WHITE PAPER

TREND MICRO™

TIPPINGPOINT™ THREAT PROTECTION SYSTEM VERSION 5.1.1

LYLE MILLER | CISA, CISSP, QSA, PA-QSA

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Trend Micro engaged Coalfire Systems Inc. (Coalfire), a respected Payment Card Industry (PCI) Payment Application–Qualified Security Assessor (PA-QSA) company, to conduct an independent technical assessment of Trend Micro TippingPoint Threat Protection System version 5.1.1 (hereinafter referred to as TippingPoint TPS). Coalfire conducted assessment activities including technical testing, architectural assessment, and compliance assessment.

In this paper, Coalfire will describe that TippingPoint TPS can increase the security posture of an organization employing the technology when implemented, according to guidance provided by Trend Micro. This paper will also describe how deployment of TippingPoint TPS can assist customers in meeting certain requirements of the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS requirements that may be met by the inclusion of TippingPoint TPS are outlined in Appendix A.

ABOUT TREND MICRO

Trend Micro is a global leader in the cybersecurity space. The company develops internet content security and threat management solutions for businesses and consumers to safely exchange digital information.

ABOUT TIPPINGPOINT TPS

TippingPoint TPS is a network-level real-time threat detection and protection solution scalable to an organization's specific needs. The solution operates in-line--at the network level at the perimeter and other critical points within the customer's environment. TippingPoint TPS identifies threats based on digital vaccines (signatures) provided by Trend Micro and can be customized by the customer to perform various actions against detected threats including permit, block, quarantine, and notify (email, etc.). By default, TippingPoint TPS checks for updated digital vaccines (signatures) at 30-minute intervals, maintaining signatures current for proactive threat protection. TippingPoint TPS then mitigates these threats as they are identified within the environment. TippingPoint TPS functions as an appliance and runs on Trend Micro's proprietary TippingPoint 8200 TX or 8400TX security devices. Customers choose the specific devices based on the specific size, needs, and complexity of their environment.

TippingPoint TPS protects against various cyber threats such as malware, ransomware, fileless malware, zero-day exploits, advanced persistent threats (APTs), and other advanced techniques applicable to the Microsoft® Windows® operating system. TippingPoint TPS also acts as a web application firewall by preventing threats to the web application (also at the network layer).

Following implementation guidance provided by Trend Micro, TippingPoint TPS can assist customers in their PCI DSS compliance efforts as well as the overall security of their environment.

AUDIENCE

This assessment white paper has three target audiences:

1. **Merchants and Service Providers:** This audience is evaluating TippingPoint TPS for deployment in their cardholder data environment (CDE) or other customer environment.
2. **Administrators and Other Compliance Professionals:** This audience may be evaluating TippingPoint TPS for use within their organization for PCI DSS and other compliance requirements.
3. **QSA and Internal Audit Community:** This audience may be evaluating TippingPoint TPS for deployment into their environment and the increased cybersecurity benefits this solution can offer.

PCI DSS COMPLIANCE

The PCI DSS is a set of industry requirements which are in place to help protect payment card information. The PCI Security Standards Council (SSC) was established by the major credit card brands (American Express®, Discover®, JCB®, MasterCard®, and Visa®) to drive this effort. The standard is based on the security programs of the card brands along with industry best practices for security.

OBJECTIVES	REQUIREMENTS
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

The PCI DSS standards apply to all organizations that store, process, or transmit Cardholder data (CHD). All affected organizations must be PCI DSS compliant.

METHODOLOGY

Coalfire completed a multi-faceted technical assessment using the below industry and audit best practices. Coalfire conducted technical lab testing in Trend Micro's lab, located in Austin, TX, from March 11-15, 2019.

At a high level, testing consisted of the following tasks:

1. Technical review of the architecture of the full solution and its components.
2. Implementation of TippingPoint TPS in Trend Micro's lab environment.
3. Introduction of malware binaries and multiple vulnerabilities into the environment.
4. Observation of TippingPoint TPS protection against attacks and vulnerabilities introduced into the system.
5. Verification that the TippingPoint TPS signature database is current and updated at 30-minute intervals.
6. Verification of TippingPoint TPS detection capabilities to confirm it is able to detect various attacks when introduced into the environment.
7. Review of the TippingPoint TPS user interface (UI) console to confirm an administrator can manage various required features through the UI console.
8. Review of notification alerts for security incident details provided to configured users from the TippingPoint TPS UI console.

