizations in 2014.

PCI DSS requirements can be challenging to meet from a time, resources and cost perspective. Requirements 6, 10 and 11 can be some of the most costly and resource intensive, requiring log management, vulnerability assessment, intrusion detection and a web application firewall. Alert Logic delivers solutions to meet these and other PCI DSS requirements. As the security industry's only provider of on-demand log management, threat management, web application security, and IT compliance automation solutions, Alert Logic provides organizations with the easiest and most affordable way to secure their networks and comply with policies and regulations.

Alert Logic's solutions include:

WEB SECURITY MANAGER AND ACTIVEWATCH

- Positive & negative security models
- Adaptive learning game
- Broad compliance coverage (PCI, OWASPI)
- 24x7 monitoring, tuning and incident response

PCI DSS REQUIREMENTS

6.5.d Protect applications from common vulnerabilities such as injection flaws, buffer overflows and others

6.6 Address new threats and vulnerabilities on an ongoing basis & ensure applications are protected against known attacks

THREAT MANAGER AND ACTIVEWATCH

- Context aware threat identification
- Integrated vulnerability scanning
- PCI Approved Scanning Vendor certified
- 24x7 monitoring by in-house, certified security analysts

PCI DSS REQUIREMENTS

5.1.1 Monitor zero day attacks not covered by anti-virus

6.1 Identify newly discovered security vulnerabilities

11.2 Perform network vulnerability scans by ASV at least quarterly

11.4 Use intrusion-detection to detect and or prevent network intrusions

LOG MANAGER AND LOGREVIEW

- Powerful analysis for security logs
- Simple, intuitive search interface
- All your data accessible online, all the time
- Daily review, analysis and monitoring of log reports by in-house GIAC security analysts

PCI DSS REQUIREMENTS

10.2 Automated audit trails

10.3 Capture audit trails

10.5 Secure logs

10.6 Review logs at least daily

10.7 Maintain logs online for 3 months

10.7 Retain audit trail for at least 1 year

This white paper highlights several reports that are critical to comply with PCI DSS. Additional reports are available. Contact Alert Logic at www.alertlogic.com if you'd like more information.

Report 1: Latest Patches Not Installed on Host Systems

The theme of Requirement 6 is to ensure that systems and applications are maintained and updated on a regular basis to guard against known vulnerabilities. The Verizon Business Data Breach Investigation Report from 2012 states that 84% of attacks were considered avoidable through reasonable controls.

Requirement 6.1 states that all systems components and software have the latest vendor-supplied security patches installed within one month of release. The report above provides a quick way to determine what systems with cardholder data do not have the current patches installed. This report is included in the Threat Manager product.

Configuration Management

Latest Patches Not Installed

The systems and applications that store, process, or transmit cardholder data and supporting infrastructure should have the latest security patches installed.

Requires Action:

Vulnerable Hosts

Host	Criticality	Exposures	Risk Level
10.0.2.46	100	24	Urgent
10.0.2.47	100	26	Urgent
10.0.2.254	100	1	Urgent

Needs Review:

