PCI DSS COMPLIANCE

STEP-BY-STEP PREPAREDNESS GUIDE

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements and industry best practices for preventing unauthorized access to cardholder data, including debit, credit, pre-paid, epurse, ATM, and point-of-sale (POS) card brands.

Complying with five of the PCI DSS requirements can be challenging because they require a combination of security tools, and threat management. This is where Alert Logic is uniquely positioned to help with a security platform, threat intelligence and experts:

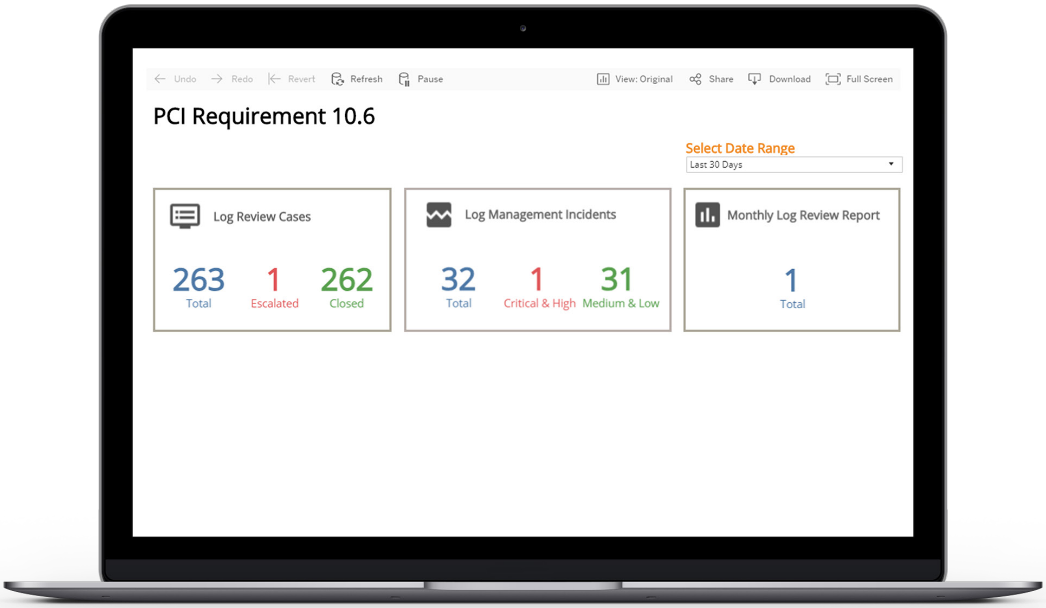
- Protect all systems against malware
- Develop and maintain secure systems and applications
- Track and monitor all access to network resources and cardholder data
- Run vulnerability scans at least quarterly, and after any significant change in your network
- Implement an Incident Response Plan

Alert Logic will help you capture the right data, minimize storage requirements, so you can address these most challenging PCI requirements, and trace activity to gain a deeper understanding of what happened when an event occurs.

To Learn more about the Alert Logic Console and Reports, visit the Alert Logic documentation page.

PCI AUDIT REPORTING:

Alert Logic provides pre-built PCI audit reports to meet your PCI security and compliance requirements.



