Log Management for Compliance

Logs are your golden record for compliance, but they don't give up their story easily.

''//'CHAPTER 1:

Tying Log Management and User Identity

Without a log management system, you won't be able to make the crucial connection between events, the people or programs who create them, and the relation of those events to others in your many logs.

''''>..CHAPTER 2:

No Log Management, No Regulatory Compliance

That's why log management is crucial to achieving regulatory compliance, and why you may need to modify your selection criteria when choosing tools.

TechTarget®
The Technology Media ROI Experts

Tying Log Management and User Identity

Compliance and security are about using sharp minds and tools to track, analyze and report on suspicious human activity.

BY STEPHEN NORTHCUTT

INCIDENT RESPONSE was tough enough when the challenge was getting to the bottom of *what* happened. For most organizations, when an incident is detected or suspected, gathering enough data to surmise what happened requires several hours of work piecing the logs together. The reason for this is simple: The majority of security appliances report what happened, but not who was behind the activity, historical information about that system or similar events.

But today, regulatory compliance requirements are built on a strong security rationale for tying identity to activity. And the reality is compliance is driving organizations to log management, and tying identity to activity helps you get a budget. The Sarbanes-Oxley Act, for example, calls for strict controls over access to financial records and that means it's critical to spot unauthorized activity by human beings.

"Organizations that perform log analysis are constantly reacting to events on the network while still trying to be proactive. When logs are tied to user identities, if there is a critical event, the user (or likely user) of the event can be quickly identified," says Ron Gula, chief technology officer at Tenable Network Security Inc. The user identity is a critical piece of information that shortens the analysis decision cycle and can help eliminate unimportant issues or offer a high confidence for events marked as actionable priorities. For example, he says, "you may have no idea how many login failures constitutes a probe, but if you were to graph all of the login failures by user, you may be able to spot patterns you didn't know you had to look for in the first place."

Knowing the "who" as well as the "what" is more than a benefit for investigators—it is absolutely essen-

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

tial to an organization's security/compliance program. Who made unauthorized access to customers' information databases? Who attempted to get root privileges on the domain server? Who cooked the financial records?

A classic compliance-related case of tying activity to identity comes from improper access of medical records. Some of these cases get a lot of press, such as when 13 UCLA Medical Center employees viewed Britney Spears' medical records in March 2008, but professionals in the field report that this is fairly common. The stolen information can be sold, not only to sensationalist tabloids—as in the case of celebrities such as Spears, Maria Shriver and George Clooney—but also to insurance firms. Needless to say, this has the potential to put medical institutions at risk for both lawsuits for breach of privacy or emotional distress and sanctions as a result of Health Insurance Portability and Accountability Act (HIPAA) violations. The Department of Health and Human Services has not done a good job of enforcing HIPAA compliance to date, but that's changing with the recent $2 million CVS Caremark Corp. fine and the Obama administration's emphasis on strong enforcement.

Tying user identity to activity is no easy task, but we're finally seeing the tools and developing the techniques that make it easier to track down the inadvertent or malicious offender.

TRACKING HUMAN EVENTS

Why is tying identity to activity so difficult? At the heart of the problem is the "skinny" or "thin" event report (the term was coined by Eric Fitzgerald of Microsoft). A computer, server or security appliance kicks out a report to syslog with the information it has at hand. It can't gather any other information about the event, state of the information, the person logged in and so forth. This results in logs that typically give:

- Time and date of the event.
- The IP address or possibly hostname(s) involved.
- The program reporting the event.
- Severity. Common values are fatal, severe, warning, info and debug. They're decided by the application and may or may not be accurate or useful.
- What happened from the reporting program's point of view.

Let's look at an example from Suhosin, a hardened version of the Hypertext Preprocessor (PHP):

Feb 24 09:56:43 [31321] ALERT - tried to register forbidden variable 'GLOBALS' through GET variables (attacker '41.204.211.204', file '/srv/www/live/sans/public_html/ne

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

wsletters/risk/index.php')

Each of those fields is useful, necessary, but not *sufficient*. What is missing? To do a complete analysis, we generally need "fat" data. That is, additional information that may not be available to the reporting program. Additional fields that are commonly needed to create actionable information from event data include:

- **When the event happened:** Feb 24 09:56:43 East Coast Time.
- **Who initiated the activity:** 41.204.211.204, according to nslookup, was assigned to webhost3.shadowrain.co.za at that time.
- **Whether this is a stimulus or a response:** It is a stimulus in this case, because webhost3 is initiating connections with www.sans.org.

If the event we have collected is a response, have we identified the stimulus—or, in this case, since it was a stimulus, did we respond?

What individuals and programs were involved? Ah, there is the rub; we know the IP address, we know the machine name, but we have no idea *who* in South Africa is behind this activity.

Did each event in the chain succeed or fail? This log entry is one of a series; webhost3 is probably running a scanner on www.sans.org. Hopefully, each probe fails.

Is this over, or is it ongoing? This probe has a start time and end time, so the event is over. We can surmise that only by looking at all the log entries from this IP address.

To do a complete analysis, we generally need 'fat' data. That is, additional information that may not be available to the reporting program.

