Event Log Monitoring & the PCI DSS

A New Net Technologies Whitepaper

MARK KEDGLEY

CTO, New Net Technologies

www.nntws.com

SECURITY THROUGH SYSTEM INTEGRITY
NOW PART OF netwrix

Striking a Balance Between Compliance Obligations and Resource Costs

Getting the balance right between the need to meet your mandatory obligations for PCI DSS, and the imperative of minimizing costs' of ownership, is a challenge.

Section 10.2 of the PCI DSS states ***"Implement automated audit trails for all system components..."*** and there are typically two concerns that we always discuss:

> *Requirement 10: Track and monitor all access to network resources and cardholder data*
>
> *https://www.pcisecuritystandards.org/*

- *What is the best way to gather and centralize event logs?*
- *What do we need to do with the event logs once we have them stored centrally? (and how will we cope with the volume!?)*

To the letter of the PCI DSS, you are obliged to make use of event and audit logs in order to track user activity for any device within scope of PCI i.e. all devices which either 'touch' cardholder data or have access to cardholder data processing systems. The full heading of the Log Tracking section of the PCI DSS is as follows:

"Requirement 10: Track and monitor all access to network resources and cardholder data"

Logging mechanisms and the ability to track user activities are critical in detecting and preventing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Put simply - determining the cause of a compromise is impossible without system activity logs.

Given that many PCI DSS estates will be geographically widespread it is always a good idea to use some means of centralizing log messages, however, you are obliged to take this route anyway if you read section 10.5.3 of the PCI DSS:

"Promptly back up audit trail files to a centralized log server or media that is difficult to alter"

> *Promptly back up audit trail files to a centralized log server or media that is difficult to alter*
>
> *https://www.pcisecuritystandards.org/*

While Unix and Linux hosts can forward audit trail and system events using syslog, Windows servers do not have an in-built mechanism for forwarding Windows Events and it is therefore necessary to use an agent to convert Windows Event Logs to syslog. The Windows Events can then be collected centrally using your audit log server. Similarly, applications using Oracle/SQL Server, or bespoke/non-standard applications, do not use syslog to forward events so it will also be necessary to use an agent to forward events. Finally, if you are using an IBM z/OS mainframe or AS/400 system you will need further agent technology to centralize event and audit log messages.

Of course, Firewalls and Intrusion Protection/Detection System (IPS/IDS), as well as the majority of switches and routers all natively generate syslog messages.

Once assembled, the Audit trail history must be securely stored in order to prevent retrospective editing or any tampering. Traditionally, write-once media has been used to ensure event histories cannot be altered but most centralized log server solutions now employ File-Integrity Monitoring for the log backup files so that any modifications can be detected and alerted.

So in terms of our two initial questions, we have fully covered the first, but what about the next logical question of 'What do we do with - and how do we cope with - the event logs gathered?'

Now - What Am I Going To Do With All These Logs...?!

10.6 Review logs for all system components at least daily

This is the part of the standard that causes most concern. If you consider the volume of event logs that may be generated by a typical firewall this can be significant, but if you are managing a retail estate of, say, 800 stores with 8,000 devices within scope of the PCI DSS, the task of reviewing logs from devices is going to be impossible to achieve.

This may be a good time to consider the potential benefits of automation of the event log analysis process...?