PCI Requirement 10.6

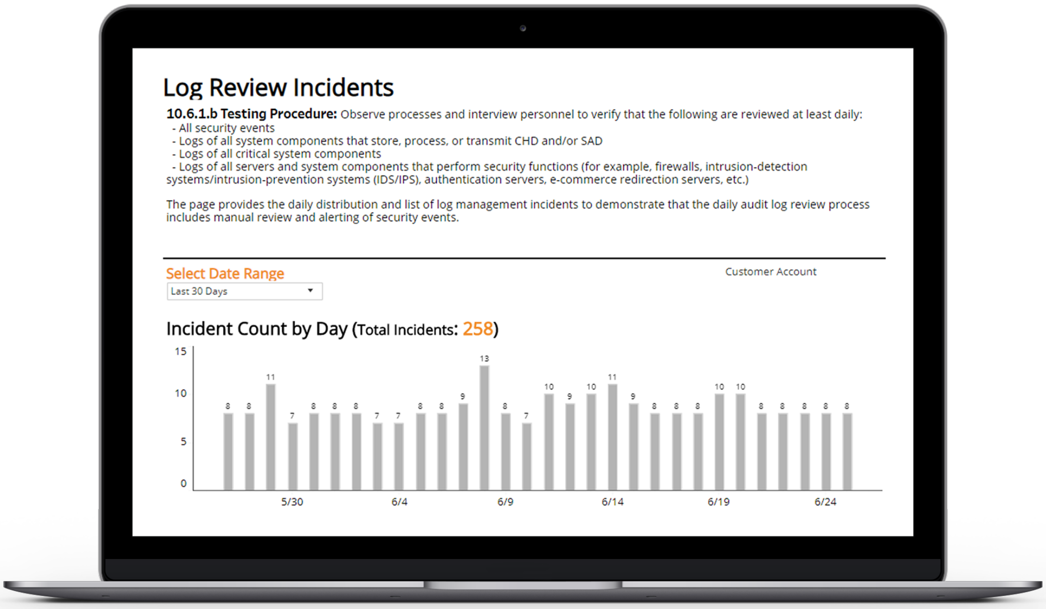
Select Date Range
Last 30 Days

Log Review Cases
263 Total
1 Escalated
262 Closed

Log Management Incidents
32 Total
1 Critical & High
31 Medium & Low

Monthly Log Review Report
1 Total

Alert Logic also provides saved views, and dashboards to meet many of your security and compliance requirements on day one. It's easy to correlate events and set automatic alerts and reporting to enable rapid response to security events.



Log Review Incidents

10.6.1.b Testing Procedure: 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.)

The page provides the daily distribution and list of log management incidents to demonstrate that the daily audit log review process includes manual review and alerting of security events.

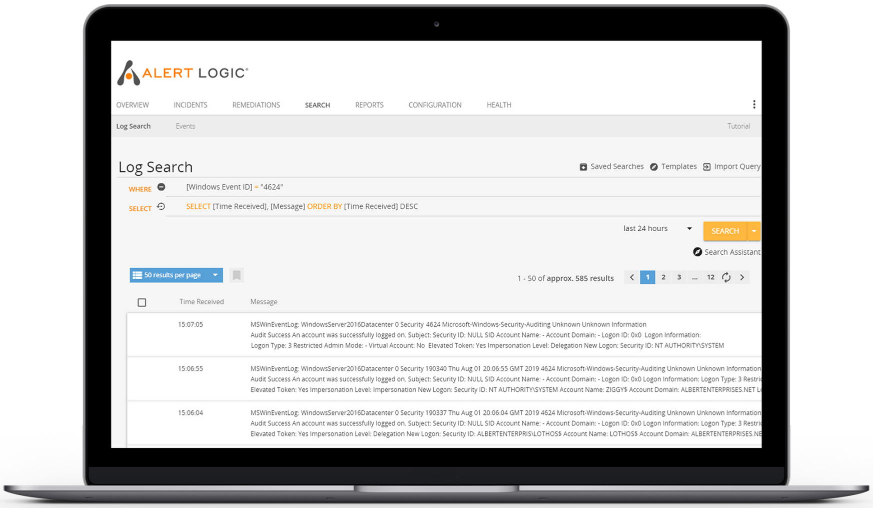
Select Date Range
Last 30 Days

Customer Account

Incident Count by Day (Total Incidents: 258)

LOG MANAGEMENT

- LOG MANAGEMENT USERS
- LOG MANAGEMENT DEPLOYMENT
- LOG MANAGEMENT TRAFFIC
- LOG RETENTION SETTINGS
- LOG SOURCES
- LOG SEARCH STATS
- LOCAL APPLIANCE ACCESS LOGS
- APPLIANCE & AGENT HEALTH
- NOTIFICATION POLICIES



Log Search

WHERE [Windows Event ID] = "4624"

