tripwire™

TAKE CONTROL.

Tripwire Log Center

NEXT GENERATION LOG AND EVENT MANAGEMENT

WHITE PAPER

Introduction

A decade or more ago, logs of events recorded by firewalls, intrusion detection systems and other network devices were considered more of a nuisance than a help. There were too many of them, they weren't easily collected, and there was no easy way to make sense of which were important.

When network administrators had log recording turned on, they were lost in a sea of data, and would have to sift through it all in an attempt at analyzing suspicious activities.

Some organizations deployed early Security Information and Event Management (SIEM) systems to help filter out the noise. The problem, however, is that the industry and government auditors found a gap in what was collected. There was no way to capture the events that those early SIEM solutions weren't aware of. The auditors said that everything needed to be captured and stored.

Compliance regulations such as Payment Card Industry Data Security Standard (PCI DSS), NERC, Sarbanes-Oxley (SOX), and the Federal Information Security Management Act (FISMA) changed at least part of that scenario. Organizations now need to be meticulous in collecting and storing log data. If they aren't they can be slapped with fines, and their executives held responsible. But aside from being compliant to avoid fines or responsibility, organizations need to comply with these standards and regulations because of their underlying purpose—to secure the IT infrastructure.

Another, and more positive, trend is emerging. Some organizations are starting to realize they can use logs to pinpoint holes in their cyber defenses and thereby boost security. The Defense Department in a recent study said that log management ranked among the highest value controls that could be used to block attacks on networks.

LIMITATIONS OF MOST SIEM SOLUTIONS

In a 2009 survey of the log management industry, The SANS Institute reported more organizations saying that top uses for log data were "tracking suspicious behavior and user monitoring," for forensics, and day-to-day IT operations. In previous years, SANS said, companies had reported trouble just collecting log data.

Mature organizations are now beginning to use logs for these more advanced purposes, it said.

But there's a disconnect between desire and application. Not only are there now even more devices that produce logs, and therefore increasingly large volumes of data to manage, but different devices and operating systems use different formats to log data. Pure log management systems focus on just collecting and storing logs. Yet traditional SIEM systems that attempt to combine both log data collection with the analytical prowess needed to meet the emerging trends are too complex and cost prohibitive for most organizations. That's not surprising since the log management industry, which focuses on collecting and managing logs, and the security information and event management (SIEM) industry, which is the analytical side of the equation, have developed more-or-less separately.

You usually have to choose between strong log management or strong security event management capabilities, with separate devices needed for each product. The combinations that do exist are essentially tools from one side bolted onto those from the other, with questionable impact on the scalability and performance needed from modern, integrated solutions.

A NEW APPROACH TO AN SIEM SOLUTION

Tripwire Log Center offers a new approach. Tripwire Log Center was built to include both log and event management in an all-in-one solution from inception. It meets IT compliance needs by capturing tens of thousands of events per second, then compressing, encrypting and storing the logs. Since it supports all the most popular log transmission protocols, it can immediately collect logs from just about any source. And since it has SIEM capabilities built right in, it provides real-time alerts about suspicious activity.

Tripwire Log Center Capabilities

The all-in-one log and event management capabilities of Tripwire Log Center make it a sophisticated security event analysis platform. With it, you can query and search all the data in the event database and then drill down to investigate any suspicious activities. It provides graphical tools for correlating events, and pinpointing parts of the infrastructure that could be affected by any incident. A centralized dashboard gives a quick view of all alerts, events and vulnerabilities.

And, though Tripwire Log Center is a standalone product, it also works hand-in-hand with Tripwire Enterprise to provide a single, integrated IT security and compliance automation solution that correlates change data and compliance status with events-of-interest produced by the log monitoring. That gives end-to-end visibility across the enterprise for both event and change activity, real-time intelligence to make better decisions about that activity, and automation that reduces the workload IT often spends performing repetitive, manual tasks.

DYNAMIC ACTIVITY ANALYSIS

Knowing what changes have been made to your IT infrastructure is vital, particularly when they are unauthorized. Identifying any suspicious events is also paramount. Even better, however, is being able to correlate those changes and events so you can get a complete view of all questionable activity.

Gaining information about the context surrounding a change or event helps as much with eliminating the mundane as it does identifying real security threats. After all, how many times have you mistyped a password? You need to be able to distinguish that from repeated logon failures that might signal an attack.

Tripwire Log Center provides real-time intelligence of events that lead to an unexpected change, as well as what resulted after the change was made so you can quickly address events of interest. In fact, when Tripwire Log Center identifies an event of interest, it automatically sends alerts that immediately notify appropriate individuals about a potential breach. Tripwire Log Center also allows for automated remediation so you can stop threats before they wreak havoc across your infrastructure. In addition, the solution's feature rich dashboards give a complete view of what is happening across the infrastructure.

When Tripwire Log Center integrates with Tripwire Enterprise, combining log management with file integrity monitoring means you also have a comprehensive, archived audit trail for reporting and compliance needs.

