SANS ANALYST PROGRAM

Sponsored by Intellitactics

Leveraging Event and Log Data for Security and Compliance

A SANS Whitepaper – April 2008

Written by Dave Shackleford

Introduction

Despite the proliferation of enterprise log management and event monitoring solutions in use today, the overall state of information security has not measurably improved after incidents and audits. "Our findings show that data breaches are a pervasive problem for most organizations in the United States today," explains Larry Ponemon in a May, 2007, Network World article. "We also show that despite negative repercussions in terms of cost outlays and reputation diminishment, many companies that experience a breach do not take appropriate steps to prevent future incidents."[1] Why is this the case, particularly in light of the growth in logging and event management solutions?

There are several reasons. First, logging solutions are commonly underutilized. Simply storing logs in a central location and producing colorful "compliance reports" doesn't really demonstrate any added security intelligence. Similarly, event monitoring and management tools such as Security Event and Information Management (SEIM) that are put in place are rarely used to their full potential. In addition, many information security teams have been more concerned with keeping pace with ever-changing checklists of compliance mandates than with improving the effectiveness of their security programs.

Most of these compliance initiatives require some form of audit to ensure that controls are in place and due care is being followed, part of which is to fix and repair vulnerabilities and non-compliant processes as they become known. One example is the Payment Card Industry (PCI) Data Security Standard (DSS). The PCI DSS standard has continued to evolve and improve since its inception in 2004, and currently enjoys widespread participation from the security community. By the end of last year, 77 percent of Level 1 (greater than 6 million annual transactions) and 62 percent of Level 2 merchants (1-6 million Visa transactions or 150,000-6 million Mastercard transactions) had completed their initial security assessments and achieved compliance, according to Visa.

For those larger merchants who had successfully passed PCI DSS compliance, over half of them indicated that "tracking and monitoring access to the network and systems with cardholder data" was a significant hurdle, according to a survey by RSA about the business impact of data breaches.[2] In August of 2007, Visa had indicated that it would ease penalties for those merchants who had not yet achieved compliance.[3] And in February it announced four different assessment checklists for different types of sales networks, reducing the intimidating 270-question checklist (still mandated for Tier 1 processors) to just 11 questions for the simplest card-not-present systems. In addition, these less complex, lower-level merchants won't have to hire a third-party assessor to do the annual reviews.[4]

This tells us that compliance with any sort of data protection regulation, even one as well-defined and clearly articulated as the PCI DSS, can present significant challenges to organizations. In particular, monitoring and logging functions are still difficult to ingrain into the daily operations of many security teams, according to a recent report by Deloitte and Touche LLP, which lists inefficient logging and monitoring as one of the top seven threats to PCI compliance. As compliance mandates, logging and monitoring is being forced to improve. So security and compliance really do go hand-in-hand, according to Simon Tang, who heads Deloitte's PCI compliance practice. "The more proactive a company is in identifying its weakest links with regards to the PCI Data Security Standard, the better chance it has of protecting itself and its customers' data from potential security breaches,"[5] he states in the report.

By working to become compliant with industry and regulatory initiatives designed to protect sensitive data, organizations will become more secure as a result. Audits are conducted regularly, and any previous deficiencies must be corrected in order to pass muster. Audits are an opportunity to perform a "gut check" on the status of security controls and processes. Rather than looking for the quick "compliance checkbox," security professionals should instead view compliance and auditing as a means to measure improvements in security over time.

The most effective way to accomplish this is through improved logging and event management. Auditors should be working closely with security and operations teams to develop processes that leverage logging and event data to measure the effectiveness of security controls, starting with asset identification. Not all events are equal and should be treated differently according to their level of risk, so organizations need to identify their assets, assign their level of risk, and tune their security tools accordingly.

This paper explores steps for using compliance to improve security incrementally over time, giving auditors and security teams alike more current and relevant event data to assess and act upon. Equally important, these progressive organizations will be more prepared to quickly adapt to new compliance mandates that they may be subject to as risks to sensitive data, and progressive regulations, continue to unfold.

