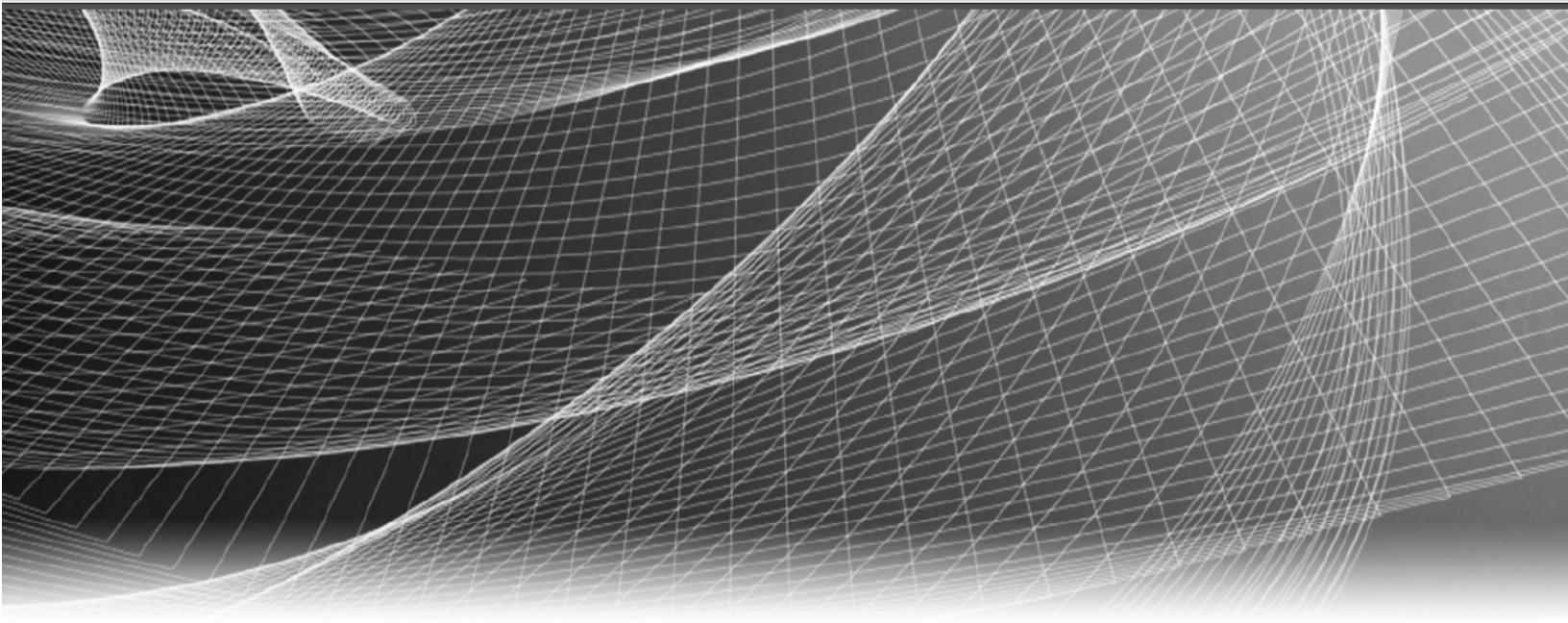


RSA Security Analytics

Hunting Feed

RSA

EMC²

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Contents

Hunting Feed

The Hunting Feed tags all resources (application rules and parsers) based on proven hunting methodologies for advanced threat detection. These concepts are used to provide a more directed discovery and inspection stage over the course of information security investigations. This is useful for front line analysts, because it minimizes the time dedicated to mining logs or sessions in support of their findings.

This document highlights an approach to information security analysis with a focus on active compromise discovery. The Hunting feed is used to introduce six new keys. These keys provide a way to support incident response through application protocol assessment, file evaluation and session scrutiny. These methods, coupled with traffic flow and existing Live content, provide a more focused means for hunting through security datasets.

Hunting Meta

We have added the following six meta keys for the Hunting profile. The Deployment section describes how to add these keys to the custom concentrator index.

Analysis Keys

Analysis keys provide an operational workflow for investigative operations through natural language descriptors. They quickly dissect collections based on features observed in network and security information.

- *Session Analysis* (`analysis.session` exists): Client-Server communication summations, deviations, conduct and session attributes.
- *Service Analysis* (`analysis.service` exists): Core application protocols identification. An underlying powerhouse of service-based inspection.
- *File Analysis* (`analysis.file` exists): A large inspection library that highlights file characteristics and anomalies.

Compromise Keys

Compromise keys provide insight and narratives into the varied attributes of an attack. These can be atomic or computed indicators.

- *Indicators of Compromise* (`ioc` exists): Indicators of Compromise are now ubiquitous across the information security landscape. It is important to classify and store them accordingly.
- *Behaviors of Compromise* (`boc` exists): The Behaviors of Compromise meta key is designated for suspect or nefarious behavior outside of standard signature-based detections.

- *Enablers of Compromise* (`eoc` exists): Enablers of Compromise are instances of poor information or operational security. Post-mortem often ties these to root cause.

Deployment

This section discusses:

- How to add the meta keys used by the feed to the Index file, and
- How to deploy the feed.

About the Meta Keys

To get value out of the Investigation feed, two new meta keys are used. The below keys should be added to your **index-concentrator-custom.xml**.

Note: These keys are now being delivered out of the box in **index-concentrator.xml** with NetWitness Suite version 10.6.2 and newer. If your installed version is prior to 10.6.2, you must add the keys to **index-concentrator-custom.xml**.

```
<key description="Session Analysis" level="IndexValues" name="analysis.session" format="Text" valueMax="10000"/>
<key description="Service Analysis" level="IndexValues" name="analysis.service" format="Text" valueMax="10000"/>
<key description="File Analysis" level="IndexValues" name="analysis.file" format="Text" valueMax="10000"/>
<key description="Indicators of Compromise" level="IndexValues" name="ioc" format="Text" valueMax="10000"/>
<key description="Behaviors of Compromise" level="IndexValues" name="boc" format="Text" valueMax="10000"/>
<key description="Enablers of Compromise" level="IndexValues" name="eoc" format="Text" valueMax="10000"/>
```

To add keys to index-concentrator-custom.xml:

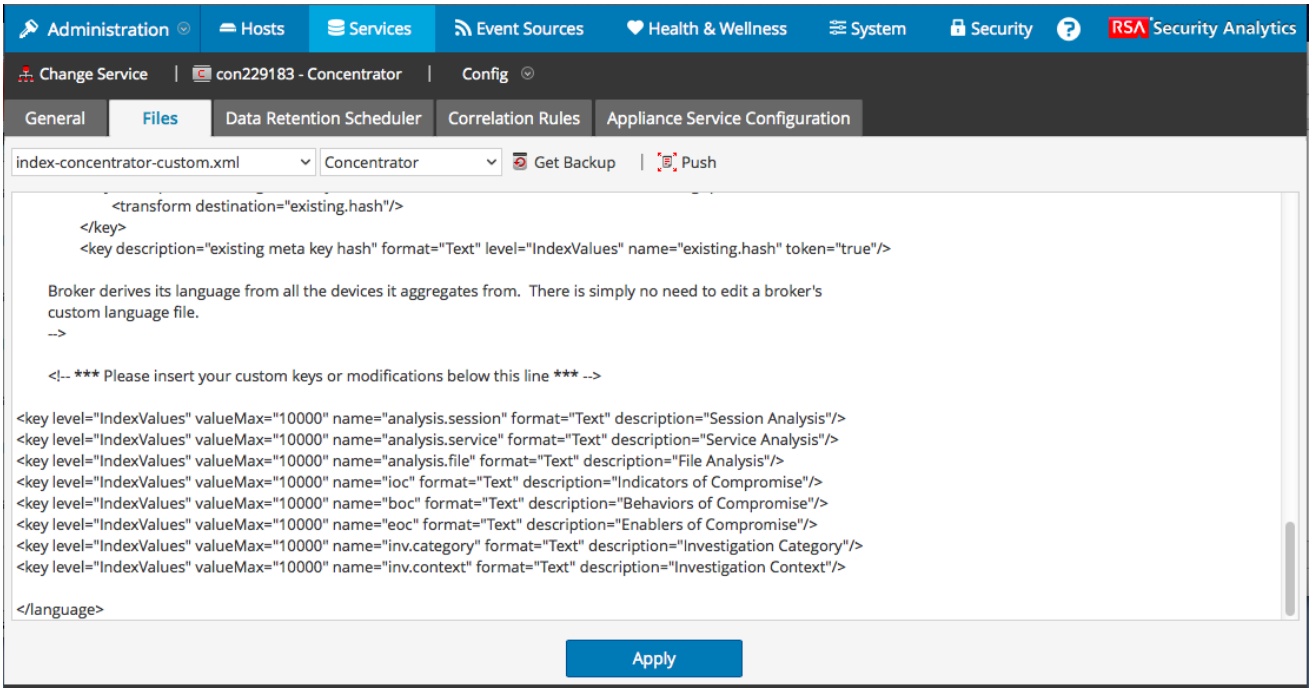
If your installed version of NetWitness Suite is 10.6.2 or newer, you can skip this procedure.

1. In the Security Analytics menu, select **Administration** > **Services**, and select a Concentrator.
2. Select **View** > **Config** from the Actions menu.
3. Select the **Files** tab, then select the **index-concentrator-custom.xml** file.
4. Add the following lines:

   ```
   <key description="Session Analysis" level="IndexValues" name="analysis.session" format="Text"
   valueMax="10000"/>
   <key description="Service Analysis" level="IndexValues" name="analysis.service" format="Text"
   valueMax="10000"/>
   <key description="File Analysis" level="IndexValues" name="analysis.file" format="Text" valueMax="10000"/>
   <key description="Indicators of Compromise" level="IndexValues" name="ioc" format="Text" valueMax="10000"/>
   <key description="Behaviors of Compromise" level="IndexValues" name="boc" format="Text" valueMax="10000"/>
   <key description="Enablers of Compromise" level="IndexValues" name="eoc" format="Text" valueMax="10000"/>
   ```

5. Click **Apply**.

This screen shows the lines being added to the file in NetWitness Suite:

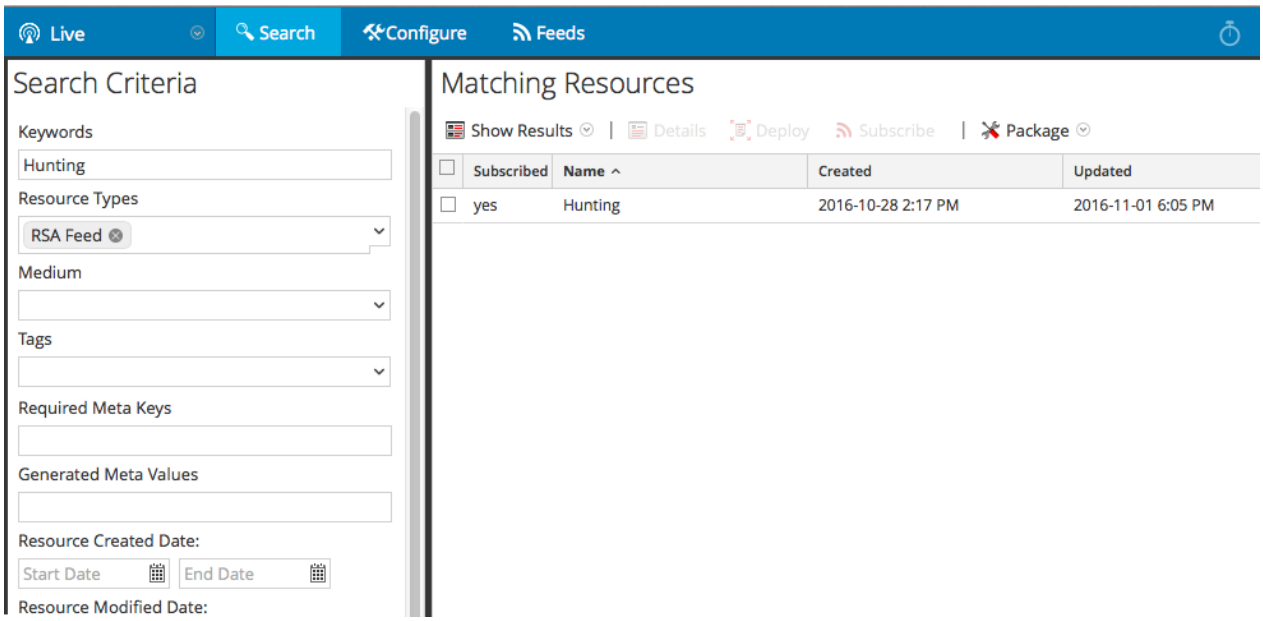


Deploy the Feed

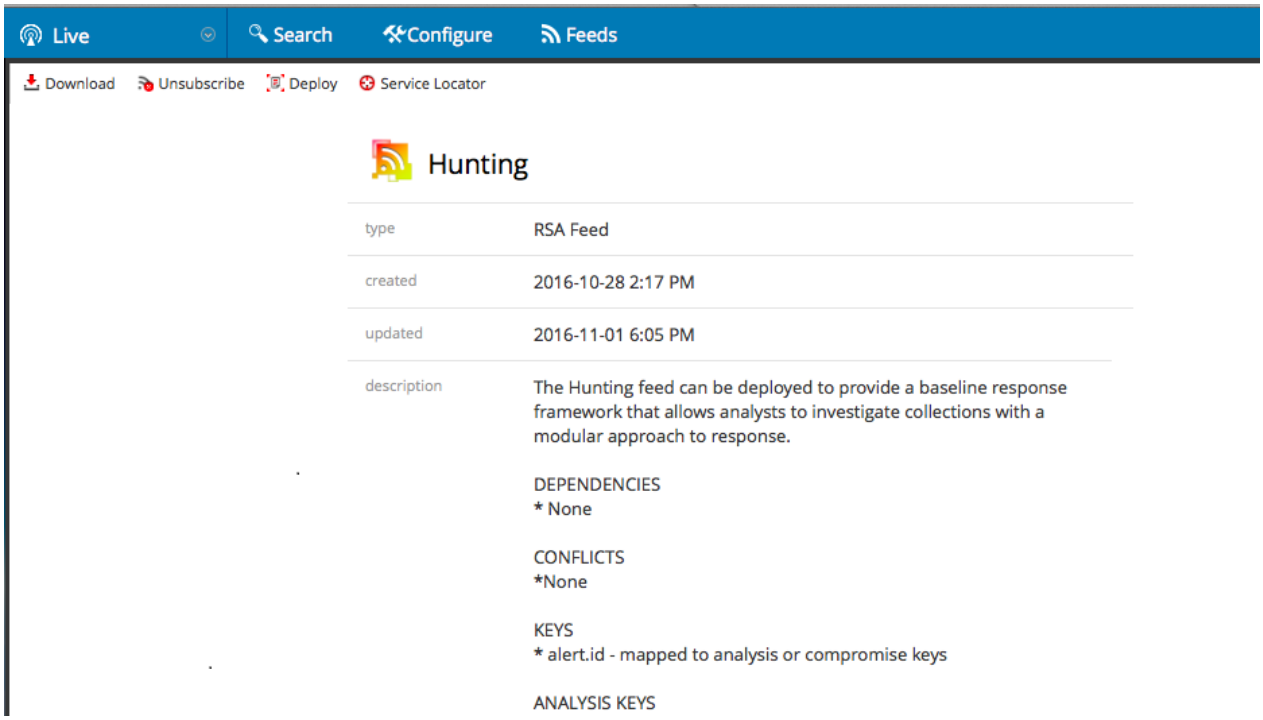
To deploy the Hunting feed:

1. From the NetWitness Suite menu, select **Live > Search**.
2. In the **Search Criteria** section, select **RSA Feed** from the **Resource Types** drop-down menu.
3. In the **Keywords** field, type **Hunting**.
4. Click **Search**.

   The **Hunting** feed appears in the Matching Resources section.



And this is a sample screen of the feed's details in Live Search:



5. Select the feed and click **Deploy** from the menu bar.

   The Deployment Wizard dialog box is displayed.

6. Click through the screens of the Wizard.

   a. In the **Resources** screen, confirm the correct feed is listed, and click **Next**.

   b. In the **Services** screen, select the services to which you want to deploy the content. You can select

any combination of services and service groups.

- Use the **Services** tab to select individual services, list of services, and service groups that are configured in the Administration Services view.
- Use the **Groups** tab to select groups of services.

c. Click **Next**.

d. On the **Review** page, make sure that you have selected correct resources and the services to which you want to deploy them.

e. Click **Deploy**.

The Deploy page is displayed. The Progress bar turns green when you have successfully deployed the resources to the selected services.

f. Click **Close**.