9. Review of logs generated through the TippingPoint TPS UI console.

Summary Findings

The following findings are relevant highlights from this assessment:

- When properly implemented following Trend Micro's guidance, TippingPoint TPS blocks intrusions before a malicious actor can breach the system.
- TippingPoint TPS actively blocks known vulnerabilities, including:
  - Structured query language (SQL) Injection
  - Buffer overflow
  - Cross-site scripting
  - Cross-site request forgery
  - Heartbleed [Secure Sockets Layer (SSL)/Transport Layer Security (TLS) vulnerability)
  - Beast (SSL/TLS vulnerability)
  - Spyware
  - Peer to peer
  - Vulnerabilities published by the National Vulnerabilities Database (NVD) with a Common Vulnerability Scoring System (CVSS) identifier
  - Operating system (OS) vulnerabilities for which a patch or update has been published by the OS vendor, and the pertinent systems have not yet been updated
  - Findings from the organization's periodic vulnerability scans by importing the scan results into the TippingPoint TPS
- TippingPoint TPS can be configured to notify the resources via email of the blocked vulnerability. TippingPoint TPS also provides capabilities to set up the Simple Mail Transfer Protocol (SMTP) server for email notifications.
- TippingPoint TPS detected and effectively prevented the execution of known malware samples introduced into the environment
- Appendix A: PCI DSS Requirements Coverage Matrix describes the detailed findings of this report.

ASSESSOR COMMENTS

Coalfire's assessment scope put a significant focus on confirming the capabilities of TippingPoint TPS and the benefits that can be achieved for an organization employing the solution in their environment.

It should not be construed that the use of TippingPoint TPS guarantees full PCI DSS compliance. Disregarding PCI requirements and security best practice controls for systems and networks inside or outside of PCI DSS scope can introduce many other security or business continuity risks to merchants or service providers. Security and business risk mitigation should be any merchant's or service provider's goal and focus for selecting security controls.

TIPPINGPOINT ARCHITECTURE AND SECURITY

Below is the typical TippingPoint TPS network architecture deployed within an organization's environment.

