PCI Solution

Version 2.0

08/06/2012

DOCUMENT VERSION CONTROL

VERSION	DATE	AUTHOR(S)	DESCRIPTION	REASON FOR CHANGE
1.0	25 Feb’ 2009	Partha Panda, Third Brigade Inc		
2.0	06 Aug' 2012	JB Cheng Trend Micro Inc		Updated for PCI 2.0

Table of Contents

Introduction

PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.
As a part of this initiative the council has published a set of standards, called the Payment Card Industry Data Security Standard (PCI DSS). These standards apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data, and affect all payment channels, including retail (brick and mortar), mail/telephone order and ecommerce. PCI DSS version 1.2 published on Oct 1' 2008 was the first version of the standard, while version 2.0 published in October 2010 is the latest version available today. This document will describe how OSSEC can help merchants meet some of the requirements stated in PCI DSS 1.2/2.0. Unless otherwise stated, the sections mentioned below are identical between PCI DSS 1.2 and 2.0.

Key Benefits

OSSEC helps merchants meet PCI DSS 1.2/2.0 compliance and help them implement a defense-in-depth strategy. It is an open source Host Based Intrusion Detection System that provides advanced visibility into malicious behavior on systems.

Some of the key benefits of OSSEC are:

a) Compliance Requirements – OSSEC helps customers meet specific compliance requirements as outlined in PCI DSS 1.2/2.0. It lets customers detect and alert on unauthorized file system modifications and malicious behavior based on entries in the log files of COTS products as well as custom applications.
b) Multi-Platform Support – OSSEC lets customers implement a comprehensive host based intrusion detection system with fine grained application/server specific policies across multiple platforms such as Linux, Solaris, AIX, HP-UX, BSD, Windows, Mac and Vmware ESX.
c) Real-time and Configurable Alerts – OSSEC lets customers configure incidents they want to be alerted on which lets them focus on raising the priority of critical incidents over the regular noise on any system. Integration with smtp, sms and syslog allows customers to be on top of alerts by sending these on to e-mail and handheld devices such as cell phones and pagers.
d) Integration with current infrastructure – OSSEC will integrate with current investments from customers such as SIM/SEM (Security Incident Management/Security Events Management) products for centralized reporting and correlation of events.
e) Centralized Management – OSSEC provides a simplified centralized management server to manage policies across multiple operating systems. Additionally, it also lets customers define server specific overrides for finer grained policies.
f) Agent and Agentless Monitoring – OSSEC offers the flexibility of agent based and agentless monitoring of systems and networking components such as routers and firewalls. It lets customers who have restrictions on software being installed on systems (such as FDA approved systems or appliances) meet security and compliance needs.

PCI Compliance

Started as a security tool, OSSEC has been influenced by PCI to a large extent. The parts of PCI DSS 1.2 (same in 2.0) that OSSEC can help address are summarized below:

PCI DSS 1.2 Compliance		
6. Develop and maintain secure system and applications		
	6.4 Follow change control procedures for all changes to system components	OSSEC can help identify and alert on unscheduled and unapproved changes at the file system level. Administrators can review the alerts to verify that changes made are as approved by the change control process.
10. Track and monitor all access to network resources and cardholder data.		
	10.2 Implement audit trails for all system components to reconstruct the following events: 10.2.1 All individual access to cardholder data 10.2.1 All actions taken by any individual with root or administrative privileges 10.2.3 Access to all audit trails 10.2.4 Invalid logical access attempts 10.2.5 Use of identification and authentication mechanisms 10.2.6 Initialization of audit logs 10.2.7 Creation and deletion of system-level objects 10.3 Record at least the following audit trail entries for all system components for each event: 10.3.1 User Identification 10.3.2 Type of Event 10.3.3 Date and Time 10.3.4 Success of failure indication 10.3.5 Origination of Event 10.3.6 Identity or name of affected data, system component or resource	OSSEC provides a very powerful logs collection and correlation engine to monitor activities inside system logs such as Windows events or inside product & custom application logs. Its centralized management server lets administrators access audit trails centrally on one server with configurable alerts for prioritization of incident response.

	10.5 Secure audit trails so that they can not altered 10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts(although new data being added should not cause an alert)	OSSEC's System Integrity Checking module can be configured to monitor file system changes (such as changes to files, new files getting created, new directories being created, files being removed etc) and in Windows, registry key changes. It can be configured to monitor integrity of log files. OSSEC will not alert on new additions to log files but instead would only alert if the new entries indicate malicious behavior. The combination of system integrity and logs inspection can help administrators monitor log files without a lot of false alerts.
	10.6 Review logs of all system components at least daily. Log reviews, must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization and accounting protocol (AAA) servers (for example, RADIUS) Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6	OSSEC provides a very powerful logs collection and correlation engine to monitor activities inside system logs such as Windows events or inside product & custom application logs. Its centralized management server lets administrators access audit trails centrally on one server with configurable alerts for prioritization of incident response.
11. Regularly test security systems and processes		
	11.5 Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical files comparisons at least weekly. Note; For file-integrity monitoring purposes, critical files are usually those that do not require regular change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).	Most malicious code attempt at modify constituents of a system such as files, registry keys in order to perform unauthorized activities. OSSEC's System Integrity Checking module can be configured to monitor file system changes (such as changes to files, new files getting created, new directories being created, files being removed etc) and in Windows, registry key changes. This feature helps enterprises thwart attacks and provide advanced visibility into suspected malicious behavior on a system. Default monitoring policies are shipped with OSSEC and these can be augmented by additional policies at customer sites.
12. Maintain a policy that addresses information security for employees and contractors		
	12.9 Implement an Incident Response Plan	OSSEC can contribute heavily to an enterprise's incident response plan by making alerts/incidents centrally available from across the enterprise. Additionally, the configurable alerts can let administrators prioritize the various incidents as a part of the Incident Response process.

Note: It is highly recommended that customers share this document with their auditors for further guidance.