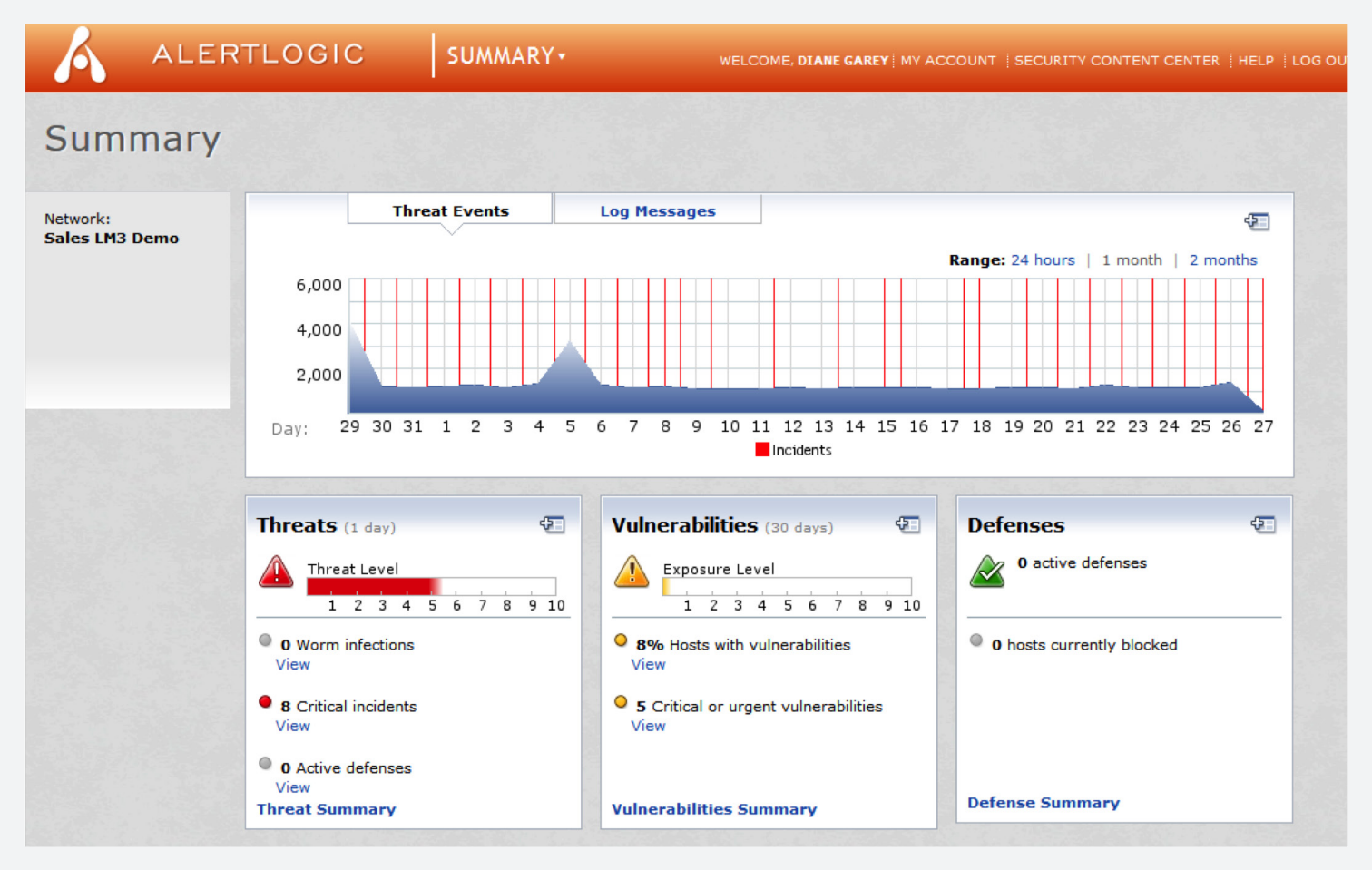
Hidden Vulnerabilities - Hosts

Host	Criticality	Hidden Exposures	Risk Level
10.0.2.46	100	3	Urgent
10.0.2.47	100	4	Urgent

Report 2: Vulnerability Dashboard

PCI DSS mandates that merchants have a system and policy in place to scan for the latest vulnerabilities in Requirement 6.2. The above dashboard provides a high level view into an environment and includes vulnerability exposure levels as well as threat incidents and log alerts.

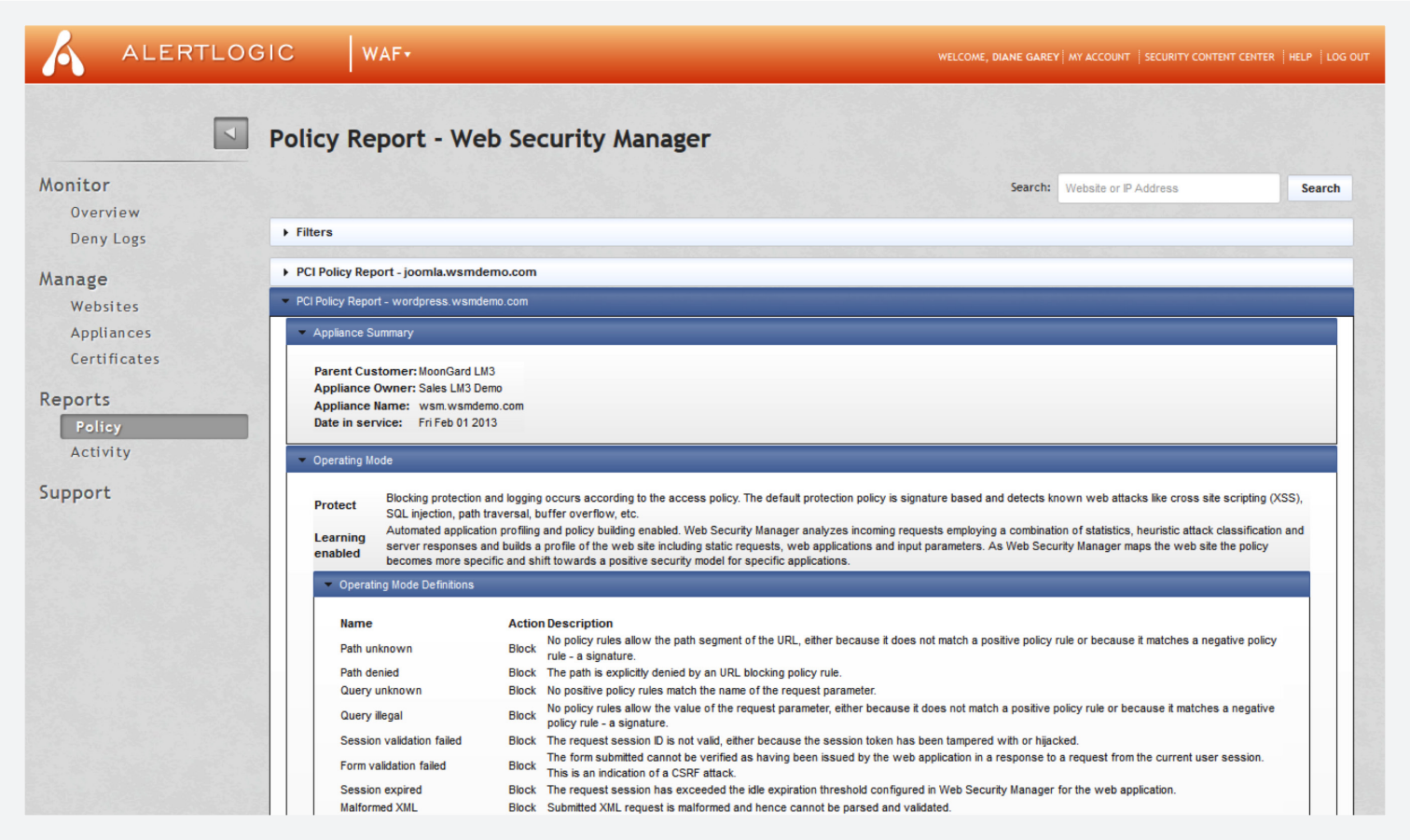
Alert Logic's Software-as-a-Service platform automatically updates to search for the latest vulnerabilities and will scan your network to maintain the highest level of security. All maintenance and vulnerability updates are performed by Alert Logic, ensuring that your environment is protected from the latest threats without using internal resources to keep your systems current.