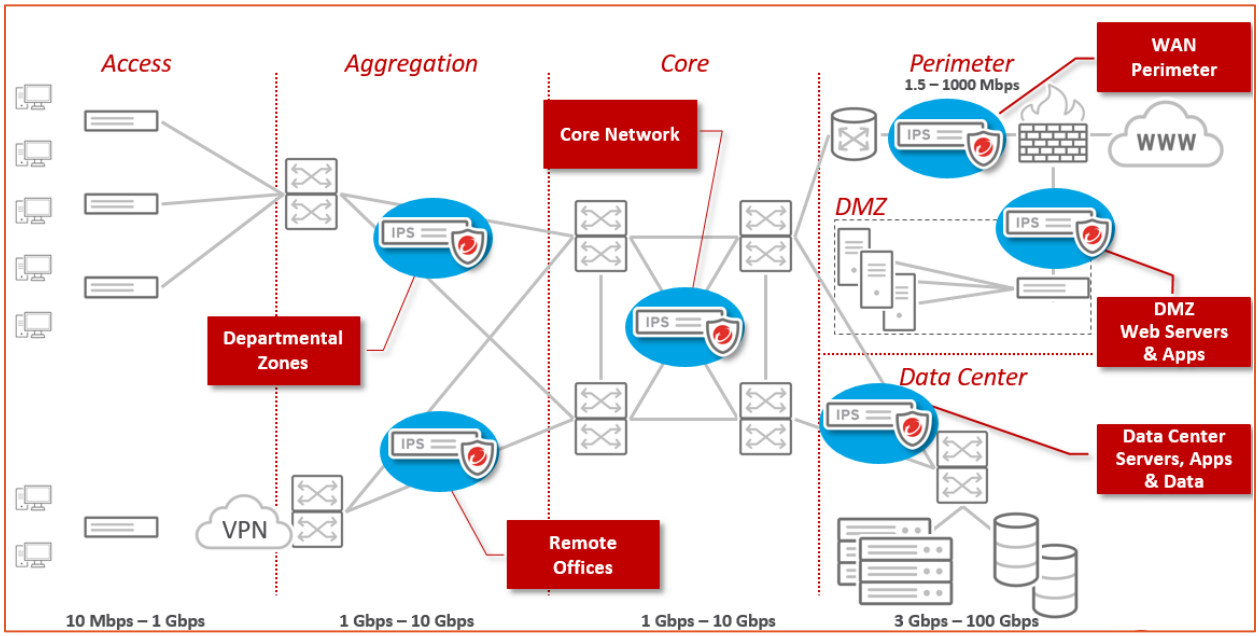

Figure 1: Network Diagram

Six TippingPoint TPS appliances are identified in the above diagram as intrusion prevention system (IPS) devices. These devices are deployed immediately behind the customer's perimeter firewall and also at the perimeter of all network segments within the environment. This ensures capture of all traffic inbound to the internal network, blocking known threats as they are received by the appliances. The deployment above also blocked threats as they were received from external or internal sources.

REFERENCES

Documents reviewed for this white paper include the following:

Trend Micro documents:

- Student Guide.pdf
- tps_5.1.1_cli_ref.pdf
- tps_5.1.1_hw_install_ug.pdf
- tps_5.1.1_lsm_ug.pdf
- tps_5.1.1_sslinspec_dg.pdf
- tps_dv_dn.pdf
- tps_rev2_8200TX_8400TX_install.pdf
- Trend Micro TippingPoint TPS Datasheet https://www.trendmicro.com/en_us/business/products/network/intrusion-prevention/tipping-point-threat-protection-system.html

Standards and Guidance

PCI SSC - Data Security Standard - https://www.pcisecuritystandards.org/documents/pci_dss_v3.pdf

PCI SSC - Which_Applications_Eligible_for_PA-DSS_Validation.pdf - https://www.pcisecuritystandards.org/documents/which_applications_eligible_for_pa-dss_validation.pdf

PCI SSC - Data Security Standard- Payment Application Data Security Standard Program Guide, v3.2 - https://www.pcisecuritystandards.org/documents/PA-DSS_v3-2.pdf

PCI SSC – Mobile Payment Acceptance Applications and PA-DSS https://www.pcisecuritystandards.org/documents/pa-dss_mobile_apps-faqs.pdf

APPENDIX A: PCI DSS REQUIREMENTS COVERAGE MATRIX AND EXECUTED TEST PLAN

COMPLIANCE LEVEL	DESCRIPTION
✓	Compliance directly supported via use of TippingPoint TPS
✓	Requires merchant action for full compliance

PCI DSS REQUIREMENT	TEST DEFINITION PER PCI VALIDATION PLAN	COMPLIANCE SUPPORTED	TIPPINGPOINT TESTING AND RESULTS
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	6.1.a Examine policies and procedures to verify that processes are defined for the following: • To identify new security vulnerabilities • To assign a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. • To use reputable outside sources for security vulnerability information.	✓	This requirement is partially supported using TippingPoint TPS. This is a process/procedure requirement and requires customers to develop a process to identify security vulnerabilities and assign a risk ranking. TippingPoint TPS uses signature analysis to detect and block vulnerabilities discovered in the environment. **Testing Procedure:** Coalfire observed TippingPoint TPS detected cyber threats, providing identification of threats introduced into the environment and the blocking of those threats. TippingPoint TPS uses ranking systems provided by OS vendors and other external, reputable sources such as CVSS. This information can be used by customers to assign a risk ranking to vulnerabilities.
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	6.2.a Examine policies and procedures related to security-patch installation to verify processes are defined for: • Installation of applicable critical vendor-supplied security patches within one month of release. • Installation of all applicable vendor-supplied security patches within an appropriate time frame (for	✓	This requirement is partially supported using TippingPoint TPS. TippingPoint TPS uses digital vaccines to block vulnerabilities for OS-based systems for which the OS vendor has published a patch, but the systems in the environment have not yet had that update installed. **Testing Procedure:** Coalfire observed TippingPoint TPS was updated to include a digital vaccine for a Microsoft vulnerability patch. The TippingPoint TPS UI console indicated the vulnerability was discovered in the environment and was blocked.