SELECT SELECT [Time Received], [Message] ORDER BY [Time Received] DESC

last 24 hours

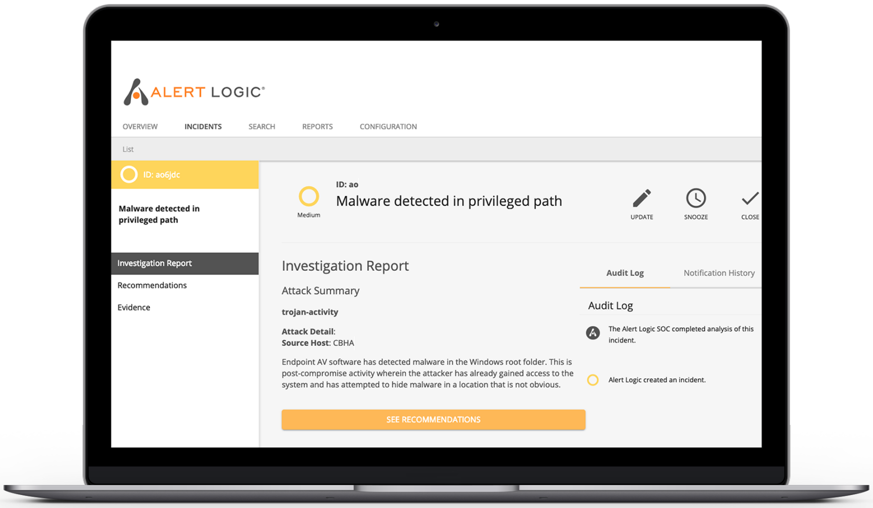
1 - 50 of approx. 585 results

```
Time Received   Message
15:07:05        MSWinEventLog: WindowsServer2016Datacenter 0 Security  4624 Microsoft-Windows-Security-Auditing Unknown Unknown Information
                Audit Success An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Information:
                Logon Type: 3 Restricted Admin Mode: - Virtual Account: No  Elevated Token: Yes Impersonation Level: Delegation New Logon: Security ID: NT AUTHORITY\SYSTEM
15:06:55        MSWinEventLog: WindowsServer2016Datacenter 0 Security 190340 Thu Aug 01 20:06:55 GMT 2019 4624 Microsoft-Windows-Security-Auditing Unknown Unknown Information
                Audit Success An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restric
                Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: NT AUTHORITY\SYSTEM Account Name: ZIGGY$ Account Domain: ALBERTENTERPRISES.NET L
15:06:04        MSWinEventLog: WindowsServer2016Datacenter 0 Security 190337 Thu Aug 01 20:06:04 GMT 2019 4624 Microsoft-Windows-Security-Auditing Unknown Unknown Information
                Audit Success An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restric
                Elevated Token: Yes Impersonation Level: Delegation New Logon: Security ID: ALBERTENTERPRIS\LOTHOS$ Account Name: LOTHOS$ Account Domain: ALBERTENTERPRISES.NE
```

Alert Logic collects, aggregates and normalizes log data whether it originates in your own data center, a hosted environment or the cloud. You get a unified view into all your data, with tools to rapidly uncover the insight and alerts you need to remain secure and compliant. Alert Logic provides hundreds of pre-built reports, saved views, and dashboards to meet many of your security and compliance requirements on day one. It's easy to correlate events and set automatic alerts and reporting to enable rapid response to security events

MALWARE PROTECTION

- AUTOMATICALLY GATHER NEW MALWARE AND GOODWARE SAMPLES
- CONTINUOUSLY TRAIN PROTECTION MODELS AGAINST NEW SECURITY THREATS
- TAILOR PROTECTION MODELS BASED ON ORGANIZATION PROFILE
- MAXIMIZE PROTECTION AND MINIMIZE FALSE POSITIVES



ID: ao6jdc

Malware detected in privileged path

Medium

ID: ao

Malware detected in privileged path

Investigation Report

Attack Summary

trojan-activity

Attack Detail:
Source Host: CBHA

Endpoint AV software has detected malware in the Windows root folder. This is post-compromise activity wherein the attacker has already gained access to the system and has attempted to hide malware in a location that is not obvious.

Audit Log

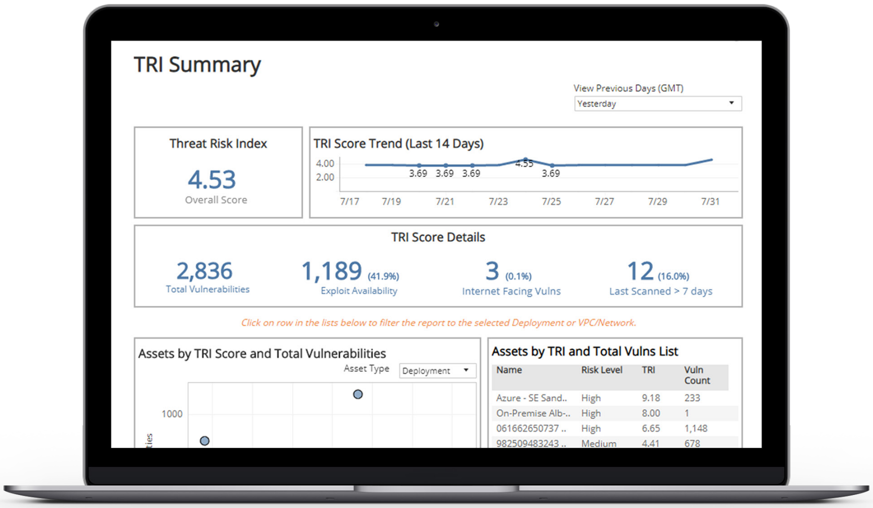
The Alert Logic SOC completed analysis of this incident.