[1] http://www.networkworld.com/news/2007/051507-data-breaches.html
[2] http://www.darkreading.com/document.asp?doc_id=121930
[3] http://www.darkreading.com/document.asp?doc_id=131608
[4] https://www.pcisecuritystandards.org/tech/saq.htm
[5] http://www.deloitte.com/dtt/article/0,1002,cid%253D158442,00.html

Audit Results and Security Operations

Logging and Event Management tools, when deployed in a pervasive fashion, can provide security and operations teams with significant benefits: namely, improved visibility and security intelligence for critical systems, applications, and data stores. With this information, operations teams can perform a vast variety of activities in a more effective and efficient manner – examples range from application and system troubleshooting to Intrusion Detection System tuning and forensics investigations.

Since auditors are uniquely positioned to routinely assess the effectiveness of security controls, they can help operations teams achieve continuous improvement as a result of their findings. For example, reviewing intrusion attempts identified in a previous audit can be used to create new network-based access controls, or help identify malfunctioning applications that were causing failed login attempts so they can be repaired.

The use of logging and event management technology as a tool for continuous improvement represents a real departure from the traditional, purely operational manner in which these tools have been used to date. There are tangible, practical reasons to keep logs. As we collect more data from more systems, we will need products that can help manage that data. However, what has been lacking is the use of that data as a measurement tool by IT organizations to chart their progress in responding to issues, implementing more effective controls, and complying with regulatory mandates.

Security Operations Perspective

Due to a dramatic increase in information, security and IT operations teams are drowning in data. This is due to a dramatic increase in the number of logs and events from servers and network devices, monitoring software and diagnostic tools, and security-specific devices. In addition to managing the data generated by these devices, compliance mandates require timely and consistent reporting that demonstrates adherence to policy, properly functioning security controls, and an audit trail. For these reasons, many security teams have implemented controls with the following key goals in mind:

- **Collect and monitor log data**
- **Aggregate security events in a centralized dashboard**
- **Produce detailed reports for managers and auditors**

These are worthy goals by themselves, but there are many more ways that logging and event management can help security operations and other operations teams to continually improve security controls and processes. "Organizations that use log management solutions only to produce regulatory reports are wasting a major opportunity for improving security, and also wasting a surprising opportunity to improve the relationship between security and operations managers," notes Alan Paller, in an April, '07 *Information Security* article. [6]

So how can security and other IT operations teams leverage these incredibly flexible tools to their full potential? Here are seven ways to leverage logging, event management and monitoring to play a much larger role in security, compliance and IT operations.

[6] http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1257129_idx3,00.html

1. Troubleshooting Applications and Equipment

System availability is an integral component of IT's role within an organization, and log and event monitoring can greatly facilitate faster recovery from errors, which relates directly to system availability. The most common place to start looking when troubleshooting system and application errors is the log files. Depending on the system or application in question, the logs may contain minimal information or very detailed descriptions of errors encountered and how the system or application handled them. If these logs are sent to a centralized log management system, they can be easily parsed and organized. In addition, if event monitoring and correlation capabilities are available, these logs can be matched with other similar events and integrated into change management and business continuity functions to improve system maintenance and security.

39 02/07/2002 08:00:13.420 SEV=6 AUTH/41 RPT=2 192.168.124.241
Authentication successful: handle = 136, server = Internal, group = ipsecgroup

45 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=75 192.168.124.241 Group [ipsecgroup]Proposal # 1, Transform # 1, Type ISAKMP, Id IKEParsing received transform: Phase 1 failure against global IKE proposal # 1: Mismatched attr types for class Hash Alg: Rcv'd: SHA Cfg'd: MD5