For years, putting the data together has been the responsibility of the security analyst. We flag an event in syslog because it has a keyword we know indicates suspicious activity, such as *rejected, dropped* or *denied*. Then we take the information that we have from the syslog entry and begin to work both backward and forward to find other, related log events. Perhaps we have the IP address and need to consult the Dynamic Host Configuration Protocol table to determine the hostname and MAC address.

Next, we might go to the system or domain controller event logs to determine who was logged on. Did the person log on the first time he tried, or were there multiple attempts? Where did he log on from: Was it local, or

We don't have to tell you that enterprises face very real security risks. Or that the cost of regulatory compliance is a growing burden. Now, more than ever, IT security and operations teams must protect digital assets and ensure their availability with greater efficiency and smaller budgets.

ArcSight Logger provides a comprehensive monitoring platform for visibility into security risk, automation of audits, and operational service level agreements. With ArcSight, you'll get the big picture so you can avoid the big problem. After all, keeping a business running is the only way to run a business and log data is now a critical business asset.

ArcSight™

ArcSight Headquarters: 1-888-415-ARST

© 2009 ArcSight. All rights reserved.

Visit us at www.arcsight.com.

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

was it a remote logon? This type of network forensic analysis is doable, but it takes a long time and a complete knowledge of where to get the information.

Each event may take between 30 minutes and several hours to run to ground, and the work is somewhat tedious—especially when we have to work with data on different time zones. The high cost of manual correlation means many potential incidents are never investigated, and that means we fail to detect some events sometimes leading to devastating consequences, such as the spectacular Barings Bank and Société Générale frauds (see "Company Killers," below).

On the other hand, if we can use software to collect this information and display it in a meaningful way, an analyst can make a pretty good decision as to the severity of a log event in a matter of seconds, and our ability to detect and respond to potentially

COMPANY KILLERS

FAILURE TO DETECT and monitor new accounts or use of excessive privilege is a critical example of the need to tie activities to users and their roles. Consider these spectacular examples:

One such failure led to the 1995 demise of the venerable Barings Bank, the oldest merchant bank in the U.K. Account 8888 had been set up to cover up a mistake made by another team member, which led to a loss of $20,000. That is bad, but it gets worse. Nick Leeson then used this account to cover his own mounting losses as a day trader. When the smoke cleared, Leeson had lost $1.3 billion and ultimately destroyed the 233-year-old bank. All of Leeson's supervisors resigned (under pressure) or were terminated.

Jerome Kerviel, a trader with the French Société Générale bank, had access that allowed him to far exceed his authority in European stock index trades. He was able to make unauthorized transactions that led to a loss of somewhere in the neighborhood of €4.9 billion Euros (more than $7 billion).

In 2006, Kerviel began a series of "fake" trades mixed with large real trades, some of which actually exceeded the bank's capitalization. Somehow, he avoided normal controls based on timing and kept winning and losing trades in balance to give the appearance of insignificant impact to the bank's bottom line. A number of DLP-friendly tools as well as simple scripts can help detect new accounts. —S.N.

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

harmful events improves dramatically.

The keys will lie in our analysts' ability to look for changes in user behavior or attitude; report on segregation of duties, dual controls and access violations; and monitor activity and report on it. The good news is we're getting the tools that are beginning to make this practical.

TOOLS TRACK USERS

Since the stakes are so high and the need is so great to tie identity to activity, vendors are starting to deliver security solutions that can help. For instance, Sourcefire Real-time User Awareness (RUA) can be configured to send an alert any time a new user identity is detected, and this identity can be checked to see if it matches specific values. RUA does not have a feature to support pattern matching on new user identities.

Take the "Zippy" example. (This really happened. Though famous bank disasters are among the most serious account-related breaches, most security professionals with a couple of years of operational security experience have a security story involving a new or modified account.) The company was a lab in which usernames were all created from the first letter of the first name and the first six letters of the last name. A new account log entry for "zippy" caught our attention immediately. Either we had an employee named Zeke Ippy, or we had a problem.

If we had a list of all users, we could examine Zippy to see if a user had a first name starting with *Z* and a last name with the string *Ippy*. This can be done with a homegrown script using regular expressions, but over time we're seeing vendors deliver more regular expression capability so tools can be configured to support business logic.

Security architects can now depend on one or more of the logging and analysis industry categories of tools that can deliver "fat" data that ties user ID and other related information to event logs. These tools include:

- **Security information event managers** (SIEMs).
- **Log management devices**, which are primarily collectors of log files.
- **The central console of a security products company that offers a number of additional capabilities, not just logging and analysis.** For instance, both Tenable and Sourcefire Inc. have several security products and they report in to central consoles that strive to deliver fat data.

These products receive the thin events and create fat data for analysis. As the vendors continue to add functionality, these product categories tend to overlap and are less defined than they were a couple of

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

years ago. SIEMs, for example are now emphasizing their log management capabilities (or spinning off separate products) to capitalize on compliance-driven market demand.

One warning note: Information isn't always what it seems, so don't leap to obvious conclusions about what the data appears to be telling you.

And some log management products are developing more SIEM-like capabilities.

