

# PCI DSS Top 10 Reports

## March 2011

The Payment Card Industry Data Security Standard (PCI DSS) Requirements 6, 10 and 11 can be the most costly and resource intensive to meet as they require log management, vulnerability assessment and intrusion detection.

New Software-as-a-Service (SaaS) solutions can now deliver these capabilities at a fraction of the cost of traditional software or appliance-based solutions.

This paper illustrates the 10 key reports needed to demonstrate compliance with PCI DSS that can be achieved with SaaS solutions from Alert Logic.

### Contents

Introduction.....	1
Compliance Pressure .....	1
Evolving Threats .....	2
In-house Is No Longer En Vogue.....	3
Opportunity for Service Providers.....	5
Alert Logic Solutions .....	5
Ensuring Partner Success.....	7
Conclusion .....	7

**Alert Logic, Inc.**

1776 Yorktown, 7th Floor, Houston, TX 77056 | 877.484.8383 (toll free) | 713.484.8383 (main) | 713.660.7988 (fax) | [www.alertlogic.com](http://www.alertlogic.com)

Alert Logic and the Alert Logic logo are trademarks, registered trademarks, or service marks of Alert Logic Inc. All other trademarks listed in this document are the property of their respective owners.

© 2011 Alert Logic, Inc. All rights reserved.

## Executive Summary

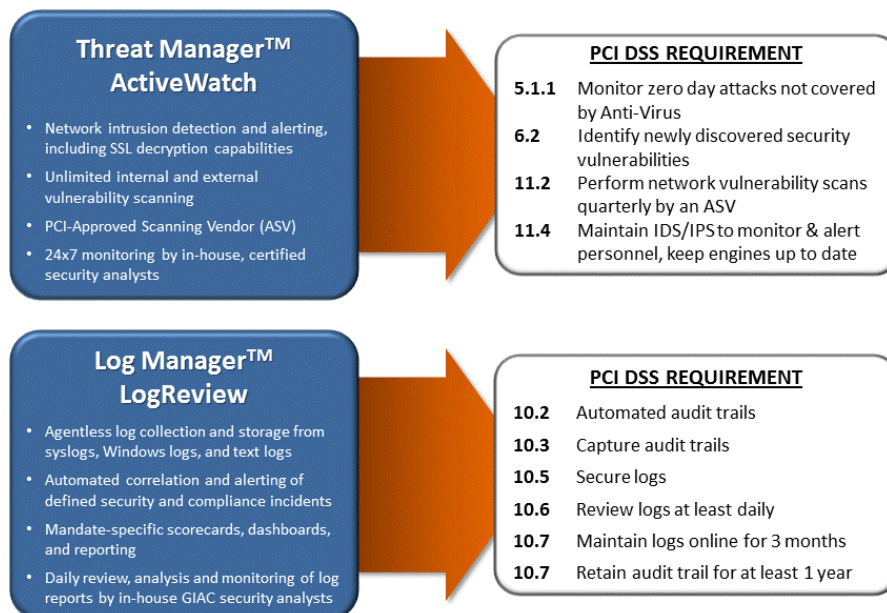
---

Headlines have been written, fines have been issued and companies across the globe are feeling the pressure of the amount of resources, time and capital that are needed to comply with the Payment Card Industry Data Security Standard (PCI DSS). Companies not only have to embrace new policies and implement changes to network configurations, but they must also ensure that technology is in place to protect cardholder data. Specifically, Requirements 6, 10 and 11 can be the most costly and resource intensive, requiring log management, vulnerability assessment, and intrusion detection.

Alert Logic is changing the way that IT compliance and security solutions are designed, delivered, and utilized. As the security industry's only provider of on-demand log management, threat management, and IT compliance automation solutions, Alert Logic provides organizations with the easiest and most affordable way to secure their networks and comply with critical policies and regulations.

