Realtime publishers

Log Management:
Best Practices for Security and Compliance

The Essentials Series

How to Leverage Your Logs to Secure Your Environment

sponsored by

Eric Schmidt

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Table of Contents

Copyright Statement

How to Leverage your Logs to Secure your Environment

Introduction

The first article in this series discussed the importance of log files and began to make a case for centralizing log collection. This article will bring more attention to centralization and present more detailed examples of the benefits it provides with respect to security, compliance, and troubleshooting. To accomplish this, three real-world scenarios will be presented. Each will compare and contrast the difference in response when logs have been centralized versus when they aren't. Alerting and reporting will also be highlighted in these scenarios as they play a critical role in driving people to action and increasing efficiency.

Scenario 1: The Security Incident

The Information Security term that has gained the most media attention recently is "Advanced Persistent Threat" or APT. While the term has been applied to various types of attacks, the simplest way to describe an APT is a security breach that is able to circumvent common security controls like firewalls and anti-virus software and go for extended periods of time undetected. In this scenario, one or more systems have been compromised by an APT style attack that is attempting to gain access to sensitive information on other systems. At some point during this attack a system has been identified as being compromised and the investigation reveals event log entries that would not be generated under normal operating conditions. These events can now be considered indicators of the APT activity and are looked for during subsequent investigations of other systems. At this point one of two things will take place depending on whether or not log files are centralized. Without centralization information security personnel or system administrators decide that every system should be examined to see if the indicator events appear anywhere else. Depending on the size of the Enterprise this will be a very time consuming process. While there may be scripts or other tools available to perform the analysis there remains the requirement to "touch" every system. On the other hand, if event logs from these systems had been centralized, determining the scope of the attack would be as simple as looking for the indicator event on the log collector. Taking this one step further, the event collector may have the capability to send an alert if the event is collected from any system. If this happens to be the case, action can be taken immediately, like pulling the system off the network, to prevent the attack from spreading to other systems. The final benefit of event log centralization is the fact that all log entries contain timestamps that indicate when the event occurred. In this scenario, the timestamps can be used to determine how long the APT has been active, the systems that have been impacted as well as identifying the first system where that was compromised. With all of this information at hand IT security personnel and systems administrators can gain a solid understand as to how the APT was able to get into the infrastructure and take steps to prevent it from happening again.

One important thing to recognize here is the assumption that the compromised system was actually forwarding its logs. One common mistake made when developing a strategy for log centralization is forwarding workstation logs is not considered because the overhead of doing so is too expensive. In large enterprises, collecting workstation logs could generate terabytes of data that could be very expensive to store and generate a substantial amount of WAN traffic. There are ways that this can be mitigated and going back to the APT scenario, it is very likely that this type of attack would start on a workstation. The bad guys also know that enterprises often don't forward events from workstation and use this to their advantage. They will compromise workstations and then launch attacks from there in ways that appear on target systems as "normal" activity. Executed this way, malware is capable of operating for extended periods of time completely undetected. The third article in this series will offer suggestions as to how a balance can be achieved between the need to collect workstation logs and the resources required to accomplish it.

Scenario 2: A visit from the auditor

The first article in this series touched on the benefits of log centralization for maintaining compliance. In this scenario an enterprise must be Sarbanes-Oxley compliant. Maintaining this compliance requires an annual, in person audit where systems administrators have to demonstrate that they have the appropriate controls in place to log access to a critical financial system. The enterprise has developed and documented processes and controls for the request, approval, and creation of user accounts and the delegation of rights to users the ability to access financial data. The auditor is provided with a sample set of existing accounts from which they identify several that will be the subjects of the audit. The requirements of the audit for systems administrators is that they must provide evidence that individuals with proper authorization created the accounts and permitted them to access the financial system in question. There are several aspects of this scenario where the required evidence would not exist in log files so for the purposes of this discussion, those will be ignored. First, the auditor requests the list of accounts that were created for a particular time period. While there are a couple ways this list could be provided, one of them would be from the centralized logs because events for the creation of a user are recorded. Second, to provide evidence of that the account was provisioned by authorized individuals, the centralized logs are critical. The events that are captured when a user is created would come from the authentication service. The event where a user was granted access to the financial system may come from the financial system itself. Since these logs exist on different systems, and potentially any number of systems that comprise either infrastructures without log centralization every system log would have to be reviewed in order to find the specific accounts that are being requested. With the logs centralized a single search can be performed for the user in question that would return both the account provisioning event and the rights delegation event even though they were on completely different systems. Of course, these log entries would also include the identity of the individuals that performed the action as well as when the actions were performed. This would be the evidence required by the auditor indicating that the account was provisioned and granted access by someone that is authorized to do so. It's important to also point out here that the scenario could be reversed to detect the provisioning and delegation of an account by someone that is NOT authorized to do so, but for whatever reason they had the appropriate rights to do so. In this case, log centralization could then be leveraged to alert

