Splunk® Enterprise Security Administer
Splunk Enterprise Security 6.1.0

List correlation searches in Splunk Enterprise Security

Generated: 2/05/2020 10:08 am
List correlation searches in Splunk Enterprise Security

To obtain a list of correlation searches enabled in Splunk Enterprise Security, use a REST search to extract the information that you want in a table.

For example, create a table with the app, security domain, name, and description of all correlation searches in your environment.

```
| rest splunk_server=local count=0 /services/saved/searches | where match('action.correlationsearch.enabled', "1\[Tt]\[Tt]\[Rr]\[Uu]\[Ee\]") | rename eai:acl.app as app, title as csearch_name, action.correlationsearch.label as csearch_label, action.notable.param.security_domain as security_domain | table csearch_name, csearch_label, app, security_domain, description
```

As another example, create a table with only the enabled correlation searches and the adaptive response actions associated with those searches in your environment. To see the adaptive response actions for all correlation searches, remove where disabled=0.

```
| rest splunk_server=local count=0 /servicesNS/-/SplunkEnterpriseSecuritySuite/saved/searches | where match('action.correlationsearch.enabled', "1\[Tt]\[Tt]\[Rr]\[Uu]\[Ee\]") | where disabled=0 | eval actions=split(actions, ",") | table title,actions
```