Figure 1: IPSec VPN Error Logs

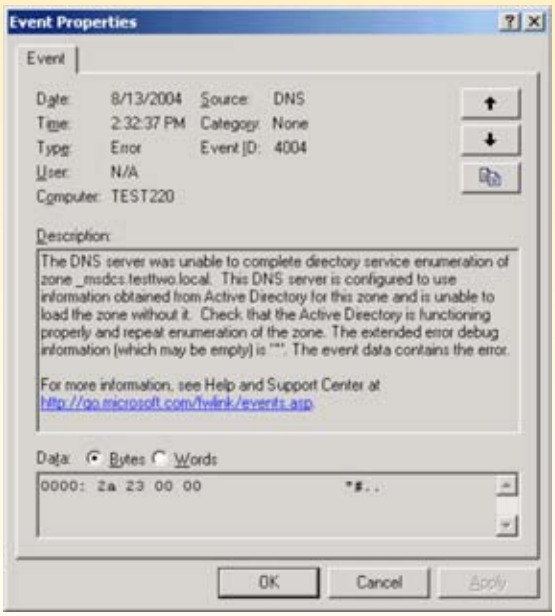

Figure 2: Windows DNS Error Log

2. Forensic Investigations

There is no such thing as an attack that leaves no traces. In many cases, these clues are preserved, to some extent, in one log file or another. In the case of internal investigations, these logs may be from users entering username and password information into systems and applications, or other types of access logs. Database logs, application-specific logs, firewall and IDS logs, and many others can play a role in recreating an incident for forensic analysis. In the 2006 SANS Analyst whitepaper "The Log Management Industry: An Untapped Market," one-third of companies surveyed used log data for forensic applications, and 11 percent used logs for this exclusively.[7]

Ultimately, forensics investigations should be carried out with the intention (real or supposed) to use the information in a legal proceeding. In order for logs to be treated as legitimate evidence in a court of law, certain preparations must be taken. For forensic work, original log data are required, making longer-term storage and maintenance of log data a requirement. In addition to this, access controls and access audit trails to this log data are key to ensuring its integrity.

```
0x04d0  801c 4011 801c 4011 801c 4011 801c 4011  ..@...@...@...@.
0x04e0  801c 4011 801c 4011 801c 4011 801c 4011  ..@...@...@...@.
0x04f0  20bf ffff 20bf ffff 7fff ffff 9003 e034  ..............4
0x0500  9223 e020 a202 200c a402 2010 c02a 2008  .#..........*..
0x0510  c02a 200e d023 ffe0 e223 ffe4 e423 ffe8  .*...#...#...#..
0x0520  c023 ffec 8210 200b 91d0 2008 2f62 696e  .#........../bin
0x0530  2f6b 7368 2020 2020 2d63 2020 6563 686f  /ksh....-c..echo
0x0540  2022 696e 6772 6573 6c6f 636b 2073 7472  ."ingreslock.str
0x0550  6561 6d20 7463 7020 6e6f 7761 6974 2072  eam.tcp.nowait.r
0x0560  6f6f 7420 2f62 696e 2f73 6820 7368 202d  oot./bin/sh.sh.-
0x0570  6922 3e2f 746d 702f 783b 2f75 7372 2f73  i">/tmp/x;/usr/s
0x0580  6269 6e2f 696e 6574 6420 2d73 202f 746d  bin/inetd.-s./tm
0x0590  702f 783b 736c 6565 7020 3130 3b2f 6269  p/x;sleep.10;/bi
0x05a0  6e2f 726d 202d 6620 2f74 6d70 2f78 2041  n/rm.-f./tmp/x.A
0x05b0  4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
0x05c0  4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
0x05d0  4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA
```

Figure 3: Network logs depicting a successful attack on a UNIX server3

[7] http://www.sans.org/reading_room/analysts_program/LogMgtIndustry_June06.pdf

3. Incident Response

Logging and event monitoring are integral components of a well-developed incident response program. Incident responders are tasked with finding answers to the following questions:

- **"What's going on?"**
- **"Have we found the problem?"**
- **"Have we fixed the problem?"**

