Finding Windows audit log tampering

Applicability

- Product: Splunk Enterprise or Splunk Cloud
- Feature: Search
- Function: Audit log monitoring

To optimize the search shown below, you should specify an index.

Problem

You are concerned that a user might have been clearing Windows logs. You want to find out if Windows audit logs have been tampered, so that if they have, you can contact the owner of the account to ensure it was a legitimate action.
Solution

Media, iframe, embed and object tags are not supported inside of a PDF.

Additional resources

For more great content from the Splunk Education and Training team, check out Splunk How-To on YouTube or sign up for a course. In addition, these Splunk resources might help you understand and implement this search:

- Data Descriptor: Windows event logs
- Splunk Add-On: Microsoft Windows