Vulnerability Scan Report: Attestation of Compliance

Scan Customer Information			Approved Scanning Vendor Information		
Company Name:	TriMark Engineering		**Company Name:**	Trustwave Holdings, Inc.	
Contact:	Marshall Dudley	**Title:**	**Contact:**	Trustwave Support	**URL:** www.trustwave.com
Telephone:	8656358136	**E-mail:** mdudley@king-cart.com	**Telephone:**	1-800-363-1621	**E-mail:** support@trustwave.com
Business Address:	110 Merlot Court		**Business Address:**	70 West Madison St., Ste 1050	
City:	loudon	**State/Province:** Tennessee	**City:**	Chicago	**State/Province:** IL
ZIP/Postal Code:	37774	**Country:** US	**ZIP/Postal Code:**	60602	**Country:** US

Scan Status

Pass	Scan Compliance Status
1	Number of unique components scanned that are in scope
0	Number of identified failing vulnerabilities
0	Number of components scanned by TrustKeeper but confirmed by the customer not to be in scope
2017-04-17	Date Scan Completed
2017-07-17	Scan Expiration Date (3 months from Date Scan Completed)

Scan Customer Attestation	Approved Scanning Vendor Attestation
TriMark Engineering attests that: This scan includes all components which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. TriMark Engineering also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of the PCI DSS; This scan does not represent TriMark Engineerings overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.	This scan and report were prepared and conducted by Trustwave under certificate number 3702-01-11 (2016), 3702-01-10 (2015), 3702-01-09 (2014), 3702-01-08 (2013), 3702-01-07 (2012), 3702-01-06 (2011), 3702-01-05 (2010), according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide.

Trustwave attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active interference. This report and any exceptions were reviewed by the Trustwave Quality Assurance Process. |

_____   _____
Signature   Printed Name

_____   _____
Title   Date

Vulnerability Scan Report: Table of Contents

Vulnerability Scan Report: Executive Summary

Part 1. Scan Information

Scan Customer Company	TriMark Engineering
ASV Company	Trustwave Holdings, Inc.
Scan Compliance Status	Pass
Date Scan Completed	2017-04-17
Scan Expiration Date	2017-07-17

Vulnerability Counts by Severity

Legend:
- 2017-03-08 16:03
- 2017-04-08 17:07
- 2017-04-17 13:14
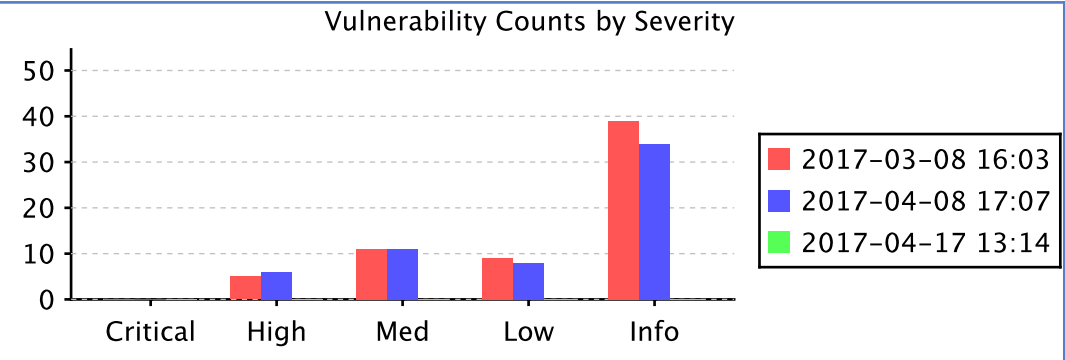
Part 2. Component Compliance Summary

#	Compliance Status	Name	Type	IP Address	Source	Critical	High	Medium	Low	Info
1	Pass	www.king-cart.com	Web Site		Domain Name	The location passed because it is hidden from our scanners*				
					Total Findings	0	0	0	0	0
					Total PCI Vulnerabilities	0	0	0	0	0

* Note: This target did not respond to probes from the TrustKeeper scanners. For some targets, such as firewalls, this is good, since the target is protected and hidden from the Internet. For websites, it could mean the web site is not available, or the domain name is misspelled. It is also possible that these targets are internal IP addresses that cannot be tested by Trustwave's Internet scanners.

Part 3a. Vulnerabilities Noted for Each IP Address

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability

Vulnerability Scan Report: Executive Summary

No vulnerabilities were discovered during the scan.

Part 3b. Special Notes by IP Address

#	IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
			No Special Notes		

Vulnerability Scan Report: Vulnerability Details

Part 1. Scan Information

Scan Customer Company	TriMark Engineering	Date Scan Completed	2017-04-17
ASV Company	Trustwave Holdings, Inc.	Scan Expiration Date	2017-07-17

Part 2. Scan Inventory (Accessible Systems and Services)

The following systems and network services were detected during this scan. This information is provided for your information. Please refer to "Part 4. Vulnerabilities & Policy Violations" for all PCI compliance-related issues.