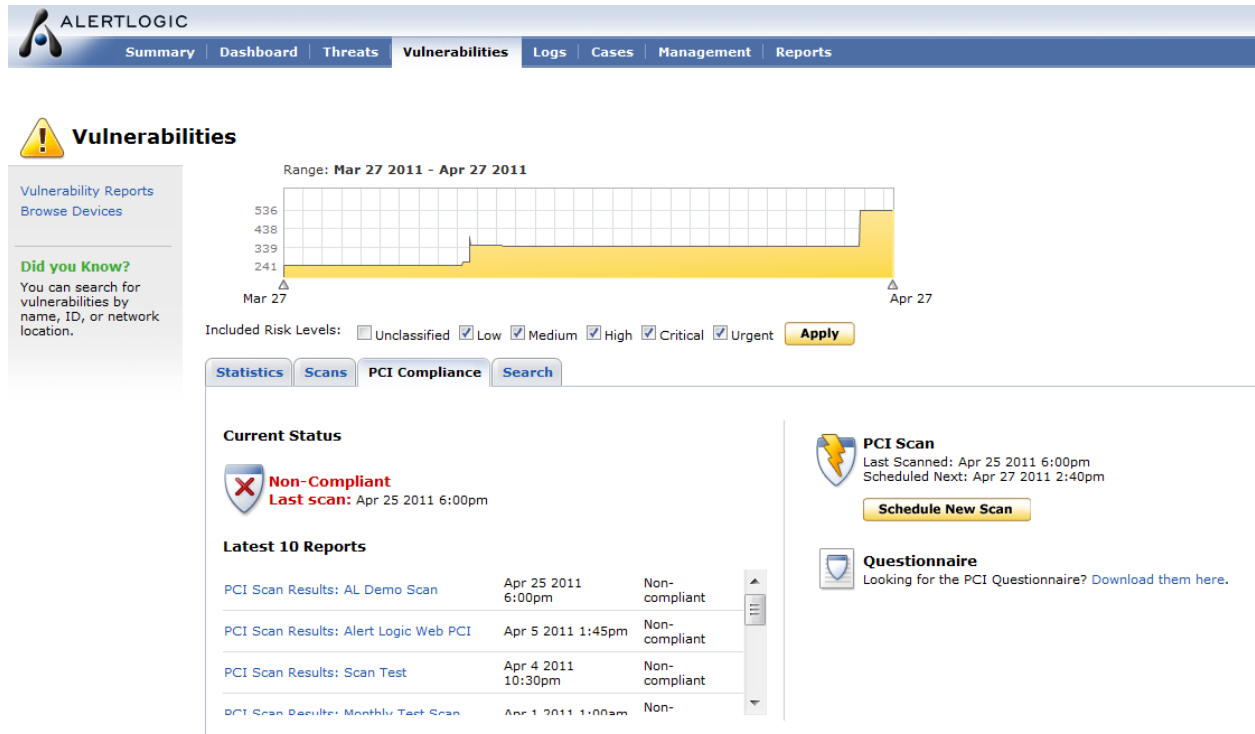
Alert Logic's solutions include:

- Log Management - leverages on-demand architecture to automatically collect, transmit, analyze, and archive log data from across your organization.
- Threat Management - combines intrusion detection and vulnerability management technology into a single integrated solution, offering both proactive and reactive protection from the latest threats.



This white paper provides the top 10 reports that are critical to comply with PCI DSS 2.0. All of these reports are delivered through a Software-as-a-Service (SaaS) model.

# REPORT 1: Quarterly Internal and External Network Scan from Approved Scanning Vendor (ASV)



Requirement 11.2 states that all merchants must run a quarterly internal and external network scan and provide the results to their acquiring banks. External vulnerability scans can identify security exposures that must be documented and remedied in order 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. Alert Logic is a PCI Security Standards Council Approved Scanning Vendor (ASV). Alert Logic's Threat Manager solution can perform external 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 2: All Users Logging Into Sensitive Servers

ALERTLOGIC

[Summary](#) | 
 [Dashboard](#) | 
 [Threats](#) | 
 [Vulnerabilities](#) | 
 [Logs](#) | 
 [Cases](#) | 
 [Management](#) | 
 **Reports**

### Login: Top 10 Successful

[← Back to Reports](#)

[PDF Version](#)

[Excel Version](#)

Company: **AlertLogic Demonstration**

Customers: **AlertLogic Demonstration**

Zones: **All Zones**

Host Groups: **All Host Groups**

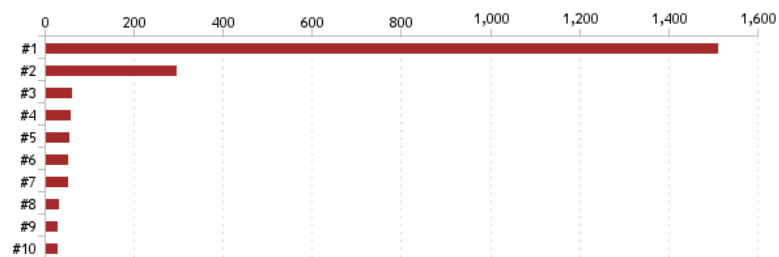
User: **Sales Account**

Date Range: **April 26 2011 12:00am to April 27 2011 11:33am**

Generated: **Wednesday, April 27 2011 11:35am**

#### 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	1,509	70%
#2	cchurch	294	14%
#3	dholm	59	3%
#4	gene	56	3%
#5	sadovnikov	52	2%
#6	user1234	51	2%
#7		49	2%
#8	abcd1234	28	1%
#9	asl	27	1%
#10	oracle	27	1%

[↑ Back to Top](#)

Requirement 10.2 states that a merchant must implement automated audit trails for all systems 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 to determine if unauthorized users have gained access to the data.