PCI DSS REQUIREMENT	TEST DEFINITION PER PCI VALIDATION PLAN	COMPLIANCE SUPPORTED	TIPPINGPOINT TESTING AND RESULTS
	example, within three months).		
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.	6.6 For public-facing web applications, ensure that either one of the following methods is in place as follows: • Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security assessment tools or methods—as follows: • Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: • Is situated in front of public-facing web applications to detect and prevent web-based attacks.	✓	This requirement is partially supported using TippingPoint TPS. Where installed or configured, TippingPoint TPS can act as a web application firewall with the ability to detect and block vulnerabilities related to web applications such as Cross-site scripting and Cross-site request forgery. **Testing Procedure:** Coalfire observed TippingPoint TPS was presented with cross-site scripting and cross-site request forgery attacks. The TippingPoint TPS UI console indicated the vulnerability was discovered in the environment and was blocked.

PCI DSS REQUIREMENT	TEST DEFINITION PER PCI VALIDATION PLAN	COMPLIANCE SUPPORTED	TIPPINGPOINT TESTING AND RESULTS
10.1 Implement audit trails to link all access to system components to each individual user	10.1 Verify, through observation and interviewing the system administrator, that: • Audit trails are enabled and active for system components. • Access to system components is linked to individual users.	✓	This requirement is partially supported using TippingPoint TPS. TippingPoint TPS logs all administrator activity occurring on the appliance and the UI console that includes user identification. **Testing Procedure:** Coalfire observed TippingPoint TPS appliances log events, which provides details through the TippingPoint TPS UI console.
10.2.2 All actions taken by any individual with root or administrative privileges	10.2.2 Verify all actions taken by any individual with root or administrative privileges are logged.	✓	This requirement is partially supported using TippingPoint TPS. TippingPoint TPS logs actions taken by administrative users on the appliance and the UI console. This information is accessible in the TippingPoint TPS UI console. **Testing Procedure:** Coalfire observed TippingPoint TPS logs can be viewed and searched for events showing actions taken by administrators.
10.2.4 Invalid logical access attempts	10.2.4 Verify invalid logical access attempts are logged.	✓	This requirement is partially supported using TippingPoint TPS. TippingPoint TPS monitors and tracks logins and failed login attempts to the UI console. This collected information is accessible through the TippingPoint TPS UI console. **Testing Procedure:** Coalfire observed TippingPoint TPS logs can be viewed and searched for invalid logical access events in the UI console.
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to; creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	10.2.5.a Verify use of identification and authentication mechanisms is logged.	✓	This requirement is partially supported using TippingPoint TPS. TippingPoint TPS records identification and authentication mechanisms. For other systems within in the customer's environment, additional audit trails must be configured to meet this requirement. **Testing Procedure:** Coalfire observed TippingPoint TPS logs can be viewed and searched for use of logical access and authentication mechanism events in the console.
	10.2.5.c Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.	✓	This requirement is partially supported using TippingPoint TPS. TippingPoint TPS monitors and tracks changes, additions, or deletion of various accounts. This collected information is accessible through the TippingPoint TPS UI console. For systems not covered by TippingPoint TPS,

PCI DSS REQUIREMENT	TEST DEFINITION PER PCI VALIDATION PLAN	COMPLIANCE SUPPORTED	TIPPINGPOINT TESTING AND RESULTS
			additional audit trails must be configured to meet this requirement. **Testing Procedure:** Observed that TippingPoint TPS logs are viewable in the UI console. Logs can be searched for change, additions, or deletions to any administrative account events to the UI console.
10.2.7 Creation and deletion of system level objects	10.2.7 Verify creation and deletion of system level objects are logged.	✓	This requirement is partially supported using TippingPoint TPS. TippingPoint TPS monitors and tracks changes and deletion of system level objects for the appliance and UI console. This collected information is accessible through the TippingPoint TPS UI console. For all other systems, additional audit trails must be configured to meet this requirement. **Testing Procedure:** Coalfire observed TippingPoint TPS logs can be viewed and searched for creation and deletion of system level objects in the TippingPoint TPS UI console.
10.3 Record at least the following audit trail entries for all system components for each event:	10.3 Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following:	✓	This requirement is partially supported using TippingPoint TPS. TippingPoint TPS can capture the events noted within 10.3.1 - 10.3.6.
10.3.1 User identification	10.3.1 Verify user identification is included in log entries.	✓	This requirement is partially supported using TippingPoint TPS. For every log entry generated by TippingPoint TPS, a user ID is tied to a specific event or entry. **Testing Procedure:** Coalfire observed the TippingPoint TPS appliances collected user details associated with the collected activity. The information was accessed from within the TippingPoint UI console.
10.3.2 Type of event	10.3.2 Verify type of event is included in log entries.	✓	This requirement is partially supported using TippingPoint TPS. For every log entry generated by TippingPoint TPS, the type of event is tied to a specific event or entry. **Testing Procedure:** Coalfire observed the TippingPoint TPS appliances captured the type of event for all collected activity. This information was viewed in the TippingPoint UI console.

