**Splunk Enterprise Security : Risk Analysis**

How to analyze risk in Splunk Enterprise Security

A risk score is a single metric that shows the relative risk of a device or user in the network environment over time. Splunk Enterprise Security classifies a device as a system, a user as a user, and unrecognized devices or users as other.

Enterprise Security uses risk analysis to take note of and calculate the risk of small events and suspicious behavior over time to your environment. The Risk Analysis dashboard displays these risk scores and other risk-related information. Enterprise Security indexes all risk as events in the risk index.

How Splunk Enterprise Security assigns risk scores

A risk score is a single metric that shows the relative risk of a device or user object in the network environment over time. An object represents a system, a user, or an unspecified other.

Enterprise Security uses correlation searches to correlate machine data with asset and identity data, which comprises the devices and user objects in a network environment. Correlation searches search for a conditional match to a question. When a match is found, an alert is generated as a notable event, a risk modifier, or both.

a) A notable event becomes a task. It is an event that must be assigned, reviewed, and closed.

b) A risk modifier becomes a number. It is an event that will add to the risk score of a device or user object.

**Risk scoring example**

The host RLOG-10 is a jump server that is generating several notable events. The correlation searches **Excessive Failed Logins**, and **Default Account Activity Detected** are creating one notable event a day for that system. As RLOG-10 is a jump server, several network credentials are being used against this host, and software or other utilities may have been installed. As a jump server, this behavior is less interesting than if the same behavior is observed on the production DNS server. Rather than ignoring or suppressing notable events generated by jump servers, you can create jump-server-specific rules to monitor those servers differently.

You can do this by creating a correlation search that assigns a risk modifier instead of creating a notable event, when the correlation matches hosts that serve as jump servers.

1. Isolate jump servers from the existing correlation searches using a whitelist.
2. Create and schedule a new correlation search based on **Excessive Failed Logins**, but isolate the search to the jump server hosts and assign a risk modifier alert type only.
3. Verify the risk modifiers are applied to the jump server hosts by raising their risk score incrementally. With the new correlation search, no notable events will be created for those hosts based on failed logins.
4. As the relative risk score goes up, RLOG-10 can be compared to all network servers and to other jump servers. If the relative risk score for RLOG-10 exceeds its peers, that host would be investigated by an analyst. If the risk scores of all jump servers are higher relative to other network hosts, an internal security policy may need to be reviewed or implemented differently.
5. It is also worth noting that risk modifiers cannot be suppressed in the same manner as notable events. Instead, the following options are available:
6. **Correlation Search Aggregation**
7. You can aggregate multiple firings of a correlation search based on fields and duration via savedsearches.conf in the alert.suppress settings.
8. **Correlation Search Modification**
9. To prevent further false positives, you can edit the correlation search syntax to filter events or results.

**How to assign risk automatically as part of a correlation search.**

Modify a risk score as a result of a correlation search or in response to notable event details with the **Risk Analysis** adaptive response action. The risk adaptive response action creates a risk modifier event. You can view the risk modifier events on the Risk Analysis dashboard in Enterprise Security.

1. Click **Add New Response Action** and select **Risk Analysis**.
2. Type the score to assign to the risk object.
3. Type a field in the search to apply the risk score to for the **Risk Object Field**.  
   For example, type "src" to specify the source field.
4. Select the **Risk Object Type** to apply the risk score to.

**How to create an ad hoc risk entry in Splunk Enterprise Security**

Creating an ad-hoc risk entry allows you to make a manual, one-time adjustment to an object's risk score. You can use it to add a positive or negative number to the risk score of an object.

1. Select **Security Intelligence > Risk Analysis**.
2. Click **Create Ad-hoc Risk Entry**.
3. Complete the form.

**Ad-hoc Risk Score field** **Description**

Score The number added to a Risk object. Can be a positive or negative integer.

Description A reason or note for manually adjusting an object's risk score. The Description field is mandatory for an ad hoc risk score.

Risk object Text field. Wildcard with an asterisk (\*)

Risk object type Drop-down: select to filter by.

**How to assign risk through a search**

You can assign risk using search rather than an alert. You can do this to modify risk on multiple risk objects, or to alter the risk score of an object based on the results of a search.

Each example uses . . . to indicate a search that includes the field to which you want to assign risk in the results

**Assign risk with the appendpipe command**

Use appendpipe to add risk to multiple objects. Replace <your\_risk\_score\_integer> with the risk score that you want to apply to the fields.