## REPORT 3: Failed Login Attempts into Sensitive Systems

### Log Messages

column width: - +    < Undo: View set to Failed | Full History        **Search**    **Filters**    **Columns**

<< - 9am | Fri 9am - 10am | Fri 10am - 11am | Fri 11am - now    **Last 60 minutes**    >> View logs by: Hour

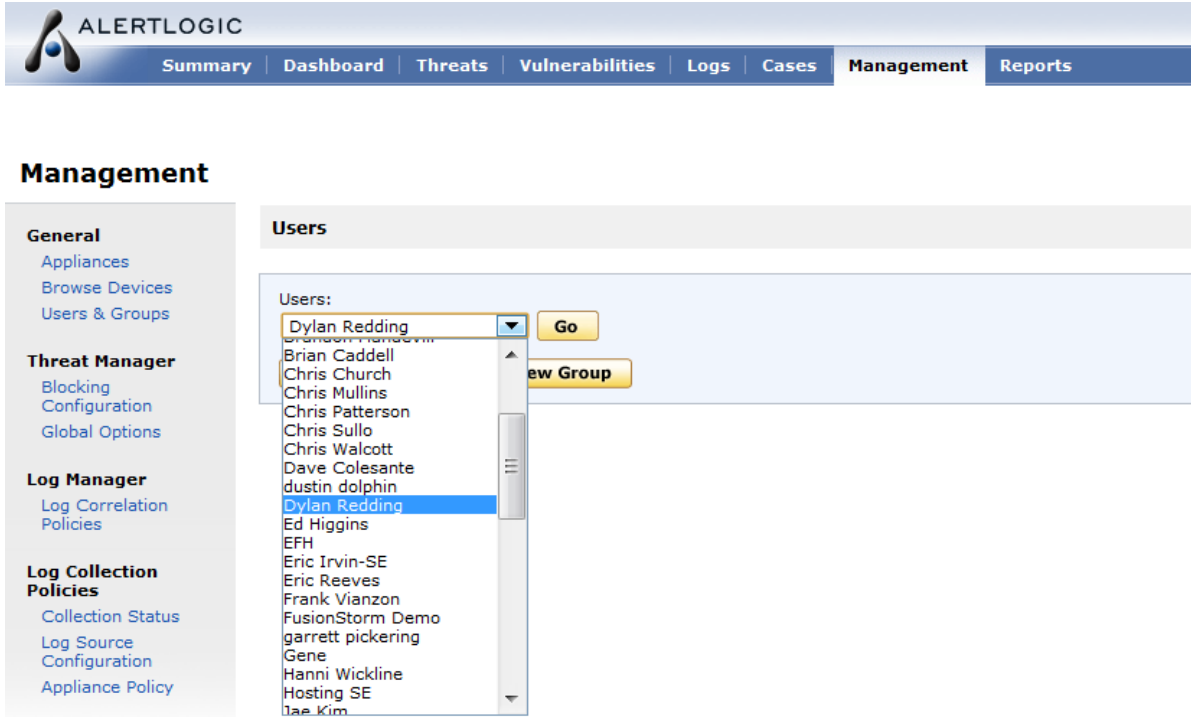
Showing: **1 - 25** of around 944 logs    View Type: **Message** | Field

	Date	Log Source	Message Type	Message
View	Apr 29 2011 11:44:50	al-demo-log-01	Juniper VPN Connection not Authenticated	Juniper: 2006-09-15 05:26:15 - ive - [10.29.50.77] System()[] - Connection from IP 10.29.50.77 not authenticated yet (URL=/dana-na/auth/welcome.cgi?p=timed-out)
View	Apr 29 2011 11:44:10	al-demo-log-01	Solaris SSH Remote Login Method Refused	sshd[11819]: [ID 800047 auth.info] Postponed <u>publickey</u> for <u>cchurch</u> from <u>192.168.0.1</u> port <u>4527</u> <u>ssh2</u>
View	Apr 29 2011 11:44:09	al-demo-log-01	Solaris SSH Remote Login Method Refused	sshd[18195]: [ID 800047 auth.info] Postponed <u>password</u> for <u>cchurch</u> from <u>192.168.0.1</u> port <u>1530</u> <u>ssh2</u>
View	Apr 29 2011 11:42:19	al-demo-log-01	Apache Authorization Header Error	apache2[26107]: [notice] [SOMETHING] Digest: missing user, realm, nonce, uri, digest, cnonce, or nonce_count in authorization header: <u>FAKE</u>
View	Apr 29 2011 11:42:18	al-demo-log-01	Apache Authorization Header Error	apache2[26107]: [notice] Digest: missing user, realm, nonce, uri, digest, cnonce, or nonce_count in authorization header: <u>FAKE</u>
View	Apr 29 2011 11:42:17	al-demo-log-01	Apache Authorization Header Error	apache2[26107]: [notice] [SOMETHING] Digest: invalid uri </someapp.php> in Authorization header

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.

