

# Logs Do Not Lie

By Ron Bernier and Steve Kallio

**Your network logs are your silent partners in enterprise defense. They are ready to spill their secrets. Are you paying attention?**

Threats to enterprise data are coming from an ever-growing number of sources. Attackers are employing increasingly sophisticated weapons in their attempts to get at and compromise corporate data. A comprehensive security strategy is required to mitigate the impact of malicious and threatening activity, and it should include close monitoring of the event and audit logs generated by applications and network devices. Done correctly and consistently, log review is a reliable and accurate way to discover potential threats and identify malicious activity. In addition to malicious attacks, event and audit log management can highlight administrative actions performed by well-meaning IT staff that have unintended consequences. Historically, enterprises with large information security budgets have been able to justify the deployment of security information management (SIM) tools to help them collect, aggregate, correlate, and normalize event logs. It is essential that smaller and mid-size organizations establish and maintain an effective event and audit log management approach as well.

Monitoring event and audit logs is an integral part of complying with a variety of federal regulations including Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Information Security Management Act (FISMA). In addition, as of October 2007, thirty-seven states have instituted security breach notification laws that require businesses to monitor and protect specific sets of consumer data.

There are solid business reasons behind these industry regulations: event logs turn up a myriad of security issues, both malicious and unintentional. In the case of one financial services firm, the daily firewall log review uncovered an unusually large amount of traffic from one external IP address. Investigation into the amount of traffic discovered that an untrustworthy customer was using an approved account to perform unauthorized activity. Because the customer's login attempts were "authorized," traditional security methods had not uncovered this activity. Unusual amounts of expected

---

**Unusual amounts of expected activity identified during the firewall log review enabled the company to remediate the situation.**

---

activity identified during the firewall log review enabled the company to remediate the situation.

Event logs also uncover simple mistakes that can have a large impact. In one company, a network engineer mistakenly assigned an Internet-accessible IP address to a new server. A daily review of the firewall logs showed unexpected traffic directed at the new server, allowed by the firewall ruleset. When this activity was reported to the organization, they immediately modified the firewall ruleset to protect the sensitive customer information contained on the server.

## Deciding what information to collect

An array of devices within a company's IT infrastructure – network switches and routers; file, print, application, database and Web servers; email systems; and firewalls – are capable of logging activity. Ideally, security professionals would collect data from every significant device and application on the network. The challenge is that network devices and applications can generate hundreds of events per minute. A network with even a small number of devices can generate millions of events per day. Reviewing the data can be an overwhelming task. Given the reality of limited resources, organizations need to prioritize which logs are essential by identifying the devices and applications that store, process, and transmit critical data.

Determining which devices are critical, and which information is significant, is not a one-size-fits-all proposition. Each organization will need to conduct an impact assessment of its network prior to establishing a log capture and review policy.

---

## When in doubt, lean toward storing more data; storage is cheap, and it is nearly impossible to research a past hacking attempt without adequate event logs.

---

Publicly accessible systems are targeted more than internal systems, simply because the number of people who can attack them is greater. eCommerce application/database servers are critical, both because they contain sensitive information that organizations must protect and because they tend to drive an organization's revenue stream. Organizations also need to prioritize the monitoring of internal servers and devices, determining the criticality level of their devices on a case-by-case basis.

The next step is to determine the type of information the organization is looking to extract from a specific log. Some organizations need to identify unauthorized access, user activity, and administrative activity; others need to measure volume of activity or document compliance of various security impacting processes (i.e., user/group administration, change management). Identifying what the organization wants to achieve through log management helps the security administrator or service provider develop a baseline upon which a plan can be customized. In addition, organizations should refer to recommended security logging templates available from the NSA, NIST, and SANS to guide them on what logging features they should enable.

At a minimum, it is recommended that organizations collect data from firewalls, web servers, and network authentication servers. When in doubt, lean toward storing more data; storage is cheap, and it is nearly impossible to research a past hacking attempt without adequate event logs.

### Firewalls

Firewalls can log all the traffic going in and out of the network. Typically, when security administrators review their logs for inbound and outbound traffic, they will check to see that the firewall is denying traffic, with the idea that accepted traffic has already been approved and the firewall is doing its job. With firewall logs, security administrators have to make sure that not only is unauthorized traffic denied, but that they understand exactly what it comprises so they can be proactive in addressing potential threats.

In addition to reviewing denied activity, security administrators should review unusual amounts of allowed activity. For example, a high number of file transfers can be a warning of malware or of a user violating company policy. If a company typically makes daily FTP transfers comprising one megabyte of data, then security administrators should investigate if a file transfer is suddenly 600 megabytes. Or, if the company allows Port 80 traffic for outbound browsing, they should take note if the traffic from a particular device increases sub-

stantially. The key is to look for *unexpected traffic* as well as expected traffic within *unexpected levels*. Security administrators should also take note of firewall admin logons, and if the device logs support it, firewall changes.

### Web servers

Web server logs are another rich source of data to identify and thwart malicious activity. Typically, a security administrator looks to Web server logs for entries that result in errors: users requesting pages that do not exist – 404 Page Not Found Errors – or users trying to access directory files for which they do not have authorization, such as 403 Forbidden Errors. Other errors to monitor include 500 Internal Server Errors, and 501 Header Value errors, both of which can indicate malicious activity as well as malfunctioning applications or bad HTML code. Checking the logs for Null Referrers can identify hackers who are scanning the website with automated tools that do not follow proper protocols. Security teams also need to monitor any access to pages that are used to update website content to ensure that only authorized users are attempting to get at this data.

Critical alerts in web server logs are when traffic to IIS servers is attempting to access database information via SQL injection, or when attempts are made to access folders on the server that are not linked to the HTML within the pages of the web server (e.g., Directory Traversals). Web server logs can also identify attempted execution of operating system commands. All of these events are indicative of malicious activity that should be reviewed in more detail.

But if security administrators are only looking for errors, they could be missing some important behaviors. What might appear to be “valid” traffic coming into a Web server could actually be the result of someone mirroring a corporate Website so they can perform phishing attacks. This activity is so common that many financial institution's sites are mirrored multiple times a week. It is difficult to spot this activity using standard web reports, since the technique criminals use may appear as if someone is simply viewing website pages. Yet, website and firewall logs can identify a site mirroring from normal user traffic: most website visitors will spend a certain amount of time on the website and only access a subset of the site's pages. Webserver logs can identify when a “visitor” methodically hits every page on a site in rapid succession. This type of activity, particularly if it comes from an IP address located outside of the company's traditional customer base, is an example of how “authorized” activity is not always the same as “safe” activity.

### Network authentication servers

An example of a network authentication server is an Active Directory Domain Controller. Authentication server logs document account activity. Reviewing administrative and user activity should include the following:

- Account lockouts
- Invalid account logons

---

## “Authorized” activity is not always the same as “safe” activity.

---

- Invalid passwords
- Password changes
- User management changes, including new accounts and changed accounts
- Computer management events, including when audit logs are cleared or computer account names are changed
- Group management events such as the creation or deletion of groups and the addition of users to high security groups
- User activity outside of logon time restrictions
- Server reboots

### After the collection

After an organization has collected event logs for all network devices, the next step is to assemble the data so that they can be analyzed. It is impossible to review every single log entry manually, so security administrators must aggregate, correlate, and normalize entries to create a report that identifies all of the important network activity into a manageable amount of information for review.

### Aggregation

This is the process of combining log entries from multiple network devices into a single repository for review. SIM products use a variety of methods of aggregating log entries. Without a SIM product however, organizations may have to write custom scripts to accomplish this task. In addition, companies may choose to use single-point solutions such as firewall log analyzers or Windows Event Reporting tools to summarize events for these particular types of devices. While these tools are less expensive than SIM solutions, they do not have the depth of functionality and they do not provide correlation capabilities.

### Correlation

This step enables security administrators to tie individual log entries together based on related information. This is where sleuthing starts to come into play: an event on a firewall log can be related to another event on a web server, enabling security administrators to determine the source and threat level. Both commercial products and custom scripts can automate this process by directing the program to search for a specific kind of event: “If X happens on the firewall, look for Y on the web server.” While this type of automation will follow the pattern of previous attacks and capture information on like events, it is a reactive strategy. It is challenging – and expensive – to continually develop new scripts to stay ahead

of threats. Therefore, most organizations need an approach that combines automated scripts with manual correlation techniques.

### Normalization

This process combines like events into a single entry to ease and streamline the review process. Rather than list 500 individual log entries detailing 500 failed logons from the same account, normalization will consolidate those into one event that notes the 500 failed attempts. SIM products automate the normalization process, but without them an organization should create custom-developed scripts to normalize events they are interested in. While many off-the-shelf products normalize attack-related events, it is equally important to capture and normalize allowed activity. Each step in this data-capture process narrows down the information that requires human oversight. It is tempting to focus on malicious events only to reduce the number of events to review, but many security incidents are the result of allowed activity.

---

**Even the best report that synthesizes the most valuable information into a concise format is worthless unless someone takes the time to review it on a regular, consistent basis.**

---

### The final step: oversight

While tools and scripts address the process of aggregating, correlating, and normalizing data, the final step in event and audit log management requires the human touch. Even the best report that synthesizes the most valuable information into a concise format is worthless unless someone takes the time to review it on a regular, consistent basis. This can be a resource-intensive activity that requires companies to invest in staff or outsource to an external service provider. For some businesses, including those in the financial services industry, it may require both internal and external review to meet industry regulations.

Successful log review requires people who understand what they are reviewing, time to perform the review, and deployment of the proper tools to achieve the organization’s objectives. Organizations should decide what it is they want to accomplish via log review and how often, who is going to review the logs, what kind of reports are going to be generated, and how often are they going to be generated. In order to achieve these objectives, organizations need to identify what tools (if any) are necessary.

Whether security administrators choose to collect and review event logs using their own teams or outsource to an external service provider, event and audit log management is a

best practice for ensuring network security. Most organizations have smart people running well-designed networks that use sound policies and procedures. Yet, they still experience threatening situations every day, some initiated by malicious intent and others due to simple human error. The key to discovering these activities and their impact upon the organization is understanding what information to capture, what to measure it against, and how to tell the difference between a blip and a true threat.

## About the Authors

*Steve Kallio, CISSP, GSNA, CHSP, is Director of Professional Services for Sage Data Security. He has worked in the information security profession for more than nine years, working as a*

*consultant with both global organizations and small businesses to assist them in securing their technology infrastructure. Steve's experience has been used to help organizations understand the complexities and compliance requirements of information security. He may be reached at [Steve.Kallio@sagedatasecurity.com](mailto:Steve.Kallio@sagedatasecurity.com)*

*Ron Bernier, CISSP, MCSE/Security, is nDiscovery Program Manager for Sage Data Security. In addition to managing the nDiscovery Security Discovery and Detection Program, he assists in the Professional Services practice. Ron has more than 15 years of experience in community and international banks within the Information Technology arena. Ron's banking expertise is in network and security design as well as information security. Ron may be contacted at [Ron.Bernier@sagedatasecurity.com](mailto:Ron.Bernier@sagedatasecurity.com)*