people to this act so that appropriate action could be taken to revoke the rights and prevent unauthorized creation and delegation from happening again. This may become one of the most critical aspects of successfully passing the audit in this scenario because the unauthorized actions would have been detected, documented, and reverted before the audit took place.

Scenario 3: "It's been going on for weeks"

The first two scenarios addressed the benefits of log centralization for security and compliance. This third and final scenario will examine the benefits of log centralization to enhance troubleshooting and proactive problem resolution.

Every user in the enterprise relies on a web based timecard application in order to account for their time worked. For the last several weeks, a portion of the users have experienced slowness when trying to update their timecards, but they didn't question or report it to IT because they thought it was "normal". It turns out that one of the web servers that participate in the cluster providing the web interface has a configuration problem that has been logged to the web logs, but since those aren't centralized or reviewed the problem went undetected. The support staff had encountered issues with the application in the past and had developed a custom "monitoring" script and scheduled it to run on a daily basis. Some period of time later they forgot the script was in place and the scheduled task had stopped executing so it was no longer "monitoring". Additionally, the individuals who support the application use it with the same frequency as all the other users. They just happened to have been using a server that didn't have the problem. The rationale for centralizing the web logs of these servers becomes obvious. If that been in place with a tool that monitors and alerts on web service events the support staff would have been made aware of the problem right away. They were also relying on, but long forgotten scheduled task that was intended to notify them if there was a problem. Expanding on that aspect, the issues with the scheduled task failing to start could have been reported on. The events that the task failed to start or if the account used to run the task had an expired password, multiple failed login attempts would have triggered an alert that could have been acted upon. Instead, were relying on users detecting and reporting the problem.

Additional things to Consider

All three of the above scenarios highlight the benefits of centralizing log collection, but there are two critical aspects that also need to be considered. The first is the real time streaming of events to the collector. In all three scenarios, real time streaming is also important because one has to assume that log files on a given system can be modified. This is of particular importance for the security incident scenario because malware like the APT has the capability to avoid detection by modifying the local event logs. Real time streaming of events avoids this risk because the events are sent in real time to the collector as they are created on the systems before malware has any opportunity to delete them. In fact, a review of an affected system may not have some of the events that were captured by the central collector. This too can be considered an indicator of malicious activity and, depending on the tool, leveraged to alert IT staff of malicious activity. Real time streaming also applies to the auditing and troubleshooting scenarios as well. In addition to the scenario above, another example would be a complete system failure. If this were to

happen and the local logs on the failed system were unrecoverable it would be impossible to either recover events required for an audit or be able to assess what happened on the system right before the failure. In these cases real-time streaming behaves much like a flight data recorder on an airplane capturing events right before a crash except in this case it's not the physical enclosure that keeps the data safe, it's the fact that events are sent to an external system in real time. Real time streaming also prevents data loss for more benign configurations like maximum log sizes reached resulting in events getting overwritten when the log rolls and starts over.

The other aspect that needs to be mentioned, which augments real time streaming is the need to ensure the integrity of the events that are forwarded. In order for the forwarded events to be trusted the collector must have the ability to validate that each event it receives has not been tampered with. The most common way to accomplish this is by creating hashes of the event on the system before being forwarded. Then, once the event is received by the collector the same hashing algorithm is used. If the hashes of the source and centralized events are the same one can be confident that it was not tampered with.

Conclusion

The scenarios outlined above demonstrate the need for log centralization as well as the benefits it provides, however, those benefits can only be realized through the implementation of a well planned and designed infrastructure. Furthermore, in order to take advantage what is collected, the right tools that provide alerting and reporting must also be selected. In the next article "Best Practices for Log File Management" there will be an examination of the criteria for gathering requirements and implementing a log centralization strategy.