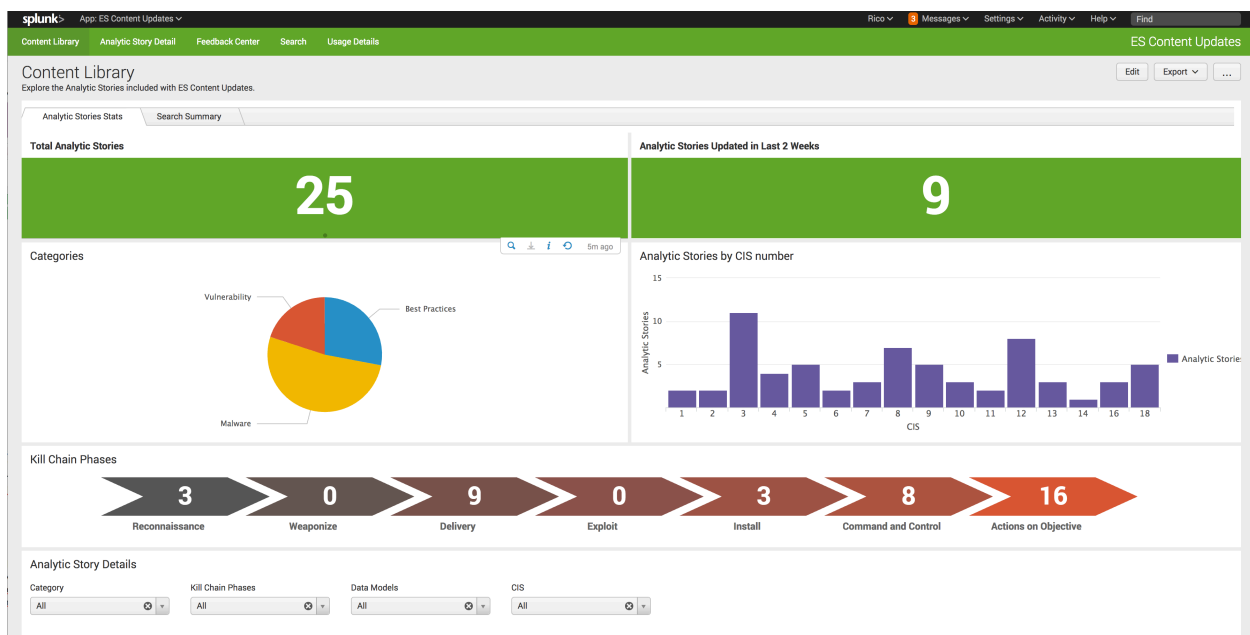


# Explore the Enterprise Security Content Updates app

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 .

The screenshot shows the 'Analytic Story Detail' page in the Splunk ES Content Updates interface. The page title is 'Analytic Story Detail' with a subtitle 'Select an Analytic Story'. A dropdown menu shows 'Apache Struts Vulnerabilities' selected. The page displays the following details:

- Category:** Vulnerability
- Version:** 1
- Created:** 9/18/2016
- Modified:** 08/24/2017

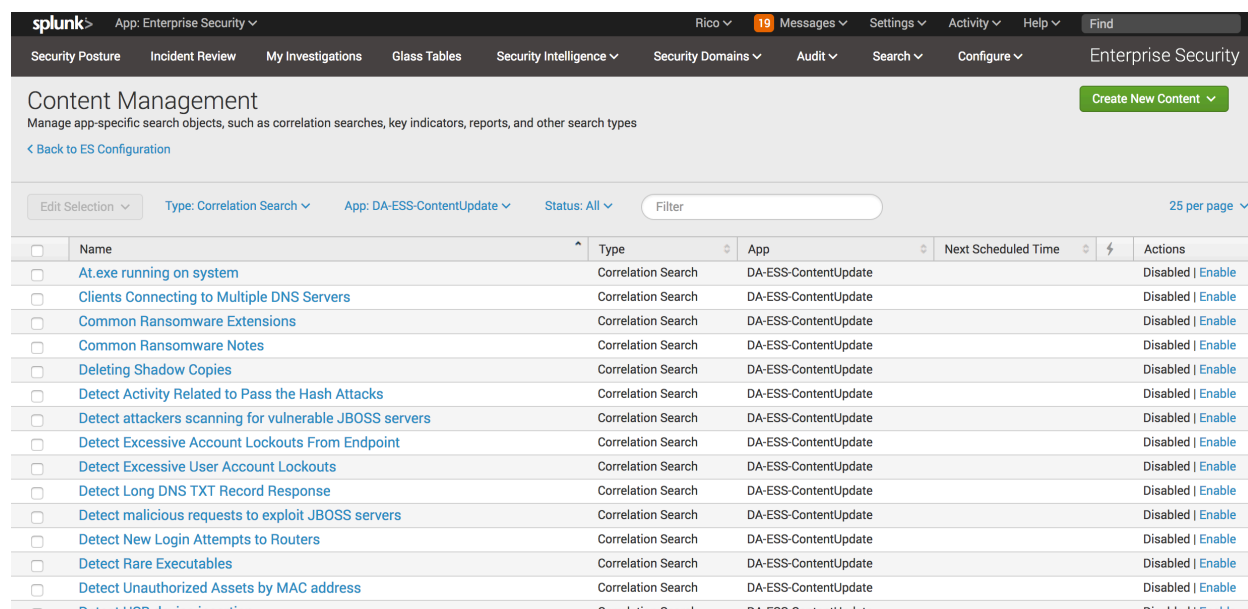
The main content area is titled 'Apache Struts Vulnerabilities' and includes a 'Run Story' button. The content is divided into two columns:

- Description:** Searches that indicate behaviors associated with Apache Struts vulnerabilities.
- Narrative:** In March of 2017, a remote code execution vulnerability in the Jakarta Multipart parser in Apache Struts was disclosed and assigned to CVE-2017-5638. This vulnerability involved manipulating the Content-Type HTTP header in such a way as to cause commands embedded in the header to be executed on the system. This analytic story contains 3 different searches that help to identify activity that may be related to this issue. The first search looks for evidence the vulnerability is present in the target environment by searching the output of vulnerability management tools such as Nessus or Nexpose. This is a simple search that can quickly inform of the exposure present to this particular vulnerability. The second search looks for characteristics of the Content-Type header consistent with attempts to exploit the vulnerability. This should be a relatively good indicator, as the Content-Type header is generally consistent and does not have a large degree of variation. The last search looks for the execution of various commands typically entered on the command shell when an attacker first lands on a system. These commands are not generally executed on web-servers during the course of day-to-day operation, but they may be used when the system is undergoing maintenance or troubleshooting. One of the first things that is helpful is to understand how often the notable event is generated, and the commonalities in some of these events. This can help inform as to whether this is a common occurrence that is of a lesser concern, or a rare event that may require more extensive investigation. It can also help to understand if the issue is restricted to a single user or system, or is broader in scope. When looking at the target of the behavior illustrated by the event, you should note the sensitivity of the user and/or system to help determine the potential impact. It is also helpful to see what other events involving the target have occurred in the recent past. This can help tie different events together, and give further situational awareness regarding the target. Various types of information for external systems should be reviewed and potentially collected if the incident is indeed judged to be malicious. Information like this can be useful for generating your own threat intel to create alerts in the future.
- Att&ck:** Exploitation of Vulnerability, Defense Evasion, Execution, System Information Discovery, Discovery.
- Kill Chain Phases:** Delivery, Actions on Objective.
- CIS 20:** CIS 18, CIS 4, CIS 12, CIS 3.
- Data Model:** Application, State, Web.
- Technologies:** Carbon Black, CrowdStrike Falcon, Linux, Microsoft Windows, OS X, Splunk Enterprise Security, Splunk Stream, Sysmon, Tanium, Ziften.

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



Content Management							
Manage app-specific search objects, such as correlation searches, key indicators, reports, and other search types							
<a href="#">Back to ES Configuration</a>							
Edit Selection ▾    Type: Correlation Search ▾    App: DA-ESS-ContentUpdate ▾    Status: All ▾    Filter    25 per page ▾							
<input type="checkbox"/>	Name	Type	App	Next Scheduled Time		Actions	
<input type="checkbox"/>	<a href="#">At.exe running on system</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Clients Connecting to Multiple DNS Servers</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Common Ransomware Extensions</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Common Ransomware Notes</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Deleting Shadow Copies</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Detect Activity Related to Pass the Hash Attacks</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Detect attackers scanning for vulnerable JBOSS servers</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Detect Excessive Account Lockouts From Endpoint</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Detect Excessive User Account Lockouts</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Detect Long DNS TXT Record Response</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Detect malicious requests to exploit JBOSS servers</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Detect New Login Attempts to Routers</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Detect Rare Executables</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Detect Unauthorized Assets by MAC address</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>
<input type="checkbox"/>	<a href="#">Detect USB device insertion</a>	Correlation Search	DA-ESS-ContentUpdate			Disabled	<a href="#">Enable</a>

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