

COMPLIANCE IN VULNERABILITY SCANNERS AND SIEM

Olyesya Shelestova

The term compliance in relation to information security means adherence to some high-level standards (such as SOX, PCI DSS, Basel II, and GLBA). Checking for compliance with such regulations is essential for assessing how strictly your organization applies the security controls described in the regulatory documents (acceptable password length, existence of internal policies and procedures, time of fixing vulnerabilities, etc.).

In addition to international standards there are their local equivalents, corporate policies and NIST requirements also exist. Assessment of compliance to these regulations is also necessary. The standards consist of security controls; where applying these controls results in one's actual state of compliance. Here is an example of a security control: "There shall be a formal disciplinary process for employees who have committed a security breach." (ISO/IEC 2005, A.8.2.3)

Compliance checks are not just for red tape, the more requirements that are met, the higher the security level within an organization and the lower the risk of financial damage in case of a breach. Needless to say that compliance maintenance should be a frequent and ongoing exercise, otherwise your next audit may result in monetary fines and additional work to update your systems in accordance with the requirements.

How to perform a compliance check

At the ISO 27001 audit course I happened to meet some information security specialists who worked for certain organization that used the 27001 standard for compliance checks, but would perform assessment and capture their results in an Excel spread sheet. And believe me, you wouldn't want to see that sheet.

Of course, one method (like this) is to make a list of controls on paper or use Excel. Another method would be to use special software for security specialists to answer typical questions with "yes", "no", "I don't know", etc. But how reliable would information obtained this way be? Can you be sure that a domain administrator really set the minimum password length to 7 characters? Can you be sure the administrator didn't make a screenshot with the expected configuration and then change group policy settings according to his (!) own goals? Some controls can only be checked by asking those responsible, however most part of compliance checking can be done with the help of automated tools.

Control types

Security controls can be technical and non-

technical. Checking technical controls compliance can be automated (via console commands, configuration files parsing, registry parameters checking, etc.).

Here is a couple of common examples of a technical control which is included in the majority of standards: PCI DSS, 8.5.10 – "Require a minimum password length of at least seven characters"; PCI DSS 5.1. "Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)."

Compliance with non-technical controls, obviously, cannot be checked with automated tools. The ISO/IEC 2005 A.8.2.3 control I mentioned above is a good example of this type.

No security standards only consist of technical controls. With no automation tools available we could consider all controls to be non-technical. However, the ability to automatically check a compliance control tells us that control is a technical one. The more controls that can be analyzed (by verifying a system's compliance with it), the quicker risks can be eliminated by bringing systems into compliance.

Let me introduce some terms. Compliance checking is usually divided into general compliance checks (verifying a system's compliance with high-level standards by default), regulatory compliance checks (here conformity to requirements of various regulatory authorities, such as for Banking, is checked), and policy compliance checks (the range can vary from enterprise to NIST policies). Let's agree that for this article all these terms mean "checks for compliance with

standards or policies".

From standards to policies

What if your enterprise systems were not required to comply with any security standards, however you want to ensure that information security policies are properly adhered to?

The term compliance check is not only for high-level standards (ISO, SOX, Basel II) and NIST guidelines, but also for internal enterprise policies. Many enterprise policies include controls from standards. This means that technical controls can be singled out from the standards used for your information security policies, to combine them into a policy and focus on ensuring this policy compliance.

The question however is how to automate the creation and processing of these controls to assess a system's compliance with security standards or policies? The answer is quite simple: using such automation tools as vulnerability scanners, compliance management system (CMS), SIEM systems or at least some DIY scripts.

How it works

In a CMS and vulnerability scanner, compliance checks can be configured with the IP addresses of enterprise information systems, which should be checked. Then the defined systems are scanned to assess their compliance with the controls of a selected standard (during this process the scanner usually collects all available relevant data), and after that the tool analyzes whether or not the defined assets comply with all the controls of the given standard.



ScriptID	ScriptName	ScriptPath	ScriptRole	ScriptCreated	ScriptModified	Script
1184	wham-mqsh-M502-062-fa321		2	NUL	NUL	20.05.2009 8:52 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4cSE8Bp9Ztdm YNUL
1185	web-cgi-campas-exv-fa321		0	NUL	NUL	14.12.2005 1:23 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4cSE8Bp9Ztdm YNUL
1186	wham-misc-mis-fie-rec-pars-v2-fa321		0	NUL	NUL	19.05.2010 16:18 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4cSE8Bp9Ztdm YNUL
1187	web-cgi-fassurev-exv-fa321		0	NUL	NUL	14.12.2005 1:23 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4cSE8Bp9Ztdm YNUL
1188	web-cgi-ionp-p-fie-disc-v2-fa321		0	NUL	NUL	19.02.2009 7:12 @vqda3kn5VXp0lDgpggN2Q/Zow1qg1ABhQ3h1TBL0NAG+6omH1Cg0vFX9Dz2rDE DMKNnk8Ug1/EtIO0k2S58Mv1/bK0R9J2LIA+ErFpW4d63Jo4wZ76C3yF0v9r8
1189	web-cgi-hmsh-fie-disc-v2-fa321		0	NUL	NUL	14.12.2005 1:23 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4cSE8Bp9Ztdm YNUL
1190	wham-misc-mis-fie-perm-canonical-v2-fa321		2	NUL	NUL	20.05.2009 8:52 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4cSE8Bp9Ztdm YNUL
1191	misc-fp-sensitive-ext-v2-fa321		0	NUL	NUL	19.02.2009 7:18 @vqda3kn5VXp0lDgpggN2Q/Zow1qg1ABhQ3h1TBL0NAG+6omH1Cg0vFX9Dz2rDE DMKNnk8Ug1/EtIO0k2S58Mv1/bK0R9J2LIA+ErFpW4d63Jo4wZ76C3yF0v9r8
1193	web-3j-fp-3j-dir-trav-v2-fa321		0	NUL	NUL	19.02.2009 7:34 @vqda3kn5VXp0lDgpggN2Q/Zow1qg1ABhQ3h1TBL0NAG+6omH1Cg0vFX9Dz2rDE DMKNnk8Ug1/EtIO0k2S58Mv1/bK0R9J2LIA+ErFpW4d63Jo4wZ76C3yF0v9r8
1194	web-is-4j-4j-overflow-v2-fa321		0	NUL	NUL	20.05.2009 8:56 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4cSE8Bp9Ztdm YNUL
1195	web-is-5j-5j-shell-stash-dos-v2-fa321		0	NUL	NUL	17.05.2005 3:11 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4cSE8Bp9Ztdm YNUL
1200	web-is-5j-5j-data-src-disc-v2-fa321		0	NUL	NUL	20.05.2009 8:58 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4cSE8Bp9Ztdm YNUL
1202	web-cgi-ifsp-filter-bow-v2-fa321		0	NUL	NUL	20.05.2009 9:04 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4cSE8Bp9Ztdm YNUL
1203	web-ib-5j-5j-dir-down-v2-fa321		0	NUL	NUL	20.05.2009 9:10 @vqda3kn5VXp0lDgpggN2Q/Zow1qg1ABhQ3h1TBL0NAG+6omH1Cg0vFX9Dz2rDE DMKNnk8Ug1/EtIO0k2S58Mv1/bK0R9J2LIA+ErFpW4d63Jo4wZ76C3yF0v9r8
1204	web-ib-5j-5j-dir-glob-v2-fa321		0	NUL	NUL	20.05.2009 9:12 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4cSE8Bp9Ztdm YNUL
1205	web-apache-xcst1-v2-fa321		0	NUL	NUL	20.07.2005 15:18551 @vqda3khHGVfUjyQU+QUE/4hAJXKmgZ5vJWVWXLkAHU6N3ZTcdm2z4JVS6A9v1l DPAPKngV0ulqjHfYEmgah2v9v9Yh2v01tY0YGTW03z4wvHm25d58Rm1CZKx60
1206	web-ion-profpd-mkd-cwd-bow-v2-fa321		0	NUL	NUL	19.11.2005 18:48 @vqda3kn5VXp0lDgpggN2Q/Zow1qg1ABhQ3h1TBL0NAG+6omH1Cg0vFX9Dz2rDE DMKNnk8Ug1/EtIO0k2S58Mv1/bK0R9J2LIA+ErFpW4d63Jo4wZ76C3yF0v9r8
1207	web-cgi-printem-csv-v2-fa321		0	NUL	NUL	20.06.2007 14:20:29 @vqda3kn5VXp0lDgpggN2Q/Zow1qg1ABhQ3h1TBL0NAG+6omH1Cg0vFX9Dz2rDE DMKNnk8Ug1/EtIO0k2S58Mv1/bK0R9J2LIA+ErFpW4d63Jo4wZ76C3yF0v9r8
1208	web-ibm-win32-rotdir-v2-fa321		0	NUL	NUL	20.06.2007 14:20:29 @vqda3kn5VXp0lDgpggN2Q/Zow1qg1ABhQ3h1TBL0NAG+6omH1Cg0vFX9Dz2rDE DMKNnk8Ug1/EtIO0k2S58Mv1/bK0R9J2LIA+ErFpW4d63Jo4wZ76C3yF0v9r8
1209	web-omninitpp-cmd-comand-exec-v2-fa321		0	NUL	NUL	19.11.2005 18:48 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4cSE8Bp9Ztdm YNUL
1210	web-is-5j-5j-long-id-xss-v2-fa321		0	NUL	NUL	20.05.2009 9:14 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4cSE8Bp9Ztdm YNUL
1211	web-cgi-mrg-dir-trav-v2-fa321		0	NUL	NUL	28.06.2009 22:39 @vqda3kn5Vj9rAPvPYEGYbha+e+xxUz1B0H+g9Hk1ZK1EftqQ1PfcGMB8HNScYEt1 SRllg8eKso+1xakH0B51d540HfNB86O5SvLBw430AdNpfHt4c

As a rule, such tools provide a list of standards with a predefined set of controls, which can be selected for compliance checking. If this is not enough, one can buy additional licenses from the vendor for some other standards or to develop their own sets of controls.

Developing your own standard

Vulnerability scanners with compliance checking modes often provide an option for creating a user standard from scratch or on the basis of existing controls. This includes an option of redefining control values or adding your own.

Adding customized controls is possible due to flexible checking mechanisms. In every security compliance system, control checks include one or several tests. Usually such tests are implemented via several scripts with various techniques and transports (e.g., WMI, RPC, etc.). For instance, in McAfee VM, some scripts stored in its database look as shown in the figure.

However a customer has no need to explore databases and even know which scripts perform which checks. Commonly software vendors provide GUI to work with controls. You can add to your new standard or policy any technical controls you need or redefine the values of the existing ones.

SIEM

Let's talk about SIEM. Some terms related to such systems are defined in my other articles.

Let's think why SIEM systems need an option for checking compliance. What stands for this in relation to SIEM? And why not use only vulnerability scanners and compliance management systems for such checks?

First, standards include controls regarding logging some events, related to user accounts, access to resources, changing group policies, etc. These controls should also be applied, and SIEM systems allow verifying whether such types of event are logged.

Second, unlike various scanners, SIEM systems continuously receive data, which can be used for dynamic, real-time compliance assessment. How rapidly will you be notified of an anti-virus protection failure on your server or a group policy change? In these cases, running a scanner will result in additional loading of your network and information systems, since a standard (e.g., PCI DSS) compliance often involves vulnerability scanning, which means serious loading, that could crash your whole production system.

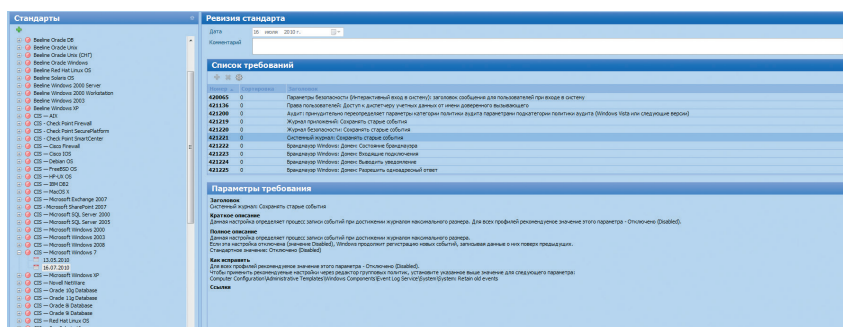
On the other hand SIEM systems can act as passive sources of compliance-related data, obtained on the fly. Such systems also solve the

Additionally, if a system provides incident management, a special employee will also receive a task to solve the problem.

Sounds great, doesn't it? Now let's return to our SIEM systems and see how they actually perform compliance assessment.

High-level standards dictate logging and storing logs for certain event types (see the table below).

Object Access	Object accessed
	Object created
	Object modified
	Object deleted
	Object handle
Logon	Successful user logons
	Successful user logoff
	Unsuccessful user logon
	Remote sessions
Policy Changes	User policy changes
	Domain policy changes
	Audit policy changes
System Events	System logs
	Audit logs cleared
Process Tracking	Process access
Account Logon	Successful account authentications
	Unsuccessful account authentications
User Access	User access to company resources
Account Management	User account changes
	Computer account changes
	User group changes
Security Assessment	Asset discovery
	Service control
Contingency Planning	Backup
	Restore from backup
Configuration Management	Software updates
	Anti-malwares



If there is no GUI, at least there should be documentation describing how to create a customized standard (e.g., in XML). Some effort ... and voilà, a unique standard, customized for your enterprise, is ready.

problem of log management. At the same time they can show what exactly is causing non-compliance based on the data they receive. Security administrators are notified in cases of non-compliance.



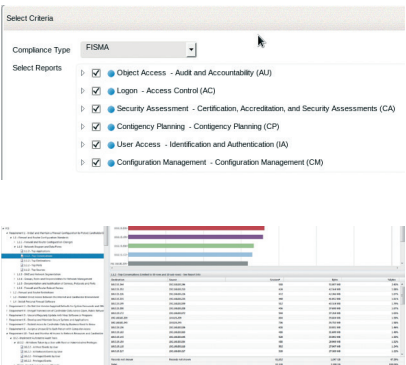
Here is what we have, taking into account some individual compliance standards.

	SOX	GLBA	PCI DSS	ISO 2700
Object Access	+	+	+	+
Logon	+	+	+	+
Policy Changes	+		+	+
System Events	+	+	+	+
Process Tracking	+			
Account Logon	+			+
User Access	+	+	+	+
Account Management	+			+
Security Assessment		+		+
Contingency Planning		+		+
Configuration Management		+	+	+

Let me accentuate this: the focus is on logging and storing logs. We won't see anything like "analysis" or "auditing of obtained data" (not to be confused with "system access audit", these are usually log data).

If you expect that a compliance check result, from your SIEM system, will return, for instance, a message "Minimum password length should be set" with an indication of compliant or non-compliant values — unfortunately, you'll definitely be disappointed.

What you can usually expect when checking an asset for compliance (with high level standards) with a SIEM system, is usually a list of logs and systems in relation to a control or, at best, a report based on logs related to a control (e.g., data flows control).



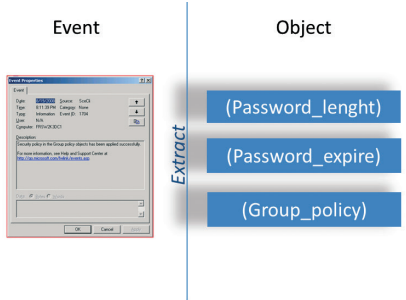
It's easy to conclude that SIEM systems are not designed for compliance management, but should only be used as a technical means of ensuring event logging and storage, and have only limited functionality for tracking and reporting.

Certainly, there are exceptions. But not many of them. Some vendors try to apply analysis of received logs to extract useful information which affects compliance. In this case controls are associated with SIEM correlation rules. One control is usually associated with several rules. This is because a certain fact (for instance, configuring minimum password length in a domain policy) can involve multiple event logs from various facilities, and the "content" of events can vary.

Moreover, in various facilities' event logs, a certain event can be described with various key words, and have different IDs.



Performing such checks requires really large amount of resources, so SIEM developers often give up.



Why do developers face such difficulties when trying to implement compliance assessment features? Here are some main reasons explaining it.

Reason one. SIEM systems don't use the concept of an object. Here we can recall the correlation technique MBR (model based reasoning), covered in one of my articles. This method could help describe, for example, an object state which results in non-compliance.

SIEM models store events, event categories and classes, statistics. However, there are no states of objects or assets (as I mentioned above, even the concept of objects does not exist in SIEM systems).

Reason two. Most SIEM systems' events are

not normalized (transformed into standardized format), which requires creating a great amount of correlation rules. Why? All vendors aim to comply with the NIST 800-92 requirement ("Original event is preserved and no data is changed during normalization") and store original event messages in RAW.

This, in its turn, makes developing a fully functional compliance management feature unreasonable.

So what should they do? One possible solution is to use the CEE standard (cee.mitre.org). This will allow standardizing events while avoiding NIST 800-92 non-compliance.

SIEM won't ever include all technical controls from standards due to one simple reason: Control values are not transferred with event logs from facilities. So, without adding a scanner feature, a SIEM system is unable to get the values. However, one of the trends is to use agentless technologies. Despite everything, SIEM systems allow monitoring states related to the majority of controls in real time. SIEM developers only need to take a step in the right direction.

I hope that in this article I managed to dispell the myth that SIEM systems could be used for compliance checks and introduced you to such concepts as standard compliance, policy compliance, and regulatory compliance.