Report 3: Protecting Web Applications

The theme of Requirement 6 is to ensure that systems and applications are maintained and updated on a regular basis to guard against known vulnerabilities. The Verizon Business Data Breach Investigation Report from 2012 states that 84% of attacks were considered avoidable through reasonable controls.

Requirement 6.1 states that all systems components and software have the latest vendor-supplied security patches installed within one month of release. The report above provides a quick way to determine what systems with cardholder data do not have the current patches installed. This report is included in the Threat Manager product.



Report 4: All Users Logging Into Sensitive Servers

Requirement 10.2 states that a merchant must implement automated audit trails for all system components, and specifically all individual access to cardholder data (10.2.1). The report above provides the specific user information on who is logging into systems where cardholder data is being stored. It is crucial to track this information on a regular basis to determine if unauthorized users have gained access to the data.

ALERTLOGIC | REPORTS

Login: Top 10 Successful

« Back to Reports

PDF Version

Excel Version

Company: **Sales LM3 Demo**

Customers: **Sales LM3 Demo**

Zones: **All Zones**

Host Groups: **All Host Groups**

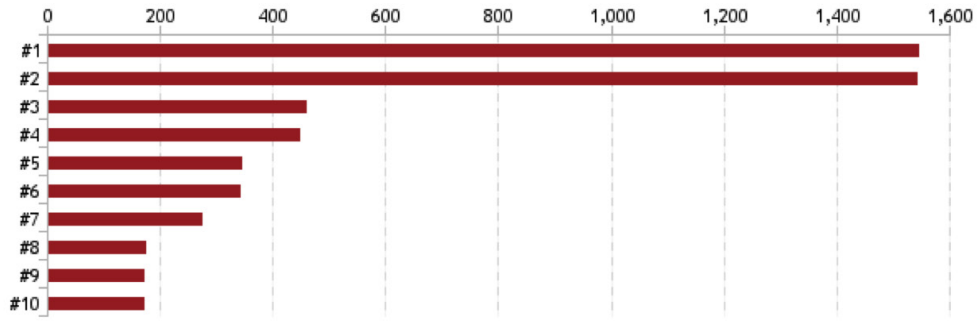
User: **Diane Garey**

Date Range: **January 27 2014 12:00am to January 28 2014 11:20am**

Generated: **Tuesday, January 28 2014 11:21am**

Top 10 Successful Logins

This section displays the top 10 users logging in during the time period of this report, based on log messages in the category 'Successful Login'.



Graph Label	User Name	Count	% of Total
#1	root	1,543	28%
#2	cchurch	1,541	28%
#3	sadovnikov	457	8%

Report 5: Failed Login Attempts into Sensitive Systems

Continuing with Requirement 10.2, merchants must also track failed login attempts into systems that contain cardholder data (10.2.4). This requirement is to ensure that companies are tracking when an unauthorized person is attempting to access cardholder data.

This report can be scheduled to run on a daily basis to ensure that attacks such as brute force attacks are not occurring. Many companies use this report to determine if contractors or onsite vendors are trying to gain access to sensitive information.

