Sysmon

Sysmon is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them. In this way, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

BENEFITS AND CAPABILITIES

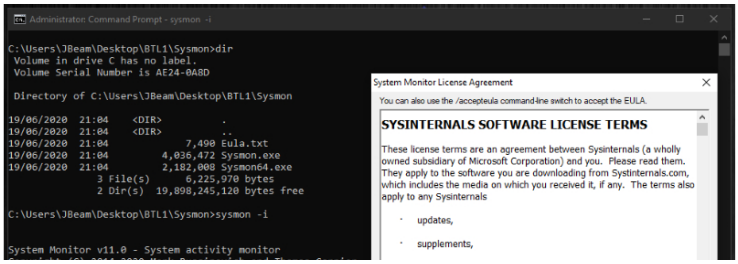
- Logs process creation with full command line for both current and parent processes.
- Include a session GUID in each events to allow correlation of events on same logon session.
- Logs loading of drivers or DLLs with their signatures and hashes.
- Optionally logs network connections, including each connection's source process, IP addresses, port numbers, hostnames and port names.
- Detects changes in file creation time to understand when a file was really created. Modification of file create timestamps is a technique commonly used by malware to cover its tracks.
- Rule filtering to include or exclude certain events dynamically.

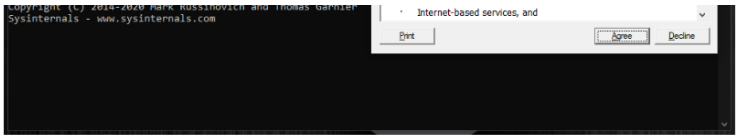
Windows Event Logs vs Sysmon Logs

Some security professionals believe that Windows event logs are.. well.. terrible, and that Sysmon is a **much** better way to log information on Windows endpoints. Why? Because the formatting is nicer, and there's just a ton more useful information compared to Windows event logs. Black Hills Information Security made a great YouTube video covering the use of Sysmon, and we recommend all students watch it at the following link: https://youtu.be/9qsP5h033Qk?t=491.

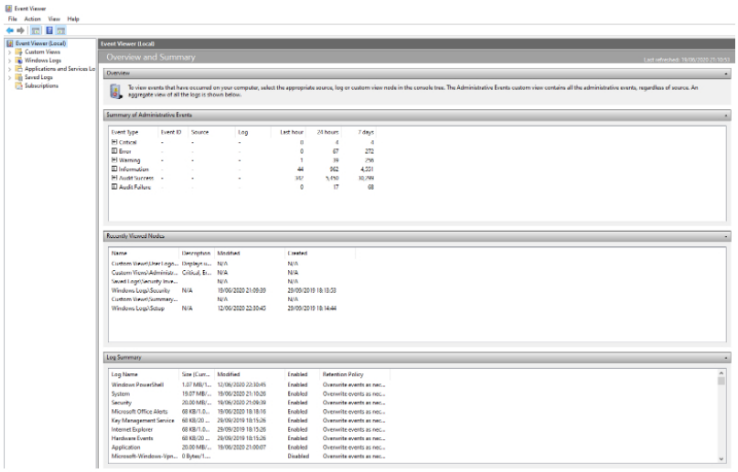
INSTALLING SYSMON

If you want to try out Sysmon on your Windows host or virtual machine, below is a quick guide on how to set it up! First, download Sysmon from the Sysinternals website here. Once you've extracted the folder within the Zip file, open a command prompt as administrator (Windows search bar > CMD > Right-click > Run as Administrator) and move to the location of the executable files. Use the command `sysmon -i` to begin the install, and click Agree when the EULA pops up.

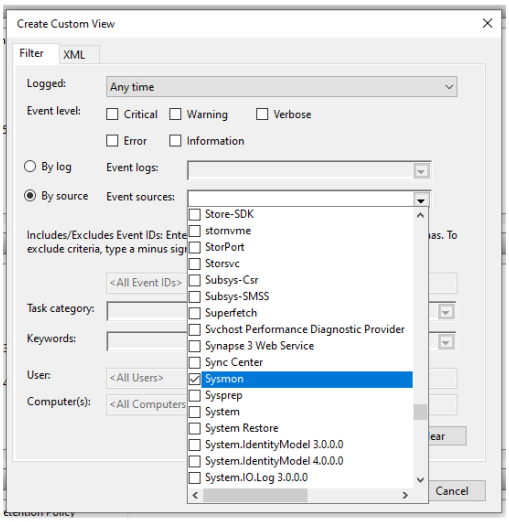




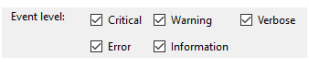
Now Sysmon is installed! Easy right? Now we want to look at Sysmon logs alongside Windows Event Logs in the tool Event Viewer. Press the Windows start button, search for "Event Viewer" and open the application.



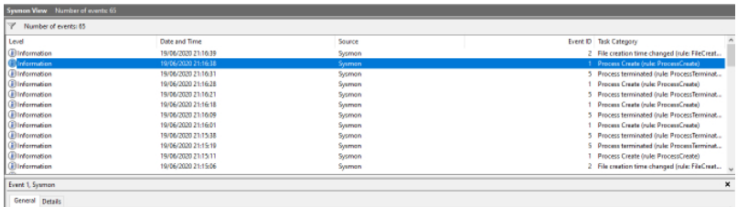
To actually see Sysmon logs, we need to create a Custom View – something we covered in the previous lesson. Click "Create Custom View" on the right-hand side, and copy what we've done in the below screenshot.



We also want to tick all of the Event Level options to ensure we can see all Sysmon logs.



Name the View whatever you want – we've decided to go for the simple name "Sysmon View", and click OK. We can now see Syslog logs, and boy do they contain a lot of information!



In an organization, we could then feed this into our SIEM to provide additional detailed logs from Windows endpoints, working alongside Windows Event Logs! The problem with Sysmon is that it's very broad, and can generate a lot of noise, something we don't want to fill our SIEM up with. To combat this, we can use Sysmon configuration files, that work to reduce logs that aren't really necessary, allowing us to focus on the logs that we really need to monitor.

An example of a Sysmon configuration file can be found here – https://github.com/SwiftOnSecurity/sysmon-config Take a look! The file has lots of comments and explanations, meaning it can also act as a tutorial on the important logs for monitoring.

Previous Topic

Mark Complete

Next Topic

Back to Lesson