Logs and normalized events can be incredibly helpful in answering these questions. For example, reviewing logs from key firewalls can alert responders to scanning activity, established connections, TCP or UDP ports in use, and certain types of unauthorized access attempts. The ability to correlate events and monitor application behavior over time is essential in incident response efforts. As logs often differ widely in format and content, having centralized aggregation and normalization capabilities is indispensable to accurately determine how an attack or malware incident is unfolding.

```
/usr/local/mysql/libexec/mysqld, Version: 3.23.54-log, started with:
Tcp port: 3306 Unix socket: /tmp/mysql.sock
Time Id Command Argument
# Time: 030207 15:03:33
# User@Host: baduser[baduser] @ b3.com [192.168.1.8]
# Query_time: 13 Lock_time: 0 Rows_sent: 117 Rows_examined: 234
use creditcarddb;
SELECT * FROM cardnumbers WHERE card_id= XXX;
```

Figure 4: MySQL logs depicting suspicious database access

[8] http://www.securityfocus.com/infocus/1676

4. Firewall/IDS Tuning and Reporting

Tuning firewall rule sets and intrusion detection systems is important to security and operations teams for a number of reasons. First, receiving too many alerts can cripple an effective monitoring and response effort. In many cases, a high percentage of these alerts are false positives, triggered by unnecessary or low-priority rules. The second reason that tuning is important is to ensure that legitimate traffic is not being blocked or alerted on, and that any known malicious traffic is blocked or generates alerts. Properly tuned log management and event monitoring tools can easily facilitate this by condensing large quantities of log and event data into more legible security information and isolating events that do not correlate with any other activity.

5. System Status/Reporting

Over half of the people surveyed in SANS' 2006 Log Management Analyst paper use logging for monitoring the health of their networks.[9] In addition to operating system and application status messages and error logs, other log and event data commonly employed for system health monitoring includes Simple Network Management Protocol (SNMP) data, host-based IDS or IPS logs, along with events generated by file integrity monitoring solutions.

6. Building Awareness and Education

As part of a more holistic enterprise security strategy, log management and event monitoring can be leveraged to produce statistics to educate other staff about information security risks. For example, tallying a monthly total of different events and attacks seen targeting Web servers, database servers, etc., can help people see real examples of what's trying to spread between their computers, how their actions are inviting malicious software onto their work and home computers, and how to practice secure computer usage. One key area that can help people understand this concept is reporting on the different systems where login credentials are employed, and demonstrating that weak or exposed credentials can easily be used by attackers to gain access to sensitive systems and data.

[9] http://www.sans.org/reading_room/analysts_program/LogMgtIndustry_June06.pdf

7. Robust Security Management and Compliance Reporting

The more visibility and insight security and operations teams have into what is occurring in the environment, the better the organization's overall security posture will be. The ability to reasonably monitor logs and correlate events from numerous systems provides the following benefits:

- **Decreased response times for handling incidents and troubleshooting problems**
- **Improved collaboration between security and other enterprise IT teams that manage systems, networks, and applications**
- **Enhanced, thorough security and compliance reporting that takes more systems and applications into consideration**

From the operations perspective, the goal should be to facilitate the improvement of information security processes and controls. Additionally, security teams need to quickly and reliably demonstrate the status and effectiveness of controls for auditors and IT management. Organizations should be able to demonstrate how logs are handled, who has access to them, and how these systems relate to the overall data protection strategy in place within the organization. For example, publicly traded companies that are subject to Sarbanes-Oxley compliance must demonstrate that financial data and financial reporting information are monitored for illicit tampering and fraud, including who accessed that data and for what purpose. Under PCI DSS, organizations that store, transmit, or process payment card data must demonstrate that systems and applications involved in handling this sensitive information are closely monitored and protected. Ultimately, auditors will need to verify that these controls are in place and effective.

Auditing Perspective

Auditors need access to event data and audit trails in order to accurately report an organization's compliance posture with regard to external regulations and internal security policies and processes. As the work of auditors becomes more essential to an organization's ability to confirm its reliability and trustworthiness, it also becomes more entwined with the day-to-day operations of information security, networking, and application development. Although to many, auditors' work has traditionally been relegated to the "checklist people," this has changed dramatically in the last several years. Auditors are increasingly relied upon to perform the following essential functions:

- **Measuring the current state of technical controls in place within the organization**
- **Comparing the current state of controls against what we consider a "known good state" as defined by our policies and procedures**
- **Producing reports that management and regulators depend on for unbiased information, and opinions regarding the organization's security and compliance posture**

Consider the daily work conducted by security operations – configuration and application of security policies for systems, network traffic and access control monitoring, along with incident response. All of these activities should be related to policies and procedures – some entirely internal in nature (like acceptable use and wireless security policies) and some mandated by external groups related to regulations or industry-specific standards (hashing or truncating personal account numbers for the PCI standard, for example).

