Creating a timebound picture of network activity

It is your second day as a security analyst at a new company, and your network has suffered a cyber attack. Not only are you new on the job, but you are also new to Splunk Enterprise. You want to start the investigation immediately, but don't know what data sources were available or what hosts were on your network at the time of the attack. You need to gather this information before you begin to ensure your investigation is thorough. You can use Splunk software to quickly obtain a complete picture of what data is written to your indexes, through what sources, and by what devices.

Required data

System log data

How to use Splunk software for this use case

You can run many searches with Splunk software to gather information about your network and hosts. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Hosts logging data in a certain timeframe
- Hosts logging more or less data than expected
- Source types available
- Baseline of user logon times
- Processes running on a host

Next steps

Measuring impact and benefit is critical to assessing the value of security operations. The following are example metrics that can be useful to monitor when implementing this use case:

- Time to create a picture of your network at the time of the incident: How fast you are able to determine where to being the investigation
- Time to complete the investigation: The time from when the user reported the ransomware to when the investigation was completed

The content in this use case comes from a previously published blog, one of the thousands of Splunk resources available to help users succeed. These additional Splunk resources might help you understand and implement this specific use case:

- Documentation: The metadata search command
- Documentation: The tstats search command

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.