SUCCESS STORY

SIEM Data Intelligence and IT Operational Efficiency

Fortune 500 Semiconductor and Telecommunications company

Over 90% of information a user creates or accesses within an organization sits within unstructured data such as text documents, spreadsheets, and presentations. These files often reside on network attached storage systems and are frequently accessed and updated by users. File owners often move or delete files and folders without prior notification to all users. Other times, files are inadvertently moved or deleted without the owner's knowledge. In worst case scenarios, these actions are the result of ransomware or insider threats.

Recently we spoke with the Security and Infrastructure & Operations teams at a Fortune 500 Semiconductor and Telecommunications company about how it is commonplace to receive numerous requests to locate files and folders.

If end users cannot locate a file they need, having the ability to track the file move events can help identify where the file now resides. Unfortunately, this information is challenging to figure out from

IN BRIEF:

- Fortune 500 Semiconductor and Telecommunications company
- Approximately 33,000 users
- Too much noise going into Splunk, thus driving up data costs and creating operational inefficiencies
- Splunk's inherent alerts doesn't provide source details for activities such as a user ID or IP address

QUOTES:

- "There are over 33,000 users updating numerous documents each day...If you add to that the number of reads, directory traversals, copies, and other operations, each Windows server will generate millions of events each day. "
- "Although a SIEM can alert an administrator when there is high activity and tell them where the suspicious activity is coming from, it fails to give more details about the source of the activity."

event logs. They've found that in order to understand a file move, it is necessary to correlate multiple events.

For example, most files are moved through a drag-and-drop or cut-and-paste operation which generates many events, including multiple 4663 events. In order to identify the origin and destination location of a file, it is necessary to look for the 4663 events that have a matching Handle ID. In addition, several other 4663 events are created that result in additional noise to filter through including access requests for ReadData, WriteData, and Delete. Given the level of effort required to correlate these events, it's no wonder this organization was spending hours each day responding to basic operational activity requests.

EVENT NOISE DRIVES UP COST OF SIEM

There are over 33,000 users updating numerous documents each day at this Fortune 500 company. If you add to that the number of reads, directory traversals, copies, and other operations, each Windows server will generate millions of events each day. This organization feeds all that data into their SIEM, which in this instance is Splunk.

Most SIEM vendors charge users based on the amount of data they receive, so it can become quite expensive to send significant amounts of data to them. To save money and cut through the noise, many administrators opt to disable file access auditing. Doing this leaves organizations without an efficient and reliable mechanism to monitor file activity, and leaves them completely in the dark in terms of understanding who is accessing data, when, from where, and what types of operations they're performing. Relying on native logging is rarely a practical, if even possible strategy for monitoring the necessary activity.

Instead of disabling file access auditing in Windows, this organization was able to use STEALTHbits Activity Monitor to consolidate the events. This prevented most of the noise from going into Splunk and saved money because it limited the amount of data Splunk could charge for.

Another benefit this organization enjoyed from having consolidated events was the ability to quickly generate one report that can identify scripts or users that have completed actions such as moving or deleting files or folders. This saved the company's administrators

time and enabled them to quickly answer the typical operational questions they received on a daily basis.

THAT MOMENT WHEN DATA INTELLIGENCE IS NOT INTUITIVE

When this organization began to be inundated with requests for information on multiple file deletions, they checked their SPLUNK dashboards to see what was going on. Although a SIEM can alert an administrator when there is high activity and tell them where the suspicious activity is coming from, it fails to give more details about the source of the activity.

In the aforementioned example, the organization was able to use STEALTHbits Activity Monitor and find that there were scripts running that would delete files without users knowing what happened. Prior to having this solution, they would be forced to manually decipher log events like this to extrapolate which user or device was compromised, what malicious activity occurred, or what happened to a file or folder. Splunk's inherent alerts, like all SIEMs, are likely to be insubstantial for events like this. When under a security attack, having details such as a user ID or IP address can make all the difference in the amount of time it takes to stop the attack. In this case they were able to quickly generate one report that found the offending script, the account associated with it and the deletion operations.

If this had been an outside threat like Ransomware, this organization would have been able to produce compliance artifacts that would prove not only how the data was being accessed, it could also isolate filers with issues and pin point not just where there was high activity but what was the source of the activity including remote IPs, users and the operation. Since STEALTHbits Activity Monitor data can be sent to any SIEM, including Splunk, this organization can now have enriched security and operations with this added activity intelligence.

FILE ACTIVITY MONITORING PROVIDED INSIGHT INTO:

DATA OWNERSHIP

- Who owns the data?
- Who is accessing data I own?

STALE CREDENTIALS AND DATA

- Who isn't leveraging their access privileges?
- Which shares/folders/files are no longer being accessed?

THREAT DETECTION

- Whose file activity is abnormal/ anomalous?
- Where is there suspicious activity indicative of threats like ransomware?

DATA ACCESS

- Who accessed/deleted a particular share/folder/file, including those stored on Windows or NAS devices?
- Who is accessing data inappropriately?
- Who is trying to access data to which they don't have permission?
- Who is accessing sensitive data or data subject to compliance?
- Who is accessing data or making changes outside of change control windows?

Schedule a Demo

stealthbits.com/demo

Download a Free Trial

stealthbits.com/free-trial

Contact Us

info@stealthbits.com

STEALTHbits TECHNOLOGIES

STEALTHbits Technologies is a cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data.