ALERTLOGIC | REPORTS

Login: Failures by Host

« Back to Reports

PDF Version

Excel Version

Company: **Sales LM3 Demo**

Customers: **Sales LM3 Demo**

Zones: **All Zones**

Host Groups: **All Host Groups**

User: **Diane Garey**

Date Range: **January 27 2014 12:00am to January 28 2014 11:25am**

Generated: **Tuesday, January 28 2014 11:26am**

Failed Login Attempts By User and Host

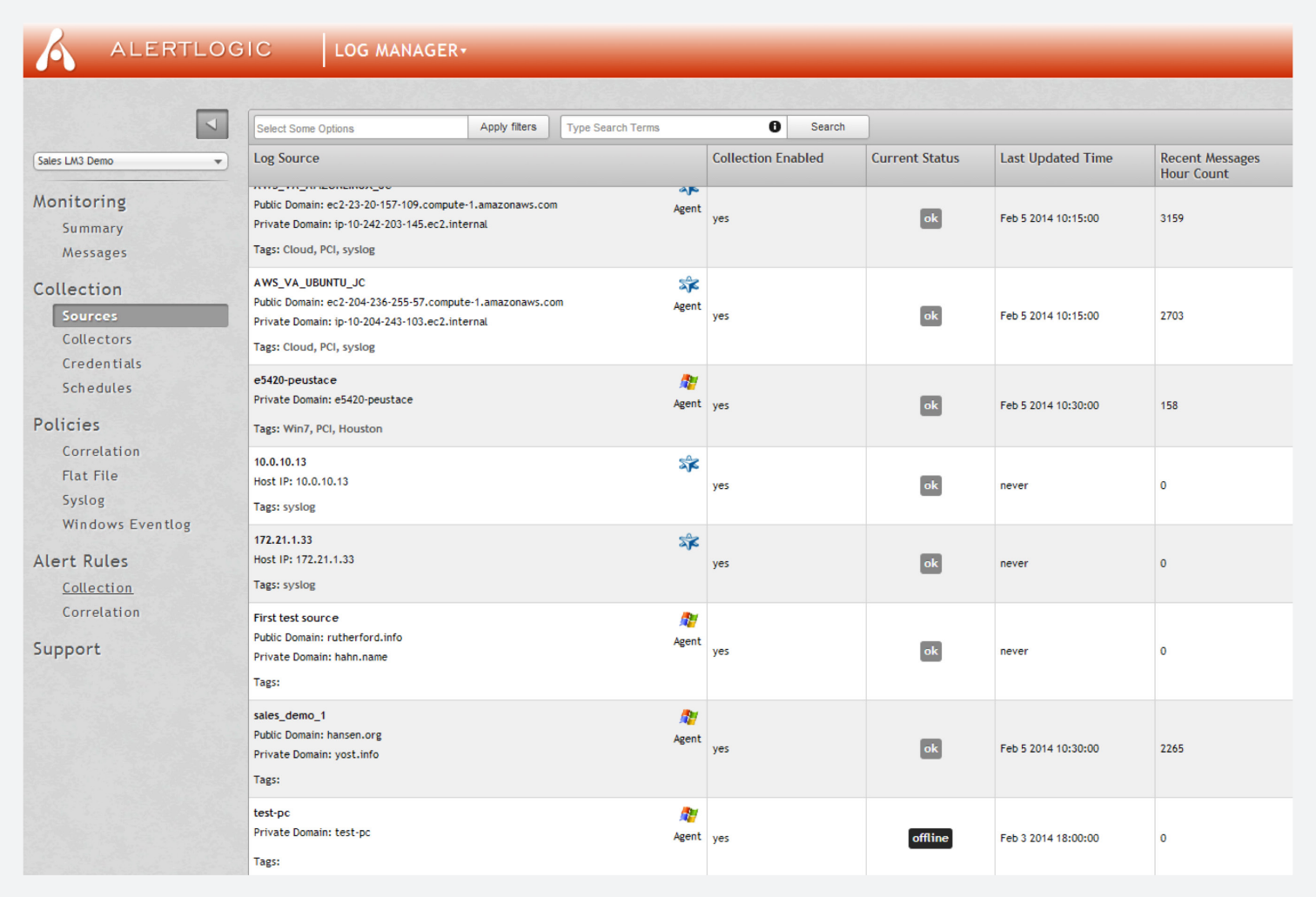
This report section shows a count of all failed login attempts grouped by user and host.

User Name	Log Source	Count	% of Total
cchurch	204.236.255.57	712	2%
cchurch	10.204.243.103	712	2%
cchurch	ec2-204-236-255-57.compute-1.amazonaws.com	712	2%
cchurch	fe80::1031:3bff:fe0a:f099	712	2%
cchurch	ip-10-204-243-103.ec2.internal	712	2%
cchurch	fe80::a870:55ff:fe62:fc5f	712	2%
phenix	109.176.212.78	401	1%
phenix	68.67.14.144	401	1%
phenix	2835:bd89:ff18:d470:f15f:ae2:9332:ac4	401	1%
phenix	2.217.118.218	401	1%

Report 6: Capturing Audit Logs

Capturing audit logs can be a very time consuming component of PCI DSS compliance. The entire theme of Requirement 10.3 is to collect logs from all points where cardholder data is stored, transmitted, or processed. The logs collected from these systems provide a tremendous amount of information that can be used for investigating security breaches, alerting on attacks, and informing security staff of unauthorized access to cardholder data.

