ManageEngine
Log360

Log forensics

Best practices guide

The importance of log forensics

In today's complex threat landscape, it has become a necessity for all organizations to use an incident detection system to identify threats, security incidents and breaches, instantly. However, attack patterns are constantly evolving, and even large-scale organizations with sophisticated incident detection systems in place, are susceptible to security attacks. An example of this is the Equifax data breach in September 2017, which compromised 143 million people's personal data. It is thus equally important to be prepared and have an efficient incident response system in place, too.

Incident forensics is the first step of any response strategy. Network logs are among the richest sources of evidence available when you wish to conduct a forensic analysis. A SIEM solution allows you to search through massive volumes of log data as part of your forensic exercise. This guide highlights how you can leverage a SIEM solution to perform efficient investigations, and the best practices to be followed to ensure that you have a robust incident forensics system in place.

Log forensics with SIEM: Best practices

1. Audit what's important.

When configuring log sources for your SIEM solution, it is important to ensure that you collect just the essential log information. Select the types of logs which you believe are important from an auditing or security perspective. This way, you can ensure that you have the right information to search through in case of an investigation, and nothing more or less. If you collect irrelevant logs, such as debug level logs, you could end up with way too much information to go through when you wish to search your log data. If you miss out on collecting logs that may not be immediately important, but could be required in future investigations, you may have gaps in your investigation.

How you can do this: As a thumb rule, include all log data that detail network users and their actions, and logs of relevant severity levels such as errors, critical, and warning logs. Eliminate any that provide very low level information. You can control what logs your SIEM collects by configuring the logging services appropriately on your log sources, and by making use of any additional filters provided by the SIEM solution.

2. Store log data securely and select an appropriate archival period.

Your log search may be compromised if the logs have been damaged or modified in any way. So any solution you use to manage the data should be able to store the data in a secure, tamper free manner. Further, since logs occupy massive amounts of space, you will have to occasionally delete certain logs, so be careful with when and what data you delete.

Apart from security, this is important from a legal perspective as well. Log archival practices are usually dictated by regulatory bodies through standard compliance policies. In case of a data breach or other security attack, if you do not have the necessary logs to present as evidence, or you are not able to prove the data is genuine, it could have serious repercussions on your company in terms of monetary cost and reputation.

How you can do this: Select a minimum retention period based on the compliance policies applicable to your industry and country. If you have the resources to retain it for a longer duration, select the longer duration, as it is better to be safe than sorry. Also, make sure that your SIEM solution can store your log data securely and in a tamper free manner, using methods such as encryption and time stamping.

3. When investigating an incident, begin with what you know.

Now that you have established you have the necessary data to search from, next comes the task of actually digging through it to investigate an incident and discover its cause. You typically have millions of logs and you would need to select an initial subset which can give you more information about an incident. If you are confused about how to start questioning your log data, a simple method is to make sure you collect all the information already known about the attack, so you can form an initial search query based on this knowledge.

How you can do this: Ask questions to determine what you know about the incident: Do you know the timeframe when it occurred? Do you know a set of devices that were definitely breached? Do you know any specific entity involved, such as an IP address, or user? Adjust the time window of your search and create your initial query with these known parameters. Be as specific as possible so that the initial set of logs you get to work with contain a good number of valid logs. Ensure your SIEM solution allows you to create complex search queries and group criteria as needed.

4. Review results at each stage and narrow down the information as needed.

Conduct your searches in an orderly manner so that you can get answers quickly and efficiently. When you get an initial set of logs, review the search report and start making interpretations to further guide your search. Keep narrowing down the information by adding new parameters, or running new searches based on the facts you uncover. Continue this systematically until you have a full picture of how and when an attack happened, who was responsible, all the network devices that were compromised, etc.

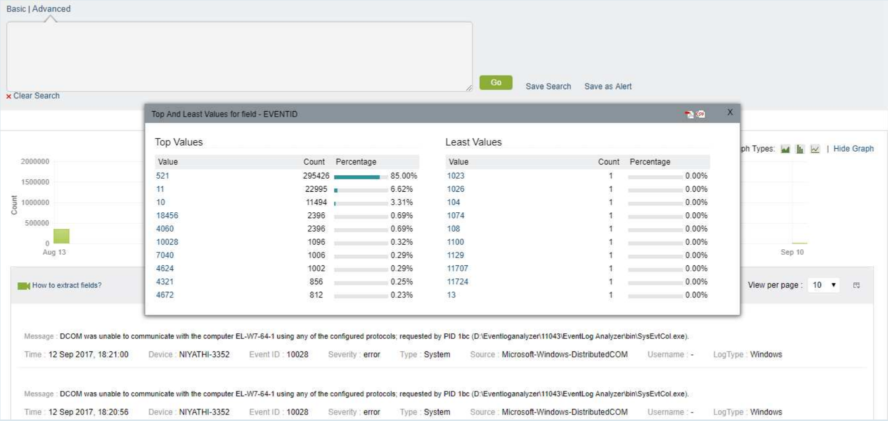
How you can do this: In your initial log data set, look at the values for log fields other than the ones you used to search with. For instance, if you started with all the logs for Device A for a period of 2 days, look at all the users who were active on the device. If you identify any user who shouldn't have had access to the device, narrow down the search to all logs pertaining to this user. Review all activities performed by the user. Next, run a new search for logs pertaining to this user on all devices, and identify how the user gained access to the device, and if they attacked any other devices. You now know who caused the incident, what exactly the user did, and how they did it. Ensure your SIEM solution allows you to easily review and filter your search results.

5. Create an incident report and save the pattern as an alert.

Finally, once an investigation is complete, create an incident report that outlines all the information you have uncovered, so it can be presented to those required. If the incident is part of a legal investigation, the report can be filed as evidence. Further, since you have now discovered an attack pattern that breached your network, set up an alert based on it so that you are immediately notified about it if it occurs again in the future.

How you can do this: Make sure your SIEM solution allows you to export the search results and save the pattern identified as an alert profile.

Incident forensics made easy with Log360



Top And Least Values for field - EVENTID

Top Values

Value	Count	Percentage
521	295426	85.00%
11	22995	6.62%
10	11494	3.31%
18456	2396	0.69%
4060	2396	0.69%
10028	1096	0.32%
7040	1006	0.29%
4624	1002	0.29%
4321	856	0.25%
4672	812	0.23%

Least Values

Value	Count	Percentage
1023	1	0.00%
1026	1	0.00%
104	1	0.00%
1074	1	0.00%
108	1	0.00%
1100	1	0.00%
1129	1	0.00%
11707	1	0.00%
11724	1	0.00%
13	1	0.00%

```
Message : DCOM was unable to communicate with the computer EL-W7-64-1 using any of the configured protocols; requested by PID 1bc (D:\Eventloganalyzer\11043\EventLog Analyzer\bin\SysEvtCol.exe).
Time : 12 Sep 2017, 18:21:00    Device : NIYATHI-3352    Event ID : 10028    Severity : error    Type : System    Source : Microsoft-Windows-DistributedCOM    Username : -    LogType : Windows

Message : DCOM was unable to communicate with the computer EL-W7-64-1 using any of the configured protocols; requested by PID 1bc (D:\Eventloganalyzer\11043\EventLog Analyzer\bin\SysEvtCol.exe).
Time : 12 Sep 2017, 18:20:56    Device : NIYATHI-3352    Event ID : 10028    Severity : error    Type : System    Source : Microsoft-Windows-DistributedCOM    Username : -    LogType : Windows
```

ManageEngine Log360 consists of a powerful log search module, to help you conduct your forensic analyses. You can use flexible options like wildcard characters and range searches, to create your search queries. The search engine retrieves the information you require extremely fast from your logs. Two search modes are provided:

- The **basic search mode** allows you to construct a search query from scratch, by simply typing it into the search box.
- The **advanced search mode** provides you with a useful interface to build your search query, by selecting the log fields, creating groups of criteria, and selecting the necessary logical operators.

Another useful feature is the click-based search option, which allows you to quickly drill down your search results by clicking on particular log fields, seeing its various values in your search results, and filtering the results by selecting a particular value. The module thus helps you quickly and easily discover how, when, and from where an incident occurred, and who is responsible.

Once you identify an attack pattern, you can save the information in an alert profile, so you are notified when similar incidents occur in the future. This helps you enhance your internal threat knowledge. The log forensics module also allows you to export or save the search results, which you can use as your incident report.

About Log360

Log360 is your one-stop solution for all log management and network security challenges. It is an integrated solution that combines EventLog Analyzer, ADAudit Plus, and Cloud Security Plus into a single console to help you manage your network security, Active Directory auditing, and public cloud management easily. Log360 helps you combat security breaches, meet compliance requirements, automate log management requirements, and perform effortless AD monitoring, alerting, and auditing from a single console, making it a truly comprehensive unique solution.

About ManageEngine

ManageEngine is bringing IT together for IT teams that need to deliver real-time services and support. Worldwide, established and emerging enterprises—including more than 60 percent of the Fortune 500—rely on our real-time IT management tools to ensure tight business-IT alignment and optimal performance of their IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corporation with offices worldwide, including the United States, India, Singapore, Japan and China. For more information, please visit buzz.manageengine.com; follow the company blog at blogs.manageengine.com, on Facebook a www.facebook.com/ManageEngine and on Twitter @ManageEngine.

ManageEngine
Log360

Website
www.manageengine.com/log360

Tech Support
log360-support@manageengine.com

Toll Free
+1-408-352-9254

$ Get Quote

Download