## REPORT 4: Approved Access to Cardholder Data Logs



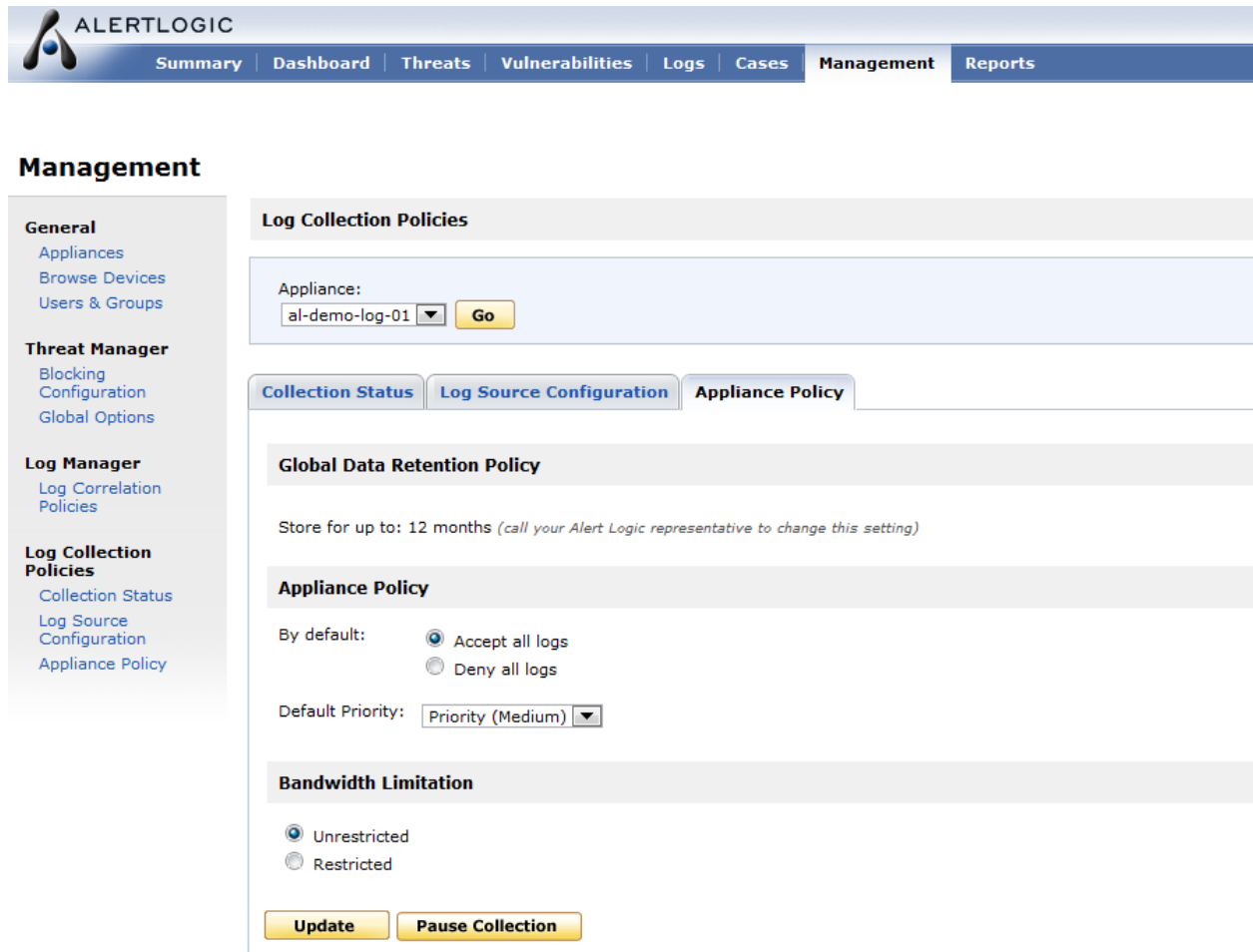
The screenshot shows the ALERTLOGIC Management interface. The top navigation bar includes Summary, Dashboard, Threats, Vulnerabilities, Logs, Cases, Management, and Reports. The Management section is active, and the Users list is displayed. The Users list includes the following entries:

User Name
Dylan Redding
Brian Caddell
Chris Church
Chris Mullins
Chris Patterson
Chris Sullo
Chris Walcott
Dave Colesante
dustin dolphin
Dylan Redding
Ed Higgins
EFH
Eric Irvin-SE
Eric Reeves
Frank Vianzon
FusionStorm Demo
garrett pickering
Gene
Hanni Wickline
Hosting SE
Jae Kim

Requirement 10.5 states that merchants must secure audit trails so they cannot be altered. This starts with verifying that only authorized individuals can view audit files (10.5.1). The report above shows exactly that information.

