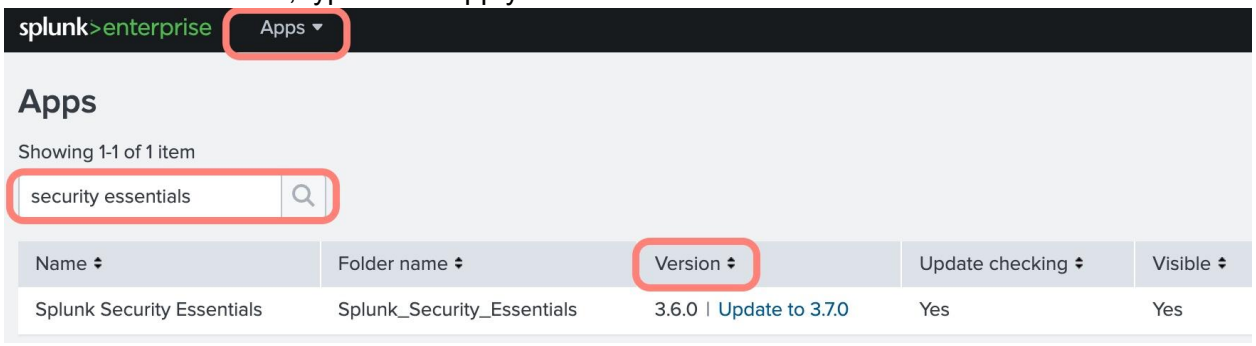
# SAM Question Guidance

# Enterprise Security

## Question Instructions

### 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

## Basic

### Query 1.1 - Security apps installed

```
Unset
| rest /services/apps/local splunk_server=local
| search disabled=0 label IN ("Enterprise Security" "ES Content
Updates" "Splunk Security Essentials" "Splunk Common Information
Model" "SA-Investigator" "Mission Control" "*soar*" "*phantom*"
"*uba*" "*behavior*" "*trustar*" "*intelligence*")
| table label version
| rename label as App
| sort label
```

### Query 1.2 - ES Version

```
Unset
| rest /services/apps/local splunk_server=local
```

```
| search disabled=0 label="Enterprise Security"
| table version
```

### Query 1.3 - Assets & Identities data model usage

```
Unset
| `identities`
| stats count
| eval "Count Type"="Identities"
| append
    [ search `assets` | stats count | eval "Count Type"="Assets"]
| table "Count Type", count
```

### Query 1.4 - ES lookups enabled

```
Unset
| rest /services/data/transforms/lookups splunk_server=local
| search eai:acl.app=SplunkEnterpriseSecuritySuite
| eventstats count as total
| search disabled=0
| stats count as "enabled" by total
| eval percentage=(enabled*100)/total
```

## Query 1.5 - Common apps installed on ES search head

```
Unset
| rest /services/apps/local splunk_server=local
| search disabled=0 label IN ("ES Content Updates" "Splunk
Security Essentials" "Splunk Common Information Model"
"SA-ThreatIntelligence" "ES Content Updates" "*soar*" "*uba*"
"*behavior*" "*trustar*" "*phantom*" "*intelligence*")
| table label version
| rename label as App
| sort label
```

## Query 1.6 - Notable events generated

```
Unset
index=notable sourcetype=stash
| stats count
```

## Query 1.7 - Incident Review page views

```
Unset
index=_internal sourcetype=splunkd_ui_access file=incident_review
| stats count
```

## Query 1.8 - MITRE ATT&CK page views in SSE

```
Unset
index=_internal sourcetype=splunk_web_access host=* user=*
| rex field=uri_path ".*/(?<title>[^/]*)$"
| join title
[| rest /servicesNS/-/-/data/ui/views splunk_server=local
| search isDashboard=1 isVisible=1
eai:acl.app="Splunk_Security_Essentials" title="*mitre*"
| rename eai:acl.app as app
| fields title app ]
| rename title as dashboard
| stats count by dashboard
```

## Query 1.9 - MITRE ATT&CK annotations

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

## Query 1.10 - Other framework annotations

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

## Query 1.11 - Out-of-the-box RBA rules enabled

```
Unset
| rest splunk_server=local /servicesNS/-/-/saved/searches
| search action.correlationsearch.label IN ("ATT&CK*" "Risk
Threshold*")
| eval disabled=case(disabled=0,"Yes",disabled=1,"No")
| eval
is_scheduled=case(is_scheduled=0,"No",is_scheduled=1,"Yes")
| table action.correlationsearch.label disabled is_scheduled
next_scheduled_time
| rename action.correlationsearch.label AS "Incident Rule"
disabled AS "Enabled" is_scheduled AS "Scheduled"
next_scheduled_time AS "Next Scheduled Time"
```

## Query 1.12 - Risk Factors enabled

```
Unset
index=_introspection sourcetype=splunk_telemetry
app=SplunkEnterpriseSecuritySuite
component="app.SplunkEnterpriseSecuritySuite.riskfactors_usage"
| table data.total
```

## Query 1.13 - Risk notables generated

```
Unset
index=notable sourcetype=stash eventtype=risk_notables
| stats count
```

# Foundations

## Query 2.1 - ESS Analyst user logins

```
Unset
| rest /services/authentication/users splunk_server=local
| fields realname title roles
| search roles="*analyst*" title=*
| appendcols
    [| search index=_audit sourcetype=audittrail tag=authentication
action=success info=succeeded
    | stats count by user]
| search title=*
| stats sum(count)
```

## Query 2.2 - Top 5 Data models

(may take >30 seconds for search completion due to map command)

```
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 2.3 - Correlation searches scheduled an running

```
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")
| stats count
```

### Query 2.4 - Searches enabled by App

```
Unset
| rest splunk_server=local /servicesNS/-/-/saved/searches
| search disabled=0
| stats count by eai:acl.app
```

### Query 2.5 - Security dashboard page views

```
Unset
index=_internal sourcetype=splunkd_ui_access
| rex "\\/data\\/ui\\/views\\/(?<dashboard>[^\?]+)"
| search dashboard=ess_use_case_library
| stats count
| eval "Count Type"="ES Use Case Library"
| append
    [ search index=_internal sourcetype=splunkd_ui_access
    | rex "\\/data\\/ui\\/views\\/(?<dashboard>[^\?]+)"
    | search dashboard=risk_analysis
    | stats count
    | eval "Count Type"="Risk Analysis"]
| append
    [ search index=_internal sourcetype=splunkd_ui_access
    | rex "\\/data\\/ui\\/views\\/(?<dashboard>[^\?]+)"
    | search dashboard=vuln_operations
    | stats count
    | eval "Count Type"="Vulnerability Operations"]
| table "Count Type", count
```

### Query 2.6 - Notable events assigned

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

### Query 2.7 - Incident status changes

```
Unset
`notable`
| stats count by status_label
```

### Query 2.8 - Vulnerability data onboarded

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

### Query 2.9 - Risk Index events

```
Unset
| tstats count where index="risk"
```

### Query 2.10 - Risk notables over 30 days

```
Unset
index=notable
| eval notable_type=if(isnotnull(risk_object) AND
isnotnull(risk_object_type), "Risk Notable", "Notable")
| fields notable_type, count
| timechart span=1d count by notable_type
```

### Query 2.11 - Threat Intelligence data model events

```
Unset
| tstats count from datamodel=Threat_Intelligence
```

## Intermediate

### Query 3.1 - Asset & Identity lookups

```
Unset
| rest /services/data/transforms/lookups
| search   filename IN ("*asset*" "*identity*") disabled=0
| table eai:acl.app title filename updated
| sort eai:acl.app
| rename eai:acl.app as App, filename as "Lookup File", title as
Title, updated AS "Last Updated"
```

### Query 3.2 - Asset & Identity lookups last updated

```
Unset
| rest /services/data/transforms/lookups
| search   filename IN ("*asset*" "*identity*") disabled=0
| table eai:acl.app title filename updated
| sort eai:acl.app
| rename eai:acl.app as App, filename as "Lookup File", title as
Title, updated AS "Last Updated"
```

### Query 3.3 - Number of enabled correlation searches

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

## Query 3.4 - Enabled searches by app

```
Unset
| rest splunk_server=local /servicesNS/-/-/saved/searches
| search disabled=0 NOT eai:acl.app IN ("*test*" "search"
"splunk_rapid_diag" "splunk_app_*" "splunk_archiver"
"splunk_instrumentation" "splunk_monitoring_console")
| stats count by eai:acl.app
| rename eai:acl.app as App
```

## Query 3.5 - ES Dashboard views

```
Unset
index=_internal sourcetype=splunkd_ui_access
| rex "\\/data\\/ui\\/views\\/(?<dashboard>[^\?]+)"
| search dashboard=ess_security_posture
| stats count
| eval "Count Type"="Security Posture"
| append
    [ search index=_internal sourcetype=splunkd_ui_access
    | rex "\\/data\\/ui\\/views\\/(?<dashboard>[^\?]+)"
    | search dashboard=ess_soc_operations
    | stats count
    | eval "Count Type"="SOC Operations"]
| append
    [ search index=_internal sourcetype=splunkd_ui_access
    | rex "\\/data\\/ui\\/views\\/(?<dashboard>[^\?]+)"
    | search dashboard=ess_executive_summary
    | stats count
    | eval "Count Type"="Executive Summary"]
| table "Count Type", count
| rename "Count Type" as Dashboard
```

## Query 3.6 - Suppressed notables

```
Unset
index=notable
| eventstats count as total
| search eventtype=notable_suppression-* OR suppression=*
| stats count as "suppression" by total
| eval percentage=(suppression*100)/total
```

## Query 3.7 - Investigation collaborators

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

## Query 3.8 - 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
| eval percentage=round(percentage,2)
```

## Query 3.9 - 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 3.10 - 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
```

## Advanced

### Query 4.1 - BA rules enabled (if applicable)

```
Unset
| rest /services/behavioral_analytics/detections count=0
splunk_server=local
| stats count
```

### Query 4.2 - UBA apps installed

```
Unset
| rest /services/apps/local splunk_server=local
| search disabled=0 label IN ("*uba*" "*behavior*")
| table label version
| rename label as App
| sort label
```

### Query 4.3 - Custom asset fields added

```
Unset
index=_introspection sourcetype=splunk_telemetry
app=SplunkEnterpriseSecuritySuite
component="app.SplunkEnterpriseSecuritySuite.identity_manager"
| table data.asset_custom_fields
```

### Query 4.4 - Custom identity fields added

```
Unset
index=_introspection sourcetype=splunk_telemetry
app=SplunkEnterpriseSecuritySuite
component="app.SplunkEnterpriseSecuritySuite.identity_manager"
| table data.identity_custom_fields
```

### Query 4.5 - Risk Analysis dashboard page views

```
Unset
index=_internal sourcetype=splunkd_ui_access file=risk_analysis
| stats count
```

### Query 4.6 - Dashboards created

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

### Query 4.7 - Reports created

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

### Query 4.8 - Percent High/Critical incidents unassigned

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

## Query 4.9 - Mean time to triage critical incidents

```
Unset
| tstats `summariesonly` earliest(_time) as _time from
datamodel=Incident_Management.Notable_Events_Meta by
source,Notable_Events_Meta.rule_id
| `drop_dm_object_name("Notable_Events_Meta")`
| `get_correlations`
| join rule_id
    [| from inputlookup:incident_review_lookup
    | search urgency=critical
    | eval _time=time
    | stats earliest(_time) as review_time by rule_id]
| eval ttt=review_time-_time
| stats count,avg(ttt) as avg_ttt,max(ttt) as max_ttt by
rule_name
| sort - avg_ttt
| `uptime2string(avg_ttt, avg_ttt)`
| `uptime2string(max_ttt, max_ttt)`
| rename *_ttt* as *(time_to_triage)*
| fields - *_dec
```

## Query 4.10 - Adaptive Response Actions scheduled

```
Unset
index=_introspection sourcetype=splunk_telemetry
app=SplunkEnterpriseSecuritySuite
component="app.SplunkEnterpriseSecuritySuite.search_actions"
"data.is_adaptive_response"=1
| stats values(data.total_scheduled)
```

### Query 4.11 - 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 4.12 - 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 4.13 - Reduction in Notables using attribution-based approach

```
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 4.14 - Percent that are risk notables

```
Unset
index=notable
| eventstats count as total
| search eventtype=risk_notables
| stats count as "risk" by total
| eval percentage=(risk*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