Reading Your Scan Inventory

The vulnerability scan reveals Internet-accessible computers and network services available on your network. The following systems (e.g., computers, servers, routers, etc.) and network services (e.g., Web and mail servers) were discovered during the vulnerability scan. As a general rule, all unnecessary network services should be disabled, and all other services should be protected by a firewall or similar device. Only those services which must be available to the public should be visible from the Internet.

- *Names* - A system may be known by many names. For example, a server that offers Web and mail services may be known as both www.mycompany.com and mail.mycompany.com. This report includes as many names as could be identified, including public domain names, Windows domain/workgroups, Windows name, and the "real" name assigned in your DNS server.

- *Ping* - One technique TrustKeeper uses is to try to "ping" systems in your network. It is generally considered to be good practice to block inbound pings as it can give attackers information about your network. However, this decision may be affected by network monitoring needs and other considerations.

- *Service Information* - A large number of services (e.g., TCP and UDP ports) are probed during the scan. Any that appear to be active on the device are listed in the table. You should review this list to ensure that only those services you intend to offer to the public are accessible. All other internal services should be protected by your firewall or similar device.

#	Device	Names	OS	Ping	Service Information			
					Port	Protocol	Application	Detail
No Systems or Network Services were detected by Trustkeeper scanners								

Vulnerability Scan Report: Vulnerability Details

Part 3a. Previous Scan Targets (Not Scanned)

The following locations were removed from your scan setup at your request and have not been included in this scan. You confirmed that these locations or domain names do not store, process, or transmit cardholder data and therefore not required to be scanned for PCI DSS compliance.

#	Name	Type	IP Address	Date Removed
No such scan locations have been removed by this customer.				

Part 3b. Discovered Scan Targets (Not Scanned)

The following systems were discovered to be related to your network during this scan. TrustKeeper only scans those systems which are explicitly identified by you; however, the following systems were identified using reconnaissance techniques based on the information you provided. While not scanned for this assessment, you should be aware that an attacker could identify the same information.

Please review this information and update your TrustKeeper Scan Setup if any of the following systems are relevant to the assessment being performed. In many cases, some of these systems will not be relevant to the assessment. Common examples include domain name servers (DNS) and mail servers maintained by your ISP. The scanner may also identify internal systems that are not directly accessible from the Internet.

#	IP Address	Domain Name	Comments
No related scan targets were discovered.			

Part 3c. Load Balancers

If you are using load balancers in your network to spread traffic across multiple servers, **it is your responsibility** to ensure that the configuration of the environment behind your load balancers is synchronized, or to ensure that the environment is scanned as part of the internal vulnerability scans required by PCI DSS.

Vulnerability Scan Report: Vulnerability Details

Part 4. Vulnerability & Policy Violations

The following issues were identified during this scan. Please review all items and address all that items that affect compliance or the security of your system.

In the tables below you can find the following information about each TrustKeeper finding.

- *CVE Number* - The Common Vulnerabilities and Exposure number(s) for the detected vulnerability - an industry standard for cataloging vulnerabilities. A comprehensive list of CVEs can be found at nvd.nist.gov or cve.mitre.org.

- *Vulnerability* - This describes the name of the finding, which usually includes the name of the application or operating system that is vulnerable.

- *CVSS Score* - The Common Vulnerability Scoring System is an open framework for communicating the characteristics and impacts of IT vulnerabilities. Further information can be found at www.first.org/cvss or nvd.nist.gov/cvss.cfm.

- *Severity* - This identifies the risk of the vulnerability. It is closely associated with the CVSS score.

- *Compliance Status* - Findings that are PCI compliance violations are indicated with a Fail status. In order to pass a vulnerability scan, these findings must be addressed. Most findings with a CVSS score of 4 or more, or a Severity of Medium or higher, will have a Fail status. Some exceptions exist, such as DoS vulnerabilities, which are not included in PCI compliance.

- *Details* - TrustKeeper provides the port on which the vulnerability is detected, details about the vulnerability, links to available patches and other specific guidance on actions you can take to address each vulnerability.

For more information on how to read this section and the scoring methodology used, please refer to the appendix.

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
No vulnerabilities were discovered during the scan.						

Vulnerability Scan Report: Vulnerability Details

Part 5a. Web Servers

It is important to pay special attention to the security of your Web servers. This section provides a convenient list of all of the Web servers found in the course of the network scan based on the locations you specified in your scan setup. Information profiled includes the server type (e.g., Microsoft IIS or Apache) and the title of the default Web page. Some tips for using this information are below.

- You should ensure that all Web servers listed in this section are authorized and intended to be running in your network since many systems will inadvertently be configured with some type of Web server when they are installed.
- In addition, many network devices (e.g., routers, switches and print servers) may have Web-based management interfaces of which you may not have been aware. Whenever possible, unused Web interfaces should be disabled or, at a minimum, password protected.
- Review the "Port" column and make sure that any sites that should be secure are using port 443 (HTTPS, or "Secure Web") to encrypt the web sessions.

Special Note: If you are using load balancers for your web sites to spread the web traffic across multiple servers, it is your responsibility to ensure that the configuration of the environment behind your load balancers is synchronized, or to ensure that the environment is scanned as part of the internal vulnerability scans required by PCI DSS.