The Alert Logic solution enables customers to assign who should have access to the log information, and then provides a report to verify which individuals have access. This report should be reviewed on an ongoing basis to determine if an unauthorized user has been added to the log access list.

## REPORT 5: 12 Month Log Retention



The screenshot displays the Alert Logic Management interface. At the top, there is a navigation bar with the following tabs: Summary, Dashboard, Threats, Vulnerabilities, Logs, Cases, Management, and Reports. The 'Management' tab is currently selected.

On the left side, there is a sidebar menu with the following sections:

- General**
  - Appliances
  - Browse Devices
  - Users & Groups
- Threat Manager**
  - Blocking Configuration
  - Global Options
- Log Manager**
  - Log Correlation Policies
- Log Collection Policies**
  - Collection Status
  - Log Source Configuration
  - Appliance Policy

The main content area is titled 'Log Collection Policies' and features a dropdown menu for 'Appliance' set to 'al-demo-log-01' with a 'Go' button. Below this, there are three tabs: 'Collection Status', 'Log Source Configuration', and 'Appliance Policy', with the 'Appliance Policy' tab selected.

The 'Appliance Policy' section includes the following settings:

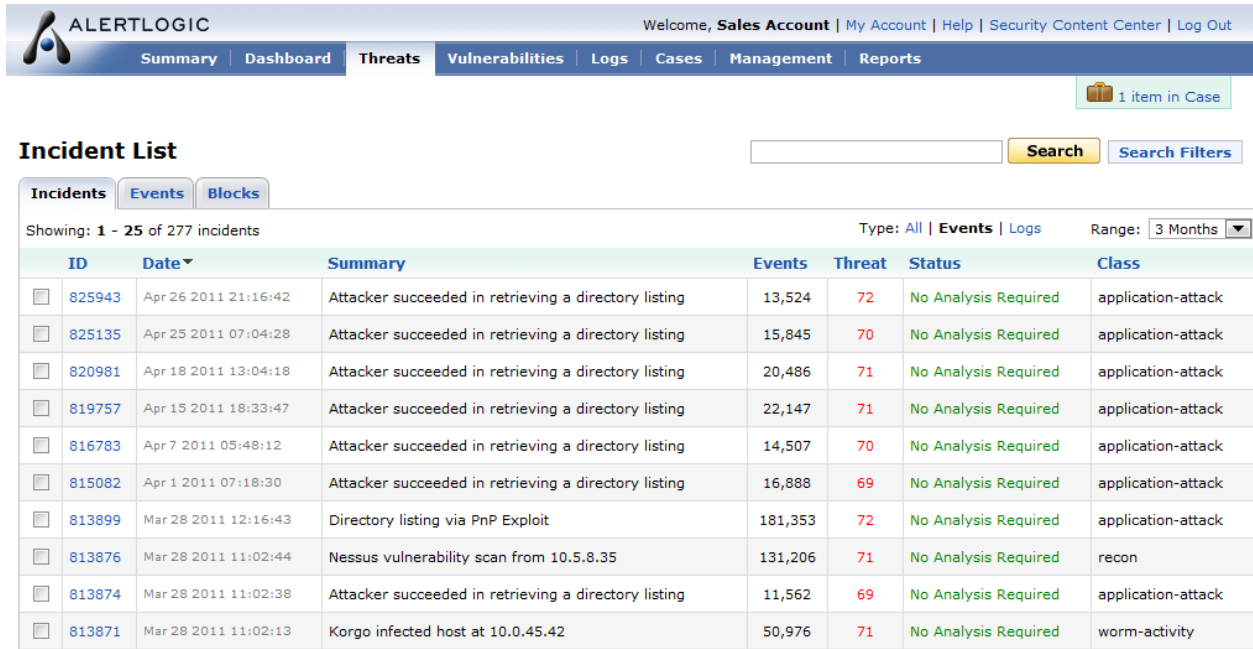
- Global Data Retention Policy:** Store for up to: 12 months *(call your Alert Logic representative to change this setting)*
- Appliance Policy:**
  - By default:  Accept all logs,  Deny all logs
  - Default Priority: Priority (Medium)
- Bandwidth Limitation:**  Unrestricted,  Restricted

At the bottom of the configuration area, there are two buttons: 'Update' and 'Pause Collection'.