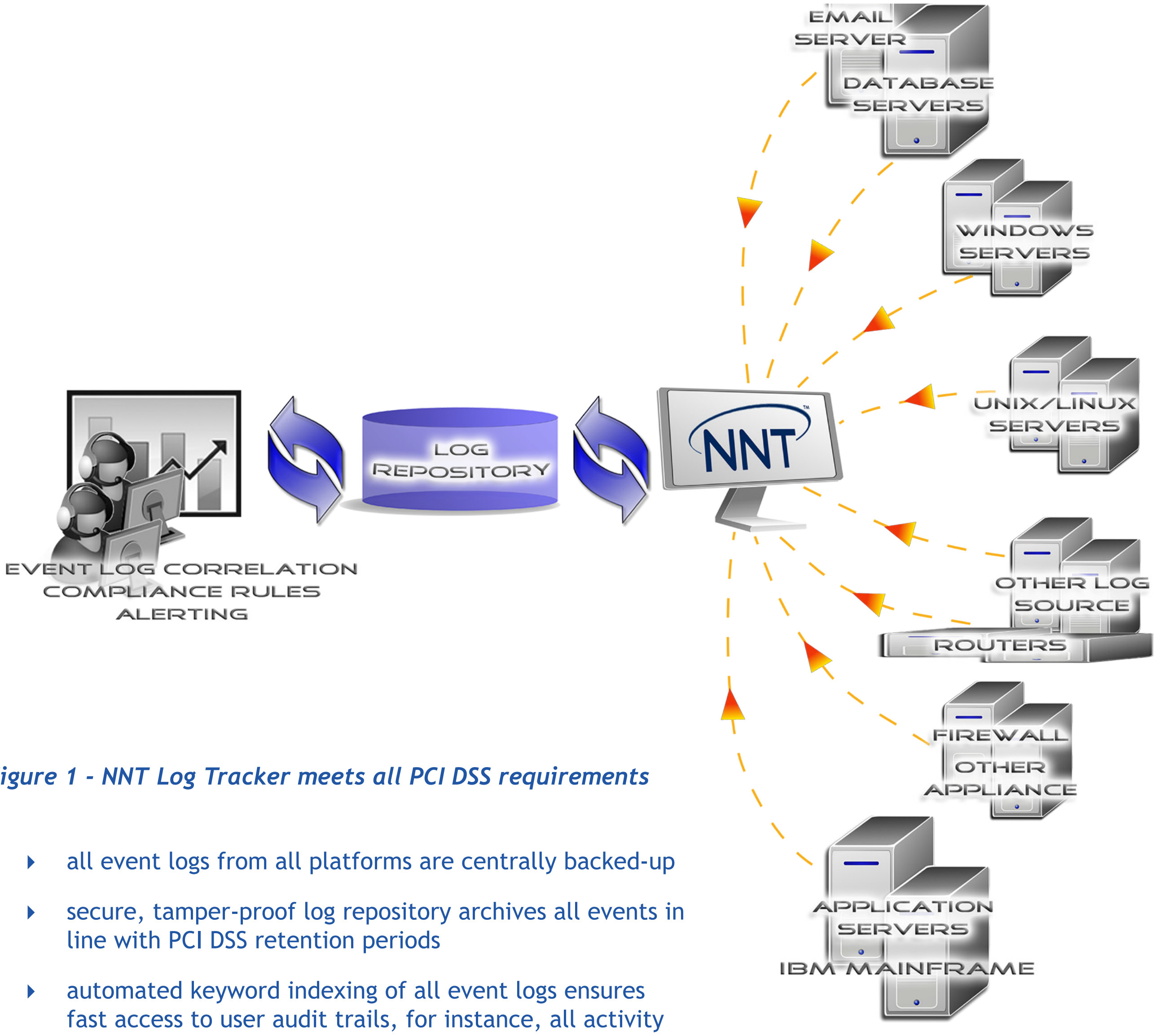


Figure 1 - NNT Log Tracker meets all PCI DSS requirements

- all event logs from all platforms are centrally backed-up
- secure, tamper-proof log repository archives all events in line with PCI DSS retention periods
- automated keyword indexing of all event logs ensures fast access to user audit trails, for instance, all activity related to a named user is available ‘out of the box’
- automated keyword indexing with pattern-matching and correlation technology ensures only key security events are highlighted

Now - What Am I Going To Do With All These Logs...?! Continued

The Security Information and Event Management, or SIEM market as defined by Gartner, covers the advanced generation of solutions that not only harvest audit logs and provide centralized log server functions, but parse event log messages e.g. store events by device, event type and severity, and analyze the details within event logs as they are stored. In fact, the PCI DSS recognizes the potential value of this kind of technology

"Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6 of the PCI DSS"

SIEM technology allows event logs to be automatically and intelligently managed such that only genuinely serious security events are alerted. The best SIEM technology can distinguish between true hacker activity running a 'brute force' attack and a user who has simply forgotten their password and is repeatedly trying to access their account. Naturally, there is an amount of customization required for each environment as every organization's network, systems, applications, and usage patterns are unique as are the corresponding event log volumes and types.

> *"Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6 of the PCI DSS"*
>
> *https://www.pcisecuritystandards.org/*

The PCI Event log management process can be approached in three stages, ensuring that there is a straightforward progression through becoming compliant with the PCI DSS standard and becoming fully in control of your PCI Estate. The three phases will assist you in understanding how your PCI Estate functions normally and, as a result, placing all genuine security threats into the spotlight.

1. GATHER - Implement the SIEM system and gather all event logs centrally – the SIEM technology will provide a keyword index of all events, reported by device type, event severity and even with just the basic, pre-defined rules applied, the volumes of logs by type can be established. You need to get familiar with the types of event log messages being collected and what 'good' looks like for your estate.