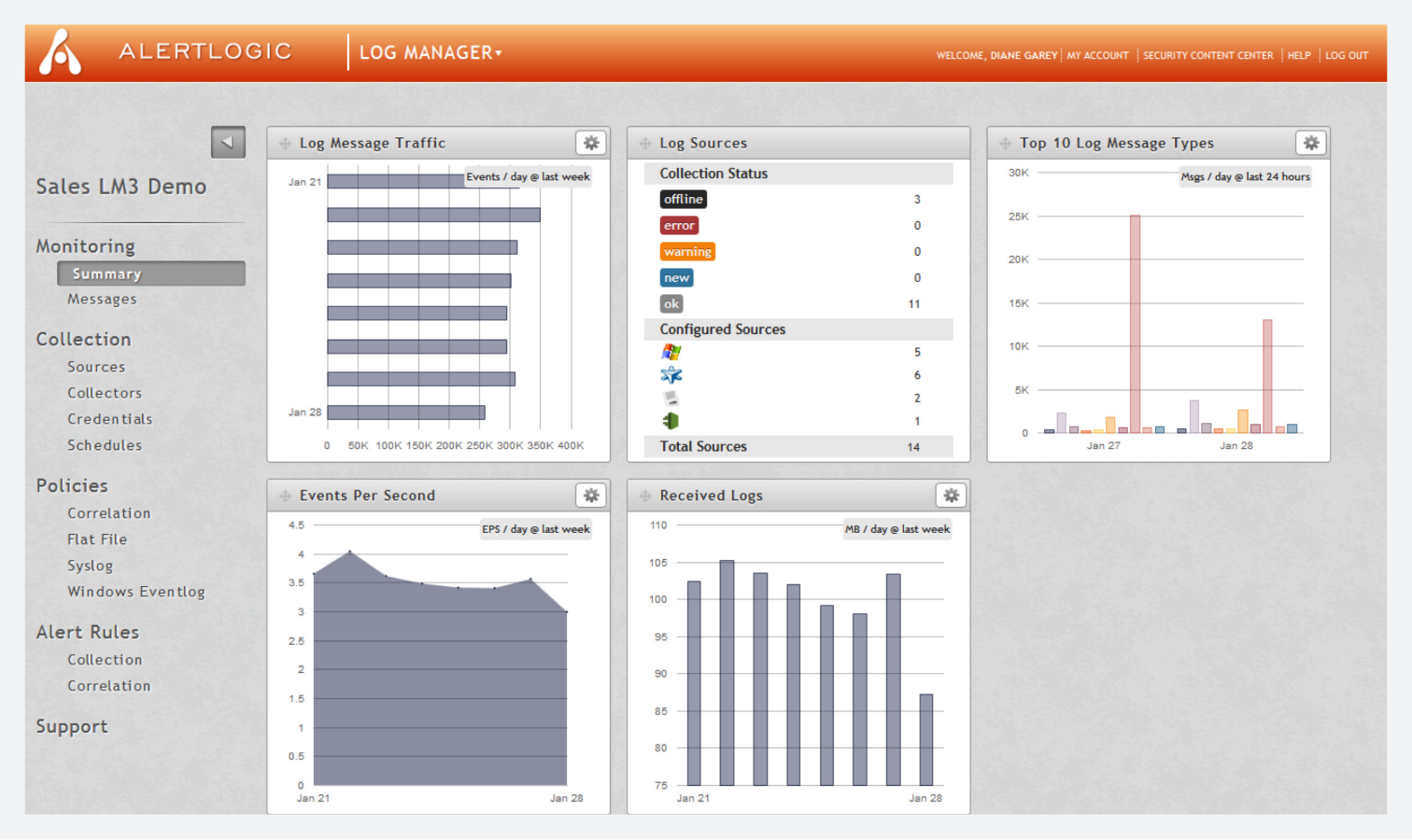
The dashboard above sheds light into all log data associated with cardholder information. Administrators can use this Alert Logic dashboard as a starting point for all log administration activity.



Report 7: Log Review Dashboard

The most time consuming aspect of PCI DSS compliance is daily log review which is mandated by Requirement 10.6. Without a log management system in place, companies can expect to spend hours each day reviewing log data.

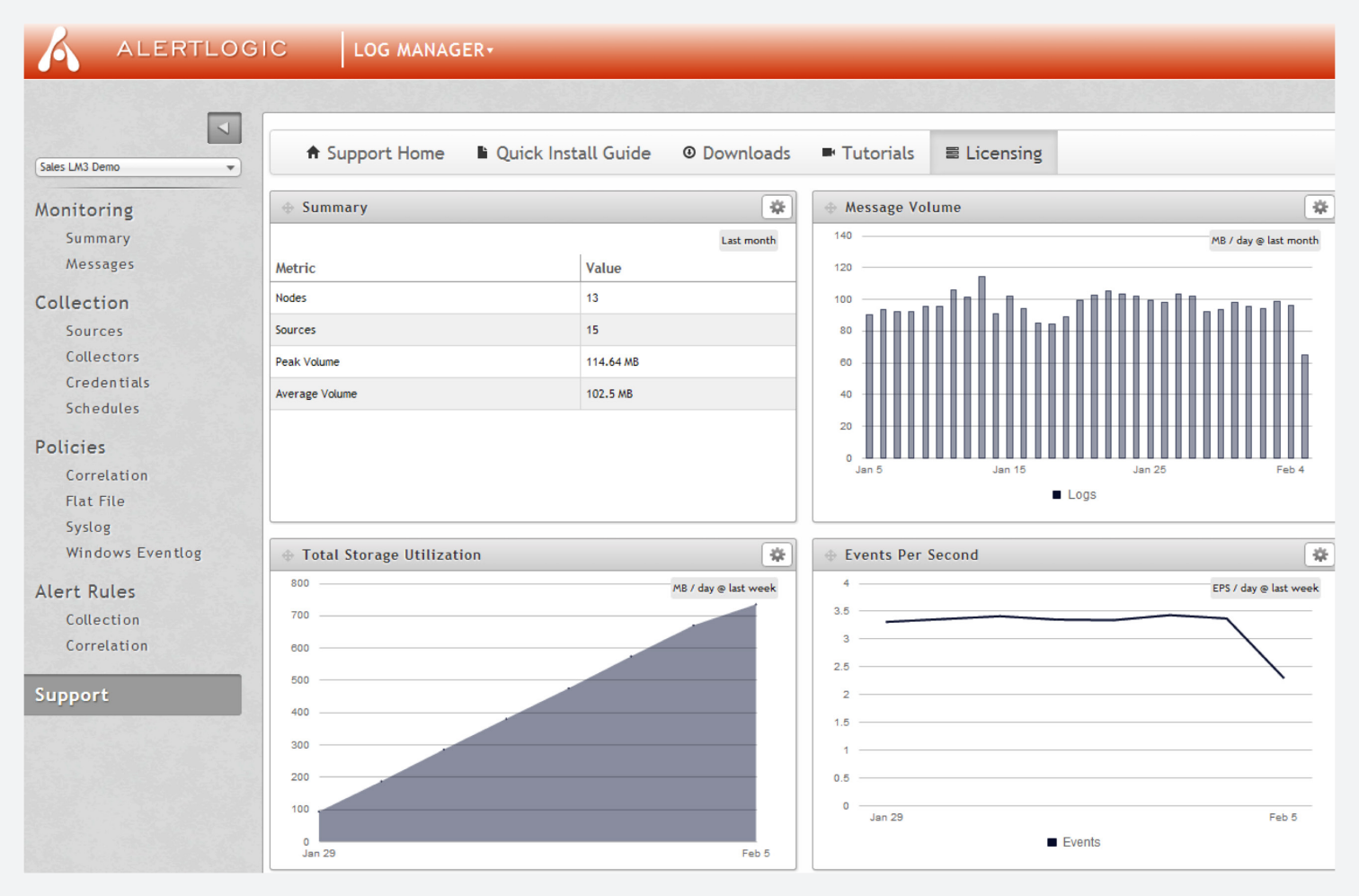
Alert Logic's Log Manager automates this daily task by providing easy to read dashboards, like the one above, which provides at-a-glance information on log files and status. Administrators can drill-down for details and/or change the layout of the dashboard to display information of interest.