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 log collection policies to ensure companies are staying in compliance with Requirement 10.7.

The Software-as-a-Service platform allows Alert Logic’s customers to not only store their logs in the Alert Logic data center for at least 12 months, but all customer logs are immediately available for analysis regardless of the size or age of the archived data. The user interface includes Google-like search capabilities, which enable customers to quickly find and report on all of their log data. subscription fee, and subscribers access their data seamlessly. In addition, customers have turned to Software-as-a-Service (SaaS) solutions to provide business-critical and security services because of the attractive pay-as-you-go model, dynamic scalability, and minimal installation or maintenance requirements.

## REPORT 6: Incident Report



ALERTLOGIC Welcome, Sales Account | My Account | Help | Security Content Center | Log Out

Summary Dashboard **Threats** Vulnerabilities Logs Cases Management Reports

1 item in Case

### Incident List

Showing: 1 - 25 of 277 incidents Type: All | Events | Logs Range: 3 Months

ID	Date	Summary	Events	Threat	Status	Class
825943	Apr 26 2011 21:16:42	Attacker succeeded in retrieving a directory listing	13,524	72	No Analysis Required	application-attack
825135	Apr 25 2011 07:04:28	Attacker succeeded in retrieving a directory listing	15,845	70	No Analysis Required	application-attack
820981	Apr 18 2011 13:04:18	Attacker succeeded in retrieving a directory listing	20,486	71	No Analysis Required	application-attack
819757	Apr 15 2011 18:33:47	Attacker succeeded in retrieving a directory listing	22,147	71	No Analysis Required	application-attack
816783	Apr 7 2011 05:48:12	Attacker succeeded in retrieving a directory listing	14,507	70	No Analysis Required	application-attack
815082	Apr 1 2011 07:18:30	Attacker succeeded in retrieving a directory listing	16,888	69	No Analysis Required	application-attack
813899	Mar 28 2011 12:16:43	Directory listing via PnP Exploit	181,353	72	No Analysis Required	application-attack
813876	Mar 28 2011 11:02:44	Nessus vulnerability scan from 10.5.8.35	131,206	71	No Analysis Required	recon
813874	Mar 28 2011 11:02:38	Attacker succeeded in retrieving a directory listing	11,562	69	No Analysis Required	application-attack
813871	Mar 28 2011 11:02:13	Korgo infected host at 10.0.45.42	50,976	71	No Analysis Required	worm-activity

Requirement 11.4 states that merchants must use an intrusion-detection system 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.

The Alert Logic Security Operations Center (SOC) staff 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 identify incidents and notify your personnel in 30 minutes or less. In addition to the rapid response, the Alert Logic security team will work with your security team to quickly resolve the issue.

## REPORT 7: Latest Patches Not Installed on Host Systems

### ✘ Configuration Management i

#### 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 i

Host	Criticality	Exposures	Risk Level
10.0.2.46	100	24 <span>+</span>	<span style="color: red;">██████████</span> Urgent
10.0.2.47	100	26 <span>+</span>	<span style="color: red;">██████████</span> Urgent
10.0.2.254	100	1 <span>+</span>	<span style="color: red;">██████████</span> Urgent