Alert Logic created an incident.

The Alert Logic Console – Event Viewer will display the latest malware attempts to help you meet PCI requirement to protect against malware attacks.

VULNERABILITY MANAGEMENT

- INTERNAL SCAN SCHEDULE
- INTERNAL SCAN RESULTS
- PCI ASV SCAN SCHEDULE
- PCI ASV SCAN RESULTS
- NEW VULNERABILITY CHECKS
- CIS BENCHMARK SCAN RESULTS
- CONFIGURATION REMEDIATIONS
- SECURITY REMEDIATIONS
- TRI SCORES



TRI Summary

View Previous Days (GMT): Yesterday

Threat Risk Index: 4.53 Overall Score

TRI Score Details

2,836 Total Vulnerabilities

1,189 (41.9%) Exploit Availability

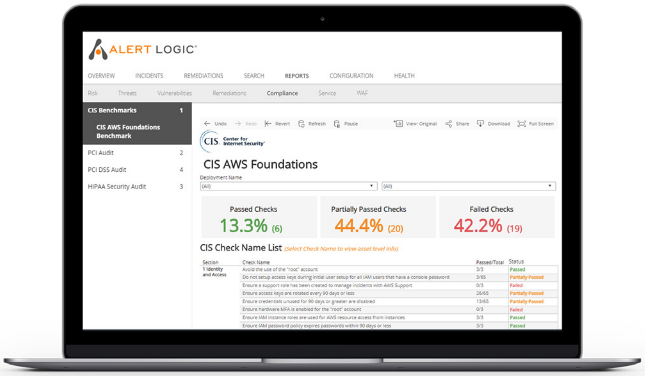
3 (0.1%) Internet Facing Vulns

12 (16.0%) Last Scanned > 7 days

Click on row in the lists below to filter the report to the selected Deployment or VPC/Network.

Assets by TRI and Total Vulns List

Name	Risk Level	TRI	Vuln Count
Azure - SE Sand..	High	9.18	233
On-Premise Alb-..	High	8.00	1
061662650737 ..	High	6.65	1,148
982509483243 ..	Medium	4.41	678



CIS AWS Foundations

Deployment Name: (All) (All)

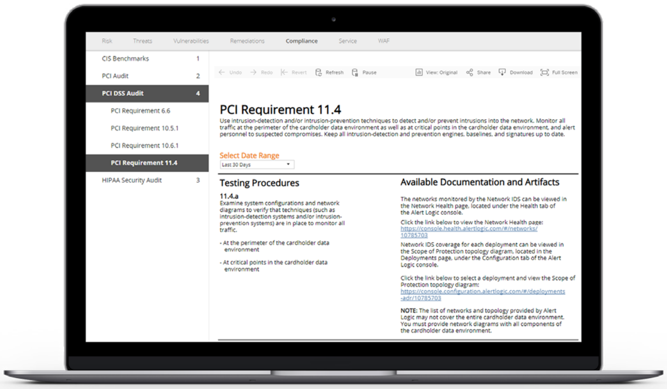
Passed Checks 13.3% (6)

Partially Passed Checks 44.4% (20)

Failed Checks 42.2% (19)

CIS Check Name List *(Select Check Name to view asset level info)*

Section	Check Name	Passed/Total	Status
1 Identity and Access	Avoid the use of the "root" account	3/3	Passed
	Do not setup access keys during initial user setup for all IAM users that have a console password	3/65	Partially Passed
	Ensure a support role has been created to manage incidents with AWS Support	0/3	Failed
	Ensure access keys are rotated every 90 days or less	26/65	Partially Passed
	Ensure credentials unused for 90 days or greater are disabled	13/65	Partially Passed
	Ensure hardware MFA is enabled for the "root" account	0/3	Failed
	Ensure IAM instance roles are used for AWS resource access from instances	3/3	Passed
	Ensure IAM password policy expires passwords within 90 days or less	3/3	Passed



PCI Requirement 11.4

Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.

