Monitoring for network traffic volume outliers

Scenario: You work for a small company and your manager wants you to put together a report on typical network usage among your 8 users. Specifically, your manager is interested in which external websites network users most often communicate with.

You need to establish usage baselines and monitor them for anomalous behavior. You can use the stats command in Splunk Enterprise to perform a number of simple statistical calculations that give you a picture of traffic flows from your network hosts to external IP addresses.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- **People**: Security analyst, threat hunter
- **Technologies**: Splunk Enterprise or Splunk Cloud Platform
- **Data**: Firewall data

How to use Splunk software for this use case

You can run many searches with Splunk software to establish baselines and set alerts. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Number of connections between source-destination pairs
- Volume of traffic between source-destination pairs
- Total bytes out from source IP addresses
- Percentage of total bytes out from a source to a single destination

As you establish baselines, you might find source IP addresses that you want to investigate immediately. You can run the following investigations based off results from the monitoring activities in this use case:

- Volume of network traffic from one user
- Network traffic patterns between a source-destination pair

Results

To maximize their benefit, the how-to articles linked in the previous section likely need to tie into existing processes at your organization or become new standard processes. These processes commonly impact success with this use case.
• Understanding cyclical usage patterns
• Understanding network management policies
• Creating inventories of physical and virtual network devices
• Creating network diagrams
• Adhering to frameworks, such as the IT Infrastructure Library

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:

• Identification of risk factors: The number of anomalies you identified that were positive security risks

Additional resources

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:

• Blog: Search command: stat, eventstats, and streamstats
• Blog: Hunting in a New Savanna