Recovering lost visibility of IT infrastructure

A malware attack has forced you to shut down your IT infrastructure monitoring software in order to protect your assets. Now, you need to recover the lost visibility into the health and operations of your infrastructure. Because you already have a Splunk universal forwarder deployed to your critical infrastructure, you know you can use Splunk to get the information you need.

Data required

- System log data
  - Windows event logs
  - *Nix operating system logs
- IT Essentials Learn
- Splunk Connect for Syslog

How to use Splunk software for this use case

You can run many searches with Splunk software to recover lost visibility of IT infrastructure. Depending on what information you have available, you might find it useful to identify some or all of the following on your hosts:

- Error and failure events on a host
- High CPU utilization alert

You might also find it useful to identify some or all of the following on your networks:

- Inventory of devices reporting network data
- Network device down
- Problems with a specific network device

Next steps

You can use the results of these searches to collect, visualize, and monitor host infrastructure, as well as to expand monitoring to include applications. Splunk software can also take on syslog receiver, log analyzer, and network traffic monitoring capabilities that you may have lost. Redirecting syslog traffic and SNMP traps to Splunk software for further analysis can be one of the quickest ways to reestablish data flow and regain basic visibility.

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:

• Demo: [Getting data in for Linux, Windows, and Cisco in Splunk Cloud](#)
• Conf talk: [Splunk Connect for Syslog: Extending the platform](#)
• Blog: [Splunk Connect for Syslog: Turnkey and scalable](#)