The flow goes like this: An event occurs, and a thin log file describing that event is created and sent to a collector. (A site may have one or more collectors.) The collector may store it as a raw, unaltered, pre-normalization event. The log event may also be stored with a matching cryptographic hash to prove it has not been tampered with.

If the site wants to do more than simply store the log, a copy of the log event is sent to an analysis engine. The log event can be evaluated by rules that are designed to either confirm and record a normal event has occurred, or to detect abnormal or bad events.

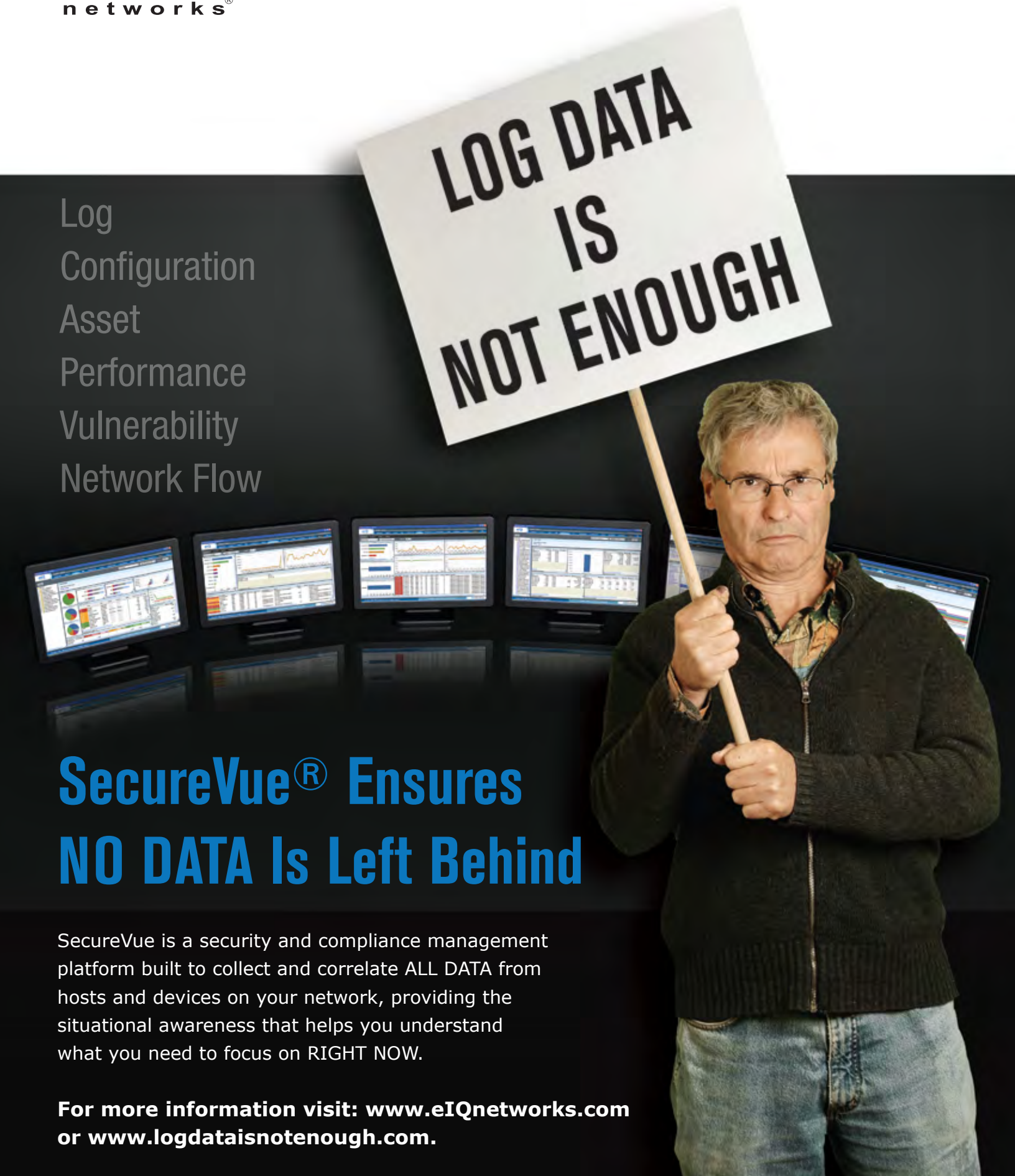
The rules may be based on regular expression technology to parse raw events, but sophisticated products normalize the logs, meaning raw data is broken down into component standardized fields and stored in a database where we may be able to correlate it with other information. Examples of the types of fields we might see in an event database include:

- Day of week
- Hour of day
- ID
- UTC time
- Local time
- Time zone
- PID
- OS name
- OS version
- Application version
- Hostname
- Host IP
- Host domain name
- MAC address
- Application reason
- Severity type

Once the data is normalized and in a database, our tools create a fat event by adding other referential data such as the history of that IP address/MAC address/system name; related vulnerability scan information; the history of similar events and login, identity or access data. This level of information can help an analyst make an informed decision much faster.

eIQ networks®

Security and Compliance Management. Redefined.



Log
Configuration
Asset
Performance
Vulnerability
Network Flow

SecureVue® Ensures NO DATA Is Left Behind

SecureVue is a security and compliance management platform built to collect and correlate ALL DATA from hosts and devices on your network, providing the situational awareness that helps you understand what you need to focus on RIGHT NOW.

