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-ContentUpdate4. In the 'Type' drop down, select Correlation Search

splur	k⇒ App: Enterprise Security ∽	Rico	✓ 19 Message	s ∽ Settings ∽	Activity	Find
Securit	Posture Incident Review My Investigations Glass Tables Security Intell	ligence 🗸 Security Don	mains ∽ Audit	∽ Search ∽	Configure 🗸	Enterprise Security
Content Management Manage app-specific search objects, such as correlation searches, key indicators, reports, and other search types < Back to ES Configuration Create New Content ~						
Edit S	election V Type: Correlation Search V App: DA-ESS-ContentUpdate V State	us: All V Filter				25 per page 🗸
	Name	^ Туре	App	¢	Next Scheduled Time	Actions
	At.exe running on system	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
	Clients Connecting to Multiple DNS Servers	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
	Common Ransomware Extensions	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
	Common Ransomware Notes	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
	Deleting Shadow Copies	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
	Detect Activity Related to Pass the Hash Attacks	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
	Detect attackers scanning for vulnerable JBOSS servers	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
	Detect Excessive Account Lockouts From Endpoint	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
	Detect Excessive User Account Lockouts	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
	Detect Long DNS TXT Record Response	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
0	Detect malicious requests to exploit JBOSS servers	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
0	Detect New Login Attempts to Routers	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
_	Detect Rare Executables	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
	Detect Unauthorized Assets by MAC address	Correlation Search	DA-ESS-Conter	tUpdate		Disabled Enable
	Datast LICE davias insertion	Correlation Coarob	DA ECC.Contor	ti Indata		Disabled I Enable

- 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