HOW TO PERFORM FORENSICS ANALYSIS USING LOG DATA

An often overlooked feature of log management software is the ability to conduct forensic analysis of historical events. If your network goes down, your network monitoring tool can tell you what happened, but knowing why it happened is even more valuable.

SolarWinds Log & Event Manager has cutting-edge IT search for fast and easy forensic analysis. Here are six ways that the forensic analysis feature of Log & Event Manager can help you piece together what really happened.

You can download a free, fully functional 30-day trial of Log & Event Manager from here.

1) ID file changes

When collecting logs, you're going to see millions of file changes. How do you know which ones to isolate? It's best to isolate file changes against critical files (protected docs, financial information, personal documents, HR records, etc.).

Look at file changes from a forensic approach to determine if suspicious activity has occurred. Often times, a virus will affect file attribute changes such as permissions changes. This could allow the retrieval of information like a password, resulting in unauthorized file or network access.

Forensic analysis can help you identify if files have been changed, when they were changed, and who made the changes.

2) Identify user activity

You can map user activity using historical data to link together event logs. You can see the activity of one user, a group of accounts, or a specific type of account.

Using Log & Event Manager to collect logs from hundreds devices makes it easy to summarize the log data to surface events, privilege changes, etc. The forensic analysis feature allows you to quickly identify anything that looks unusual in the accounts you are investigating.

3) Monitor network traffic logs

Monitoring traffic logs is as simple as asking why you are seeing an excessive amount of outbound traffic from one IP address. If you have detailed information about the IP address, you can quickly recognize that the increased traffic is suspicious unless you know that the IP is allowed to communicate outbound.

Traffic logs hold source, destination, port, and protocol details. You can use this information to determine if the abnormality is something you can ignore or if it's worth investigating.

4) Monitor authorization and access attempts

All authentication and access logs are collected in Log & Event Manager. With forensic analysis, you can quickly see if someone has gained unauthorized access, if there were repeated attempts by a single account, or if the attempting IP address looks suspicious.

You can also filter by an account that's not part of an authorized account list or not in AD. One of the simplest ways to identify unusual access activity is to look for IP addresses that don't belong.

If you start seeing external or different types of IP addresses, then you know it's something to investigate.

5) Troubleshooting system outages

Your monitoring technology will let you know there is an outage before Log & Event Manager would. The monitoring technology will indicate what system had an outage, and possibly provide some additional data. But the logs are going to contain more details.

From a forensic analysis approach, you're going to use the logs as evidence of foul play, or to identify root cause (i.e. you'll be able to see that a piece of software was installed 30 seconds before an outage occurred).

Exceptions, warnings, file changes, etc. are all recorded so you can use those as evidence for the cause of the outage.

6) Incident response

Say goodbye to complex queries. Conducting forensic analysis, in general, is a quicker and simpler way to do incident response. The faster you get the data, the better.

Where Log & Event Manager helps is by removing the need to build complex queries to get the data. More often than not, you're responding so fast that you don't have time to build a complex search to find a needle in a haystack.

A better way is to identify the information you have (this IP, this warning, this exception, etc.) and plug that into a search and see what you can find from the log data.

Log & Event Manager surfaces information to make it easy to quickly scan and find what is out of the ordinary so you can start drilling down from there.

Additional features of Log & Event Manager:

Quickly conduct forensic analysis to figure out what happened before, during, and after an event to isolate fault and determine root cause.

Explore and analyze data intuitively with visual search tools, including word clouds, histograms, tree maps, and charts to easily spot anomalies and trends.

Leverage basic keyword searches and partial information to surface events. Then, with the click of a button, drill down for more detailed data.

Build complex searches fast with a simple drag-and-drop interface, as well as save and reuse custom searches.

Run scheduled searches with the ability to automatically export and email results upon completion.

SolarWinds® Log & Event Manager (LEM) gives you advanced IT search functionality that enables you to view log data in a way that makes sense for fast and effective event forensics, troubleshooting, root cause analysis, and overall log management. This makes it much easier to analyze events.