LogicHub

Intelligent Security Automation Use Case

Monitoring Files Written to USB

Introduction:

LogicHub is the leading Intelligent Security Automation Platform that marries a powerful Decision Engine to a flexible Workflow Engine. Proven to deliver 10x the performance of traditional Security Orchestration Automation and Response (SOAR) solutions, it is the only platform of its kind to deliver analysis and decision-making automation to exponentially improve alert triage, incident response, and threat hunting.

One of the many use cases that LogicHub customers have implemented and benefited from is that of automating the monitoring of users writing files to external USB drives.

User File Copy Monitoring Challenges:

Monitoring user behavior within the network has grown in importance over recent years and this need adds to the growing list of tasks and challenges for the SOC to take on, specifically:

- Constant flow of IOCs
- High volume of log entries per day to analyze
- Tedious and repetitive process for analysts that is time consuming
- No easy and consistent way for analysts to manually determine what is unusual activity
- Limited analyst resources to process every log entry and/or alert

LogicHub Solution:

Automated analysis of logs related to external file copies and automate the escalation of alerts for suspicious activity. This gives the SOC consistent monitoring of the logs, potentially helping with both DLP needs and/or audit requirements.

Collect and Organize the Data

Logs for files written to external drives can generally be found in a couple places depending on the environment including antivirus (AV), endpoint detection and response (EDR), or data loss prevention (DLP). A SIEM connection can be used in order to get the raw logs into

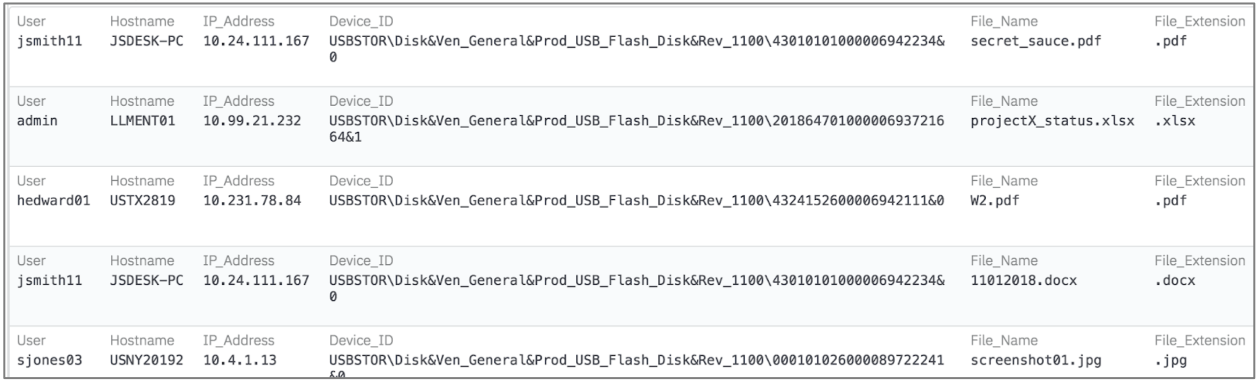
LogicHub. Once there they can be parsed, analyzed, and trimmed down to a subset for either human analysis and/or escalation. For this flow Symantec SEP logs were used.

Figure 1: Sample Symantec SEP Logs - Raw

```
2018-11-01 19:13:19,Minor,NVGTAN9-C5XQCHP,10.12.251.16,Continue,[AC5-1.1] Log files
written to USB drives - Caller MD5=c2af87b360db66e076881938c29fb136,File
Write,Begin: 2018-11-01 19:12:17,End: 2018-11-01 19:12:17,Rule: Log
files written to USB drives | [AC5-1.1] Log writing to USB
drives,14240,C:/Windows/explorer.exe,0,No Module Name,E:/to
Bingyi/這不是一個真正的文件名希望你沒有花時間翻譯0925.docx,User: jchin01,Domain: NAM,Action
Type: ,File size (bytes): 0,Device ID:
USBSTOR\Disk&Ven_General&Prod_USB_Flash_Disk&Rev_1100\8633330000062739&0
```

The raw logs are ingested into LogicHub and parsed for processing by the flow.

Figure 2: Sample USB Write Logs - Parsed



User	Hostname	IP_Address	Device_ID	File_Name	File_Extension
jsmith11	JSDESK-PC	10.24.111.167	USBSTOR\Disk&Ven_General&Prod_USB_Flash_Disk&Rev_1100\43010101000006942234&0	secret_sauce.pdf	.pdf
admin	LLMENT01	10.99.21.232	USBSTOR\Disk&Ven_General&Prod_USB_Flash_Disk&Rev_1100\2018647010000069372l664&1	projectX_status.xlsx	.xlsx
hedward01	USTX2819	10.231.78.84	USBSTOR\Disk&Ven_General&Prod_USB_Flash_Disk&Rev_1100\432415260000694211l&0	W2.pdf	.pdf
jsmith11	JSDESK-PC	10.24.111.167	USBSTOR\Disk&Ven_General&Prod_USB_Flash_Disk&Rev_1100\43010101000006942234&0	11012018.docx	.docx
sjones03	USNY20192	10.4.1.13	USBSTOR\Disk&Ven_General&Prod_USB_Flash_Disk&Rev_1100\00010102600008972224l&0	screenshot01.jpg	.jpg

Once parsed it then becomes easier to apply whitelisting to the logs to remove anything that does not need to be escalated. These whitelist definitions will be unique to your own environment. Items to whitelist on include:

- Username
- Hostname
- File type

After both parsing and whitelisting has been applied the remaining logs are ready for either human analysis or escalation.

Determining Anomalous Activity

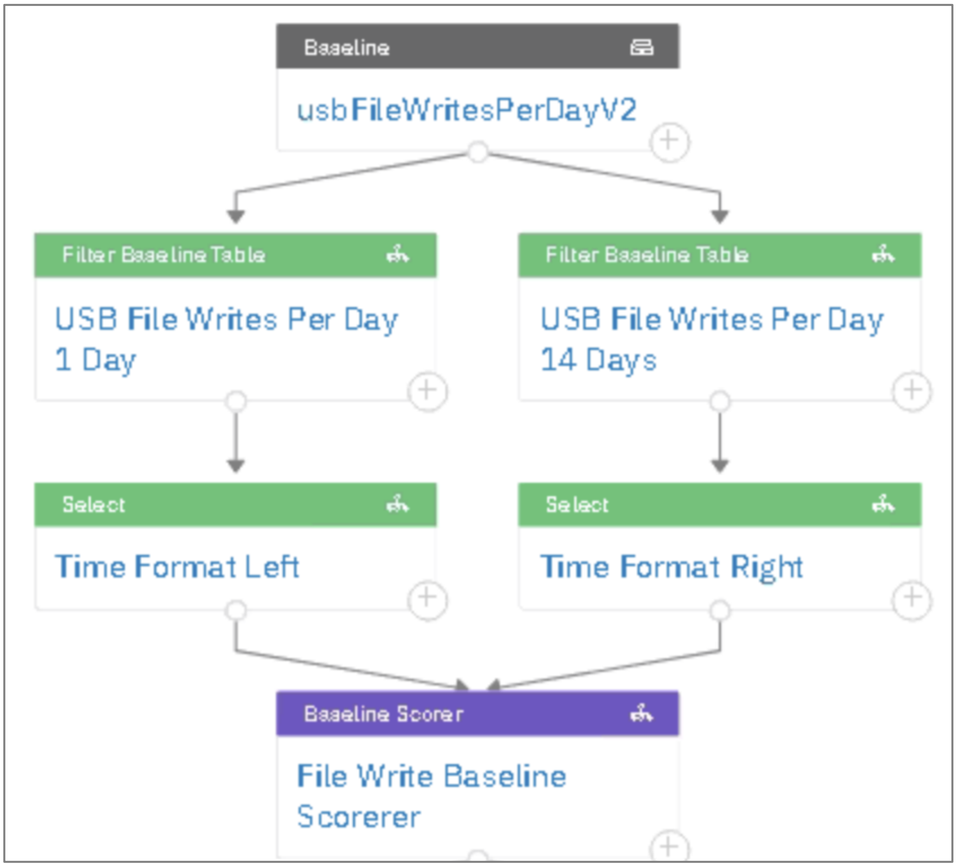
In addition, we want to track USB file writes per user per day and look for outliers that could indicate a possible change in behavior. This type of monitoring can be performed with LogicHub with a feature that is built into the product itself, a feature called “baselining”.

