15/9/25

**TASK:** Creating a Security Related Dashboard In Splunk.

Also include drill down feature.

Csv data:

timestamp,incident\_id,incident\_type,severity,status,vulnerability\_id,vuln\_type,vuln\_severity,vuln\_status,compliance\_area,compliance\_status,user\_id,login\_success,login\_time,alert\_id,alert\_type,alert\_severity

2025-09-10T10:00:00Z,INC001,Malware,High,Open,VULN001,SQL Injection,Critical,Open,PCI-DSS,Non-Compliant,user001,True,2025-09-10T09:55:00Z,ALERT001,Unauthorized Access,High

2025-09-10T11:00:00Z,INC002,Phishing,Medium,Resolved,VULN002,Cross-site Scripting,Medium,Resolved,ISO27001,Compliant,user002,False,2025-09-10T10:58:00Z,ALERT002,Brute Force Attempt,Critical

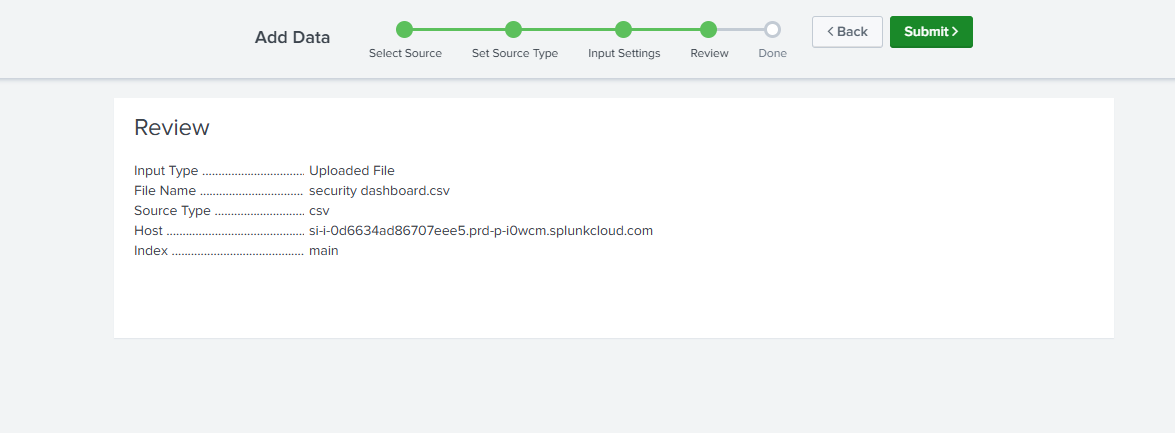
2025-09-10T12:00:00Z,INC003,Data Leak,High,Open,VULN003,Unpatched Software,Critical,Open,GDPR,Non-Compliant,user003,True,2025-09-10T11:59:00Z,ALERT003,Privilege Escalation,Medium

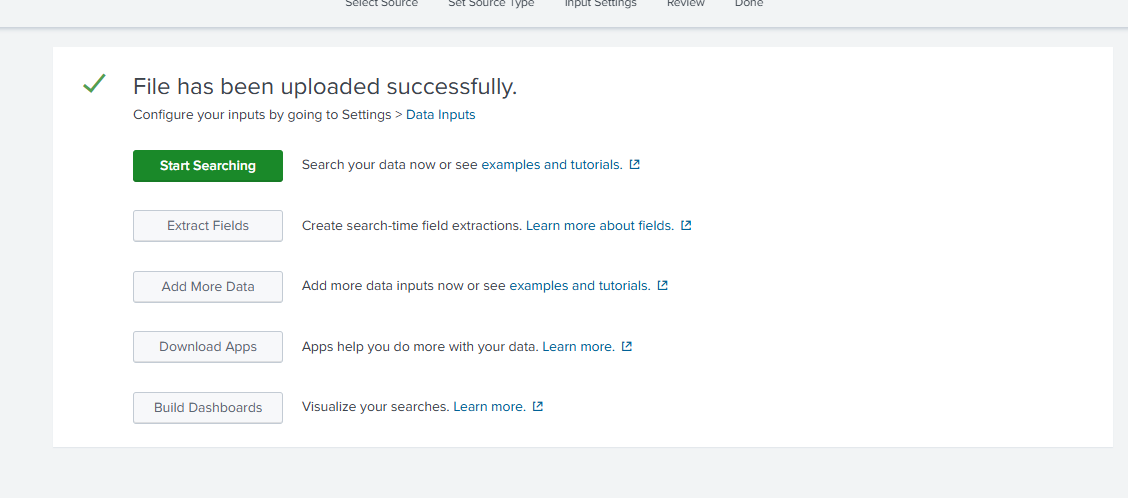
2025-09-10T13:00:00Z,INC004,Malware,Low,Open,VULN004,Weak Password Policy,Low,Open,NIST,Compliant,user004,True,2025-09-10T12:59:00Z,ALERT004,Malware Behavior,High