Report 8: 12 Month Log Retention

Requirement 10.7 states that a merchant must retain audit trail history for at least one year, with a minimum of three months immediately available for analysis. This report verifies message collection and storage over time to ensure companies are staying in compliance with Requirement 10.7.

The Software-as-a-Service platform allows Alert Logic's customers to store their logs in the Alert Logic cloud for at least 12 months, and all customer logs are immediately available for analysis regardless of the size or age of the archived data. The user interface includes pre-built reports as well as search capabilities that enable customers to quickly find and report on all of their log data.

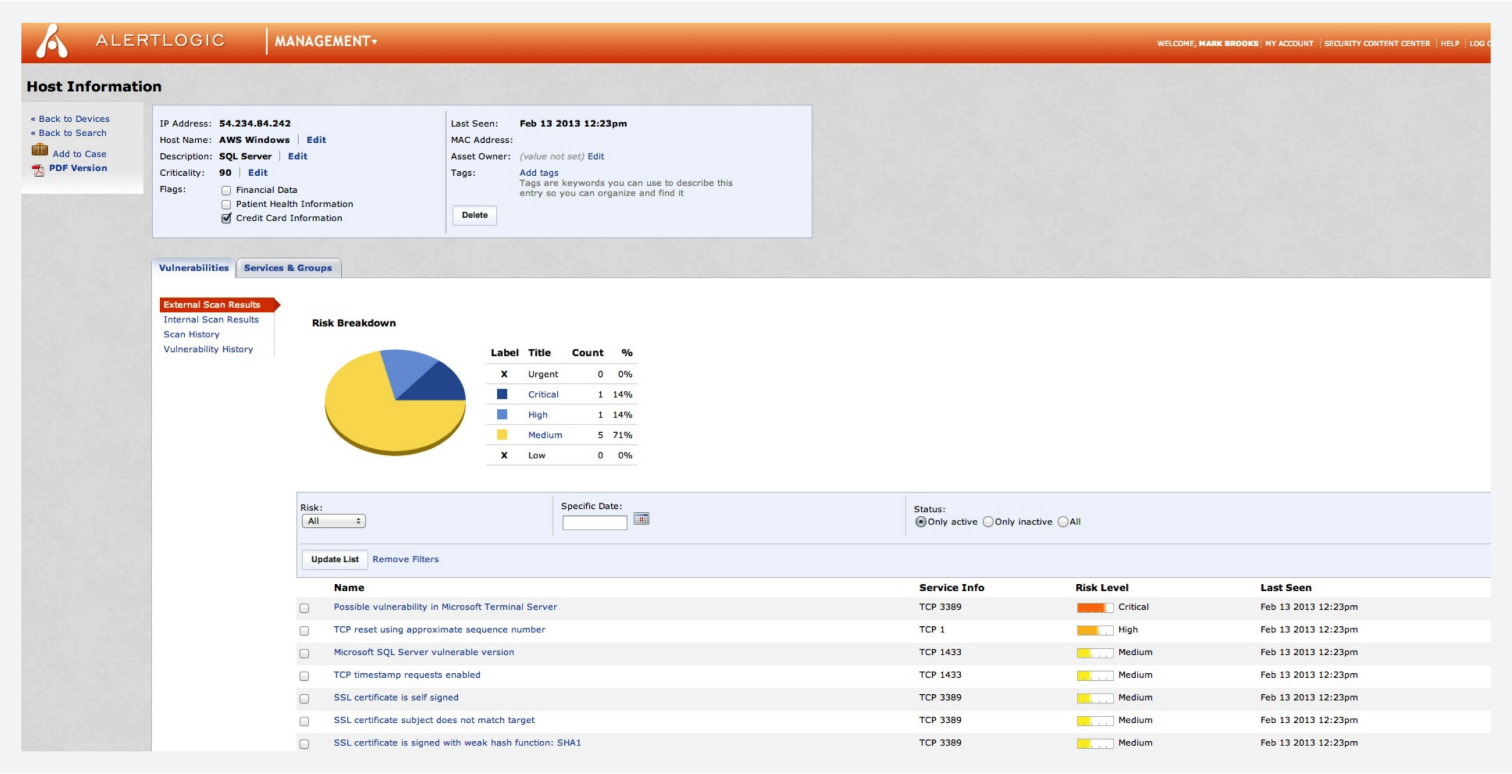


Report 9: Internal and External Network Scans

Requirement 11.2 states that all merchants must run internal and external network vulnerability scans at least quarterly, and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

Vulnerability scans identify security exposures that must be documented and remedied to stay compliant with PCI DSS. These scans can also identify vulnerabilities in your environment that can't be properly mitigated because of technical or business constraints. In this case, a compensating control can be implemented to sufficiently mitigate the risk associated with the identified vulnerability. These compensating controls must be identified and documented to effectively maintain your PCI compliance status.

PCI DSS scans must be performed by an Approved Scanning Vendor (ASV). Alert Logic is a PCI Security Standards Council ASV. Alert Logic's Threat Manager solution can perform vulnerability scans, and offers an online PCI self-assessment questionnaire. Threat Manager provides a constant view of your PCI compliance posture and helps you identify issues that could potentially impact your compliance status. Alert Logic can also assist with the documentation of compensating controls.



Report 10: Incident Visibility

Requirement 11.4 states that merchants must use an intrusion-detection system or techniques to monitor all of the traffic in the cardholder data environment and alert personnel to suspected compromises. The report above gives an example of all the incidents within a particular environment.

This report provides the security staff a complete listing of incidents, so they can identify where threats are occurring. It's important to point out that the spirit of Requirement 11.4 is to not only identify these threats, but also to react quickly to resolve them.