Select Date Range: Last 30 Days

Testing Procedures

11.4.a

Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic.

- At the perimeter of the cardholder data environment
- At critical points in the cardholder data environment

Available Documentation and Artifacts

The networks monitored by the Network IDS can be viewed in the Network Health page, located under the Health tab of the Alert Logic console.

Click the link below to view the Network Health page: https://console.health.alertlogic.com/#/networks/10785703

Network IDS coverage for each deployment can be viewed in the Scope of Protection topology diagram, located in the Deployments page, under the Configuration tab of the Alert Logic console.

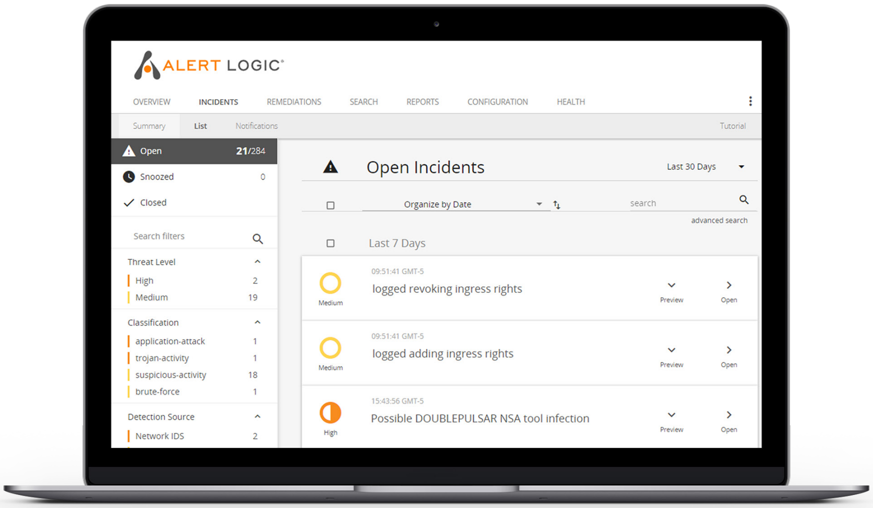
Click the link below to select a deployment and view the Scope of Protection topology diagram: https://console.configuration.alertlogic.com/#/deployments-adr/10785703

NOTE: The list of networks and topology provided by Alert Logic may not cover the entire cardholder data environment. You must provide network diagrams with all components of the cardholder data environment.

Alert Logic is an approved PCI Scanning vendor. Through the Alert Logic console, you can schedule quarterly external scans that are required for PCI compliance.

THREAT DETECTION

- NETWORK IDS DEPLOYMENT
- PROTECTED NETWORKS & HOSTS
- NETWORK IDS TRAFFIC
- NETWORK IDS EVENTS
- NETWORK IDS INCIDENTS
- DEPLOYED IDS SIGNATURES
- SIGNATURE UPDATE HISTORY
- LOG REVIEW INCIDENTS
- LOG MANAGEMENT INCIDENTS
- LOG CORRELATION POLICIES
- WEB APPLICATION IDS INCIDENTS
- APPLIANCE & AGENT HEALTH
- NOTIFICATION POLICIES



Open	21/284
Snoozed	0
Closed	
Threat Level	
High	2
Medium	19
Classification	
application-attack	1
trojan-activity	1
suspicious-activity	18
brute-force	1
Detection Source	
Network IDS	2

Open Incidents

Last 7 Days

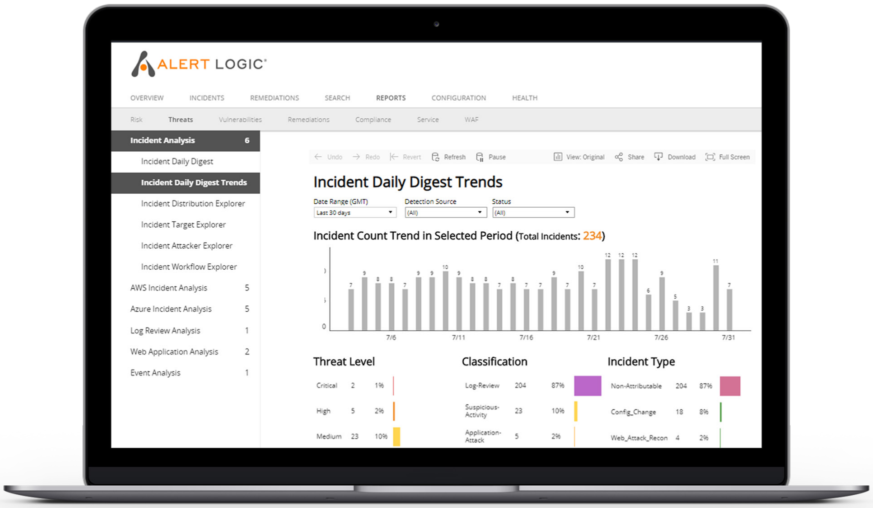
○ Medium	09:51:41 GMT-5	logged revoking ingress rights
○ Medium	09:51:41 GMT-5	logged adding ingress rights
◐ High	15:43:56 GMT-5	Possible DOUBLEPULSAR NSA tool infection

