Identifying new Windows local admin accounts

Applicability

- Product: Splunk Enterprise or Splunk Cloud
- Feature: Search
- Function: Windows user event searching

Problem

Often an attack will include the creation of a new user, followed by permissions being elevated to an admin level. You need to find these accounts so that you can take action, if needed.
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