Splunk Adoption Motion (SAM)

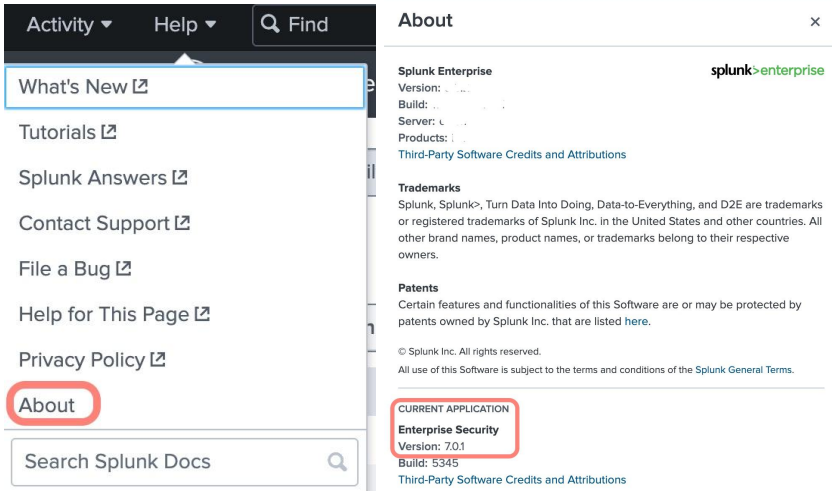
Enterprise Security

Question Instructions

ES Version

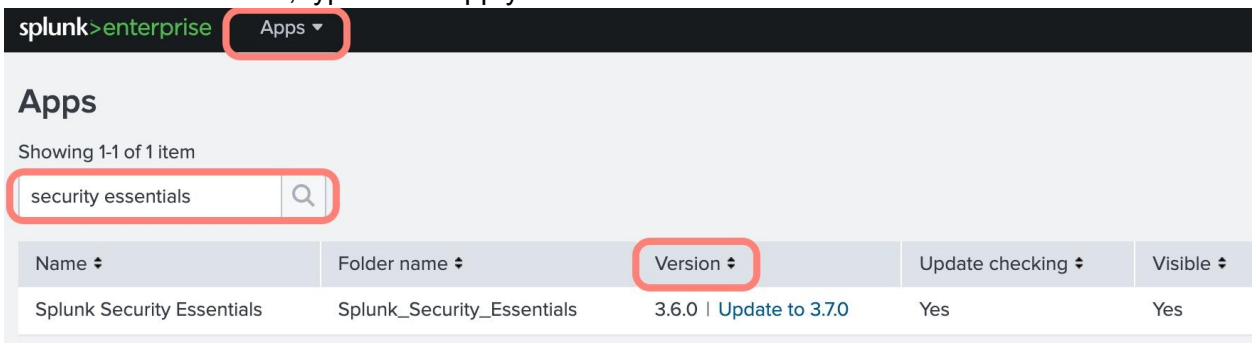
On Splunkbase, view the Enterprise Security app page
Scroll down to the Summary and click on the "Version History" tab
The latest version is at the top
Compare that version to the currently installed version:

- On the Enterprise Security Search Head, click on the Apps dropdown
- Click on Enterprise Security to open the app
- In the upper right corner, click on “Help”
- In the dropdown, click “About”
- The Enterprise Security version is displayed at the bottom of the pop-up box



Manage Apps View

Click on the Apps dropdown at the top of the page
Click on Manage Apps at the bottom of the dropdown menu
In the search filter box, type in the app you want to search for and click the search button



Search Queries

Query 1 - Activity by page

```
Unset
index=_internal sourcetype=splunkd_ui_access
| rex "\\/data\\/ui\\/views\\/(?<dashboard>[^\?]+)"
| stats count by dashboard
```

Query 2 - MITRE ATT&CK annotations

```
Unset
index=notable "annotations.mitre_attack"="*"
| stats count by "annotations.mitre_attack"
```

Query 3 - Other framework annotations

```
Unset
index=risk "annotations._frameworks"="*"
| stats count by "annotations._frameworks"
```

Query 4 - Risk objects

```
Unset
index=risk risk_object_type="*"
| stats count by risk_object_type
```

Query 5 - Active users

```
Unset
index=_audit sourcetype=audittrail NOT user="n/a" NOT
user="splunk-system-user" NOT "scheduler__nobody__search"
"info=succeeded"
| stats count by user
```

Query 6 - List of apps on local server

```
Unset
| rest /services/apps/local splunk_server=local
| search disabled=0
| table label version
```

Query 7 - Top 5 Data models

```
Unset
| datamodel
| spath "objects{}.tsidxNamespace"
| rename "objects{}.tsidxNamespace" as objectName
| stats count by objectName
| rex field="objectName"
"datamodel=\"(?<model>[^.]+).(?<dataset>[^\"]+)"
| where objectName!=""
| map search="|tstats summariesonly=t count dc(host) as dc_host
values($dataset$.tag) as tags
            from datamodel=$model$.$dataset$ by index sourcetype | eval
model=\"$model$.$dataset$\"" maxsearches=99
| eval tags=mvjoin(tags,"|")
| eval datamodel=mvindex(split(model,"."),0)
| search datamodel IN ("Authentication" "Identity_Management"
"Network_Traffic" "Incident_Management" "Threat_Intelligence")
| table datamodel, index, sourcetype, count
| rename count as dm_events
```

Query 8 - Notable event status changes

```
Unset
index=_audit sourcetype=incident_review
orig_action_name=notable_event_edit
| stats count
```

Query 9 - Correlation searches enabled and scheduled

```
Unset
| rest /services/saved/searches splunk_server=local
| where match('action.correlationsearch.enabled',
"1|[Tt]|[Tt][Rr][Uu][Ee]") and match('is_scheduled',"1") and
match('disabled',"0")
| table title next_scheduled_time
```

Query 10 - Searches enabled by App

```
Unset
| rest splunk_server=local /servicesNS/-/-/saved/searches
| search disabled=0 action.correlationsearch.enabled=1
| fields eai:acl.app action.correlationsearch.label eai:acl.app
action.correlationsearch.label search disabled author
| rex field=search max_match=0
"datamodel[:\"\(=\s]*?(?<datamodel>\w+)"
| rex field=search max_match=0 "index=(?<indexes>[\w\*\_]+)"
| eval datamodel=coalesce(datamodel,"")
| mvexpand datamodel
| join type=left overwrite=f datamodel
    [| rest splunk_server=local /servicesNS/-/-/datamodel/model
    | fields title description
    | rename title as datamodel
    | rex field=description max_match=0 "\`(?<macro>\w+)\`"
    | rex field=description max_match=0
"index=(?<indexes>[\w\*\_]+)"
    | eval indexes=mvdedup(indexes), macro=mvdedup(macro)
    | fields - description
    | mvexpand macro]
| join type=left macro
    [| rest /services/admin/macros
    | fields title definition
    | rename title as macro, definition as macro_definition]
| eval search_field=""
| foreach eai:acl.app action.correlationsearch.label search
disabled author
    [ eval search_field=search_field + " " +
coalesce('<<FIELD>>',"")]
| search search_field="***"
```

```
| search eai:acl.app="*" datamodel="*"
action.correlationsearch.label="*" author=*
| fields - search_field
```

Query 11 - Notable events assigned

```
Unset
index=_audit sourcetype=incident_review
orig_action_name=notable_event_edit
| stats count by owner
```

Query 12 - Vulnerability data

```
Unset
| `tstats` dc(Vulnerabilities.dest) from
datamodel=Vulnerabilities.Vulnerabilities where * by _time
span=1d
| stats dc(Vulnerabilities.dest)
```

Query 13 - Notable index count

```
Unset
| tstats count where index=notable by index
```

Query 14 - ES Lookup files modified

```
Unset
index=_audit sourcetype=audittrail
path="/opt/splunk/etc/apps/SplunkEnterpriseSecuritySuite/lookups/
*.csv" action=modified
| table file_name action modtime
```

Query 15 - Number of enabled searches

```
Unset
| rest splunk_server=local /servicesNS/-/-/saved/searches
| search disabled=0 action.correlationsearch.enabled=1
| stats count
```

Query 16 - Investigation collaborators

```
Unset
| `investigations`
| table name collaborators
```

Query 17 - Percent of MITRE annotations

```
Unset
| rest /services/saved/searches splunk_server=local
| where match('action.correlationsearch.enabled',
"1|[Tt]|[Tt][Rr][Uu][Ee]") and match('is_scheduled',"1") and
match('disabled',"0")
| eventstats count as total
| search action.correlationsearch.annotations="*mitre*"
| stats count as "mitre" by total
| eval percentage=(mitre*100)/total
```