A baseline allows you to compare current (most recent) behavior with past behavior to determine whether the current behavior is consistent. This is helpful in determining deviations in users' or systems' behaviors.

We can use the existing playbook to gather the data for the baseline, and then from there we can define how much data to capture and use as a historical barometer for comparing a user's actions against their past actions.

The baseline playbook has the captured data at the top and from there takes input of 1 day of activity on the left side, and 14 day history of activity from the right side, and then those are processed by the baseline scoring node.

Figure 3: Sample Baseline Flow

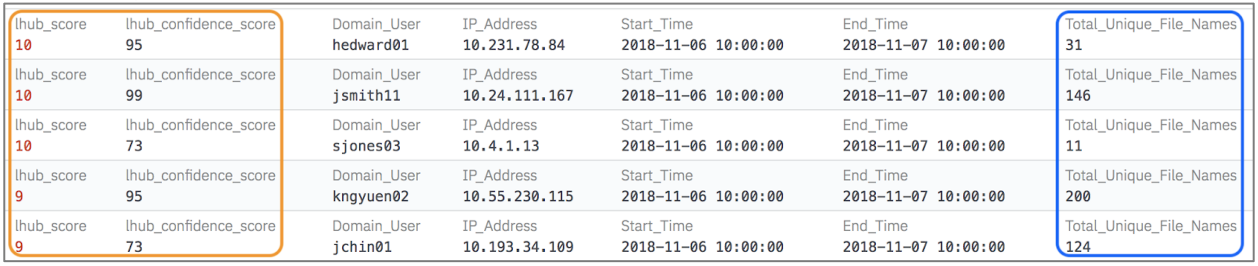


The baseline scoring node assigns both an "lhub_score" and an "lhub_confidence_score" to each unique row from the left input node. The lhub_score can be translated as a severity and the lhub_confidence_score is just as inferred, the confidence of the assigned lhub_score.

From this point the thresholds for both lhub_score and lhub_confidence_score can be decided upon. A takeaway from the sample score logs below is to notice that each

Domain_User and IP_Address pair are scored according to their own baseline history. For one user 31 files written to a USB in a day warrants a high score, while for another it takes 200 files to be considered an anomaly.

Figure 4: Sample Baseline Scoring Output



lhub_score	lhub_confidence_score	Domain_User	IP_Address	Start_Time	End_Time	Total_Unique_File_Names
10	95	hedward01	10.231.78.84	2018-11-06 10:00:00	2018-11-07 10:00:00	31
10	99	jsmith11	10.24.111.167	2018-11-06 10:00:00	2018-11-07 10:00:00	146
10	73	sjones03	10.4.1.13	2018-11-06 10:00:00	2018-11-07 10:00:00	11
9	95	kngyuen02	10.55.230.115	2018-11-06 10:00:00	2018-11-07 10:00:00	200
9	73	jchin01	10.193.34.109	2018-11-06 10:00:00	2018-11-07 10:00:00	124

Conclusion

LogicHub's intelligent automation goes beyond orchestration and data enrichment to automatically perform baseline analysis on normal behavior, in this case for copying files to external drives. The same baseline function can be easily applied to any other data source for more accurate and effective alert triage and prioritization. In this use case, the security team was able to not only automate a job, but also gained a new anomaly detection method.

For more security automation use cases, visit www.logichub.com.