

Choosing compliance management system

Sergey Gordeychik, science editor of SecurityLab by Positive Technologies portal
<http://en.securitylab.ru>, <http://serggordey.blogspot.com/>

If we consider PCI DSS compliance management process in terms of vulnerability assessment and compliance management systems, it is possible to see a number of requirements which are directly or indirectly related to PCI DSS.

The most straightforward requirements are in section 11.2 which is related to local and external scanning made quarterly with automated tools. Detailed requirements to the process and tools could be found in PCI DSS Security Scanning Procedures. Summarizing the requirements, the used tool should analyze the system in penetration testing (black box) mode, support secure (SSL/TLS) services, and check password security. The additional requirement is a possibility to analyze the custom Web application security to find common vulnerabilities, such as Cross-Site Scripting, SQL Injection, etc. The necessity to check Web applications is confirmed by requirement 11.3 (Penetration Testing, Application Pentest) и 6.6 (Security review for public facing applications).

First of all, the listed requirements refer to the systems available through Internet. However, there are some requirements in PCI DSS which are related to security assessment of internal resources. There are already mentioned sections 11.3 and 6.5, and requirements 2.1 (Default passwords), 6.1 (Patch installation), 6.2 (Vulnerability identification). As a rule, for local networks assessment security should be made more often. For example, patches should be installed during a month which requires minimum 2 scanning a month – to detect vulnerabilities and to check that they are fixed. Audit mode is used in the majority of tools for vulnerability assessment where frequent scanning is necessary. This mode allows to detect a lot of vulnerabilities in “spare” mode with privileged account. Audit mode unlike Pentest, has minimum impact on scanning host and high efficiency.

Section 2.2 (Configuration Standards) makes demands for design and implementation of security configuration templates for all system components. Compliance management systems could allow to generate configuration standards based on internal knowledge base and control their use. Automatic tools essentially reduce efforts to maintain the system in compliant state. To cover the requirements fully Compliance management system should support analysis of configurations of all components – from network devices to business applications.

In addition, Compliance management systems could be used to analyze PCI DSS specific requirements, such as 3.2 (Sensitive data storage) , 5 (Antivirus software), 8.5 (Password Management), etc. In this case, there should be special checks for PCI DSS in the system.

An additional advantage of such systems is the ability to integrate with products of Security Information and Event Management (SIEM) class, such as Cisco MARS, Arcsight, Symantec SEIM, Netforensics. SIEM id often used to implement Requirement 10 (Access monitoring), and cooperation with compliance management systems improves the event analysis efficiency.

In order not to sound proofless, lets assess, whether the popular commercial products of vulnerability assessment and compliance management class meet the formulated

Vendor	Products	Links
eEye Digital Security	REM Management Console Retina Network Security Scanner Retina Web Security Scanner	http://www.eeye.com
IBM	IBM Proventia Management SiteProtector Internet Scanner Proventia Network Enterprise Scanner IBM Rational AppScan Tivoli Security Compliance Manager	http://www.ibm.com
Positive Technologies	MaxPatrol Compliance Management System	http://www.ptsecurity.com
Qualys	QualysGuard Security and Compliance Suite	http://www.qualys.com
Symantec	Symantec Control Compliance Suite	http://www.symantec.com

Below you can see the results of analysis based on the functions declared by vendors:

	eEye	IBM	MaxPatrol	Qualys	Symantec
Pentest					
Vulnerability Assessment	+	+	+	+	+/-
Password Guessing	+	+	+	+	+/-
Web-applications	+/-*	+/-**	+	+	-
Audit					
Vulnerability Assessment	+	+	+	+	+/-
Configuration Standards Analysis					
Network Equipment	-	-	Cisco Juniper Huawei Nortel	-	-
Windows Systems	+	+***	+	+	+
Unix Systems	Solaris HP-UX AIX Linux	Solaris*** HP-UX AIX Linux	Solaris HP-UX AIX Linux	Solaris HP-UX AIX Linux	Solaris HP-UX AIX Linux
Databases	-	-	MS SQL Oracle IBM DB2	MS SQL Oracle	MS SQL Oracle
Applications	-	-	Active Directory Exchange IIS Apache SAP/R3 Lotus Notes	-	Active Directory Exchange NDS eDirectory

* With Retina Web Security Scanner

** With IBM Rational AppScan

*** With Tivoli Security Compliance Manager

As one could see, all the vendors adequately cover the requirements for vulnerability assessment and compliance management systems for PCI DSS. However, in some cases it is necessary to use a few products instead of one product.