Alert Logic Security Operations Center (SOC) staff helps customers with security response. The SOC is an around-the-clock monitoring team who review all incidents and network threats in your environment. The team is made up of security experts who can quickly identify incidents, notify your personnel, and if needed will work with your security team to quickly resolve the issue.

ALERTLOGIC | INCIDENTS

WELCOME, DIANE GAREY | MY ACCOUNT | SECURITY CONTENT CENTER | HELP | LOG OUT

Monitoring
- Events
- Incidents

Alert Rules
- Event
- Incident

Incident # Search Search Filters

Showing: 1 - 20 of 20 incidents

Type: All | Events | Logs Range: 1 Week

ID	Date	Summary	Events	Threat	Status	Class
1722393	Feb 13 2014 23:31:03	Medfos trojan infected host at 78.140.131.159	6	34	Closed	trojan-activity
1720996	Feb 12 2014 23:48:45	SQL Injection Exploit Attempts from 10.4.184.139	254	70	In Analysis	application-attack
1720985	Feb 12 2014 23:34:04	Fareit/Kazy/PWS.Siggen trojan infection on 172.29.0.116	12	78	Closed	trojan-activity
1720984	Feb 12 2014 23:33:51	Zeus Bot infected host at 172.29.0.116	111	78	Open	trojan-activity
1720983	Feb 12 2014 23:33:37	Blackhole Exploit Kit download detected on 198.100.45.44	26	34	In Analysis	trojan-activity
1720982	Feb 12 2014 23:32:48	Cool Exploit Kit download detected on 10.0.2.15	28	34	In Analysis	trojan-activity
1720981	Feb 12 2014 23:32:01	ZeroAccess infected host at 192.168.106.131	94	44	No Analysis Required	trojan-activity
1720980	Feb 12 2014 23:30:19	FTP login brute force attempt from 58.241.31.18	90	50	No Analysis Required	brute-force
1719377	Feb 11 2014 23:31:40	Medfos trojan infected host at 78.140.131.159	6	34	No Analysis Required	trojan-activity
1717837	Feb 10 2014 23:47:29	SQL Injection Exploit Attempts from 10.4.184.139	270	70	No Analysis Required	application-attack
1717817	Feb 10 2014 23:32:48	Fareit/Kazy/PWS.Siggen trojan infection on 172.29.0.116	12	78	No Analysis Required	trojan-activity
1717815	Feb 10 2014 23:32:29	Zeus Bot infected host at 172.29.0.116	128	78	No Analysis Required	trojan-activity
1717807	Feb 10 2014 23:30:14	ZeroAccess infected host at 192.168.106.131	141	44	No Analysis Required	trojan-activity
1716252	Feb 9 2014 23:30:56	Medfos trojan infected host at 78.140.131.159	3	34	No Analysis Required	trojan-activity

LogReview Overview

Alert Logic LogReview builds on Alert Logic Log Manager to virtually eliminate the need for processes and personnel to satisfy PCI DSS daily log review requirements. Each day, our 24x7 security analysts use Log Manager to analyze event log data, track and escalate incidents, send notifications and assess the health of your log collection.