Over time, aspects of these daily operations activities gradually change or otherwise fail to adhere to the intended policies and compliance requirements. In many of the most publicized data breaches in recent history, auditors had pointed out significant security deficiencies in those organizations' controls prior to the breaches being discovered. Some examples include:

- **TJX, accused of exposing over 94 million credit card numbers between 2005 and 2007, had been audited in early 2005 and found to be missing key security controls. A Visa vice president acknowledged the issues in a December 29, 2005 letter to TJX's credit card processor. Fines for PCI non-compliance were suspended until December 31, 2008, as long as TJX demonstrated that diligent remediation efforts were pursued.[10]**
- **In July 2007, the US General Accounting Office (GAO) conducted a follow-up audit of several key medical centers run by the Department of Veterans Affairs that found a significant lack of adequate controls in place to secure sensitive medical data. The previous audit had been conducted in July 2004, and numerous issues were found then as well.[11] The Department of Veterans Affairs suffered the loss of over 1.5 million social security numbers in May 2007 when an employee lost a portable hard drive.**

In both of these cases, audits had been conducted, but where was the follow-up? A real opportunity for improvement in both of these organizations was lost, and significant financial and reputational damages ensued as a result. These examples sharply illustrate the need for a new role for audit teams today as they work more closely with information security to create a feedback loop that can be used to chart progress over time.

[10] http://www.eweek.com/c/a/Security/Visa-Gave-TJX-Until-2009-to-Get-PCI-Compliant/
[11] http://www.gao.gov/new.items/d07505.pdf

Leveraging Log and Event Data for Audit Reports

Any logging and event data should help answer three questions:

- **Who? What user or identifiable entity are we tracking or assessing the behavior of?**
- **What? What event are we interested in and what assets are involved?**
- **When? At what time did the event occur?**

These three elements comprise the foundation of an effective audit trail. There are a number of additional considerations that impact the effectiveness of auditing with logs and event data, including:

- **Normalization: In order for auditors to assess controls by examining log and event data, this data must be in a consistent format that contains all necessary and relevant fields as well as any context needed for proper interpretation. For example, firewall logs and IDS events will both typically contain source and destination IP addresses, date and time stamps, rule(s) triggered, and the device name that is reporting the event. Depending on the device, however, these logs and events can be very different in appearance, and auditors should not be expected to analyze log format as well as function.**
- **Retention period: Depending on the policy or regulatory controls, log and event data should be available in a native format for a specified time period. For instance, the PCI DSS requires that one year of log data be retained, with three months' worth available immediately if requested.**
- **Audit Trails for Event Data Access: As logging and security event data are considered sensitive information, the confidentiality and integrity of the logs themselves should be demonstrable via some type of access controls with logs that indicate how those controls are performing. A related area is log data review and the audit trails that support this log analysis, which are used to demonstrate to auditors that policies or compliance mandates are adhered to. The PCI DSS, under which logs must be reviewed daily to achieve compliance, is an example.**

How Can Auditors Measure Improvements?