REAL-TIME THREAT MONITORING

Security threats these days happen fast and often, so it's essential to have some way to track down in real-time the kinds of suspicious flurries of activity or coordinated events that can signal an attack is underway.

With Tripwire Log Center, security analysts have a dashboard they can customize for their needs to show them just where the suspicious activity is happening. Heat maps show the relative levels of activity at certain locations, for example, and color-coded links between nodes show what the highest priority events are for each link instance.

Analysts can then also use the dashboard to drill down into any areas of activity to see in more detail what's happening and what the potential causes are so you can identify the proverbial needle in the haystack.

The event management capabilities of Tripwire Log Center allow managers to compare activity against a set of pre-defined policies and thresholds. If any of those are breached, notifications and alerts automatically go out to the people who need to know so that issues can be fixed before they become actual problems.

And events are captured and stored to enable a slow-motion replay of activity maps. Just as with slo-mo in televised sports that show the exact moment when a football player's knee hits the ground, in this case it can reveal in exacting detail how suspicious events developed, and if anything was missed on the first go-around of an analysis.

AUTOMATED EVENT RESPONSE

Monitoring and detection are the first line of defense, but they are less effective if they generate a less than immediate response. With the speed at which security threats develop today, automated reaction and response is a must.

Tripwire Log Center allows for real-time notifications based on any series of events from many different sources. When those events affect a policy or hit a preset threshold,

Tripwire Log Center Capabilities (cont'd)

notification is sent to relevant personnel via email or Syslog, using scripts, or even directly to the Tripwire Log Center console.

The event manager includes a security event ticketing system to help pinpoint high-priority events so they can be fixed first.

Tripwire Log Center also enables auto remediation of a problem. That's admittedly not a major factor yet for network and security managers, most of whom prefer to act on notifications and alerts. But with the number and frequency of security threats accelerating, the consequent increase in the speed with which issues need to be addressed, and the need for IT to handle an increased workload with the same level of resources, it's only a matter of time before auto remediation becomes essential.

COMPREHENSIVE LOG MANAGEMENT

Although organizations collect logs to address growing security concerns, compliance is also a significant driver for having log management capabilities. In fact, SANS reported that just under 60 percent of the respondents to its 2009 survey reported compliance as their main reason for collecting and managing logs.

Tripwire Log Center collects every event that happens on IT infrastructure devices, applying Google-like indexing, compressing and encrypting the data before storing them as a flat file. The indexing enables fast, complex searches using plain keywords to look for forensic evidence as needed, while the flat file format means you can use standard storage mediums such as storage area network and network attached storage.

Tripwire Log Center applies normalization rules to the raw log data after it has been captured rather than before, which eliminates the need to know the log schema before having the ability to capture the log for a new device. This approach also enables Log Center to capture raw logs from any device. You can dynamically edit the schema later to support the log format when generating reports and queries.

INTEGRATED CONFIGURATION CONTROL

This is where the combination of Tripwire Log Center and Tripwire Enterprise comes into its own. Given that file integrity monitoring – the focus of Tripwire Enterprise – is as much of a mandatory requirement for most regulatory compliance as log management is, it's a beneficial union of best practices.

With both solutions in play, organizations have an end-to-end understanding of both log information and change data, and how they interact. No change can be made in the IT infrastructure that isn't accounted for in the device logs, and any unauthorized change is detected immediately in the log information.

All data is collected both before and after the change is made, so changes that aren't authorized under existing compliance policies can be automatically examined. Inconsequential changes—those that don't affect compliance—can be ignored or labeled as low priority concerns. Those that do can be flagged for immediate response.

The Next Generation

Compliance regulations have made log management a mandatory IT practice for organizations, but there's an increasing awareness of what those logs can also do for security through tracking suspicious activity and user behavior. However, there's a dearth of ready solutions that can provide for both sides of this scenario. You can have strong log management and strong SIEM, but making the two work together to provide the intelligence needed to make good decisions on security is complex work. The result is usually something that's much less than optimum, which doesn't scale well and which doesn't have the speed and performance to meet the needs of modern IT security.

On it's own, Tripwire Log Center integrates both log management and sophisticated event analysis. The result is next generation log and event management, without the complexity and bloat associated with traditional log management and SIEM systems. Plus, when Tripwire Log Center is used in concert with Tripwire Enterprise, Tripwire's industry-leading configuration control solution, organizations achieve total visibility and intelligent threat control across all events and changes with no compromise to performance and scalability.

ABOUT TRIPWIRE

Tripwire is the leading global provider of IT security and compliance automation solutions that help businesses and government agencies take control of their entire IT infrastructure. Over 7,000 customers in more than 86 countries rely on Tripwire's integrated solutions. Tripwire VIA™, the comprehensive suite of industry-leading file integrity, policy compliance and log and event management solutions, is the way organizations proactively prove continuous compliance, mitigate risk, and achieve operational control through Visibility, Intelligence and Automation. Learn more at tripwire.com.

tripwire™
TAKE CONTROL.