Event Logs and Security: Cutting Through the Noise

Whitepaper

As businesses expand to all geographies and time zones, the task of defending an ever-enlarging and ever-changing perimeter becomes increasingly daunting. Infrastructure endpoints, workstations in particular, are critical points of attack – and defense.

Event logs are an important source of information about these attacks and play a pivotal role in protecting corporate data. Event logs contain information not only about breaches themselves, but about suspicious behavior that, unchecked, could lead to a breach and significant financial loss. It is essential, therefore, to monitor and analyze event log data.

According to the SANS Institute, "Because it is at the workstation level that most initial compromises happen, and additionally where many of the subsequent steps of the attack life cycle also happen; it follows that looking at workstation events is a very logical place to focus attention when trying to combat APT-style attacks."[1]

Breach indicators vs. noise

Despite the importance of monitoring event log data, organizations frequently neglect paying sufficient attention to it. The main reason is that many event logs either contain or are excessive noise, or superfluous information. The sheer number of event log items, often containing irrelevant data, is simply too large to analyze promptly and accurately. However, that noise may conceal suspicious behavior or a breach.

[1] Detecting Security Incidents Using Windows Workstation Event Logs," SANS Institute, June 2012, p. 2

Failure to perceive breaches through noise can have devastating consequences. A notorious example is the Target breach of 2013. Hackers obtained credentials from an HVAC contractor and proceeded to breach corporate systems and compromise 40 million credit and debit cards. Although information about the breach was available to Target personnel, they reportedly were unable to separate the breach indicators from a vast amount of noise. It was only after the federal government notified Target of suspicious activity that the company responded. Ultimately, net losses to Target from the breach totaled $162 million, according to the company.

Analyzing event log data: INPUT VS. OUTPUT

There are two basic approaches to gathering and analyzing event log data:

- **Input-driven** methods collect all data. But because the quantity of data is so large, this approach inevitably gathers far more data than is needed and can be quite inefficient. Nonetheless, companies that specialize in analyzing event log data often encourage input-driven practices, since they are paid by the byte of data that they analyze.

- **Output-driven** methods collect only data that is relevant to reports and alerts. While more efficient than the input-driven approach, this method requires the use of tools as well as understanding the log data itself – which information is relevant and worth studying and which is not.

How output-driven collection works

Properly executed, the output-driven approach can pay significant dividends, removing 90% of the noise from desktop systems' event logs and greatly improving the chances of identifying breaches and suspicious behavior. An effective output-driven methodology includes three steps:

1. **Managing the audit service.** The audit service determines which events will be generated. Examples of events are logon/logoff, reboot events, and security policy events. The audit service allows an administrator to either include or exclude an event and to indicate the level of criticality.

2. **Whitelisting and blacklisting.** Whitelisting is the application of a filter to determine all permitted log data. Once that has been done, a blacklist is applied, which eliminates all data that is not wanted. This whitelist/blacklist procedure should be applied to event log data from desktops, hosts and reflectors. A reflector is a system that gathers information from different locations and forwards it along to a central system.

3. **Truncating.** Some event log text, particularly that of Windows, can be very verbose. For example, Windows includes significant amounts of text that, repeated for every log event, can use up large amounts of storage without delivering any benefit. This text can be shortened, or truncated, so there is far less data to store and transmit – with no reduction in the relevance of that data. An effective truncation algorithm can reduce the size of event log data by 75%, creating significant savings on disk space and bandwidth.

Output-driven approach in action: SNARE

Snare performs output-driven collection and filtering of event log data. Because most organizations have multiple operating systems in their IT infrastructure, Snare includes agents not only for Windows, but for Linux, Apple Macintosh and Solaris with coverage for desktops and servers. Snare agents on those systems perform whitelist and blacklist filtering, as well as

text truncation of verbose events. As a result, only 10% of event log data may be forwarded to the security information and event management (SIEM) system. The SIEM is the source of information for the following:

- **Management console** – presents key facts to administrators.
- **Alerts** – notifies administrators of unusual events.
- **Compliance reports** – sends information required for regulatory
  purposes.
- **Analytics** – subjects event log information to algorithms to deduce activity patterns.
- **Forensics** – tracks and investigates suspicious patterns and events.

In a distributed environment, a mid-tier reflector plays a critical role. Snare agents (Windows, Linux, Mac, Solaris) filter at the source, then send relevant data to the reflector, which in turn can filter and archive logs before sending information as required to different central systems for various users and purposes.

These include:

- **Sysops** – information about critical Windows events.
- **Top-secret systems** – User Datagram Protocol (UDP) information and security event information.
- **Centralized view** – a syslog server or service handles TCP information and truncated event data, presenting alerts, reports, analytics and forensics to a management console.
- **Analytics** – Transport Layer Security (TLS) information and truncated event data, as well as security, system and application information.
- **Forensics** – TCP information in verbose form for thorough research and analysis.

Benefits

Snare's output-driven approach yields significant dividends. By winnowing out event log data that is irrelevant to data breach prevention, it not only streamlines event log analysis, but makes that analysis possible for many companies that otherwise might not have been able to spare the time and expense.

It also shortens mean time to detection by going through event logs faster. By shaving days, weeks or even months off the time it takes to detect a breach, Snare can enable an organization to take action to stem data losses before they spiral out of control.

And Snare saves money. Analysis providers such as Splunk that charge by the amount of data they analyze can be very expensive when unfiltered data is sent their way. Snare reduces the data and therefore the charges – up to 46% of Splunk fees, according to Prophecy International estimates.

SNARE IN ACTION: Case studies

European digital identity and security products provider

A maker of digital identity and security products, and the world's largest producer of subscriber identity module cards, sought to increase its own security across a global infrastructure. With many different event log formats emanating from a large number of sites worldwide, the 3.1 billion EUR Netherlands-based company of 14,000 employees faced significant challenges.

By deploying Snare, the provider's solution integrates analysis of event logs in multiple formats from many different sites with the company's corporate SIEM server. By collecting, filtering and then forwarding security events to the central SIEM system, the solution gains a comprehensive corporate view of security events across the enterprise.

Airline

In the midst of changing SIEM systems, a major U.S. airline needed SIEM agents to monitor and report logs between both the outgoing SIEM server and the new one as it was being deployed. Because of its ability to interoperate with multiple SIEM systems, the airline chose Snare to enable the migration.

The many features of Snare have made it a permanent fixture in the airline's SIEM environment. The airline is benefiting from Snare's output-driven event filtering and truncation, as well as failover and redundancy capabilities. Snare is also helping the airline, which embarks more than 700 aircraft on 5,000 flights per day in over 60 countries, meet the compliance requirements of the following: the National Industrial Security Program Operating Manual, a guide for safeguarding classified information; the Payment Card Industry Data Security Standard for credit card transactions; and Sarbanes-Oxley for financial reporting.

State government

Faced with vast quantities of log data, one state's department of revenue implemented Snare as part of its SIEM solution. Working together, Snare agents and Snare server eliminate unnecessary logs, archive potentially important logs and forward logs needed for compliance purposes to the state's IBM QRadar SIEM system. State IT leaders praise Snare's ease of use as well as security. "The server and agent combination provide the state [department of revenue] with a highly secure environment," says an employee in the state's department of information security. Security Standard for credit card transactions; and Sarbanes-Oxley for financial reporting.

Conclusion

As organizations grow in today's global economy, their endpoints multiply, increasing vulnerability to a wide array of ever more sophisticated attacks. Desktop and server event logs are an important source of information about suspicious activity and breaches. Analyzing that event log information is essential to an effective security strategy, but too often is thwarted by large amounts of noise. Snare filters out and truncates the noise at the desktop, host and reflector to deliver faster and more accurate analysis, significant savings and tighter security for organizations of all sizes, in all industries.

About Prophecy International

Prophecy International is the developer of Snare, a security information and event management (SIEM) software solution. Snare is utilized in private companies and government agencies alike, but also used in conjunction with other SIEM systems. Originally an open source project, Snare Enterprise was released to support a more aggressive road map to meet and then exceed the increasingly diverse demands of users around the world. Prophecy International strives to go well beyond what is required of security software, thereby helping their customers to exceed their own goals.

Reach Out To Us!

On the web: http://www.prophecyinternational.com

By phone: +1 (800) 834-1060

Via e-mail:
AMERsales@prophecyinternational.com
APACsales@prophecyinternational.com
EMEAsales@prophecyinternational.com

We look forward to hearing from you!