PCI DSS REQUIREMENT	TEST DEFINITION PER PCI VALIDATION PLAN	COMPLIANCE SUPPORTED	TIPPINGPOINT TESTING AND RESULTS
10.3.3 Date and time	10.3.3 Verify date and time stamp is included in log entries.	✓	This requirement is partially supported using TippingPoint TPS. For every log entry generated by TippingPoint TPS, a date/timestamp is tied to a specific event or entry. **Testing Procedure:** Coalfire observed the™ TPS appliances captured the date and time for all collected activities. This information was viewed in the TippingPoint TPS UI console.
10.3.4 Success or failure indication	10.3.4 Verify success or failure indication is included in log entries.	✓	This requirement is partially supported using TippingPoint TPS. For every log entry generated by TippingPoint TPS, a success or failure is recorded for a specific event or entry. **Testing Procedure:** Coalfire observed the TippingPoint TPS appliances captured success or failure for all collected activities. This information was viewed in the TippingPoint TPS UI console.
10.3.5 Origination of event	10.3.5 Verify origination of event is included in log entries.	✓	This requirement is partially supported using TippingPoint TPS. For every log entry generated by TippingPoint TPS, the origination of event is tied to a specific event or entry. **Testing Procedure:** Coalfire observed the TippingPoint TPS appliances logged all collected activities. This information was viewed in the TippingPoint TPS UI console and includes event origination.
10.3.6 Identity or name of affected data, system component, or resource	10.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.	✓	This requirement is partially supported using TippingPoint TPS. For every log entry generated by TippingPoint TPS, the affected data, system, and resource are identified and tied to a specific event or entry. **Testing Procedure:** Coalfire observed the TippingPoint TPS appliances logged all collected activities. This information was viewed in the TippingPoint TPS UI console and includes the identity of affected data.
10.5.1 Limit viewing of audit trails to those with a job-related need	10.5.1 Only individuals who have a job-related need can view audit trail files.	✓	This requirement is partially supported using TippingPoint TPS. For all logs generated by TippingPoint TPS, role-based access provides control over who has access to collected data. In addition, user actions taken within the TippingPoint TPS UI console are logged. User action logs (audit logs) can be accessed by either downloading the log files from the Users Screen or

PCI DSS REQUIREMENT	TEST DEFINITION PER PCI VALIDATION PLAN	COMPLIANCE SUPPORTED	TIPPINGPOINT TESTING AND RESULTS
			via a syslog feed. For any required logging done outside of TippingPoint TPS or that TippingPoint TPS does not generate, those logs must be protected in a similar fashion. **Testing Procedure:** Coalfire observed TippingPoint TPS The users and corresponding roles were added or viewed from the TippingPoint TPS UI console "Authentication" section. Privilege levels were assigned to the users based on the need. Various privilege levels that could be assigned from the UI console included: None, Low, Medium (default level), and High. Each level has an increasing password length requirement.
10.5.2 Protect audit trail files from unauthorized modifications.	10.5.2 Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.	✓	This requirement is partially supported using TippingPoint TPS. Role-based access provides control over who has access to collected data, and all logs are protected from modification by default. In addition, user actions taken with the TippingPoint TPS UI console are logged. User action logs (audit logs) can be accessed by either downloading the log files from the console or via a syslog feed. For any required logging done outside of TippingPoint TPS or that TippingPoint TPS does not generate, those logs must be protected in a similar fashion. **Testing Procedure:** Coalfire observed users and corresponding roles were added or viewed from the TippingPoint TPS UI console "Authentication/Create User" section. Privilege levels were assigned to the users based on the need. Various privilege levels that could be assigned from the UI console included: None, Low, Medium (default level), and High. Each level has an increasing password length requirement.
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	10.5.3 Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.	✓	This requirement is partially supported using TippingPoint TPS. All data collected by the TippingPoint TPS appliances and UI console, including user action logs (audit trails), is configurable to be sent to a centralized syslog server. TippingPoint TPS does not generate logs for systems outside of TippingPoint TPS; logs from these systems must be protected in a similar fashion. **Testing Procedure:** Coalfire observed audit log information could be downloaded from the TippingPoint TPS UI console.