... | eval risk\_score=<your\_risk\_score\_integer>

| eval risk\_object=if(isnotnull(dest),dest,null()),risk\_object\_type=if(isnotnull(dest),"system",null())

| appendpipe [| eval risk\_object=if(isnotnull(user),user,null()),risk\_object\_type=if(isnotnull(user),"user",null())]

| sendalert risk param.\_risk\_score=<your\_risk\_score\_integer>

For example, run this search to assign a risk score of 15 to mysystem and myuser.

| makeresults | eval dest="mysystem", user="myuser"

| eval risk\_object=if(isnotnull(dest),dest,null()),risk\_object\_type=if(isnotnull(dest),"system",null())

| appendpipe [| eval risk\_object=if(isnotnull(user),user,null()),risk\_object\_type=if(isnotnull(user),"user",null())]

| sendalert risk param.\_risk\_score=15

**Assign risk with sendalert**

You can use sendalert without appendpipe to assign risk directly to field values, without performing conditional evaluations of the field values.

... | sendalert risk param.\_risk\_object\_type="system" param.\_risk\_score=<your\_risk\_score\_integer> | eval risk\_object=user | sendalert risk param.\_risk\_object\_type="user" param.\_risk\_score=<your\_risk\_score\_integer>

For example:

| makeresults | eval dest="mysystem", user="myuser" | sendalert risk param.\_risk\_object="dest" param.\_risk\_object\_type="system" param.\_risk\_score=15 | sendalert risk param.\_risk\_object="user" param.\_risk\_object\_type="user" param.\_risk\_score=20

**Compute and assign a risk score**

You can also set a risk score based on a calculation performed in the search, rather than setting it to a static integer.

For example, if you want to set a higher risk score for users that log into multiple infected assets, write a search that collects the users that logged in to infected assets, then does a count of the users in the results, split by user so that you see how many login attempts there are by each user.

...

| stats count by user

| eval risk\_score=(count\*2)

| sendalert risk param.\_risk\_object="user" param.\_risk\_object\_type="user" param.\_risk\_score="risk\_score"

For example, the Threat Activity Detected correlation search uses search-assigned risk in addition to an alert-type risk modifier. When the search finds an asset or identity communicating with a host that matches a configured threat list, the search modifies the risk score accordingly. In this case, the risk modifier reflects the number of times the system or user communicated with the threat list, multiplied by the weight of the threat list. As a formula, risk score of a system or user + (threat list weight x event count) = additional risk.

... | eval risk\_score=case(isnum(record\_weight), record\_weight, isnum(weight), weight, 1=1, null()) | fields - \*time | eval risk\_object\_type=case(threat\_match\_field="query" OR threat\_match\_field=="src" OR threat\_match\_field=="dest","system",threat\_match\_field=="src\_user" OR threat\_match\_field=="user","user",1=1,"other") | eval risk\_object=threat\_match\_value

See the changes that you made by searching the data model or the risk correlation lookups:

| from datamodel:Risk.All\_Risk | search (risk\_object=myuser OR risk\_object=mysystem)

or

| makeresults | eval dest="mysystem" | `risk\_correlation`

Score ranges for risk

Risk scoring offers a way to capture and aggregate the activities of an asset or identity into a single metric using risk modifiers.

The correlation searches included in Enterprise Security assign a risk score between 20 and 100 depending on the relative severity of the activity found in the correlation search. The searches scope the default scores to a practical range. This range does not represent an industry standard. Enterprise Security does not define an upper limit for the total risk score of an identity or asset, but operating systems can impose a limit. For example, 32-bit operating systems limit a risk score to two million.

Risk score levels use the same naming convention as event severity. You can assess relative risk scores by comparing hosts with similar roles and asset priority.

20 - Info

40 - Low

60 - Medium

80 - High

100 - Critical

**How to manage risk objects**

Enterprise Security associates risk modifiers with risk objects.

**Risk object field**

The risk object field is a reference to a search field returned by a correlation search. Correlation searches use fields such as src and dest to report on matching results. The risk object field represents a system, host, device, user, role, credential, or any object that the correlation search is designed to report on. Review any correlation search that assigns a risk score for examples of fields that receive a risk score.

**Risk object types**

Splunk Enterprise Security defines three risk object types.

**Object type** **Description**

System Network device or technology. Can represent a device in the asset lookup.

User Network user, credential, or role. Can represent an identity in the identity lookup.

Other Any undefined object that is represented as a field in a data source.

If a risk object matches an object in the asset or identity table, Enterprise Security maps the object as the associated type. For example, an object that matches an asset in the asset lookup is mapped to a risk object type of system. However, devices and users do not need to be represented in the corresponding asset and identity tables to be identified as system or user risk objects. ES categorizes undefined or experimental object types with a risk object type of **Other.**.