Alert Logic uses colors and icons to help you easily identify the threat levels of exposures.

● High ● Medium ○ Low ℹ Info

THREAT RESPONSE

- CURRENT ESCALATION CONTACTS
- INCIDENT NOTIFICATION CONTACTS
- ESCALATED INCIDENTS
- INCIDENT WORKFLOW ACTIONS
- MONTHLY LOG REVIEW
- WAF BLOCKING
- ALERT PREFERENCES



Incident Analysis	6
Incident Daily Digest	
Incident Daily Digest Trends	
Incident Distribution Explorer	
Incident Target Explorer	
Incident Attacker Explorer	
Incident Workflow Explorer	
AWS Incident Analysis	5
Azure Incident Analysis	5
Log Review Analysis	1
Web Application Analysis	2
Event Analysis	1

Incident Daily Digest Trends

Date Range (GMT): Last 30 days · Detection Source: (All) · Status: (All)

Incident Count Trend in Selected Period (Total Incidents: 234)

Threat Level

Critical	2	1%
High	5	2%
Medium	23	10%

Classification

Log-Review	204	87%
Suspicious-Activity	23	10%
Application-Attack	5	2%

Incident Type

Non-Attributable	204	87%
Config_Change	18	8%
Web_Attack_Recon	4	2%

Alert Logic provides you with information about the exposure, including threat level, evidence, and recommendations to address the exposure.

DETAILED SOLUTION MAPPING FOR PCI COMPLIANCE

PCI	ALERT LOGIC MDR ESSENTIALS	ALERT LOGIC MDR PROFESSIONAL	ALERT LOGIC MDR ENTERPRISE
6.1 (a)(1)(i)(A) - Identify newly discovered security vulnerabilities	●	●	●
6.6 (a)(1)(ii)(B) - Address new threats and vulnerabilities on an on-going basis and ensure these applications are protected against known attacks			●
10.1 (a)(1)(ii)(D) - Implement audit trails to link all access to system components to each individual user		●	●
10.2 (a)(1)(ii)(D) - Automated audit trails		●	●
10.3 (a)(1)(ii)(D) - Caputre audit trails		●	●
10.5 (a)(1)(ii)(D) - Secure logs		●	●
10.5.5 - Change detection to ensure integrity for log files		●	●
10.6 (a)(1)(ii)(D) - Review logs at least daily		●	●
10.7 (a)(1)(ii)(D) - Maintain logs online for three months		●	●
10.8.1 (a)(1)(ii)(D) - Retain audit trails for at least one year		●	●
11.2 (a)(1)(ii)(D) - Perform network vulnerability scans by an ASV at least quarterly or after any significant network change (Includes 11.2.1, 11.2.2, 11.2.3)	●	●	●
11.4 (a)(1)(ii)(D) - Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the networks		●	●
11.5 - Change detection to ensure integrity for critical system files, configuration files, or content files		●	●
12.10.1 (a)(1)(ii)(D) - Implement an incident response plan. Be prepared to respond immediately to a system breach		●	●

Using these capabilities, Alert Logic helps you to address the most challenging PCI DSS compliance requirements, so you get better outcomes across your entire compliance program.

SAVE MONEY

- Single Integrated Solution.
- Suite of Security Capabilities.
- One Monthly Subscription.

STAFFING RELIEF

- Our Experts are Included.
- 24/7 Threat Monitoring.
- 15-Min Live Notifications

START FAST

- Ready-to-Use Services.
- Expert Onboarding Assistance.
- Personal Tuning & Training.

LET'S GET STARTED

SCHEDULE A DEMO | TRY IT NOW | CONTACT SALES

CONNECT WITH YOUR ACCOUNT MANAGER TODAY TO LEARN MORE