2025-09-10T14:00:00Z,INC005,Phishing,Critical,Resolved,VULN005,Open Ports,Critical,Resolved,PCI-DSS,Compliant,user005,False,2025-09-10T13:55:00Z,ALERT005,Data Exfiltration,Critical

SOLUTION:

1. Uploading the csv data
   1. Settings -> add data -> uploading the csv data.
   2. index=main(i have selected)





1. Dashboard studio-> grid
2. **Panel 1: Incident Severity vs Status Overview**
   1. Spl query:

source="security dashboard.csv" index="main"

| stats count by severity, status

* 1. Visualization type: bar chart
     1. In the right side -> edit ->general -> visualization type.

1. **Panel 2: Vulnerability Status Breakdown**
2. Spl query:

source="security dashboard.csv" index="main"

| stats count by severity, status

1. Visualization type: bar chart

5. **Panel 3: Compliance Status Summary**

source="security dashboard.csv" index="main"

| stats count by compliance\_area, compliance\_status

Visualization type: Bar chart

6. **Panel 4 – Login Success Rate**

source="security dashboard.csv" index="main"

| stats count by login\_success

Visualization type: pie chart

7. **Panel 5 –** **Alerts by Severity**

source="security dashboard.csv" index="main"

| stats count by alert\_severity

Visualization Type: Bar chart.

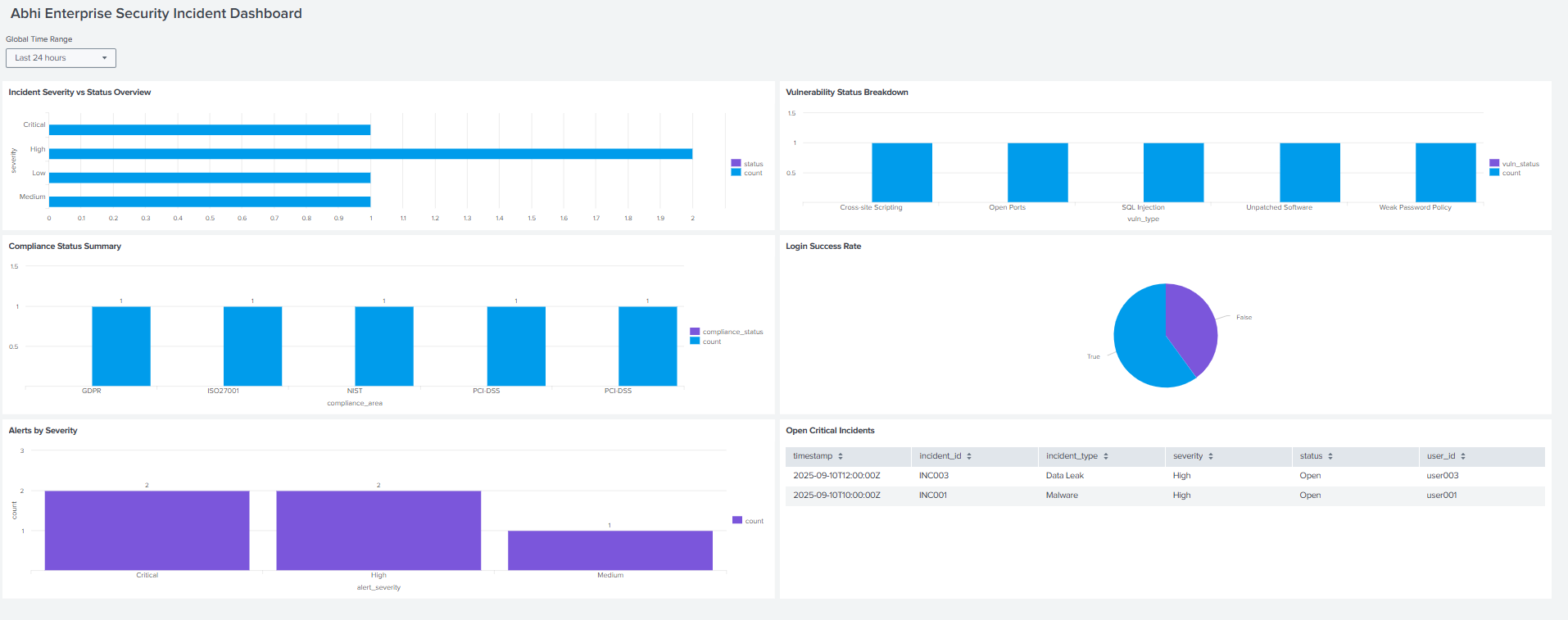
8. **Panel 6 – Open Critical Incidents (Table)**

source="security dashboard.csv" index="main" (severity="Critical" OR severity="High") status="Open"

| table timestamp, incident\_id, incident\_type, severity, status, user\_id

Visualization Type: table

DASHBOARD:



9. Creating drill down

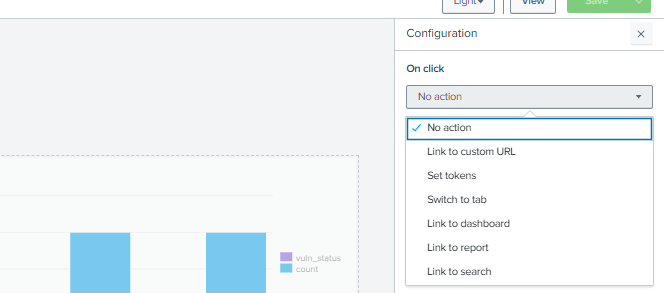
Click a panel

Edit

Bottom u can see interactions (+)

Click the + symbol

There u can see some options:



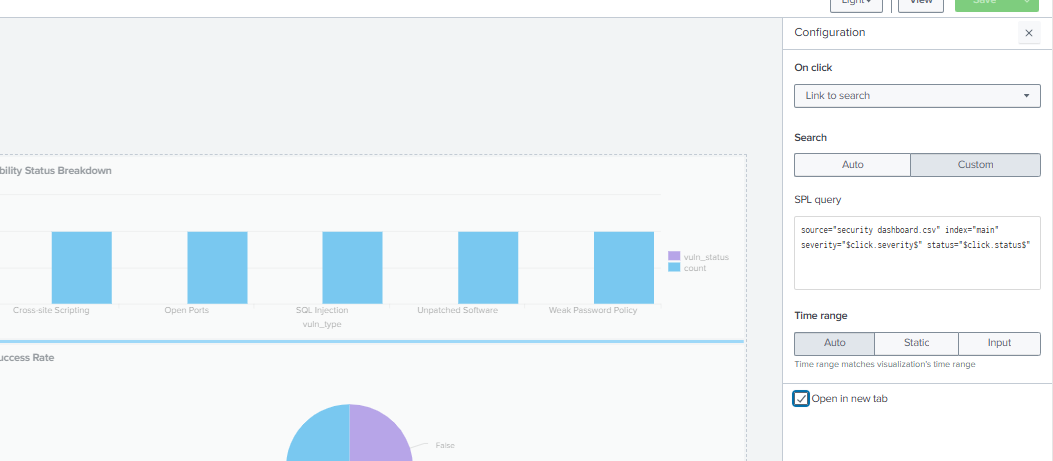
* Click **link to search**
* Custom
* Spl query:

source="security dashboard.csv" index="main"

severity="$click.severity$" status="$click.status$"

source="security dashboard.csv" index="main"

severity="High" status="Open’"



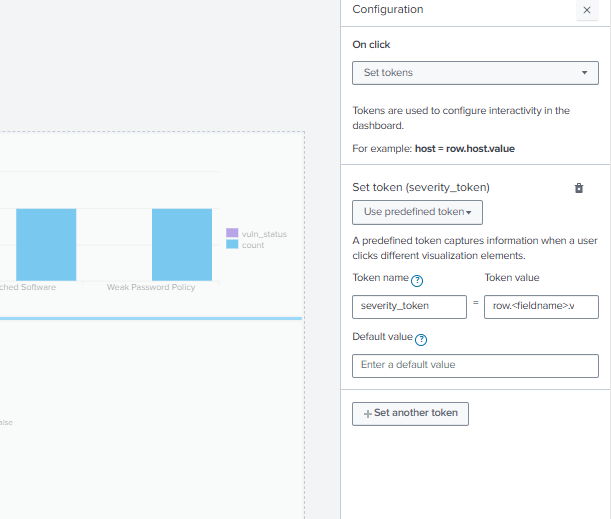
NOT WORKED

10. When i used this query it shows no results. So i changed the values into high and Open to check hardcoded values shows output/not.

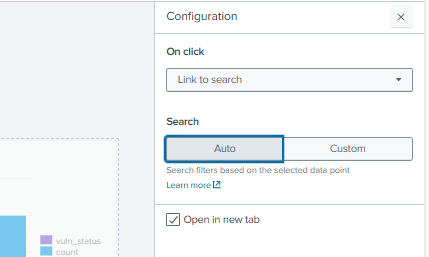
So when i click on the High it is opening a new tab and giving results.

