Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Use default risk incident rules in Splunk Enterprise Security

Generated: 6/13/2022 9:54 am

Use default risk incident rules in Splunk Enterprise Security

Use default risk incident rules to run correlation searches that create adaptive response actions or generate notable events.

The following correlation searches use the default incident rules and are enabled in Splunk Enterprise Security:

1. The correlation search `ATT&CK Tactic Threshold Exceeded for Object Over Previous 7 days` creates notables when the number of MITRE tactics exceeds three over the last seven days i.e. `tactic_count >=3 and source_count >=4`.

```
| tstats `summariesonly` values(All_Risk.annotations.mitre_attack.mitre_tactic_id) as tactic,
dc(All_Risk.annotations.mitre_attack.mitre_tactic_id) as tactic_count,
values(All_Risk.annotations.mitre_attack.mitre_technique_id) as technique,
dc(All_Risk.annotations.mitre_attack.mitre_technique_id) as technique_count, values(source) as source,
dc(source) as source_count from datamodel=Risk.All_Risk by All_Risk.risk_object,All_Risk.risk_object_type |
`drop_dm_object_name("All_Risk")` | where tactic_count >= 3 and source_count >= 4
```

2. The correlation search `Risk Threshold Exceeded for Object Over 24 Hour Period`.
creates notables when the risk score for an object exceeds 100 over the last 24 hours i.e. `risk_score_sum > 100`.

```
| tstats `summariesonly` sum(All_Risk.calculated_risk_score) as risk_score_sum,
values(All_Risk.annotations.mitre_attack.mitre_tactic_id) as tactic,
dc(All_Risk.annotations.mitre_attack.mitre_tactic_id) as tactic_count,
values(All_Risk.annotations.mitre_attack.mitre_technique_id) as technique,
dc(All_Risk.annotations.mitre_attack.mitre_technique_id) as technique_count, values(source) as source,
dc(source) as source_count from datamodel=Risk.All_Risk by All_Risk.risk_object,All_Risk.risk_object_type |
where risk_score_sum > 100 | `drop_dm_object_name("All_Risk")` | eval severity=case(risk_score_sum>=100 and
risk_score_sum<250, "medium", risk_score_sum>=250 and risk_score_sum<500, "high", risk_score_sum>=500,
"critical")
```

You can also customize these correlation searches and edit them to change specific conditions. For example, you may want to increase the risk score threshold by 200 instead of 100 over the last 24 hours. For more information on editing correlation searches, see Edit correlation searches.