2. PROFILE - Refinement of event type identification and thresholds – once an initial baselining period has been completed we can then customize rules and thresholds to meet the profile of your estate, with the aim of establishing a profiled, 'steady-state' view of event types and volumes. Even though all logs must be gathered and retained for the PCI DSS, there is a large proportion of events which aren't significant on a day-to-day basis and the aim is to de-emphasize these in order to promote focus on those events which are significant.

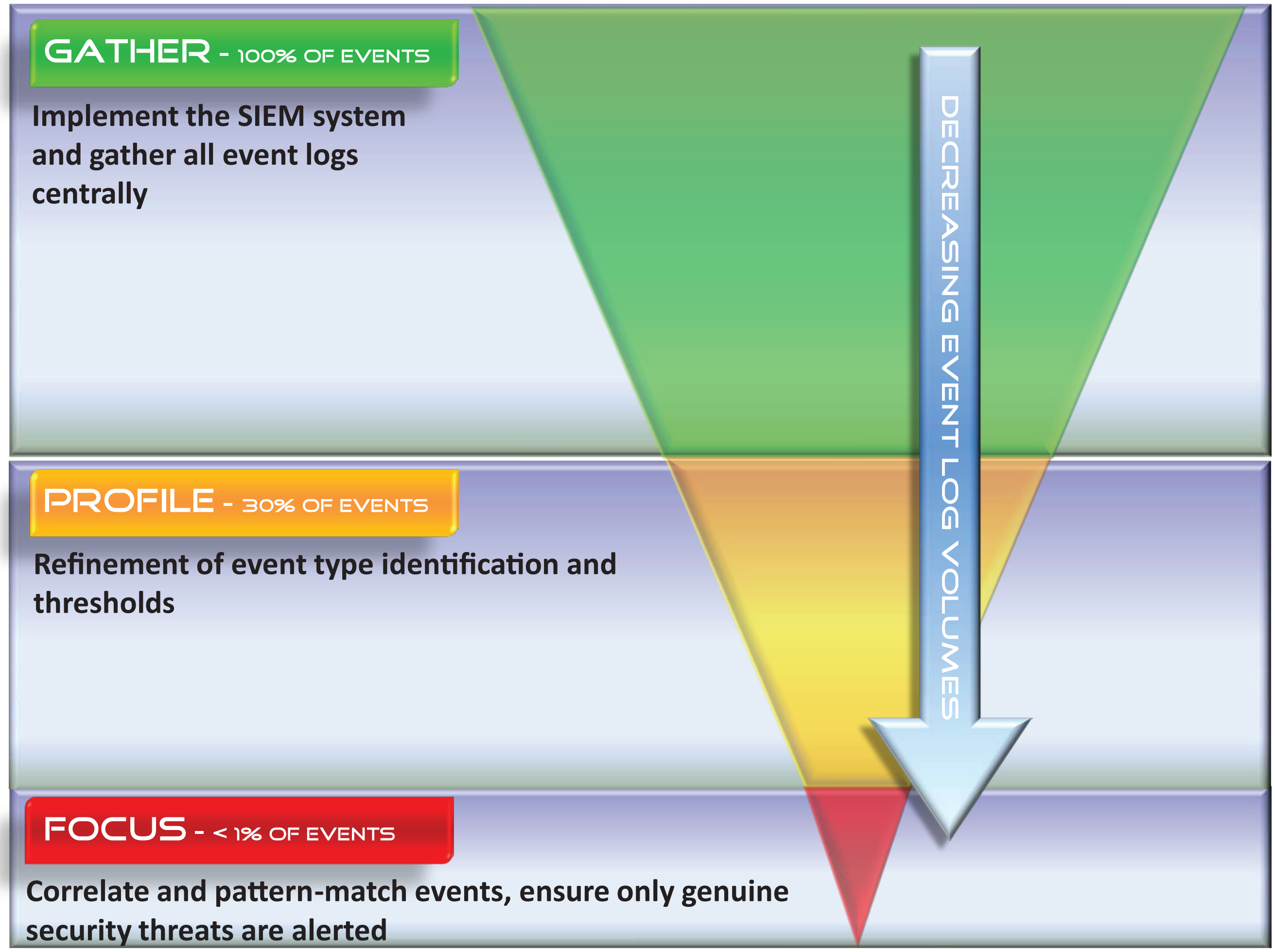
3. FOCUS – correlate and pattern-match combinations and sequences of events - simple thresholding for event types is adequate for some significant security events, such as anti-virus alerts or IPS signature detections, but for other security events it is necessary to correlate and pattern-match combinations and sequences of event. SIEM only becomes valuable when it is notifying you of a manageable number of significant security events.

It is important to note that even when certain events are being de-emphasized, these are still being retained in line with the PCI DSS guidelines which are to retain logs for 12 months. At least 3 months of event logs must be in an on-line, searchable format for at least 3 months, and archived for 12 months.

Again, the archived and on-line log repositories must be protected from any editing or tampering so write-once media and File Integrity Monitoring must be used to preserve log file integrity.

Security Information and Event Management - NNT Log Tracker

As discussed earlier, the right event log management technology not only makes it easy to gather all events, but will automate the analysis and interpretation of events so that you can meet PCI DSS requirements for log retention and review of logs, but without any unnecessary burden of sifting through unimportant messages.



GATHER - 100% OF EVENTS

Implement the SIEM system and gather all event logs centrally

PROFILE - 30% OF EVENTS

Refinement of event type identification and thresholds

FOCUS - < 1% OF EVENTS

Correlate and pattern-match events, ensure only genuine security threats are alerted

Figure 2: NNT Log Tracker technology will take you through a 3 phase process for gathering events, profiling events through analysis of thresholds of common events, before finally using powerful correlation and pattern-matching to ensure only genuine security events are highlighted.

Conclusion - The NNT View

The PCI DSS is still confusing for many, and seen as too expensive in terms of resource and budget requirements. As a result, many merchants are delaying the implementation of essential measures, leaving their customers' payment card details, and their organization's reputation, at risk.

NNT can help - using NNT Log Tracker will provide everything that a Payment Card merchant needs to become, and remain, PCI DSS compliant.

NNT Log Tracker is provided as a stand-alone SIEM solution or as part of the integrated NNT Compliance Management Suite, comprising NNT Change Tracker and NNT Log Tracker.

NNT PCI DSS Compliance solutions cover the following

- Configuration Hardening
- Change Management
- Event Log Correlation
- File Integrity Monitoring

NNT Change Tracker and Log Tracker Enterprise - Compliance Clarified

- Audit Configuration Settings - The core function of NNT Change Tracker Gen7 is to first understand how your IT estate is configured.
- Compare Audited Settings Against Policy - Configuration settings are assessed for compliance with any policy or standard relevant to your organization and deviations highlighted.
- Continuously Monitor Configuration Settings - Configuration attributes are then monitored continuously for all changes, both from a compliance standpoint and from a general change management/control standpoint.
- Change Management Process Underpinned - Authorized changes which have been approved via the formal change management process are reconciled with the original RFC to ensure the correct changes were implemented accurately.
- The Change Management 'Safety Net' - All unplanned changes are flagged up for review immediately to mitigate security integrity or service delivery performance.
- SIEM Event Log Correlation - Centralize and correlate event logs messages from all Windows, Unix/Linux, firewall, and IPS systems

TO REQUEST A FREE TRIAL OR DISCUSS ANY AREA COVERED IN THIS WHITEPAPER, PLEASE CONTACT US AT info@nntws.com

About NNT

NNT Change Tracker Gen provides continuous protection against known and emerging cyber security threats in an easy to use solution, offering true enterprise coverage through agent-based and agentless monitoring options.

- NNT analyzes every configurable component within your IT Estate and allows you to define a 'Known, Good, Secure and Compliant State' for all of your in scope systems.
- NNT-Change Tracker scans your devices and compares them to a standard policy, either user defined or based on an industry standard such as the Center for Internet Security (CIS).
- Policies can be automatically assigned based on the device type or priority via a centrally managed console.
- Gen7 is able to fully automate change approval for you, using the NNT FAST (File Approved-Safe technology) that combines unique intelligent change control knowledge base and whitelists.
- With NNT's real-time capabilities, unlike traditional scanning or exclusively agentless technologies, potential breaches to systems or policies are spotted immediately.

NNT Change Tracker Gen 7 helps you to prevent security breaches of your systems by providing you with a powerful feature-rich, easy to use and affordable solution for validating, achieving and maintaining compliance with corporate governance or security standards.

www.nntws.com

©New Net Technologies

UK Office - Spectrum House,
Dunstable Road, Redbourn,
AL3 7PR
Tel: +44 8456 585 005

US Office - 9128 Strada Place,
Suite 10115, Naples, Florida
34108
Tel: +1-888-898-0674