Monitoring command line interface actions

Scenario: Your Security Operations manager has requested that you monitor command line actions of users in your organization. They haven't specified exactly what you should set alerts for, but you know that the MITRE ATT&CK framework lists more than 150 attacks associated with the command line. You can use Splunk software to view command line strings, calculate their length to evaluate them against others in their peer groups, and determine how much time has passed since their related processes ran.

Prerequisites

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

- People: Security architect, security tools engineer
- Technologies:
  - Splunk Enterprise or Splunk Cloud Platform
  - Microsoft: Sysmon
- Data: System log data

How to use Splunk software for this use case

You can run many searches with Splunk software to detect this activity. Depending on what information you have available, you might find it useful to search for some or all of the following:

- Command line string length
- Time elapsed between two related events
- String conversion to a common format
- Previously seen command line argument
- First time seen command line argument

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:

- Enabling self-protection so that CLI commands must include the authentication password
- Requiring the use of libraries or APIs for commands
- Providing whitelists or other mechanisms for input validation

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.
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:

- **CLI execution attacks detected**: The number of true positive malicious CLI executions detected using Splunk software

### 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.