Working quickly with slash commands

When you work, you prefer to use the command-line whenever possible. You work more efficiently on a keyboard than with a mouse and want to use shortcuts like tab-complete when working in Splunk SOAR.

Use slash commands

Slash commands are a command-line interface for investigating Splunk SOAR events. Slash commands are instructions written into Splunk SOAR activity pane text box that begin with a forward slash ( / ) followed by a command. These allow you to run playbooks and actions by simply typing into your CLI, saving you time and effort by removing the need for excess mouse clicks. Paired with keyboard navigation from Phantom’s 508 compliance, slash commands are a powerful tool for every Phantom user.

When you start with a forward-slash, Splunk SOAR automatically gives you a list of available commands:

• Run an action
• Run a playbook
• Add a note to a container
• Update or edit a container
• Get datapath information for use with other actions

Slash commands come with some excellent accessibility features and in a few cases, are quicker than the same process using just a mouse and keyboard. In addition to showing proper syntax, slash commands feature suggested arguments and allow you to tab auto-complete your work, as well as use the keyboard directional keys to select which item from the pop-out menu you want to select. Lastly, it wouldn’t be a command-line interface without a --help command. If you’re ever lost, you can always enter --help to figure out what information is required.

Example

1. Type /action to see the full syntax for executing an action.
2. Select the action command and pick which action to use. If you don’t know which action to run, press space to see all the available actions.
3. Either click the action with a mouse, type in the first letters and use tab auto-complete, or use the keyboard directional keys to select an action and press Enter.
4. Review the apps available to perform the action and select one.
5. Enter any additional required information, such as selecting a specific asset with the optional flag --asset, and run the action.
6. View the command in the audit trail and the resulting summary.
7. Use enhanced keyboard navigation to select details or view the results in full screen.
Next steps

The content in this article 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 these recommendations:

- Webinar: Super speed with Splunk SOAR slash commands