PCI DSS REQUIREMENT	TEST DEFINITION PER PCI VALIDATION PLAN	COMPLIANCE SUPPORTED	TIPPINGPOINT TESTING AND RESULTS
			The backing up of logs and its protection remains the responsibility of the end customer where they plan to back-up the log information.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note: Log harvesting, parsing, and alerting tools may be used to meet this requirement.***	10.6 Perform the following:	✓	This requirement is partially supported using TippingPoint TPS. This is a policy and procedures-based requirement. TippingPoint TPS can support the logging of security events relevant to the appliances installed within the customer's network. TippingPoint TPS supports this requirement by enabling the merchant to review the security logs created by TippingPoint TPS. Merchant must still review logs from other systems. TippingPoint TPS can help identify log events related to incidents with information related to accessed system components that could either be anomalous or suspicious activity. **Testing Procedure:** Coalfire observed the TippingPoint TPS UI console's ability to indicate security-related events in a dashboard that could be reviewed by administrators or security personnel daily for determining threats and suspicious activity for any deployed appliance.
10.6.1 Review the following 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**	**10.6.1.a** Examine security policies and procedures to verify that procedures are defined for reviewing the following at least daily, either manually or via log tools: • 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-	✓	This requirement is partially supported using TippingPoint TPS. The TippingPoint TPS UI console can be configured to provide notifications or alerts for malicious activities for the supported system components. Administrators can view the event details from within the UI console and retrieve logs for the appliances through the UI console or configure the solution to send it to a syslog server. The types of log files downloaded include: • Appliance logs • Application control log Note, however, that collection of logs from systems that perform security functions, such as PCs, servers, firewalls, and file-integrity monitoring (FIM) systems, remains the responsibility of the end customer. **Testing Procedure:** Coalfire observed the TippingPoint TPS UI console provided notifications in email or alerts for malicious activities (identified and blocked malware and vulnerabilities).

PCI DSS REQUIREMENT	TEST DEFINITION PER PCI VALIDATION PLAN	COMPLIANCE SUPPORTED	TIPPINGPOINT TESTING AND RESULTS
redirection servers, etc.).	prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).		Coalfire observed event details from within the UI console. Coalfire also observed the logs are available for download as necessary.
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	10.7.a Examine security policies and procedures to verify that they define the following: • Audit log retention policies • Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online.	✓	This requirement is partially supported using TippingPoint TPS. This is a policy and procedure-based requirement. All data recorded by the TippingPoint TPS appliances can be retained indefinitely. This means that TippingPoint TPS can support an organization's policies and procedures for audit log retention for those logs that TippingPoint TPS provides coverage. For any required logging done outside of the TippingPoint TPS appliances and UI console, the customer is responsible for the retention of those logs in accordance to PCI DSS or other relevant standard. **Testing Procedure:** Coalfire confirmed by review with TippingPoint personnel that data is retained by the solution. Any subsequent reviews of how long the audit information is retained will need to be validated during Trend Micro's customer's PCI DSS assessment.
	10.7.b Interview personnel and examine audit logs to verify that audit logs are retained for at least one year.	✓	
	10.7.c Interview personnel and observe processes to verify that at least the last three months' logs are immediately available for analysis.	✓	
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,	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	✓	TippingPoint TPS supports network-based intrusion prevention functionality. The TippingPoint TPS appliances can monitor all activity for malicious behavior. These executables or processes are compared with known "signatures" and/or behaviors of compromise types and administrators are alerted within the TippingPoint TPS UI console and, if configured to do so, the UI console notifies defined administrators via email. **Testing Procedure:** Coalfire observed the TippingPoint TPS appliances monitored various system activity or processes for malicious behavior. The malicious files compared

