|  |
| --- |
| ITG\_IPS\_IRB |
| ALERTE SPLUNK DOWN |

|  |
| --- |
| SAURON TEAM  22/01/2018 |



Description

En tant que communauté je veux que l’équipe reçoive une alerte quand Splunk ne reçoit plus d’infos Splunk depuis plus de 5 minutes

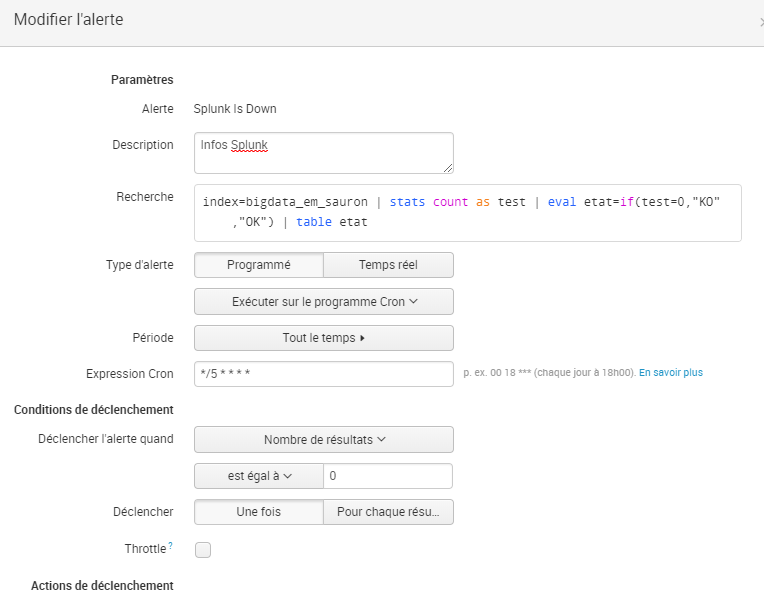
Dans Splunk

Rajout d’un panneau « Etat Splunk » dans le tableau de bord Administrration

|  |
| --- |
| **index=bigdata\_em\_sauron | stats count as test | eval etat=if(test=0,"KO","OK") | table etat** |

**Création de l’Alerte**

****

****