#### Needs Review:

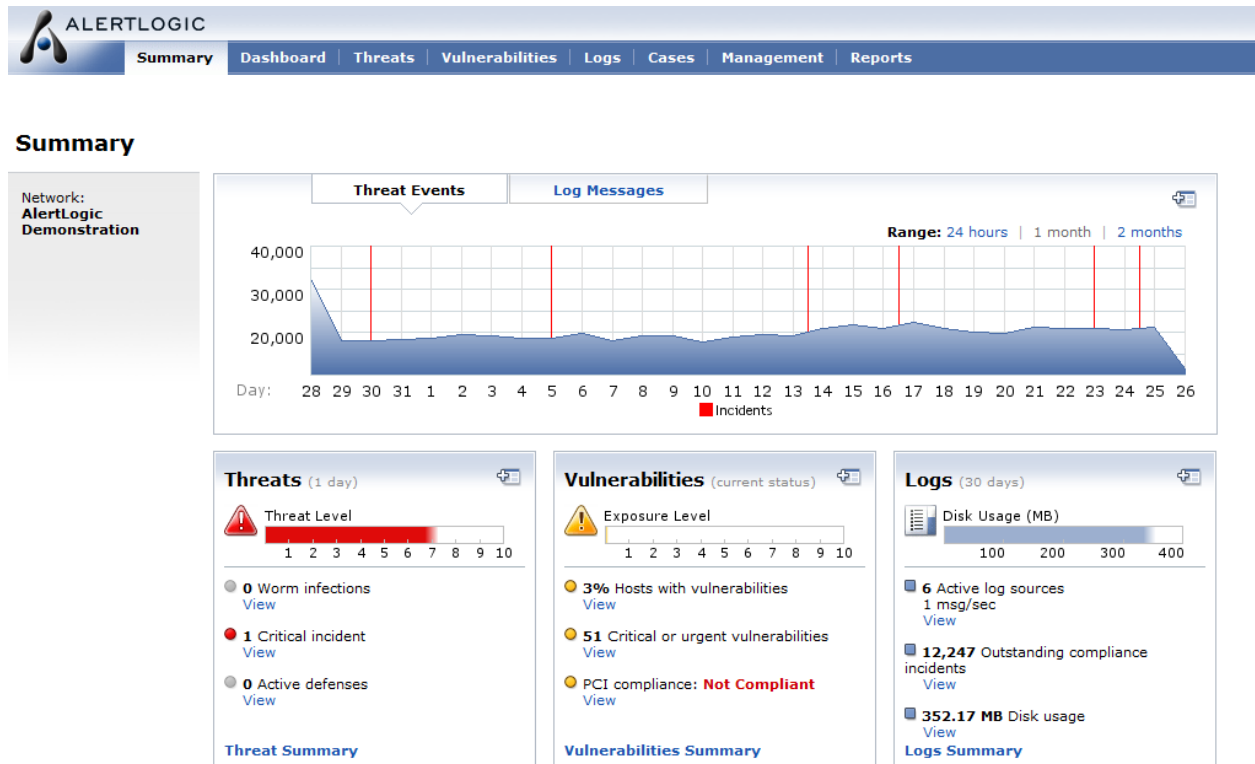
##### Hidden Vulnerabilities - Hosts i

Host	Criticality	Hidden Exposures	Risk Level
10.0.2.46	100	3 <span>+</span>	<span style="color: red;">██████████</span> Urgent
10.0.2.47	100	4 <span>+</span>	<span style="color: red;">██████████</span> Urgent

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 2010 states that 86% 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.

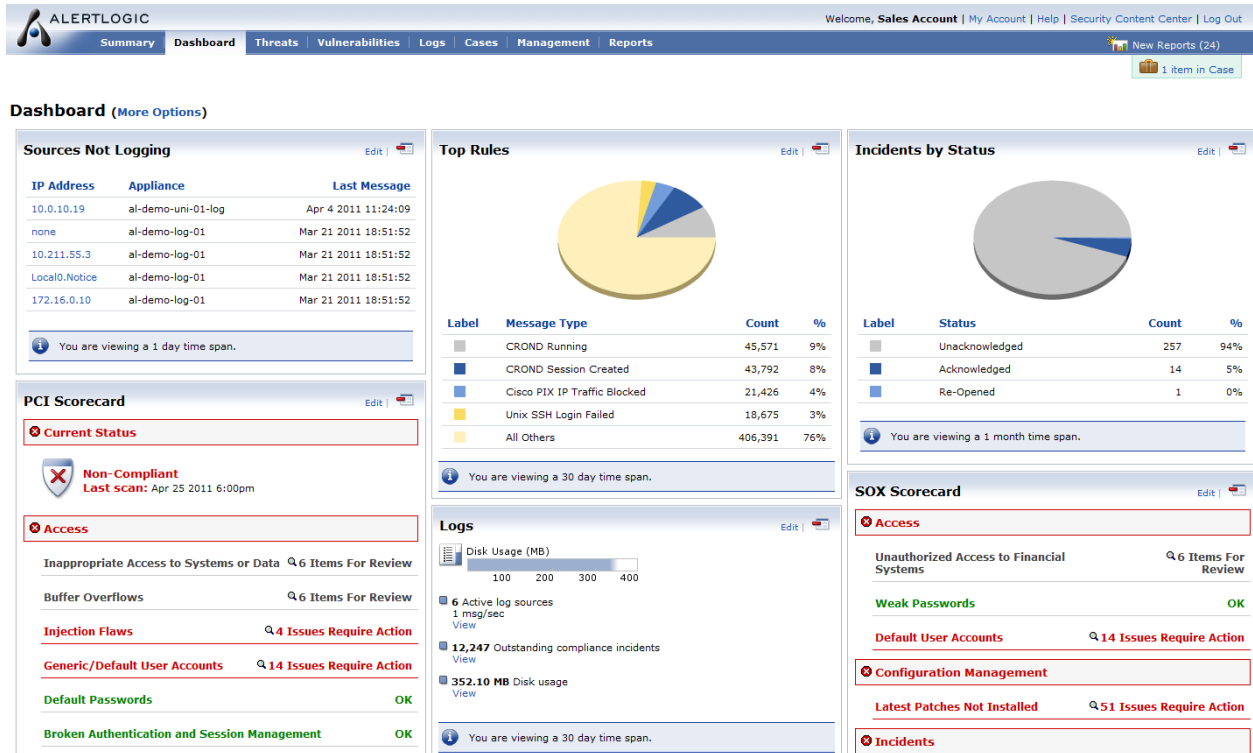
## REPORT 8: Vulnerability Dashboard



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.

