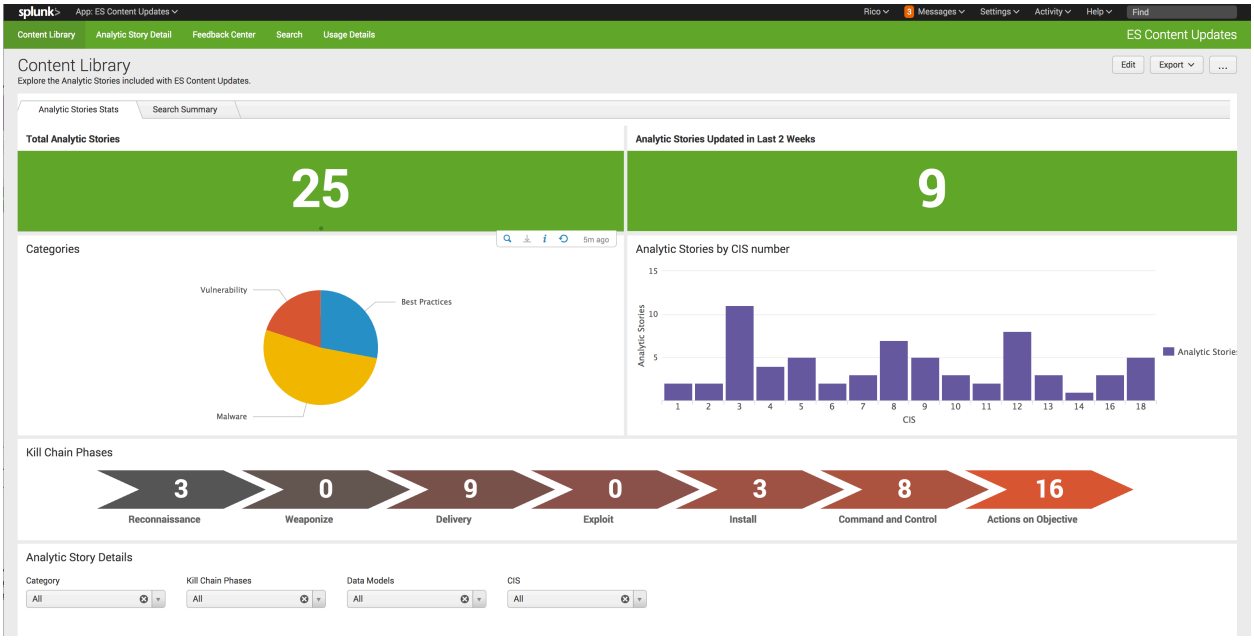
Explore the Enterprise Security Content Updates app

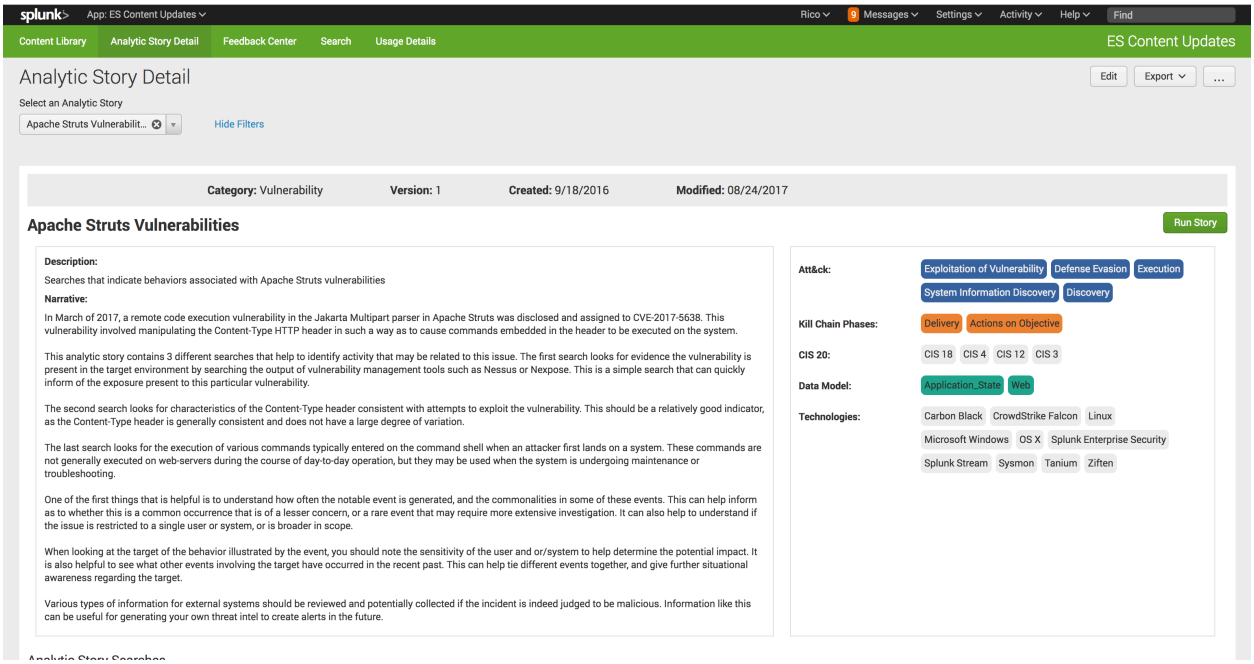
1. Navigate to the ‘Content Library’ from the navigation bar. This is typically the landing page.
2. Ensure ‘Analytic Stories Stats’ tab is selected.



3. Review the contents to identify coverage for various security frameworks.
4. Scroll down to view a listing of the Analytic Stories.
5. Select the ‘Search Summary’ tab.
6. Review the various searches and details.

Explore the Analytic Stories

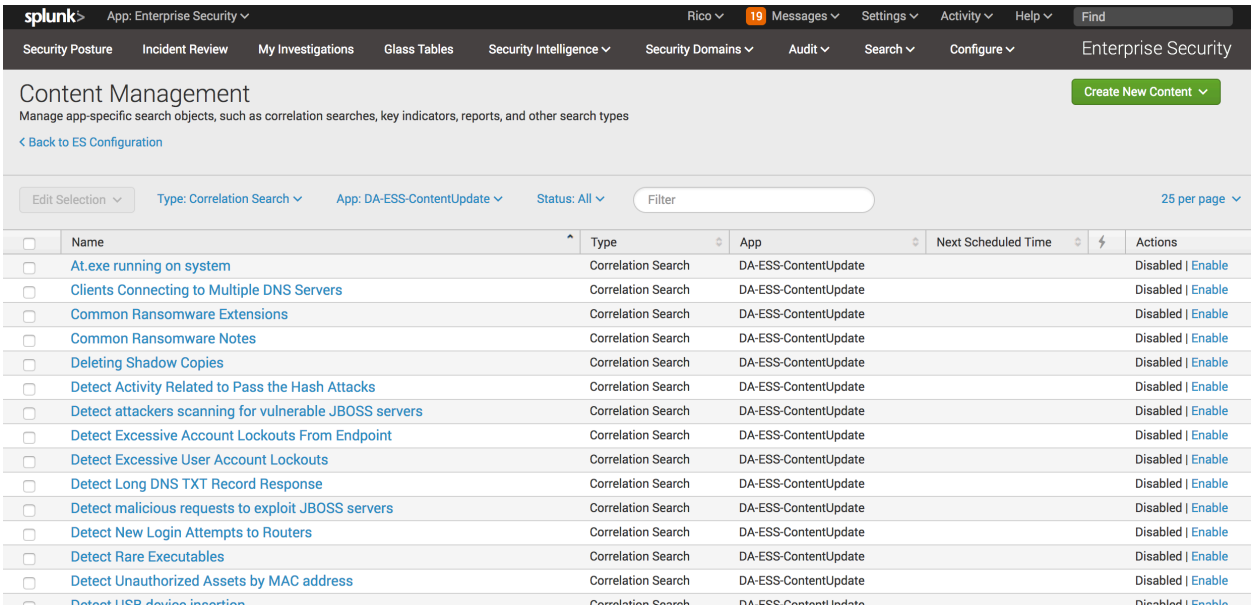
1. Navigate to the ‘Analytic Story Detail’ page from the navigation bar.
2. Select an Analytic Story from the drop down .



3. Review the various searches that make up the Analytic Story
    3.1. Detection searches, contextual searches, and investigative searches

Enable and customize a search

1. Go to the Enterprise Security app
2. Navigate to Configuration -> Content Management
3. In the ‘App’ drop down, select DA-ESS-ContentUpdate
4. In the ‘Type’ drop down, select Correlation Search



5. Select the search ‘Clients Connecting to Multiple DNS Servers’
6. Edit the search to alert when the number of different DNS servers contacted is > 7
7. Click Save