For more information visit: www.eIQnetworks.com or www.logdataisnotenough.com.

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

One warning note: Information isn't always what it seems, so don't leap to obvious conclusions about what the data appears to be telling you (see "Caveat Analyst," below).

Since referential data is important, organizations that take log analysis seriously want as much data as they can get. One useful tool is the passive sniffer. It's typically placed near aggregation points such as the firewall to listen to and analyze traffic passing by. Passive sniffers are able to determine which operating sys-

CAVEAT ANALYST

ANY DATA MODELING professional will quickly warn you that referential data is powerful and helpful to analyze and classify an event, if and only if that information is correct and is correlated correctly. If you visualize yourself as the analyst making a decision on how to classify an event, then you can clearly see that if these types of fields are misleading or wrong, you could easily arrive at the wrong conclusion.

As an example, if you were an analyst for a university investigating a log event:

Feb 25 02:55:19 [16934] ALERT - configured request variable name length limit exceeded - dropped variable '___df9d5760ba1af926bed589c89//modules/My_eGallery/index_php?basepath' (attacker '10.12.82.4', file '/srv/www/live/college/public_html/new/CS423/grades/display.php'

The login information for IP address 10.12.82.4 yielded a student name of John Brown, and the event history showed past warnings for hacking-type behavior. One might immediately leap to a conclusion that the event was hacking-related and John Brown was at it again.

However, if any of that information was wrong, or correlated incorrectly, we might accuse John unfairly. What if John had plugged a wireless access point to the network connector in his dorm room and another student was using it while attempting to access the grades for his class? In fact, still another piece of referential data pointed out that John Brown was not even enrolled in CS 423. Why would you hack the grade server to change your grade for a class you aren't taking? —S.N.

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

tems are associated with particular addresses. They can also determine the version of software that's running. This is a huge step up from the basic firewall log of port and IP address. In addition, they can pinpoint the existence of vulnerabilities. Because they are creating their referential state tables by listening to traffic, passive sniffers are more current than static network inventory tables that are manually updated.

There is an open source example of a passive sniffer called pof, and Sourcefire and Tenable have commercial products—Sourcefire Real-time Network Awareness and Tenable Passive Vulnerability Scanner. Both companies offer a central console, sort of a mini-SIEM, to collect and manage the event data their various products create. It is still a manual step to identify the event in syslog and then query these vendor consoles, but it's a huge step up from everything being a manual task.

With sophisticated SIEMs, it is becoming increasingly possible to tie thin events to an identity in useful ways. It's been hard to do previously because the average person has multiple accounts—email, windows, virtual private network, intranet, app-specific IDs, instant messenger, etc.

While a SIEM can collect activity across these accounts, for the data to be actionable we must associate all of these accounts to a single person. Using ArcSight ESM, for example, an analyst selects one account ID as the user's unique ID. Then it is possible to map all the other accounts for that user to the unique ID. SIEMs such as ESM use several methods to connect log activity to identity, including utilizing agents and sending native operating system credentials.

With sophisticated SIEMs, it is becoming increasingly possible to tie thin events to an identity in useful ways. It's been hard to do previously because the average person has multiple accounts.

The only way to detect changes in behavior with technical controls is to tie identity to activity over a long enough period of time to establish a baseline. What if the amount of Web connection time to social media sites such as Twitter and Facebook suddenly increases? It might indicate that a user is less motivated to do his work assignments. Or a major increase in time on LinkedIn might indicate an employee establishing connections in advance of leaving the current organization. However, there is no way to detect an increase if we

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

do not have a baseline.

You can expect a SIEM that supports identity to activity mapping to be able to integrate with Active Directory or Network Directory. This means in addition to the accounts, you also get group or role information. Even though organizations have been slow to implement network access control at the enterprise level, the capability is built in to more and more software and appliances and it is starting to happen.

One exciting capability of tying identity to activity is to use historical activity data into ArcSight's activity profiling technology to generate statistical patterns and create new rules. For example, you might run the activity of the last 50 people who quit, to see what activities they did that those who are still there didn't do. Then if you see that activity, you can autoescalate a watch list and make sure the person doesn't leave with data, files, etc.

Or, in a down economy, if you have to announce that your organization can't issue bonuses one year, you might profile the activity of users before the announcement compared with after the announcement. A recent study by Ponemon Institute LLC (sponsored by Symantec Corp.) interviewed 945 adults in the U.S. who had been laid off, fired or changed jobs within the past year and found that more than half took company information with them when they left their former positions. The rationales for taking the data included help getting another job or starting their own business, or simple revenge. All of the participants in the survey had access to proprietary information, including customer data, employee information, financial reports, software tools and confidential business documents. The survey also found that just 15 percent of the companies examined the paper and/or electronic documents their former employees took when they left.

Every organization struggles ... to get real benefit from log analysis. Obviously, one big win is compliance. Most regulation bodies either require or strongly suggest log monitoring.

THE PAYOFF

Every organization struggles with the amount of effort it takes to get real benefit from log file analysis. Obviously, one big win is compliance. Most regulation bodies either require or strongly suggest log monitoring. The latest, the Consensus Audit

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

Guidelines, specifically refer to the importance of tying identity to activity. Two examples are enforcing controls on dormant accounts and continuously evaluating the need to know. In both cases, you have to know who the user is and what his role should be.

> Nothing succeeds like success. ... Logging, which is usually considered dull and boring work, becomes exciting.

With log monitoring, nothing succeeds like success. If a suspicious event occurs and an analyst takes the time to run it to ground and finds something significant, such as an employee collecting a list of customer personally identifiable information and sending it to a Hotmail account, people get excited. The damage can be minimized by rapid detection and response. Logging, which is usually considered dull and boring work, becomes exciting.

That is really one of the biggest benefits of tying identity to activity. Hits on the firewall, dropped spam messages, error conditions in a program and the amount of free disk space are all important, of course. Humans, though, do the craziest things, and when you add the human part of the equation to log events, it is a whole new ballgame. It wouldn't be surprising if the next few years yield a number of exciting security detection techniques as we correlate identity and get better at creating fat events for analysts to review. ■

Stephen Northcutt founded the GIAC certification and currently serves as president of the SANS Technology Institute, a postgraduate-level IT security college. He is author/co-author of *Computer Security Incident Handling: Step-by-Step, Intrusion Signatures and Analysis, Inside Network Perimeter Security (2nd Edition), IT Ethics Handbook: Right and Wrong for IT Professionals, SANS Security Essentials, SANS Security Leadership Essentials* and *Network Intrusion Detection (3rd Edition).*

UNLEASH LOG POWER

COMPLY, PROTECT & SAVE

AUTOMATE COMPLIANCE • SIMPLIFY SECURITY • UNIFY DATABASE SECURITY

LogLogic offers log-powered applications in compliance management, database activity monitoring and security event management that seamlessly integrate with our **Open Log Management Platform** and work together – delivering the industry's only one-stop shop for corporate security, IT efficiency and compliance management.

FOR MORE INFORMATION
www.loglogic.com

READ OUR LATEST REPORT FROM BLOOR
www.loglogic.com/bloor

loglogic®

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

No Log Management, No Regulatory Compliance

Regulatory compliance demands that you save, analyze and report on log data from key systems. Without automation, the operational burden will overwhelm you.

BY LINDA TUCCI

LOG MANAGEMENT WAS rarely a topic of conversation among senior IT managers until recently. What's elevated it from an obscure task practiced by admins to a strategic concern is regulatory compliance. Suddenly, enterprises need to demonstrate that they examine logs, not only in response to known incidents, but also as a matter of course—even daily review. In short, if you're not doing log management, you will not be compliant with a number of regulations, including the PCI DSS standard for payment card transactions.

In addition to their newfound importance, logs pose a strategic puzzle for IT. Logs have a long history of being used by systems and network admins for troubleshooting. More recently, they've become the evidence trail for security incidents. Add regulatory compliance in its many and varied forms to that requirements list, and selecting tools that meet your shop's mix of needs in all three arenas becomes a thoughtful exercise in balancing different constituencies. Fortunately, there are some basic needs that most shops will have with which you can start.

Take the case of Alliant Energy Corp. in Madison, Wis. About a year ago, Joe Kubesheski, who oversees strategy, security and records at Alliant, was looking for a log management tool to make sense of the voluminous data generated by the utility company's computer logs. The aim was not only to enhance the firm's layered security systems, but also to comply with log review requirements for the Sarbanes-Oxley Act and the cybersecurity standards recently mandated by the North American Electric Reliability Corp., the regulatory body for bulk electric systems. Until then, "everything was home-

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

grown," Kubesheski says.

Kubesheski, like IT pros at most shops, needed log management tools that would do three things:

- Provide protection on the security front;
- Remove the manual work of examining multiple logs on multiple devices; and
- Generate audit reports attesting that the company was doing the right things to meet its regulatory requirements.

Kubesheski's situation is one that many IT departments are wrestling with at the moment. Servers, routers, gateways, firewalls, databases, operating systems, applications—virtually anything worth noting in the computing environment—generate logs that constitute the golden record of access and action, if you can collect their data and verify that it has not been tampered with. That makes such tools important for compliance.

The profusion of security devices used to protect corporate networks (firewalls, intrusion protection devices, content-filtering devices) alone can create millions of records per day, says Trent Henry, an analyst who covers security and risk management at Midvale, Utah-based Burton Group Inc.

Manually monitoring, aggregating and correlating log information from across the infrastructure is time consuming, exacerbated by disparate logging standards and formats.

Senior IT mangers trying to either bring log management for compliance into their shops for the first time or build on existing troubleshooting or forensics use have several options:

- **Look at standalone log management packages.** These tend to emphasize very broad and diverse log aggregation capabilities and extensive reporting. Some are delivered as appliances, some as software that runs on generic servers.
- **Consider SIEM systems.** Security information and event management (SIEM) systems combine near-real time alerting of security incidents with longer time-frame log analysis capabilities.
- **Use larger security suites.** Many of the household-name large security software vendors have log management modules in their suites.
- **Narrow your log management requirements.**

Whichever way you wind up going, the most basic requirement is straightforward: You'll need a tool that can aggregate all the relevant log formats in your shop.

TAKE YOUR TIME

However, from a project perspective, you may not want to tackle everything at once.

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

Steve Eaton, information security manager for the city of Oklahoma City, strongly advises organizations to know their criteria for selection and "start small"—advice echoed by every user we interviewed. Oklahoma City started on its server farm, and "that's all we concentrated on, nothing else," Eaton says. Then came network devices and now he's adding clients.

"The thing is, you have got to keep your scope exactly to the criteria you want," Eaton says. "You can make it too big, and you'll always fail."

The same can be said for the second major selection point: reporting. While security pros and system admins may have some flex in what they need on the reporting front, various compliance standards mandate specific information. If you're not getting reports on those specifics, you're not getting the full benefit.

DOES LOG MANAGEMENT EQUAL PCI COMPLIANCE?

PASSING THE PCI DSS log management audits will help your organization by mitigating insider threats, identifying attacks from outside the enterprise and addressing application vulnerabilities, according to compliance expert Rebecca Herold.

The operative word is *meeting*. Logs require an organization to really understand its infrastructure.

In her report "PCI Compliance," Herold interviews auditor Ben Rothke on common problems qualified security assessors often find when performing PCI DSS reviews concerning insider threats. Among them are:

- **Completely misconfigured logs.**
- **Default log settings left unchanged.**
- **Wrong items being logged.**
- **No one reads the logs.**
- **No one follows up on log issues.**
- **Logs not correlated to any threats or vulnerabilities.**

Some of the logs organizations need in order to identify insider threats and be in compliance with PCI DSS include remote access logs, RADIUS authentication logs, file access logs, database logs, application logs, email logs, IP address logs, authentication logs and FTP server logs. —L.T.

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

Eaton, for example, went with Prism Microsystems Inc.'s EventTracker, a software-only, agent-optional framework that comes with around 100 preconfigured compliance reports. He says the package cost the city $93,000.

The shift from incident analysis to compliance, even just the security aspects of compliance, can be subtle. For example, LogLogic Inc. touts a compliance report it has for Payment Card Industry (PCI) standards that goes the extra step. Many log management systems generate daily firewall reports, but LogLogic's PCI Compliance Suite also generates reports on whether the firewall reports are actually being read by the appointed individuals daily, a requirement of PCI.

On the other hand, some shops have found that there's more to log management life than reports.

Kubesheski says he learned that the hard way, when Alliant initially chose a tool with good analyst recommendations and customer references that gushed about the appliance's nifty dashboard and its templates for numerous compliance standards.

"It had a lot of graphical reporting and, 'Oh look at that presentation!' but when it came right down to it, it couldn't deliver," Kubesheski says. His team worked with the vendor for several weeks to get a single system logging. A second system required a similar effort.

"It became apparent to us that it was going to take years to get the logging implemented, and we just didn't have that time," says Kubesheski, who declined to name the vendor.

> While security pros and system admins may have some flex in what they need on the reporting front, various compliance standards mandate specific information.

The second time around, Kubesheski bypassed the analyst rankings and "did more bottom-up research," conferring with security peers in the University of Wisconsin E-Business Consortium, a local business group. The vendor name that kept coming up was San Francisco-based Splunk Inc. The solution "didn't have the pretty charts and graphs, but it has a very customizable interface. And it just worked!" Kubesheski says.

"We had systems logging the week we installed and it, and nobody was complaining about calling the vendor a bunch of times," he says.

In addition to automation, size matters. Large, geographically distributed organizations should look for flexible

Log & Event Management

File Integrity Monitoring

Endpoint Protection

Analysis & Reporting

ONE INTEGRATED SOLUTION

available only from LogRhythm

LogRhythm®

COMPLY. SECURE. OPTIMIZE.

www.logrhythm.com

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

solutions with distributed collectors that can accommodate high data rates and large storage repositories, says Burton's Henry. Small organizations will want simple appliance-based solutions that can be deployed quickly and do not require sophisticated security skills.

For large companies, the task of managing logs to meet compliance objectives is compounded by the scale and complexity of IT infrastructures that span multiple locations and utilize numerous control products from many different vendors.

"Scalability and integration are key," says Bilhar (Bill) Mann, senior vice president, security management at CA Inc., whose CA Audit management solution is pitched to the enterprise market.

Mann says vendor offerings for log management and SIEM have evolved during the past five years, as the focus of SIEM tools has shifted from guarding against external threats—e.g., intercepting a virus and stopping its spread—to internal threats, such as an employee who might be inadvertently or maliciously accessing data he shouldn't. As the use cases have changed, so have the vendor offerings.

A TASK FOR SHOPS OF ALL SIZES

Many companies will find themselves with aspects of both large, enterprise shops and midmarket, or even small, shops. That was the case for retailer Wilsons Leather, which was driven by the need to meet PCI Data Security Standard (DSS).

"We needed to implement a system that would monitor and analyze log activity at both the store and corporate-office level and did not break our IT budget," says Frank Carrigan, manager of production control at the Minneapolis-based retailer, in an email. Wilsons operates 120 stores across 30 states.

"In the past, we relied on manually researching logs when we needed to, which was incredibly time-consuming, expensive and didn't necessarily give us the accuracy we needed to capture and correlate activities that were taking place on our network," Carrigan says.

The company looked at enterprise solutions such as Cisco Systems Inc.'s Security Monitoring, Analysis and Response System (MARS) and ArcSight, Carrigan says, but liked TriGeo Network Security Inc.'s product because the technology was designed for midmarket networks.

"The enterprise SIEM solutions were very cumbersome, expensive and required a significant time commitment. TriGeo's SIM was significantly less than the competition and was a very hands-off solution, meaning that we could dedicate IT resources to other projects while SIM kept an eye on our network activity," he says.

Wilsons Leather is still in the early

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

stages of using the TriGeo solution, Carrigan says, but the company likes its ability to generate compliance-specific reports—in particular the auditor-ready packaged PCI reports that detail what is happening on the Wilsons Leather network and what steps the retailer is taking to secure its business from internal and external threats. (TriGeo has a log archive and reporting function that is based on embedded technology from Splunk.) Wilsons handles Section 11.5 of PCI DSS, which requires the monitoring of critical file and applications for changes, with a homegrown tool.

Meanwhile, some large vendors are responding to the charge that their offerings are cumbersome and expensive. CA, whose SIEM offerings got

SEM, SIM AND SIEM: DECODING THE TOOLS

IT MANAGERS TRYING to pick tools for log management will quickly discover that many such tools have emerged from the security arena. If you're not familiar with that particular world, here's a primer:

■ **Security event management (SEM) tools pick up data from across the organization and use rule-based and algorithmic correlation to detect probable threats and policy violations (unauthorized access) that demand attention and might require immediate remediation. Sophisticated alarm bells, SEM tools alert operators in near-real time. The cherry-picked event data is typically stored for no more than 90 days, and sometimes for much less time.**

"SEM emerged to help correlate activities on firewalls and other traffic patterns on hosts, giving us much better intelligence about whether alerts were real, or not," says Trent Henry, an analyst at Burton Group Inc.

■ **Security information management (SIM), the quiet twin, is the keeper of security data for forensic purposes. SIM tools collect, store and protect ever-larger volumes of raw security information of hosts systems and applications for long periods of time, as increasingly is required by many compliance mandates.**

Slicing and dicing data is critical for real-time alerts, but normalized data can also gloss over details that might prove important in retrospect. Hence, there has been a shift to raw log storage, Henry says. (Indeed, vendor SenSage Inc. has developed proprietary storage capabilities in response to the demand.) —L.T.

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

rapped by consultancy Gartner Inc. for being hard to implement and not doing enough to support log management use cases, is addressing those issues with next month's launch of a new log management appliance engineered for ease of deployment, Mann says.

PCI DRIVING PRODUCT DEVELOPMENT

IT managers who go shopping for log management will discover that for vendors, regulatory compliance is the primary driver of the North American security and event management market, according to Gartner. And within the overall compliance field, PCI DSS is the regulation with probably the most explicit log monitoring requirements.

Vendors have realized that forensics and reporting requirements differ from real-time event management, and that many enterprises need both for compliance, according to Henry. PCI DSS, in particular, has fueled the amalgam of security information management (SIM) and security event management (SEM) (see "SEM, SIM and SIEM: Decoding the Tools," p. 17), by requiring near-real time event management and daily monitoring of logs (SEM) as well as the detailed periodic summary reports (SIM's province).

Vendors now sell both SIM and SEM offerings, under the rubric *SIEM*, loaded with packaged templates for compliance and regulatory mandates. But there are cautions: Many vendors tend to be weaker in the category that was not their specialty. Customers need to pay attention to whether the vendor meets both SIM and SEM

Vendors have realized that forensics and reporting requirements differ from real-time event management, and that many enterprises need both for compliance.

requirements, Henry adds, and indeed might be better off choosing one vendor for SEM functions and one for SIM. On the flip side, beware of vendor claims that compliance requires, for example, collection of 100% events from 100% sources, or alerting on all events from all sources.

Stamford, Conn.-based Gartner also makes this point in its May 2008 Magic Quadrant for security and event management technology, noting that the SIEM market comprises vendors with products that are "optimized for a specific use case, provide a mix of 'good enough' functions for the most common use cases, or are

HIPAA, PCI, SOX 404, NISPOM, FFIEC, GLBA, FISMA, FDCC, and more...

Meet the broadest set of compliance requirements

Reduce the cost of preparing for audits and remaining in compliance. Event Tracker provides:

- **Over 500 predefined auditor-ready reports**
- **Automated compliance with built-in workflows**
- **Efficient and secure event storage sealed with SHA-1**
- **Integrated change management**

PRISM MICROSYSTEMS

www.prismmicrosys.com/comply

Log and change management are recognized as critical strategies for improving overall security, increasing operational efficiency and, of course, meeting compliance requirements. Customers today are demanding not only full featured enterprise solutions, but ones that deliver a quick return on investment and a low total cost of ownership as well.

EventTracker is a market leading Security Information and Event Management solution that offers unique and powerful integrated log and change management functionality. With this unique combination EventTracker enables an organization to substantially increase security through a more robust and active defense in depth, achieve confident compliance with the latest regulatory requirements, and to increase the overall effectiveness of IT service delivery by reducing system and network downtime.

EventTracker is quick to implement, and easy to use and maintain. It represents the most solid choice for a log management solution for enterprises of all sizes.

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

broad and flexible but complex."

Gartner points to the example of Cisco and its MARS appliance, which Cisco markets as a component of its self-defending network strategy.

> "It's become very fashionable to say you're doing log management, because that is what is selling in the market."
>
> **—A.N. ANANTH, CEO**
> PrismMicrosystems Inc.

Indeed, the vendor has cornered the SIEM market by selling to network-focused buyers, the consultancy adds, wielding considerable influence on other SIEM vendors because of its large installed base. The MARS appliance, touted for its ease of deployment, delivers a potent combination of SEM, SIM and network behavior analysis capabilities.

The MARS appliance, priced on a per-unit-plus-annual-support basis, supports compliance monitoring for servers. But Gartner cautions that it "is not optimal" for companies, big or small, requiring highly customized audit/reporting functions, a point that Rand Wacker, senior product manager for Cisco's security products group, does not dispute.

SIM and SEM aren't the only software tools newly recast as log management.

"It's become very fashionable to say you're doing log management, because that is what is selling in the market, but a lot of these vendors come from different spaces," says A.N. Ananth, CEO of Prism Microsystems Inc., a log management software vendor that focuses heavily on the small and medium-sized business market. Vulnerability scanners, network anomaly detectors, correlation engines all go by the name of log management tools these days.

THE POLITICS OF LOG MANAGEMENT

SIM and SEM solutions don't work in a vacuum. Burton's analysts recommend that you get all players involved early on. The event streams come from security and network devices and applications. Reports get funneled to not only security admins, but also to the C-suite, auditors, legal counsel and even external parties such as regulators and judges. The SIEM technologies must meet the needs of all constituencies. And if you do business in Europe, you will need to educate yourself about privacy laws regarding what data you can and cannot collect before deploying SIEM tools there.

While compliance is the big driver for SIEM in the United States, about 40% of SIEM customers buy the technology for threat detection, says

↘ TYING LOG MANAGEMENT AND USER IDENTITY

↘ NO LOG MANAGEMENT, NO REGULATORY COMPLIANCE

Cisco's Wacker, citing Gartner.

That means "the compliance guys are writing the checks," he says, and security professionals are tasked with looking for a solution to meet the compliance need. "The security guys are looking to see what they can get out of this technology."

Don't discount the politics of automating log management, says Alliant's Kubesheski: "Any change represents risk. If I own an application or a server and you come to me and want to put something on it, or you want to access it, that represents a risk and the tendency will be to resist."

In many shops, the next log management tools installed will be the first. That was the case in Oklahoma City.

"What were we doing before that? Nothing—that was the problem," Eaton says. The logs were there, of course. Someone had to go from server to server and look at the log files, which could be stored for anywhere from a half day to two weeks, depending on the activity on that server.

Kubesheski agrees that if your colleagues are already implementing manual workarounds for logging, "you and your automation tool can be a blessing, and it's welcome to the neighborhood." ■

Linda Tucci is a senior news writer for SearchCIO.com. Write to her at ltucci@techtarget.com.

TechTarget®
The Technology Media ROI Experts

Log Management for Compliance
is produced by CIO/IT Strategy Media and Security Media, © 2009 by TechTarget.

MANAGING EDITOR
CIO/IT STRATEGY MEDIA GROUP
Jacqueline Biscobing

ART DIRECTOR
Linda Koury

CONTRIBUTING WRITER
Stephen Northcutt

SENIOR NEWS WRITER
CIO/IT STRATEGY MEDIA GROUP
Linda Tucci

VICE PRESIDENT, EDITORIAL
Mark Schlack

EDITORIAL DIRECTOR
SECURITY MEDIA GROUP
Kelley Damore

SENIOR TECHNOLOGY EDITOR
SECURITY MEDIA GROUP
Neil Roiter

SENIOR VICE PRESIDENT AND GROUP PUBLISHER
Andrew Briney

PUBLISHER, SALES
Jillian Coffin

For sales inquiries, please contact:
Stephanie Corby,
Senior Director of Product Management,
scorby@techtarget.com
(781) 657-1589.

- Alert Logic Log Manager Demo
- Satisfy Log Management Requirements on a Shoestring Budget
- Is Log Management the Killer App for Cloud Computing?

- ArcSight Helps Healthcare Company Become HIPAA Compliant
- HIPAA Compliance Achieved for Major Medical Center
- Healthcare Security Oversight for HIPAA Audit and Compliance

---

- Going Beyond Traditional Security Information and Event Management (SIEM) Solutions
- Bridging the Gap: Security, Operations & Compliance
- 10 Reasons Your Existing Security Information and Event Management Isn't Good Enough

---

- LogLogic Corporate Brochure
- Buy vs. Build vs. Outsource: What's the best log management strategy?

- LogRhythm Product Demo
- LogRhythm Product Review
- LogRhythm Product Review

- Meet the Broadest Set of Compliance Requirements with Integrated Log Management and Change Management