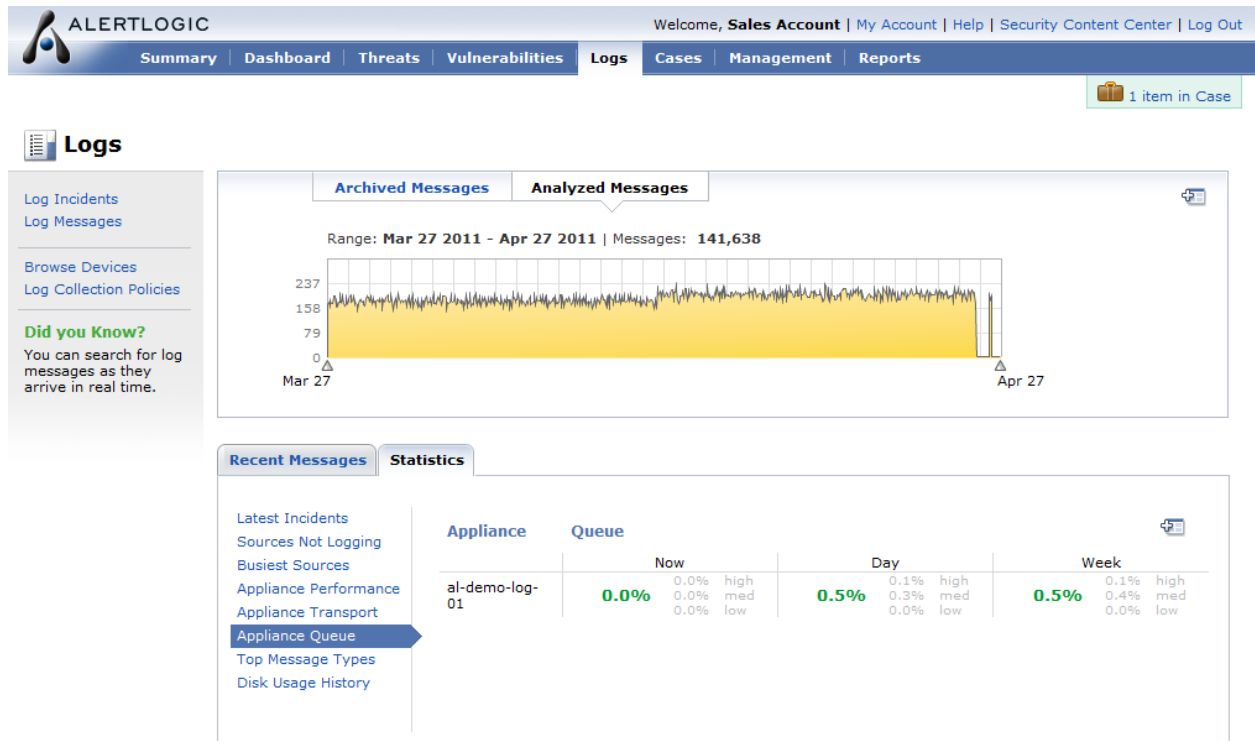
# REPORT 9: Log Review Dashboard



The most time consuming aspect of PCI DSS compliance is daily log review which is mandated by Requirement 10.6. Without an automated log management system many companies can spend over eight man hours a day reviewing log data.

Alert Logic’s Log Manager automates this daily task by providing easy to read dashboards, like the one above, which shows alerts triggered by log data. Administrators can quickly determine what areas need to be addressed immediately. The team reviewing this dashboard can see that unauthorized access is being granted, the latest patches are not installed, and that security incidents require attention. This dashboard also shows the current PCI compliance status based on the log data collected.

## REPORT 10: 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.

## Summary

---

IT compliance and security management is becoming more complicated and expensive every day. Alert Logic simplifies this by delivering an integrated solution consisting of Software-as-a-Service products and 24x7 Security Operations Monitoring services for intrusion detection, vulnerability assessment, and log management. These tightly coupled solutions enable customers to address the most costly and painful requirements of expanding compliance mandates while lowering costs and accelerating deployment.

Alert Logic's Threat Manager™ and Log Manager™ solutions utilize a combination of patented grid-based technology and cutting edge 7-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 nearly a decade of experience and over 1,200 satisfied customers, Alert Logic's solutions are proven to meet and radically simplify your compliance and security needs.