PCI DSS REQUIREMENT	TEST DEFINITION PER PCI VALIDATION PLAN	COMPLIANCE SUPPORTED	TIPPINGPOINT TESTING AND RESULTS
and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	• At critical points in the cardholder data environment.		with known digital vaccines and alerted administrators for events blocked.
	11.4.b Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises.	✓	TippingPoint TPS can alert personnel for any suspected compromise in the environment via emails or through the TippingPoint TPS UI console. The TippingPoint TPS UI console provides alerts for all blocked malware, vulnerability, and malicious activity events. **Testing Procedure:** Coalfire observed TippingPoint solution sent out email alert notifications as well as notified through the UI console of the detected and blocked malware, vulnerability, and malicious activity events.
	11.4.c Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection.	✓	TippingPoint TPS allows users to configure security profiles uniquely for the needs of their organization. **Testing Procedure:** Coalfire observed users can customize the appliance and solution on a granular level to meet their individual needs. Observed threats covered in the UI console and the specific actions that can be taken by the user.
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	12.10 Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach by performing the following:	✓	TippingPoint TPS can assist in executing an organization's incident response plan. However, the organization's incident response team is responsible for preparing the plan and responding to a system breach following the incident. TippingPoint TPS monitors and detects malware and vulnerabilities across environment. The TippingPoint TPS UI console identifies the presence of a malware/vulnerability event, which is identified and displayed within the TippingPoint TPS UI console in real-time. TippingPoint TPS immediately blocks the malware/vulnerability. Additionally, when configured by the customer to do so, TippingPoint TPS sends an email notification of the event to defined email addresses.

PCI DSS REQUIREMENT	TEST DEFINITION PER PCI VALIDATION PLAN	COMPLIANCE SUPPORTED	TIPPINGPOINT TESTING AND RESULTS
			Analysis of the compromised source and identification of issues caused can help incident response teams mitigate and address the risk to prevent further damage and exposure to the system following a breach. **Testing Procedure:** This requirement is partially supported using TippingPoint TPS. Coalfire observed TippingPoint TPS was able to identify and display malware/vulnerability events in real time and displayed in the UI console. An organization's users must analyze the data within the console or export logs for further investigation purposes.

CONCLUSION

TippingPoint TPS demonstrated a high level of flexibility for signature-based identification and prevention of multiple malicious threats. TippingPoint TPS capabilities can be utilized by an organization for various system components to analyze any suspicious activity or attacks on the endpoints. TippingPoint TPS also provides capabilities to set up the SMTP server for email notifications.

After reviewing the requirements of the PCI DSS, Coalfire determined, through a review of business impacts and a technical assessment, that TippingPoint TPS, as outlined in this document, can assist an organization with the technical requirements incident log information gathering (10.6, 10.6.1),

TippingPoint TPS provides partial coverage for the PCI DSS web application firewall requirement (6.6).

TippingPoint TPS provides partial coverage for PCI DSS general logging requirements (10.1, 10.2.2, 10.2.4, 10.2.5, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.5.1, 10.5.2, 10.5.3, and 10.7).

TippingPoint TPS provides partial coverage for PCI DSS incident response plan management requirement 12.10.

TippingPoint TPS provides full coverage for PCI DSS Intrusion Prevention requirement (11.4) for the supported operating systems.

The ability to achieve overall compliance with any regulation or standard will be dependent upon the specific design and implementation of TippingPoint TPS.

ABOUT THE AUTHOR

Lyle Miller | Principal: CISA, CISSP, QSA, PA-QSA

Lyle Miller (lmiller@coalfire.com) is an application security specialist at Coalfire. Lyle has over 18 years of experience in the IT security industry and over 8 years of experience working as a QSA and PA-QSA helping clients secure their systems and software for use in PCI DSS environments. He currently holds CISA, CISSP, QSA, and PA-QSA certifications. As a lead PA-QSA, Lyle supports assessments for some of the largest payment software providers in the world helping teams recognize the importance of secure code development and information security within their operational practices.

Bhavna Sondhi | Principal

Bhavna Sondhi is the practice subject matter expert for the Solution Validation team at Coalfire. Bhavna performs advisory work and assessments for PCI DSS, PA-DSS, and P2PE compliance frameworks as well as authors technical white papers. Bhavna joined Coalfire in 2013 and brings over 12 years of software engineering and information security experience to the team. Her software engineering experience plays a vital part in ensuring the teams recognize the importance of secure code development and Information Security within their operational practices.

Published April 2019.

ABOUT COALFIRE

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit Coalfire.com.