The LogReview service is designed to meet the following PCI DSS requirements:

> Daily log review as specified in requirement 10.6 of PCI DSS.
> Analyze event log data for potential security incidents such as account lockouts, failed logins, new user accounts, improper access attempts, etc.
> Identify incidents that warrant investigation and send notifications to you for review.
> Create an incident audit trail for auditors and regulators.
> Monitor log collection activities and alert you when logs are not being collected.
> Reports mapped to PCI DSS standard.

What We Review

ACTIVE DIRECTORY	**Active Directory Global Catalog Change (PCI DSS 10.2.2, 10.2.7).**	The Microsoft Active Directory Global Catalog provides searchable information about every object controlled within your AD forest. Additionally, it provides the ability to search across multiple different domains without being required to access the AD for each domain directly. This report details all changes to the AD Global Catalog that are recorded as log messages.
	Active Directory Global Catalog Demotion (PCI DSS 10.2.2, 10.2.7).	The Microsoft Active Directory Global Catalog provides searchable information about every object controlled within your AD forest. Additionally, it provides the ability to search across multiple different domains without being required to access the AD for each domain directly. This report provides log message details each time a domain controller in your AD forest has been demoted, and can no longer serve the global catalog.
DATABASES	**Database Failed Logins (PCI DSS 10.2.4).**	This report is generated to identify and display database login failure log messages received from all monitored hosts. This report is applicable to Oracle and SQL Server.
NETWORK DEVICES	**Network Device Failed Logins (PCI DSS 10.2.4).**	This report is generated to identify and display network device login failure log messages received from all monitored hosts.
	Network Device Policy Change (PCI DSS 10.2.2).	This report is generated when a policy is added/changed/removed on network devices.

WINDOWS SERVER (2008 R2, 2008, 2003)	**Excessive Windows Account Lockouts (PCI DSS 10.2.4).**	This report is generated when a threshold of two log messages has been exceeded. The messages indicate that Windows user accounts have been locked out.
	Excessive Windows Account Lockouts by Administrative User (PCI DSS 10.2.2 & 10.2.4).	This report is generated when a threshold of two log messages has been exceeded. The messages indicate that the Windows Administrator account has been locked out.
	Excessive Windows Failed Logins (PCI DSS 10.2.4).	This report is generated to identify and display excessive Windows login failure log messages received from all monitored hosts with a threshold greater than five messages.
	Excessive Windows Failed Logins by Administrative User (PCI DSS 10.2.2 & 10.2.4).	This report is generated when an excessive amount of Windows login failure log messages are received from a single host for the Administrator account. The threshold is messages greater than five.
	Windows FTP Failed Logins (PCI DSS 10.2.4).	This report is generated when log messages indicate that accounts have failed to successfully login to IIS.
	Windows User Account Created (PCI DSS 10.2.2).	This report is generated when log messages indicate that user accounts have been successfully created.
	Windows User Account Modified (PCI DSS 10.2.2).	This report is generated when log messages indicate that user accounts have been modified (changed, created and deleted).
	Windows User Group Created (PCI DSS 10.2.2).	This report is generated when log messages indicate that a user group has been created.
	Windows User Group Modified (PCI DSS 10.2.2).	This report is generated when log messages indicate that user groups have been modified (changed, created and deleted).
UNIX	**Failed UNIX Switch User Command (PCI DSS 10.2.2 & 10.2.4).**	This report provides details of all recorded failed uses of the UNIX switch user (su) command.
	UNIX Account Created (PCI DSS 10.2.2).	This report is generated when log messages indicate the creation of UNIX accounts.
	UNIX Failed Logins (PCI DSS 10.2.4).	This report is generated when log messages indicate that local and remote accounts have failed to successfully login.
	UNIX Group Created (PCI DSS 10.2.2).	This report is generated when log messages indicate that a UNIX user group was added.
	UNIX SSH Failed Logins (PCI DSS 10.2.4).	This report is generated to identify and display SSH login failure log messages received from all monitored hosts.
	UNIX Sudo Access (PCI DSS 10.1 & 10.2.2).	This report is generated when a user has executed the UNIX sudo command.
	UNIX Switch User Command Success (PCI DSS 10.1 & 10.2.2).	This report is generated when log messages indicate that a user has successfully executed the UNIX switch user (su) command.

Summary

IT compliance and security management can be complicated and expensive. Alert Logic simplifies compliance and security by delivering an integrated solution consisting of Software-as-a-Service products and 24x7 Security Operations Monitoring services for intrusion detection, vulnerability assessment, log management, and web application security management. These tightly coupled solutions enable customers to address expanding compliance mandates while lowering costs and accelerating deployment.

Alert Logic's Threat Manager, Log Manager and Web Security Manager solutions utilize a combination of patented grid-based technology and cutting edge multi-factor threat scenario modeling to accurately identify and prioritize threats in your environment. Integrated with those solutions, Alert Logic ActiveWatch and LogReview are around-the-clock services that provide expert human analysis, review and insight on real-time security threats and alerts. These services satisfy compliance requirements for daily log review or 24x7 monitoring at a fraction of the cost of employing these skills in-house.

Alert Logic's Security-as-a-Service model is the picture of simplicity and efficiency. All solution capabilities can be access from any browser and all configuration, tuning, maintenance, and solution upgrades are performed automatically and seamlessly by Alert Logic. With more than a decade of experience and more than 2,400 satisfied customers, Alert Logic's solutions are proven to meet and radically simplify your compliance and security needs.