#	System IP Address	Domain Name	Port	Server Type	Default Status and Title/Redirect
No web servers were discovered during the scan.					

Part 5b. SSL Certificate Information

Several network services, most notably HTTPS ("Secure Web"), employ certificates which contain information about the service which can be used by connecting clients to authenticate the identity of the server. For Web servers, the certificate is intended to authenticate the domain name (e.g., www.yoursite.com) of a web site. For example, a home banking application should be run on a web server which provides a certificate to its clients' Web browsers proving that the web server they are connected to is actually the one they intended to use.

In order to provide users with confidence in the site they are visiting, the certificate should be issued by a well-known certificate authority instead of self-generated. In some cases, such as in a private network, self-generated certificates may be used; however, those users should have confidence in the internal issuing authority.

This table provides a summary of the certificates found in your network, including expiration date and issuer of each certificate.

#	Service	Common Name	Expires	Details
No SSL certificate information was discovered during the scan.				

Vulnerability Scan Report: Vulnerability Details

Part 6. Disputed Vulnerability & Policy Violations

The following vulnerabilities and policy violations were successfully disputed by you and have been removed from the scoring of your report. These items no longer affect any compliance assessment that this report may support. All disputes listed here were approved based on information which you have provided and represented and warranted to be complete and accurate.

#	Severity	IP Address & Port	Expires	Detail
No disputes found that have been removed from the scoring of this report.				

ASV Feedback Form

This form is used to review ASVs and their work product, and is intended to be completed after a PCI Scanning Service by the ASV client. While the primary audience of this form are ASV scanning clients (merchants or service providers), there are several questions at the end, under "ASV Feedback Form for Payment Brands and Others," to be completed as needed by Payment Brand participants, banks, and other relevant parties. This form can be obtained directly from the ASV during the PCI Scanning Service, or can be found online in a usable format at https://www.pcisecuritystandards.org. Please send this completed form to PCI SSC at: asv@pcisecuritystandards.org.

ASV FEEDBACK FORM	
Client Name (merchant or service provider):	**Approved Scanning Vendor Company (ASV):**
Name	Name
Contact	Contact
Telephone	Telephone
E-Mail	E-Mail
Business location where assessment took place:	**ASV employee who performed assessment:**
Street	Name
City	Telephone
State/Zip	E-Mail
For each question, please indicate the response that best reflects your experience and provide comments. **4 = Strongly Agree 3 = Agree 2 = Disagree 1 = Strongly Disagree**	
1) During the initial engagement, did the ASV explain the objectives, timing, and review process, and address your questions and concerns?	
Response:	
Comments:	

2) Did the ASV employee(s) understand your business and technical environment, and the payment card industry?
Response:
Comments:
3) Did the ASV employee(s) have sufficient security and technical skills to effectively perform this PCI Scanning Service?
Response:
Comments:
4) Did the ASV sufficiently understand the PCI Data Security Standard and the PCI Security Scanning Procedures?
Response:
Comments:
5) Did the ASV effectively minimize interruptions to operations and schedules?
Response:
Comments:
6) Did the ASV provide an accurate estimate for time and resources needed?
Response:
Comments:
7) Did the ASV provide an accurate estimate for scan report delivery?
Response:
Comments:

8)   Did the ASV attempt to market products or services for your company to attain PCI compliance?
Response:
Comments:
9)   Did the ASV imply that use of a specific brand of commercial product or service was necessary to achieve compliance?
Response:
Comments:
10)   In situations where remediation was required, did the ASV present product and/or solution options that were not exclusive to their own product set?
Response:
Comments:
11)   Did the ASV use secure transmission to send any confidential reports or data?
Response:
Comments:
12)   Did the ASV demonstrate courtesy, professionalism, and a constructive and positive approach?
Response:
Comments:
13)   Was there sufficient opportunity for you to provide explanations and responses during the scans?
Response:
Comments:

14)   During the review wrap-up, did the ASV clearly communicate findings and expected next steps?
Response:
Comments:
15)   Did the ASV provide sufficient follow-up to address false positives until eventual scan compliance was achieved?
Response:
Comments:
Please provide any additional comments here about the ASV, your PCI Scanning Service, or the PCI documents.

ASV FEEDBACK FORM FOR PAYMENT BRANDS AND OTHERS	
Name of ASV Client (merchant or service provider reviewed):	**ASV Company Name:**
Payment Brand Reviewer:	ASV employee who performed assessment:
Name	Name
Telephone	Telephone
E-Mail	E-Mail

For each question, please indicate the response that best reflects your experience and provide comments.

4 = Strongly Agree   3 = Agree   2 = Disagree   1 = Strongly Disagree

1)   Does the ASV clearly understand how to notify your payment brand about compliance and non-compliance issues, and the status of merchants and service providers?

Response:

Comments:

2)   Did you receive any complaints about ASV activities related to this scan?

Response:

Comments:

3)   Did the ASV demonstrate sufficient understanding of the PCI Data Security Standard and the PCI Security Scanning Procedures?

Response:

Comments: