# PCI DSS Compliance in 10 Minutes a Day

## *Best Practices for Addressing File Integrity and Event Log Monitoring Requirements*


A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies



**www.newnettechnologies.com**

## Abstract

*Many organizations choose to delay the implementation of their PCI program, being wary of the resource requirements necessary to manage PCI compliance.*

*This whitepaper provides practical advice on how taking a 'baby steps' approach to PCI compliance and leveraging automated monitoring technology for file integrity and event logs will only require a few minutes each day.*


> "The principles of good security remain the same...you can only identify security threats if you know what business-as-usual, egular running looks like"

## PCI Compliance Is Hard for Everyone

In some respects, it can be argued that, the less IT 'stuff' an organization has, the fewer resources are going to be needed to run it all. However, with PCI compliance there are still always 12 Requirements and 650 sub-requirements in the PCI DSS to cover, regardless of whether you are a trillion dollar multinational or an SME company.

Spending some time recently with one of our smaller-scale resourced customers we were discussing – what else – PCI compliance for their IT Systems. The customer in question is a West-Coast USA based Metropolitan Theatre Operator and, being a theatre, their core business activity is bringing artistic productions to the people. IT is very much a necessary evil and as such in this instance there is essentially a four man team tasked with delivering IT.

## What does 'Secure' look like?

The principles of good security remain the same for both ends of the organization-size scale – you can only identify security threats if you know what business-as-usual, regular running looks like.

Establishing this baseline understanding will take time – 8 to 24 weeks in fact, because you are going to need a sufficiently wide perspective of what 'regular' looks like – and so we strongly advocate a baby-steps approach to PCI for all organizations, but especially those with smaller IT teams.

We argue strongly that doing the basics well first, then expanding the scope of security measures is much more likely to succeed and be effective than trying to do everything at once and in a hurry. Even if this means PCI Compliance will take months to implement, this is a better strategy than implementing an unsupportable and too-broad a range of measures. In other words, it's better to work at a pace that you can cope with, than to go too fast and go into overload.

This is the five step program we recommended to our Theatre Group client, although it actually has merit for any size of organization.

***Note: If you are reading this and thinking you do not have 8 weeks, let alone 24, to implement PCI measures, then NNT can still help but we will need to adopt a more intensive program that will need more than 10 minutes per day - talk to your NNT representative for an alternative plan***

## PCI Compliance in 10 Minutes per Day

> "...this isn't cutting corners or sweeping dirt under the carpet, but a pragmatic approach to doing the most important basics well first"

### *1. Classify Your 'In Scope of PCI' Estate*

You first need to understand where cardholder data resides. When we talk about cardholder data 'residing' this is deliberately different to the more usual term of cardholder data 'storage'. Card data passing through a PC, even it is encrypted and immediately transferred elsewhere for processing or storage, has still been 'stored' on that PC. You also need to include devices that share the same network as card data storing devices.

Now classify your device groups. For the example of our Theatre client, they have six core servers that process bookings. They also have around 25 PCs being used for Box Office functions. There are then around 125 other PCs being used for Admin and general business tasks.

So we would define 'PCI Server', 'Box Office PC' and 'General PC' classes. Firewall devices are also a key class, but other network devices can be grouped together and left to a later phase, simply because switches and routers are relatively less significant from a security standpoint.

Remember – this isn't cutting corners or sweeping dirt under the carpet, but a pragmatic approach to doing the most important basics well first, or in other words, taking the long view on PCI Compliance.

### *2. Make a Big Assumption*

We now apply an assumption to these Device Groups – that is, that devices within each class are so similar in terms of their make-up and behavior, that monitoring one or two sample devices from any class will provide an accurate representation of all other devices in the same class.

We all know what can happen when you assume anything but this assumption is a good one. This is all about taking baby steps to compliance and, having declared up front that we are adopting a strategy that is practical for our organization and our available resources, this provides an effective strategy.

The idea is that we get a good idea of what normal operation looks like, but in a controlled and manageable manner. We won't get flooded with file integrity changes or overwhelmed with event log data, but we will see a representative range of behavior patterns to understand what we are going to be dealing with.

Given the device groups already outlined, we recommend targeting one or two servers – say a web server and a general application server – one or two Box Office PCs and one or two general PCs.

### *3. Watch...*

You'll begin to see file changes and events being generated by your monitored devices and about ten minutes later you'll be wondering what they all are. Some will be self explanatory, some not so.

Either way, the imperative of tight Change Control will become very apparent.

If changes are being made at random, how can you begin to associate change alerts from your FIM system with intended 'good' changes and consequently, to detect genuinely unexpected changes which could be malicious?

Much easier if you can know in advance when changes are likely to happen – say, schedule the third Thursday in any month for patching. If you then see changes detected on a Monday these are exceptional by default. OK, there will always be a need for emergency fixes and changes but getting in control of the notification and documentation of Changes really starts to make sense when you begin to get serious about security.

Similarly from a log analysis standpoint – once you begin capturing logs in line with PCI DSS Requirement 10 you quickly see a load of activity that you never knew was happening before. Is it normal, should you be worried by events that don't immediately make sense? There is no alternative but to get intimate with your logs and begin understanding what regular activity looks like – otherwise you will never be able to detect the irregular and potentially harmful.


*Figure 1: The Anatomy of FIM - File Integrity Monitoring has three key dimensions - protecting system and program files, protecting configuration settings and protecting confidential data. These three dimensions require different technologies and approaches to cater for the varying demands of access and change detection*

### *4. ...and learn*

You'll now have a manageable volume of file integrity alerts and event log messages to help you improve your internal processes, mainly with respect to change management, and to 'tune in' your log analysis rule set so that it has the intelligence to process events automatically and only alert you to the unexpected, for example, either a known set of events but with an unusual frequency, or previously unseen events.

At this point, Summary Reports collating file changes on a per server basis are essential as a means of easily verifying that the Change Management discipline is being observed. This is the time to hold your nerve and see this learning phase through to a conclusion where you and your monitoring systems are in control – you see what you expect to see on a daily basis, you get changes when they are planned to happen.

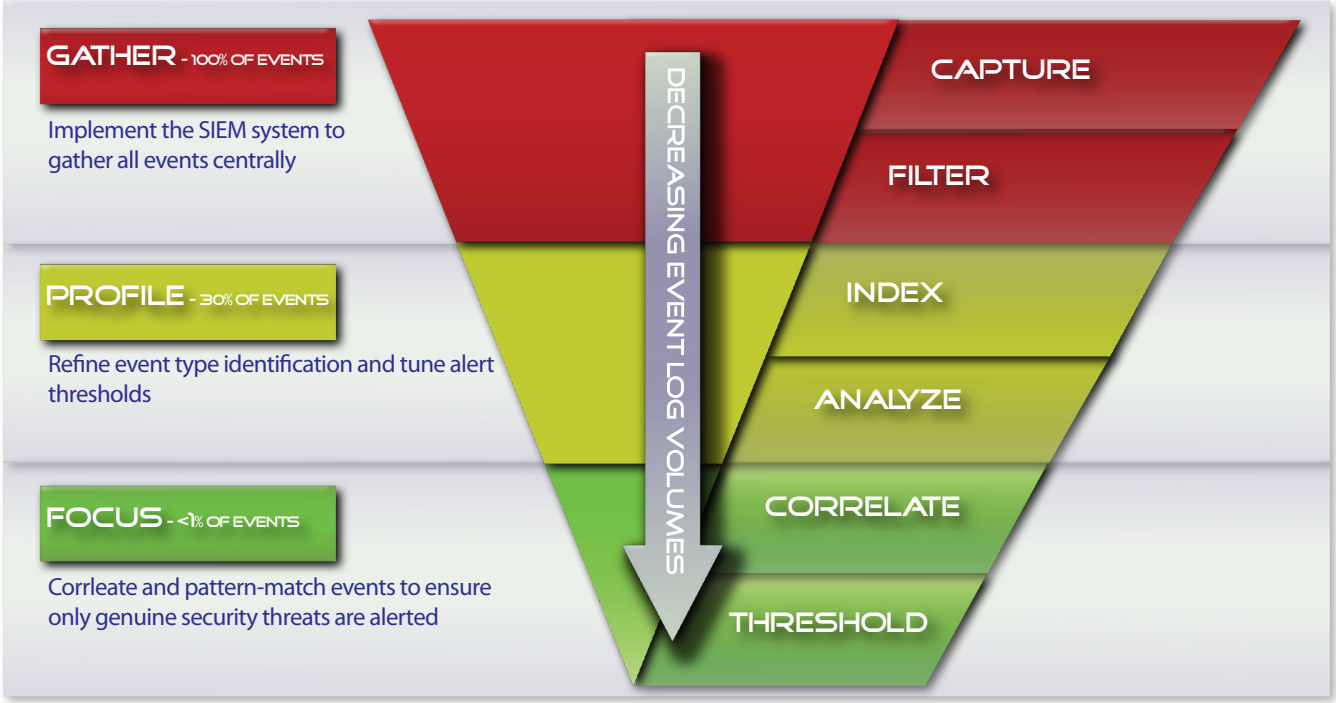


***Figure 2: The Event Log Funnel - whilst it is vital to gather all events and not have any 'security blind spots' the use of automated and intelligent event filtering and analysis to identify true security incidents is imperative***

### *5. Implement*

Now you are in control of what 'regular operation' looks like, you can begin expanding the scope of your File Integrity and Logging measures to cover all devices.

Logically, although there will be a much higher volume of events being gathered from systems, these will be within the bounds of 'known, expected' events. Similarly, now that your Change Management processes have been matured, file integrity changes and other configuration changes will only be detected during scheduled, planned maintenance periods. Ideally your FIM system will be integrated with your Change Management process so that events can be categorized as Planned Changes and reconciled with RFC (Request for Change) details.

## About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative.