INFORMATION SECURITY®

ESSENTIAL GUIDE TO SIMs

Today security information management systems can be used for proactive risk management and business intelligence. We'll explain how this can be achieved.

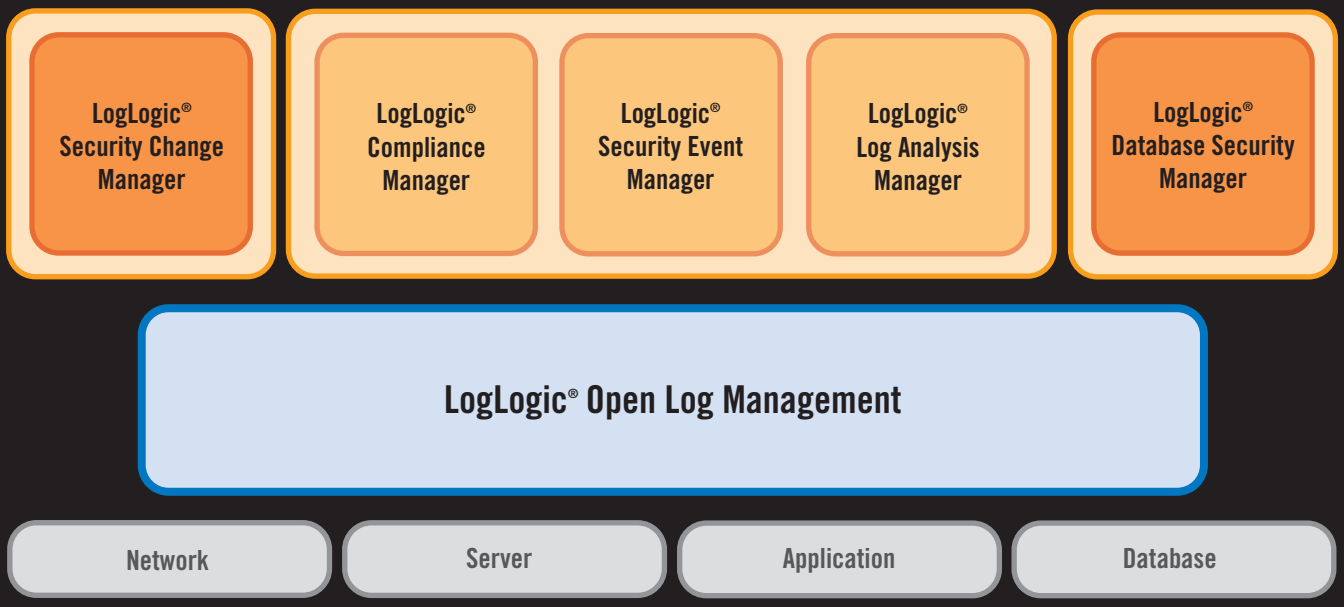
INSIDE

TechTarget
The Technology Media ROI Experts

INFOSECURITYMAG.COM

The most widely deployed and innovative Log and Security Event Management solutions in the market.

Gain Visibility and Control.



loglogic.com
blog.loglogic.com
info@loglogic.com

loglogic®

contents

ESSENTIAL GUIDE

SIMs

FEATURES

Worried the wrong people are getting at your corporate data?

Protect your data from the perimeter to the application layer to the end user.

Businesses today are under siege from threats originating from inside and outside the firewall. Targeted and zero-day attacks are constantly testing your security, while insider abuse is emerging as a widespread security issue. Compliance mandates that stress security are here to stay.

It is within this challenging environment that Security Information and Event Management (SIEM) has emerged as a critical component for ensuring defense in depth – from perimeter devices to the application layer.

Get the most relevant, actionable data from logs across your enterprise with:

- Event filtering, consolidation, and correlation
- Real time alerts
- Analysis, forensics and reporting
- Change monitoring and configuration control
- User activity monitoring including USB monitoring
- Automatic remediation

Event Tracker from Prism Microsystems is a unique SIEM solution that offers a powerful combination of Log and Change Management to protect crucial IT assets from a wide variety of attack vectors.

Get an in depth look of how EventTracker can help your organization increase security, maintain compliance and reduce IT operational overhead: http://www.prismmicrosys.com

PRISM MICROSYSTEMS

www.prismmicrosys.com

You've Come A Long Way Baby...

BY KELLEY DAMORE

While security information management systems have helped security pros detect intrusions and respond more quickly to incidents, the products are evolving into tools that can also help organizations with data protection and risk management.

CLOSE TO A DECADE AGO when SIMs first came to the market, they were primarily used by large enterprises hoping to get a big-picture view of their threat and security posture. SIMs solved a critical problem: They aggregated and correlated logs allowing IT security to prioritize security events. As a result, SIMs enabled security pros to detect and react more quickly to attempted penetrations and filter out the "noise" that they didn't necessarily need pay attention to. The downside was these log aggregators needed a lot of customization to be effective and they came with a hefty price tag.

Fast forward to today: SIMs have blossomed into a technology that offers mature aggregation, correlation and management at a more competitive price point.

And while the product was maturing, new regulations and industry standards were being developed. Organizations were forced to have a clear process for log inspection to meet these compliance mandates. Consequently, SIMs now provides deeper compliance intelligence and reporting, better visualization and improved incident response. Some organizations are even looking at SIMs as a method to create proactive risk management and business intelligence.

And it doesn't stop there. Today, SIMs vendors are marrying the technology with directories. By doing so, SIMs will be able to authenticate and authorize users based on pre-defined rules around roles and entitlements; past patterns of activity will help determine whether a particular user is indeed who they say they are. SIMs can also help with provisioning. For instance a successful login from a deprovisioned user could help prevent data leakage and close an audit loop.

Vendors are also looking to SIMs to help with transaction integrity, specifically around fraud prevention and enterprise applications. SIMs would integrate with existing third-party fraud prevention tools and based on models of risk activity, monitor transactions for fraudulent patterns. Similarly, SIMs vendors are writing connectors to enterprise apps such as SAP, Oracle and various flavors of CRM to begin watching those types of transactions.

As we all know technology does not stand still and SIMs will need to adjust to the highly complex and challenging IT landscape of tomorrow. For instance, as cloud

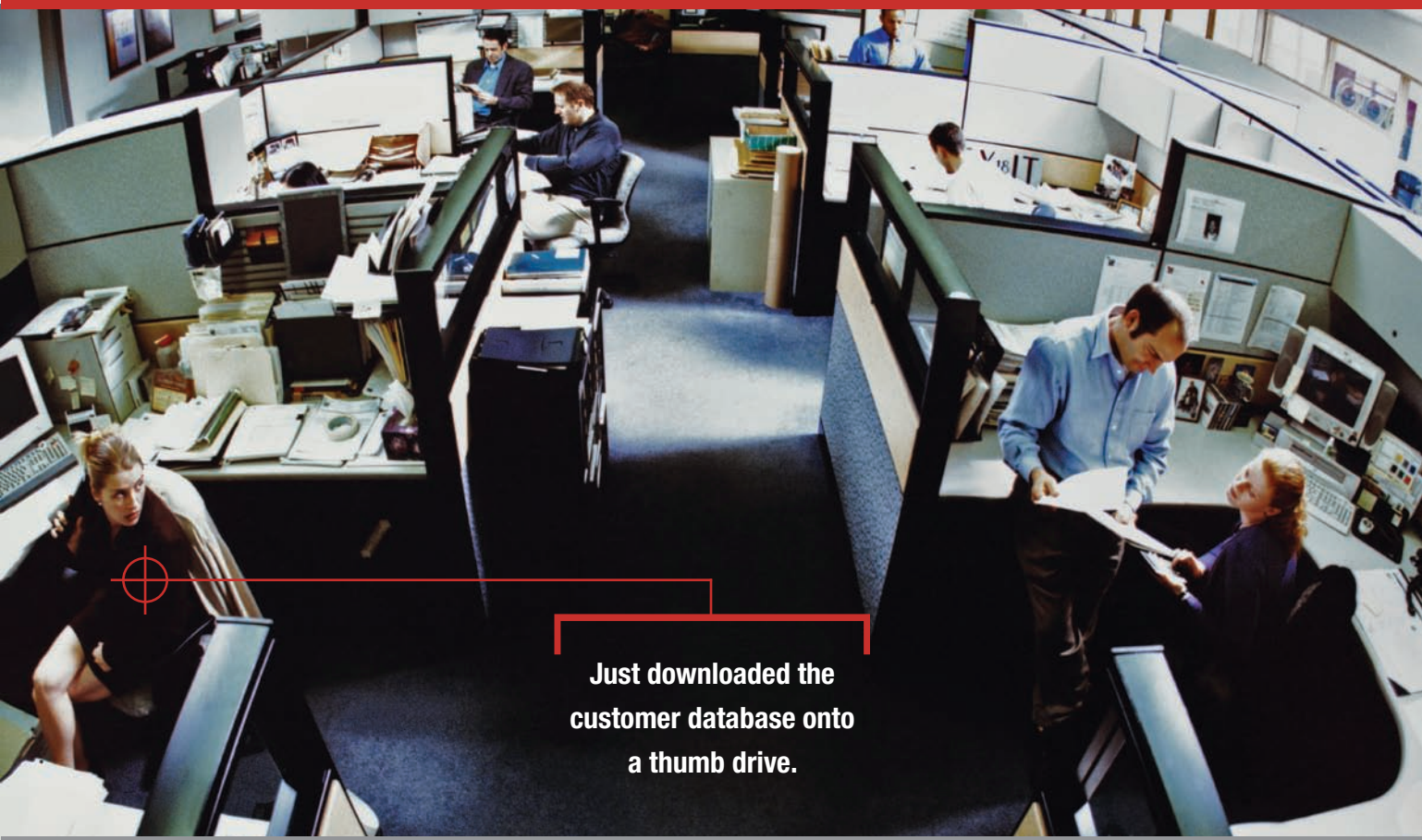
computing becomes more pervasive, SIMs could monitor who is accessing sensitive information. SIMs may also be able to help manage employees and third parties, and monitor what they have permission to access and see. Another problem that SIMs may be able to help with is controlling mobile devices.

This Essential Guide to SIMs gives you some forward-looking and practical information as you investigate the opportunities and challenges of implementing SIMs within your organization. We hope you find it useful.›

Kelley Damore is the Editorial Director of the Security Media Group at TechTarget.

Find the cybercriminal.

(Never mind. ArcSight Logger already did.)



Stop cybercriminals, enforce compliance and protect your company's data with ArcSight Logger 4.

Learn more at www.arcsight.com/logger.

ArcSight™

THE STATE OF SIMs

Today mature security information management systems do more than log aggregation and correlation.

BY DIANA KELLEY

IT'S BEEN ALMOST A DECADE since security information management (SIM) systems were introduced. During that time, SIM products have evolved from relatively immature log aggregation products that were too expensive for all but the largest enterprises, to mature aggregation and management solutions that provide network and security insight to organizations of all sizes. But SIM solutions aren't done evolving.

As SIM use increases, enterprises are asking vendors for additional functionality, including deeper compliance intelligence and reporting, better visualization, improved incident response and integration of identity awareness. Many companies are leveraging SIMs to increase efficiency and cost savings in their security programs. And some businesses are going beyond security awareness and exploring how the comprehensive view of network and user activity that is collected and parsed by the SIM can be used for proactive risk management and business intelligence.

A CONFUSING BEGINNING

Early on, the SIM space suffered from a number of identity crises. To start with, there wasn't even consensus about what to call the products, and vendors used a variety of acronyms. Part of the problem stemmed from the fact that vendors and their customers approach functionality in different ways. For some, the great promise of SIM was bi-directional management of heterogeneous security devices (also known as MoM—the manager of managers). Others saw the consoles as a hyper-intelligent processor of complex correlation rules and predictive attack analysis. And some enterprises found simple, but effective, centralized log aggregation to be the core business justification for installation.

In early deployments, SIMs were installed in large enterprises and used primarily as log aggregation tools. Although some enterprises spent a significant amount of time and resources crafting custom correlation rules, most gained the greatest value from the ability to collect critical log information from multiple sites and sources in a single, searchable repository using pre-set rules and templates for alerts management. But the landscape changed and the products matured. SIMs became more user friendly and compliance aware. New offerings emerged that were scaled for small and midmarket companies [http://searchmidmarketsecurity.techtarget.com/tip/0,289483,sid198_gci1354209,00.html]. And most SIM users realized that, although deeply complex correlation rules were not always cost-effective, there were many efficiencies to be gleaned from the powerful log aggregation and reporting that enterprise-ready SIM solutions offered.

MEETING COMPLIANCE DEMANDS

Compliance requirements for protection of personal information and industry standards such as PCI DSS drove many initial SIM purchases and still do today. Trent Henry, principal analyst for research firm Burton Group, says, "Companies that were only monitoring the perimeter devices are moving toward complete log and event aggregation" to meet audit and regulatory requirements. SIM solutions are, at heart, log aggregation engines because the information and events need to be collected and parsed at a central point before prioritized event reporting or correlation rules can be applied.

Compliance requirements for protection of personal information and industry standards such as PCI DSS drove many initial SIM purchases and still do today.

Most companies using SIM report that centralized log aggregation is the baseline function; without it, the product would not even be installed [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1257083,00.html]. But centralized logs and reporting comprise only a portion of the overall compliance landscape. For example, while requirement 10 of PCI explicitly mandates log aggregation, other portions of PCI could be supported with SIM such as the ability to report on who accessed data stores of credit card numbers.

Similarly, properly tuned SIMs can provide reporting and alerting that ease compliance with privacy related regulations such as HIPAA and the new Nevada and upcoming Massachusetts protection standards for personal information.

Section 17.04 of the Massachusetts law requires secure authentication, secure access control to records, and periodic reviews of audit trails. While log aggregation helps with the audit trail reviews by centralizing the information, a SIM tuned to monitor for access control or one that is integrated with a database monitoring tool from vendors such as Application Security, Guardium or IPLocks, will provide deeper coverage for compliance monitoring and reporting.

SIM tools come with a variety of templates for compliance reporting and basic correlation rules for alerting on access violations. Organizations can use the default

Where are you on the curve?

SIM has evolved from a security only solution sitting on the periphery of network operations to an integrated part of the business. Here's a look at the different stages of implementation for organizations.

- **ENCOMPASSING WHOLE CURVE:** Transformational usage can occur when business process information captured by the SIM is used by security and operational personnel to assess process efficacy and identify areas for improvement.
- **HIGH END:** A proactive risk prevention tool and, in some cases, a business process transformation enabler.
- **MIDDLE:** Expanded SIM monitoring to multiple services and devices, incorporating the solution into a compliance program, and implementing both risk and business related rules, reports, and alerts.
- **BEGINNING:** Use SIM for log aggregation from security devices and a few critical systems.

One of the most interesting aspects of how SIM has evolved is the move from a security only solution sitting on the periphery of network operations to an integrated part of the business. While this trend is a natural evolution, it is not yet the norm. Companies that are at the beginning of the curve are using SIM only for log aggregation from security devices and a few critical systems. In the middle of the curve are companies that have expanded SIM monitoring to multiple services and devices, incorporating the solution into their compliance program, and implementing both risk and business related rules, reports and alerts. At the other end of the curve are the organizations that see SIM as a proactive risk prevention tool and, in some cases, a business process transformation enabler. Transformational usage can occur when business process information captured by the SIM is used by security and operational personnel to assess process efficacy and identify areas for improvement.›

–DIANA KELLEY

templates and reports or customize them as needed. Alberto Cardona, CISO for a large New York newspaper that uses a SIM, says the newspaper was able to use the templates included with the SIM, for the most part, "out of the box." Although some customization was required, it wasn't labor intensive and was mostly due to legacy applications with older login mechanisms, he adds.

Now that companies have learned to "walk" through compliance with SIM log aggregation, many of them are breaking into a run and integrating the solutions into a broader compliance program.

CLOSING THE RESPONSE WINDOW

Enterprises also are using SIMs to get a better view of their security posture and to improve their incident response. What separates a security event from a user error can be difficult to assess in a limited-view analysis, but becomes clear when understanding the context of the larger system as a whole. A SIM consolidates information from multiple sources including applications, servers, security and perimeter devices, making it possible to determine root causes.

Enterprises also are using SIMs to get a better view of their security posture and to improve their incident response.

At the newspaper, the layered data inputs are used to hone responses. As Cardona explains, in a narrow view, an event such as a spike in CPU usage on a server, the root cause might not be apparent. An administrator could attribute the usage increase to a bad patch while an application developer might fear it was a memory leak in the code written for the application running on the server. And a security administrator might assume the spike was caused by a malicious denial-of-service (DoS) attack. With the consolidated view provided by the SIM, an administrator could see that the application log and event data is normal, no recent patches have been applied, and the IDS or IPS is reporting a huge increase in attempted connections to the server, making it likely that the company is experiencing a DoS.

John Menezes, president and CEO of Cyberklix, a managed security service provider (MSSP), calls this consolidation "the holistic view of security." [http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1327864,00.html] Burton Group's Henry agrees, observing that many Burton customers are tweaking their SIMs to get better value out of their IDSes and other security devices. At Ontario, Canada-based Cyberklix, vulnerability management tool information is cross-checked with IDS or IPS events at the SIM console. For example, while an IDS or IPS may report that an exploit is being launched against a target, the vulnerability manager reports "show the target device was patched, so the IDS scan information is a false positive," Menezes says

Of course there's always a possible downside to too much information. And enterprises that suffered through multiyear roll-outs of SIMs slowed by extremely complex correlation rules may read the above with a world-weary sigh. To be effective with a holistic approach, be selective with what is monitored. Start slowly, focus on the highest priority systems, and a limited number rules. Grow the rule-set only when the processes are well understood and the existing rules are functioning smoothly.

In addition to helping sort out the root case of an event, organizations are using SIMs

Endace Power to See All.

SIM systems that you can rely on 100% run on Endace.

The only platform that delivers 100% packet capture, on any network, at any speed up to 40 Gb/s.

For more information : www.endace.com

endace
power to see all

to proactively stop attacks or fix improper changes to systems. At TruMark Financial Credit Union in Pennsylvania, Matt Roedell, vice president of information security and infrastructure, has configured a SIM to monitor and alert on configuration changes such as add a user, add a firewall, and AD [Active Directory] reassignment. The SIM automatically emails the change control committee inbox when a change is made. If any process or service works improperly after the change occurs, the team "can immediately call who made the change and ask them what they did and have them back it out," he says.

WHAT'S IDENTITY GOT TO DO WITH IT?

Managing events and logs from security devices is common practice in the SIM world. But what about identity related information? [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1351973,00.html] Login information is closely tied to security and risk and SIMs have correlation engines that could use this information to improve the company's security posture. Henry calls identity information the "classic example" of SIM intelligence gathered from devices that are not deployed for security only purposes such as firewalls, vulnerability management, and IDS. Vendors with robust identity management offerings, such as CA, IBM, and Novell, have focused on this issue, offering close integration between their identity management solutions and SIM products.

Companies are reporting that some or all logins to sensitive servers and applications are being monitored by a SIM.

With this integration, a SIM could report a successful login, alerting a company that thought the user was de-provisioned, according to Henry. The login itself is significant but this could also trigger a call to the identity management team to ascertain whether the de-provisioning system is malfunctioning or perhaps not configured to properly deactivate all of a user's accounts. In this way, a SIM could help close the audit loop for identity management systems that don't have mechanisms for monitoring themselves or function as a separate channel for audit monitoring and control.

Companies are reporting that some or all logins to sensitive servers and applications are being monitored by a SIM. This information is used for data protection purposes, ensuring that only legitimate, approved users are accessing protected information, and for compliance reporting of the access. For one business, a SIM helped flag a problem with a new password policy. An auditor had recommended a very strict policy with more than eight characters, no dictionary words, and a password time-to-live (TTL) of two weeks. Because the company had a single sign-on (SSO) solution in place, users only needed to remember one password, but with the new rules, even that one password was too much. Lock-outs shot up and the help desk was overwhelmed with reset calls. While help desk records would have eventually shown the new policy was causing problems with users, the SIM alerts indicated a problem within a couple of days.

At the newspaper, Cardona saw a corollary usage. By using the SIM to monitor key systems, each with a different password, and correlating them with logs, alerts, lock outs and help desk calls, the security team was able to use this information as business justification for investing in an SSO solution.

Perhaps one of the more complex identity options for integrating a SIM with identity

management is to create comprehensive user activity profiles that follow a user's activities through the network. This information can be used to track anomalies and possible misuse. An example of this is limiting access to a database using location information. The database administrators may have access to the database from inside the data center or using an approved remote access solution, such as an IPSec VPN, from an approved remote device. If access is granted to a legitimate user from an unapproved network or device, the SIM could issue an alert or possibly trigger an automatic shutdown of the session through communication with network management systems. Though these usage scenarios require more integration and customization work, the pay-offs could be significant depending on your business.

CONTINUOUS IMPROVEMENT

Better integration with operational consoles is one feature of the SIM evolution *[see chart, p. 9]*. The days of a separate SOC and NOC may be numbered for many companies that simply can't afford the costs. But the importance of the security information doesn't disappear. And, for some entities, not having some sort of separate audit channel and monitoring solution in place is not an option. To make this work in the enterprise, operation teams are consuming the information from the SIM console into the large meta-consoles such as HP OpenView, IBM's Tivoli, and CA's NSM (formerly Unicenter). The security team still maintains administrative control of the SIM, but the operations team can use the information as well. For example, if a slowdown is detected in an area of the network, the operations team may discover that the root cause is a security event such as a DoS attack or a bandwidth-intensive worm.

Menezes says the architecture of the SIM solution can be a contributing factor to whether or not the SIM can be more widely deployed throughout the infrastructure. In his experience, agent-based solutions created "all sorts of political issues with whether the tool could be installed." Also, he found that the administrator uninstalled the agent if anything unexpected happened on the device. Agent-based solutions, on the other hand, may be preferred by companies that want a separate monitor agent on a server.

To make a SIM more valuable to the business, Cardona advises answering some questions up front: What is your core requirement? What is the main objective that you want to accomplish? What reports will you generate and give to the CIO and other stakeholders? And how can you make this information valuable to them? Armed with the knowledge of what information will be of value to the stakeholders, security administrators can customize the standard reports that come with a SIM for their own business needs.

Out of the box, a SIM delivers meaningful solutions that satisfy auditors, Roedell at TruMark says. But to get business value from a SIM, he adds, "You have to spend time to tailor it to your business and your network. Risk mitigation strategies are only effective when they're implemented and managed by IT professionals who understand your business." In SIM parlance, that can mean identifying when a password policy has gone bad, finding the root cause of a CPU usage spike, or even justifying additional hardware resources because a critical server is overloaded.

Long-term, SIM alerts can be quantified into metrics-based assessments. Again, this is a fairly advanced use of the tools, but it is one that some end-users are exploring and a few are already adopting. At TruMark, using a SIM means "residual risk scores will be

reduced," Roedell says. To make that matter to the business, security experts will "have to do a better job showing what they're going to do and how these tools are going to reduce risk in a dollars and cents way," he says. For another organization, repetitive alert suppression rules reduced redundancy so what was effectively a full-time job for three people was reduced to a part-time job for one.

EXPANDED OPPORTUNITIES

For many, SIM is the Holy Grail for log aggregation compliance, but a number are looking beyond compliance to business improvement. SIM can be "used as a foundation for making the organization more compliant while being leveraged in the long run for continuous improvement," Menezes says. Compliance is a starting point for SIM use but by reviewing the information captured by the SIM, companies can begin to make process improvements such as understanding which devices or areas of the network are more prone to malware attacks and then shoring up controls or fine-tuning a password policy to reduce help-desk calls, he says. Cardona echoes this view: "Start with compliance but tune the SIM in the long run to make it a tool for business enablement."

It's been an interesting decade for SIM. SIM has evolved from the confusion of the early days, through the toehold of log aggregation for compliance, to its current emerging usage as a risk and business tool. If you're using SIM for basic log aggregation and you're happy with it, that's great. If you think it can do more, you're right. Some of your peers are expanding usage for increased business intelligence and better risk awareness.

Diana Kelley is founder and partner at consulting firm SecurityCurve [http://www.securitycurve.com/]. She has worked in computer and network security for 19 years. Send comments on this article to feedback@infosecuritymag.com.

Marrying LOG & IDENTITY MANAGEMENT

Tying user identity and activity is no easy task but tools and techniques are now available to track a malicious offender.

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 piece together what happened requires hours of log analysis. The reason 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. The reality is that compliance is driving organizations to do log management [http://searchsecurity.techtarget.com/magazineFeature/-0,296894,sid14_gci1274439,00.html], and tying identity to activity helps get budget. SOX, 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," says Ron Gula, CTO Tenable Security. "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." User identity is a critical piece of infor-

mation that shortens the analysis decision cycle and helps eliminate unimportant issues or gives us a high confidence for the events we mark 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 a 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 essential to an organization's security and compliance programs. You need to know: Who gained unauthorized access to customer information databases? Who attempted to get root privileges on the domain server? Who cooked the financial records?

A classic compliance-related example of tying activity to identity comes from cases where the medical records of celebrities were improperly accessed. Some of these cases, such as Britney Spears' at UCLA Medical Center [13 employees improperly accessed her records in March 2008], get a lot of press. But professionals in the field report 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 of both lawsuits for breach of privacy or emotional distress, and HIPAA compliance 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 fine [http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1330457,00.html] and the Obama Administration's emphasis on strong enforcement.

Tying user identity or activity is no easy task, but we're finally seeing the tools and developing the techniques that make tracking 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 (a term 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 information, the person logged in and so forth. You're left with logs that typically report:

- Time and date of the event.
- IP Address or possibly hostname(s) involved.
- The program reporting the event.
- Severity. Common values are Fatal, Severe, Warning, Info, Debug, which are 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) [http://www.hardened-php.net/suhosin/]:

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/newsletters/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—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 Eastern 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 of the probes fails.
- Has the event ended or is it ongoing? This probe has a start time and end time, so the event is over. We can only surmise that by looking at all the log entries from this IP address.

For years, putting the data together has been the responsibility of the security analyst. We flag an event in syslog because it has a key word 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 backward and forward to find other related log events. Perhaps we have the IP address and need to consult the DHCP table to determine the host name and MAC address.

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.

Next, we might go to the system or domain controller event logs to determine who was logged on. Did they log on the first time they tried, or were there multiple attempts? Where did they log on from: Were they local, or was it a remote log on? This type of network forensics analysis is possible, 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 Societe General frauds *(see "Company Killers," p. 19)*.

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

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 that we're getting the tools that are beginning to make this practical.

Tools Track Users

Since the stakes are so high and the need to tie identity to activity is so great, 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.

Take the "Zippy" example. (This really happened. Though famous bank disasters are among the most serious account-related breaches, most security professionals

LESSONS LEARNED

Company Killers

Account abuse did banks in.

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 UK. 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 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 Societe Generale 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 US).

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 managed to keep winning, and losing, trades in balance to give the appearance of insignificant impact to the bottom line. A number of DLP-friendly tools as well as simple scripts can help us detect new accounts.›

–STEPHEN NORTHCUTT

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 user names were 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 any user had a first name starting with "Z" and a last name with the string "Ippy." This can be done with a home-grown script using regular expressions, but over time, we're seeing vendors deliver more regular-expression capability so that tools can be configured to support business logic.

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

- Security information event managers (SIEMs).

DECISIONS

Caveat Analyst

Your conclusions are only as good as your data.

ANY DATA MODELING professional will quickly warn you that referential data is powerful and helpful to analyze and classify an event, but 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 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 showed 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?

–STEPHEN NORTHCUTT

- Log management devices, which are primarily collectors of log files.
- Centralized consoles that offer a number of additional capabilities, not just logging and analysis. For example, Tenable and Sourcefire have several security products, which report in to central consoles and 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 years ago. SIEMs, for example are now emphasizing their log management capabilities (or spinning off separate products) to capitalize on compliance-driven market demand. 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 the 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 normal events, or designed 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. Normalizing breaks down raw data into component standardized fields that are stored in a database, so 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, host name, host IP, host domain name, MAC address, application reason and severity type.

The rules may be based on regular expression technology to parse raw events, but sophisticated products normalize the logs.

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; history of similar event sand login, identity or access data. This level of information will help the analyst make an informed decision much faster. 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," p. 20)*.

Since referential data is important, organizations that take log analysis seriously want as much of it as they can get. One useful tool is the passive sniffer. These tools are typically placed near aggregation points such as the firewall and listen to and analyze the traffic passing by. They are able to determine what operating systems are associated with particular addresses. They also can determine the version of software that is 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, they are more current than static network inventory tables that are manually updated.

There is an open-source example called P0f [http://lcamtuf.coredump.cx/p0f.shtml], and Sourcefire and Tenable Security have commercial products—Sourcefire Real-time Network Awareness (RNA) 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. Identifying the event in syslog and querying these vendor consoles is still a manual process, but it's a huge step up from everything being manual.

With sophisticated SIEMs, it is becoming increasingly possible to tie thin events to an identity in useful ways. It's been difficult to do previously because the average person has multiple accounts—email, Windows, VPN, intranet, app-specific IDs, IM, etc. While a SIEM can collect activity across these accounts, we must associate all of these accounts to a single person for the data to be actionable. 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 agents and sending native operating system credentials.

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 such as Twitter and Facebook [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1349703,00.html] suddenly increases? It might indicate that user is wasting time instead of working. Or, a major increase in time on LinkedIn might indicate establishing connections in advance of leaving the current organization. However, there is no way to detect an increase if we do not have a baseline.

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.

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 (NAC) [http://searchmidmarketsecurity.techtarget.com/tip/0,289483,sid198_gci1351628,00.html] 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 compare and contrast their activities to those who haven't quit. When that activity is spotted again, you can auto-escalate a watchlist and make sure the person doesn't leave with data.

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 to after the announcement. A recent study by The Ponemon Institute

(sponsored by Symantec) interviewed 945 U.S. adults who had been laid-off, fired, or changed jobs within the last year and found that more than half took company information with them when they left [http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1348948,00.html].

The rationale for taking the data included help getting another job, help 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 with them when they left."

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 regulatory bodies either require or strongly suggest log monitoring. The Consensus Audit Guidelines [www.sans.org/cag] specifically refers to the importance of tying identity to activity. Two examples are enforcing controls on dormant accounts and continuously evaluating need to know. In both cases, you have to know who the user is and what his role should be.

With log monitoring, nothing succeeds like success. Think of the value of an analyst who takes the time to run a suspicious event into the ground and finds something significant, such as an employee collecting a list of customer personally identifiable information and sending it to his Hotmail account. 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, spam messages dropped, error conditions in a program, 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 ball game. 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 post graduate level IT Security College. He is author/coauthor of Incident Handling Step-by-Step, Intrusion Signatures and Analysis, Inside Network Perimeter Security 2nd Edition, IT Ethics Handbook, SANS Security Essentials, SANS Security Leadership Essentials *and* Network Intrusion Detection 3rd edition. *Send comments on this article to feedback@infosecuritymag.com.*

Is your SIEM delivering value?

Is it **SCALING** with your event data growth and long-term storage requirements?

Is it easy to write new **QUERIES**?

Is it easy to add new event **SOURCES** without rebuilding your reports and dashboards?

Does it support software, appliance and virtual machine **FORM FACTORS**?

Ineffective SIEM products are wasting your budget and increasing your risk.

SenSage can help.

More than 400 enterprises and government agencies have adopted SenSage to reduce security, fraud and compliance risks.

SenSage delivers real-time monitoring, long term archiving, forensic investigations and integrated compliance reporting, all in one solution that scales to meet your needs.

Get more value out of your SIEM. Today's cyber-threats, regulations and economic pressure demand it.

http://www.sensage.com/SIEM

SENSAGE

Combining NetFlow and SIMs

Integrating the two tools can help administrators more effectively respond to the network's highest-priority problems.

BY TOM BOWERS

FROM HUMBLE BEGINNINGS, NetFlow has today become a commonly used network monitoring tool. Alone, NetFlow analysis provides powerful management capabilities. When combined with security information and event management systems (SIMs) and correlated with data from other devices and layers, NetFlow becomes indispensable.

What is NetFlow?

Initially, network monitoring was performed with the Simple Network Monitoring Protocol (SNMP). Although SNMP eases capacity planning, it does little to characterize traffic applications, which are essential for understanding how well the network supports the business. Port flows were monitored, but newer applications dynamically select new ports for each session and thus were inadequate. What was needed was a more granular picture of bandwidth usage. The arrival of NetFlow allowed network administrators to characterize and analyze network traffic flows via UDP.

NetFlow analysis is now built into most enterprise-class switches and routers, and has become a primary network accounting and anomaly-detection technology in the industry. NetFlow essentially answers the following questions about network traffic: Who, what, when, where, and how? Each flow is a collection of packets characterized by flow-specific information, such as the source and destination IP addresses, as well as port information. The packets in a particular flow are counted and reported via a collector. The collector classifies all the traffic collected on a network, based on its source, destination and application. The resultant reports allow an administrator to view the flows as prioritized by bandwidth utilization. Bandwidth may be broken down even further into smaller subclassifications such as applications, users and servers.

Network behavior anomaly detection

NetFlow creates a behavior-based system that profiles the typical connections made between devices. This creates a baseline that may be as granular as hourly or daily. After the network is "learned," any variation that is considered anomalous may be acted on.

How SIM uses NetFlow data

NetFlow data is aggregated with data from other sources, such as IPSes, firewalls, VPNs, the application layer and, in some systems, identity data. This data is then correlated using several techniques including:

- Rules-based
- Statistical
- Historical
- Vulnerability

These correlations are conducted per monitoring site and across sites as well.

This correlated data is prioritized based on traffic flows, attacks within a site or attacks across sites. A risk analysis is then performed to discover which attack has the greatest potential for harm to the enterprise. Ideally this risk assessment will include attacks on at least:

- Business processes
- Network processes
- Site versus enterprise

Finally, this data is provided to a reporting engine. Graphs and charts are provided by a series of dashboards and text-based reports. The newest generation of security information management systems allows for visualization techniques with drill-down capability.

Advantages of SIM/NetFlow together

One of the clearest gains in combining NetFlow with SIMs is the improvement in security insight and response. With real-time NetFlow views, priority-based alerts can be created. Threats can also be correlated with other attack vectors, so that the highest-priority problems are seen first and administrators can respond accordingly.

This combination now allows us to view threats across an enterprise to spot things like salami attacks, or a series of small attacks with a larger purpose, which are still used in the hacker community today. Automated vulnerability assessment tools use this technique to evade IPS devices. When you collect NetFlow data from across the enterprise and correlate it, you can spot this type of stealth attack more readily.

One of the most interesting advantages gained is the ability to see adverse events in one flow with its associated flows. This is possible because the security information management system correlates NetFlow data from across the enterprise, allowing an administrator to view both the attack flow and those flows supporting the attack.

Freeware tools

If you do not have an SIM installed and you would like to "see" NetFlow in action, there are several tools available to gain added insight. Sourceforge.net is an open source community with some outstanding open source (freeware) security tools available. Sourceforge.net's NetFlow listings currently offer 44 tools to view, manipulate and use NetFlow data. Two of the most popular are:

- Extreme Happy NetFlow Tool [http://sourceforge.net/projects/ehnt/]
- NFDUMP—NetFlow processing tool [http://sourceforge.net/projects/nfdump/]

Since NetFlow provides real-time views of bandwidth use and application and user priorities, it has become a powerful tool for security professionals. The faster this data can be turned into useful information, the faster security pros can respond to incidents and minimize the impact on an organization's business. When combined with security information and event management systems, NetFlow can reveal previously hidden threats happening across an enterprise. NetFlow and SIM is like peanut butter and jelly: they simply belong together.

Tom Bowers, managing director of security think tank and industry analyst firm Security Constructs, holds the CISSP, PMP and Certified Ethical Hacker certifications, and is a well-known expert on the topics of data leakage prevention, global enterprise information security architecture and ethical hacking. His areas of expertise include aligning business needs with security architecture, risk assessment and project management on a global scale. Bowers serves as the president of the 600-member Philadelphia chapter of Infragard, is a technical editor of Information Security *magazine, and speaks regularly at events like Information Security Decisions.*

MINING ENTERPRISE SIM LOGS

We will explore efficient ways to get the most relevant data from enterprise security information management systems.

BY ADRIAN LANE

SECURITY INFORMATION MANAGEMENT SYSTEMS, or SIMs for short, are effective platforms for the collection, analysis and storage of events from a broad range of systems and devices within the IT infrastructure. Many enterprises are overwhelmed by the myriad of choices and types of data a SIM can provide. For example, any given application might produce an access log, an event log, a transaction log and an audit log, each used for a slightly different purpose and containing slightly different information. Taking some time to understand the difference and selecting just the information you need helps produce better reports and reduce resource overhead.

Understand the regulations

With storage costs incredibly low, many organizations manage compliance by taking the path of least resistance. Rather than evaluate the regulatory requirements for data retention—like what data needs to be kept and for how long—many IT professionals will simply turn logging and auditing functions on and collect every available event. In turn, the record retrieval, analysis and reporting process becomes overwhelming, taking days instead of minutes.

Many regulations, however, don't actually

require long-term storage. As an example, many have treated the amended rules for the Federal Rules of Civil Procedure (FRCP) [http://searchfinancialsecurity.techtarget.com/sDefinition/0,,sid185_gci1294514,00.html?int=off] as a requirement to store audit trails for an extended period. But a review of the Electronic Discovery Rule Amendments actually reveals that an organization has the ability to define "electronic data which is reasonably accessible." It is perfectly acceptable for an organization to dictate what is appropriate, since few people know a business as well as those helping to run it. As long as the policy documentation specifies what is considered appropriate, you are in compliance. For example, for a university on the semester system, a 120-day email retention policy may be perfectly acceptable.

Collect the right data

Often companies collect system logs in their entirety or turn on audit features for their application platforms and incur a great deal of overhead when all they wanted was a report detailing failed logons. What could have been done with simple network monitoring with no performance cost to the application instead generated gigabytes of log files and reduced overall application throughput. Even so, as some of the applications didn't view failed logins as an application-level event, most access control-related failures were not recorded by design, and service-level interruptions were missing altogether.

As many data collection methods have overlapping information, and each method has an associated cost in terms of performance and quantity of data—not to mention quality of data—spend some time ensuring that the data being collected is appropriate for the type of problem being addressed. Sometimes a simple adjustment in this area leads to much more accurate reports.

Assess your efficiency

As SIM is not a new technology platform, there are many companies that have had the technology for several years but are less than happy with the performance and value of the platform. A lot has changed in the last couple of years, however, with new methods of data collection, new ways of analyzing data, and new ways of solving IT problems. Enterprises that implemented a SIM product a few years ago should re-examine their assumptions and deployment choices now that the platforms have evolved and become more efficient. Your SIM may offer a new method of data collection, like network packet collection, which can provide a more efficient method of collecting activity. Or you may have implemented virtualization, which can affect the data that is collected. Most company networks undergo constant change, and vendors are improving their products, so periodic review is recommended.

Know the value of normalized data

When collecting data from hundreds or thousands of disparate devices and systems, normalization helps to provide a unified view of the events. Normalization for SIM means automatically pulling common data items from each event (like who, what, when and where) and storing this subset into a common format. In essence, SIM normalization is making dissimilar data all look the same. This process makes cross-

system analytics feasible. And since all events share a common format, reporting and analysis is far easier as well.

But in many cases, the data that is kept in this normalized form is insufficient to really understand if there is a problem and what steps are necessary to remediate it. If a SIM platform identifies a failed or illegal transaction—for example, if someone uses an unapproved application to make an ad-hoc adjustment to the general ledger—a normalized event record will not include enough information. Identifiers like transaction ID, customer name, dollar amount, or any of the contents of the transaction needed to identify the transaction is missing. In order to fix review and fix the questionable entry, it will most likely be necessary to manually sift through hundreds or even thousands of legitimate changes.

Normalized records are a great way to reduce data volume and provide aggregation and correlation report, but to provide value from a security or audit standpoint, normalized event detection is not enough. Make sure to store enough of the original record, or better yet, have "drill down" capabilities, to cross reference the normalized record with the original record.

SIM platforms are both powerful and flexible. They provide a fast and efficient way to gather data, and a lot of options on how to process and analyze this data. What you collect and how you process it affects your ability to meet business drivers and compliance requirements, so take the time up front to understand your options and how best to achieve your goals; it will save you time and money in the long run.

Adrian Lane is a senior security strategist with Securosis LLC, an independent security consulting practice. He has 22 years of industry experience, specializing in database architecture and data security. Prior to joining Securosis, Lane was the CTO at the database security firm IPLocks, and he has also served as the vice president of engineering at Touchpoint, three years as the CIO of the brokerage CPMi, and two years as the CTO of the security and digital rights management firm Transactor/Brodia.

Next-Generation SIEM and Log Management Solutions

www.Q1Labs.com | 890 Winter Street | Suite 230 | Waltham, MA 02451 USA | 781-250-5800

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 117 Kendrick St., Suite 800, Needham, MA 02494 U.S.A.; Phone 781-657-1000; Fax 781-657-1100.

SPONSOR RESOURCES

ArcSight, Inc.

See ad page 6

- ArcSight White Paper: Combat Cybercrime, Demonstrate Compliance and Streamline IT Operations
- ArcSight Logger 4 Product Brief: Combat Cybercrime, Demonstrate Regulatory Compliance and Streamline IT Operations
- ArcSight Logger 4: Chief Technology Officer, Hugh Njemanze, Provides an Overview

Endace

See ad page 11

- Ninjaprobe: the only multi-function network monitoring platform delivering 100% packet capture
- Ninjaprobe + CACE Pilot delivers enterprise grade network monitoring and analysis to 40Gbps
- Can your IDS handle the load? Scale to 10Gbps and beyond with Ninjaprobe

LogLogic, Inc.

See ad page 1

- The 451 Group: Enterprise Security Information Management Report
- Gartner Magic Quadrant for Security Information and Event Management
- LogLogic Security Event Management Datasheet

netForensics

See ad page 15

- Think Data Breaches Can't Happen to You? Think Again
- Discover Why Event Correlation is an Essential Component of Effective Security Practices
- Top 10 Ways to Get the Most Out of Your Log Data

Prism Microsystems

See ad page 3

- Watch an online demo of EventTracker
- Download a free EventTracker trial
- Contact Prism Microsystems

Q1 Labs

See ad page 32

- The 2009 Magic Quadrant for SIEM
- The Business Case for a Next-Generation SIEM
- Leveraging Log Management to Boost Enterprise IT Security

RSA, The Security Division of EMC

See ad page 28

- ROI for SIEM White Paper
- Streamlining Security Operations with RSA enVision® and RSA® Data Loss Prevention Solutions
- Case Study: Salford City Council

SenSage Inc.

See ad page 24

- SenSage Award Winning SIEM Solutions
- SenSage Continuous Monitoring & Auditing for SAP
- SenSage - 400+ SIEM Customer Successes

Novell

- *bwin* Success Story with Novell Sentinel®
- Novell® Sentinel™ Log Manager: Secure, Simple and Powerful Log Management
- Secure, Simple and Powerful Log Management with Novell® Sentinel™ Log Manager