Before they are able to move past the "checkbox mentality," auditors must first have a sense of what they are measuring and why. As Andrew Jaquith states in his book Security Metrics, "I want a set of key indicators that tells customers how healthy their security operations are, on a stand-alone basis and with respect to peers."[12] Here are several steps and methods that auditors can follow to help continually measure and report on the effectiveness of security controls:

- **Understand the policies and regulations at hand. Although opinions differ widely on what security controls are most important, always consider the ramifications of non-compliance first and foremost.**
- **Ensure that logging and event data are gathered automatically from all systems storing or processing critical and sensitive data. If even one system is overlooked, major problems can occur. This was the case with CardSystems International in 2005 – external auditors were told that a testing and archival system was out of scope, and this system was the cause of a data breach exposing over 40 million credit card numbers.**
- **Correlate audit trail data with asset identification and system inventory efforts. Since auditors are tasked with cyclical measurement of controls and data protection, they are in an excellent position to keep up with information assets and note the relative criticality of those systems and the data that they store or process.**
- **Work with security and other operations teams to determine what the highest-risk control violations are after each audit has been completed. This will also be relative to the asset identification and data classification efforts that are ongoing during the audits as well, since auditors can more easily conduct effective risk assessments on assets with up-to-date asset inventories and identification and classification of controls. Some of these answers may be predetermined by compliance initiatives, but many will be decided in a more collaborative fashion depending on business risk tolerance and input from many other stakeholders.**
- **Once critical areas of measurement have been established, maintain meticulously detailed records of audit findings and track changes (both positive and negative) over time. Examples of trends that can be followed include:**
  - **Number of failed logins to systems**
  - **Vulnerability scan data such as missing patches and open ports (this can often be interpreted by SEIM solutions)**
  - **Malware blocked/quarantined or successful malware infections**
  - **System configuration or firewall/router access control changes**
- **Leverage existing process improvement efforts within the organization, or look to instill new process definitions based on control frameworks such as Control Objectives for Information Technology (COBIT), ISO 27001, and the Information Technology Infrastructure Library (ITIL). In particular, the combination of COBIT (audit guidance) and ITIL (process improvement) can be put to good use. Work to integrate recommendations into change and configuration management processes. This can make assignment of tasks and tracking changes much easier, particularly in larger organizations.**

Although these recommendations are more easily facilitated by internal audit teams, external audit results can be tracked and leveraged to achieve the same results.

[12] Andrew Jaquith, Security Metrics (Upper Saddle River: Addison-Wesley, 2007), p.6.
[13] http://www.technologyexecutivesclub.com/PDFs/ArticlePDFS/GettingInControl.pdf

Conclusion

Security and audit professionals need a significant amount of information in order to protect regulated information assets and validate that the controls in place are working. As the volume of logging and event data grows, and more distinct types of devices and applications come online, the need for centralized, correlated, scalable log management is more important than ever. Many information security teams have been implementing and tuning log management and event monitoring and correlation to improve their analysis of security events and better protect sensitive data.

This is driven as much by risk aversion as it is by HIPAA, GLBA, PCI DSS and other compliance mandates concerned with demonstrating that an organization has taken basic and fundamental steps to ensure the privacy and security of sensitive data. Although this approach has been fairly successful in demonstrating that due care has been taken, such mandates, and enterprises' response to them, should be considered as the first phase of compliance. The painful first round of compliance has been achieved by the majority of large stakeholders -- a process that some call the "checkbox mentality." Yet, as a result of having to check all these boxes, auditors, many of whom come from technical backgrounds themselves, are becoming more involved than ever in the planning and design of security controls.

One of those controls is leveraging and organizing log and security event data for more streamlined audits. Leveraging this data improves visibility into systems and can be used to strengthen weak processes as they're discovered. This, in turn, integrates security deeper into the overall organizational infrastructure, achieving the overall effect of a more secure enterprise.

About the Author

Dave Shackleford, Director of Configuresoft's Center for Policy & Compliance, is a course and exam author for the SANS Institute, where he also serves as a GIAC Technical Director. He is the co-author of ***Hands-On Information Security*** from Course Technology, as well as the "Managing Incident Response" chapter in the Course Technology book, ***Readings and Cases in the Management of Information Security***.

Previously, he worked as CTO for the Center for Internet Security, as well as for a security consulting firm in Atlanta. He has also worked as a security architect, analyst, and manager for several Fortune 500 companies. He has consulted with hundreds of organizations in the areas of regulatory compliance, security and network architecture and engineering. His specialties include incident handling and response, intrusion detection and traffic analysis, and vulnerability assessment and penetration testing.

SANS would like to thank its sponsor: