Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Enable notables for correlation searches

Generated: 4/17/2022 6:45 pm

Copyright (c) 2022 Splunk Inc. All Rights Reserved

Enable notables for correlation searches

When you upgrade to Enterprise Security 6.4.x or higher, notable actions for some correlation searches may be disabled. If you want these correlation searches to generate notables, you must re-enable the notable actions for the correlation searches.

Use the following list to identify the correlation searches that may be disabled:

- Access - Account Deleted - Rule
- Access - Brute Force Access Behavior Detected - Rule
- Access - Cleartext Password At Rest - Rule
- Access - Default Account Usage - Rule
- Access - Default Accounts At Rest - Rule
- Audit - Anomalous Audit Trail Activity Detected - Rule
- Endpoint - Should Timesync Host Not Syncing - Rule
- Endpoint - High Number of Hosts Not Updating Malware Signatures - Rule
- Network - Substantial Increase in an Event - Rule
- Network - Substantial Increase in Port Activity (By Destination) - Rule
- Asset - Asset Ownership Unspecified - Rule
- Identity - Activity from Expired User Identity â Rule

Steps

1. From the Enterprise Security menu, select **Configure > Content > Content Management**. This displays the list of knowledge objects and correlation searches.
2. Click on the correlation search for which you want to re-enable the notables.
   This opens the correlation search editor.
3. Scroll down to **Adaptive Response Actions** and click on **Add New Response Action**.
4. From the list of adaptive response actions, select **Notable**.
5. Scroll to **Recommended Actions** and select the notable actions that you want to enable for the correlation search from the list.
6. Click **Save**.

In releases 6.4.0 and higher, the audit search [Audit - Notable Default Modify for Correlation Searches] generates a health check warning if default correlation searches that have been changed to generate risk notables are run as searches that generate notables. To prevent the searches from running in an infinite loop and remove the health check warning, disable the [Audit - Notable Default Modify for Correlation Searches] search on Splunk Enterprise Security UI.