Query 18 - Percent of other framework annotations

```
Unset
| rest /services/saved/searches splunk_server=local
| where match('action.correlationsearch.enabled',
"1|[Tt]|[Tt][Rr][Uu][Ee]") and match('is_scheduled',"1") and
match('disabled',"0")
| eventstats count as total
| search action.correlationsearch.annotations IN ("*cis*"
"*nist*" "kill_chain*")
| stats count as "frameworks" by total
| eval percentage=(frameworks*100)/total
```

Query 19 - Percent of searches are risk rules

```
Unset
| rest /services/saved/searches splunk_server=local
| where match('action.correlationsearch.enabled',
"1|[Tt]|[Tt][Rr][Uu][Ee]")
| eventstats count as total
| search action.risk.param._risk="*score*"
| stats count as "riskrules" by total
| eval percentage=(riskrules*100)/total
```

Query 20 - Asset & Identity custom fields added

```
Unset
index=_configtracker sourcetype=splunk_configuration_change
"data.path"="/opt/splunk/etc/apps/SA-IdentityManagement/local/pro
ps.conf" "data.changes{}.properties{}.new_value"="*"
| table component data.action "data.changes{}.properties{}.name"
"data.changes{}.properties{}.new_value"
```

Query 21 - Risk index populating with data past 7 days

```
Unset
|tstats count where index="risk" sourcetype="*" earliest=-7d@d
```

Query 22 - Dashboards created

```
Unset
index=_audit sourcetype=audittrail action=created
file_name="*.xml"
| table modtime action file_name host
```

Query 23 - Reports created

```
Unset
index=_audit sourcetype=audittrail action=create_saved_search
| table action type savedsearch app owner host
```

Query 24 - Percent unassigned notables

```
Unset
`notable`
| search urgency IN (high critical)
| eventstats count as total
| search owner=unassigned
| stats count as "unassigned" by total
| eval percentage=(unassigned*100)/total
```

Query 25 - Adaptive Response Actions Enabled

```
Unset
| rest /services/saved/searches splunk_server=local
| where match('action.correlationsearch.enabled',
"1|[Tt]|[Tt][Rr][Uu][Ee]") and match('is_scheduled',"1") and
match('disabled',"0")
| table actions
```

Query 26 - Percent of risk notables with MITRE

```
Unset
index=risk sourcetype=stash
| eventstats count as total
| search annotations._frameworks="*mitre*"
| stats count as "mitre" by total
| eval percentage=(mitre*100)/total
```

Query 27 - Percent of risk notables with MITRE

```
Unset
index=risk sourcetype=stash
| eventstats count as total
| search annotations._frameworks IN ("*cis*" "*nist*"
"kill_chain*")
| stats count as "frameworks" by total
| eval percentage=(frameworks*100)/total
```

Query 28 - Reduction in Notables

```
Unset
index=notable|eval notable=if(eventtype="risk_notables","Risk
Notable","Notable")|stats count by notable
|transpose 0 header_field=notable
|eval p=round(100-('Risk Notable'/Notable)*100,1)
|table p
```

Query 29 - Percent that are risk notables

```
Unset
index=notable sourcetype=stash
| eventstats count as total
| search eventtype=risk_notables
| stats count as "risknotables" by total
| eval percentage=(risknotables*100)/total
```

SOAR

SOAR Version

On my.phantom.us (login required), click Product view the Official Unprivileged Releases
The latest version is at the top, located in Product Version column
Compare that version to the currently installed version:

- On the SOAR instance, click on “Home” dropdown
- In the upper right corner, version is listed

Common SOAR apps configured (Top 10 Categories)

Within the SOAR console, choose Apps from the drop down menu on the left side. Provide a count of Configured Apps from each of these categories, using the All Categories selector on the right hand side of the interface :
Ticketing
Reputation
Threat Intel
Email
Endpoint
Identity Management
Splunk HTTP

Common active actions (automation of SOC tasks)

Evidence in playbooks or workbooks that SOC tasks are in early stages of automation. The following use cases for SOC automation may be applicable:
Customer and Host information
Reputation enrichment for observables
Endpoint alert enrichment
Ticket creation, update, and closure
Reassign event, set status, and other basic case management automations