11. Understood it is because of not setting up tokens. So in interactions -> set tokens -> added the tokens.After that again go to the link to search query and edit it to previous one and try. Still i didnt got the output( Got no results).

12. Again i added the token: didnt worked

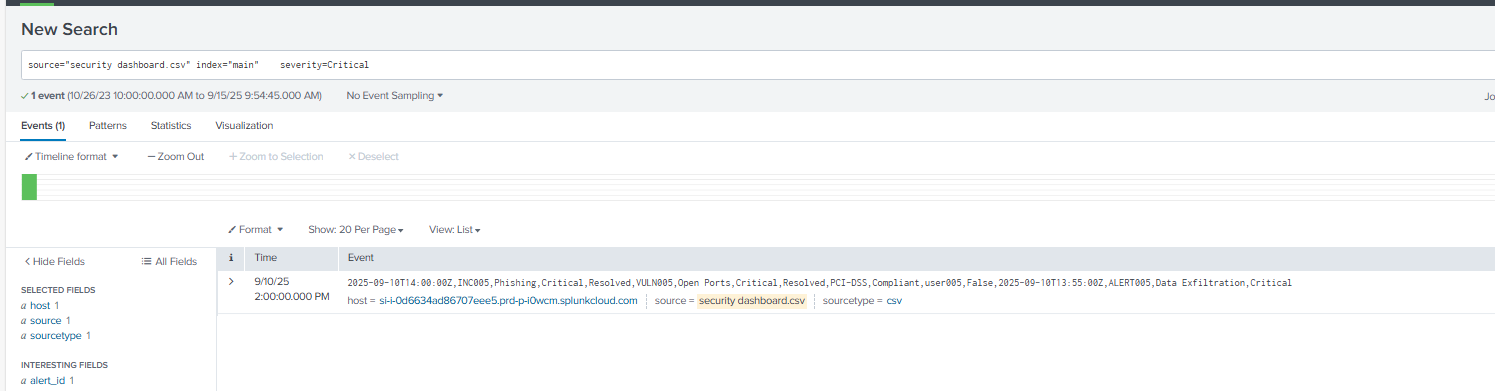


13. Tried with Auto than giving custom queries.

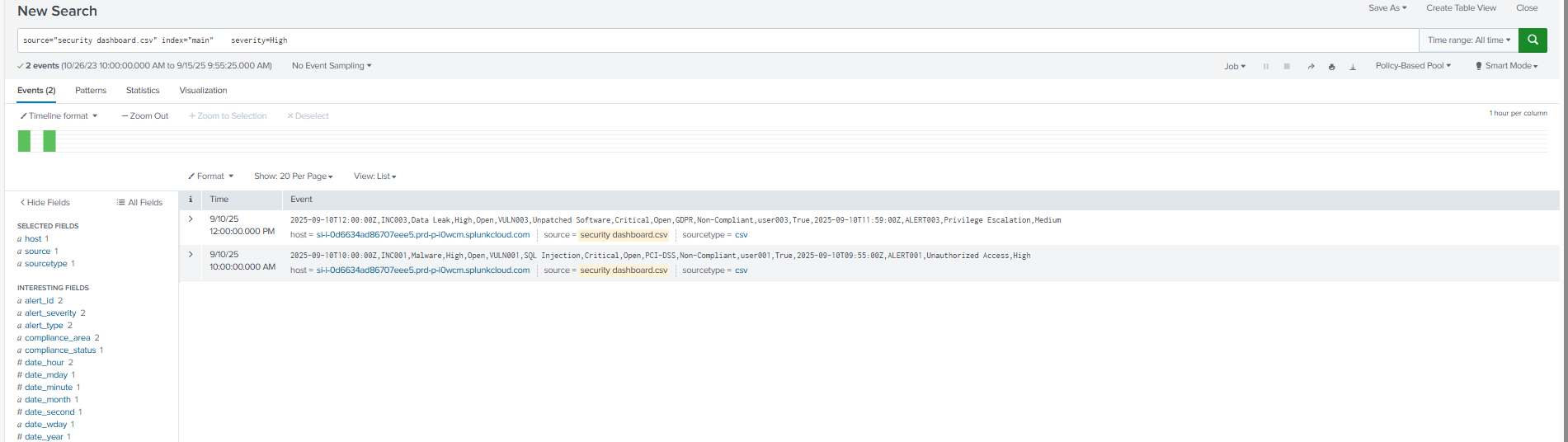


Auto it worked.Token was not needed for Auto.

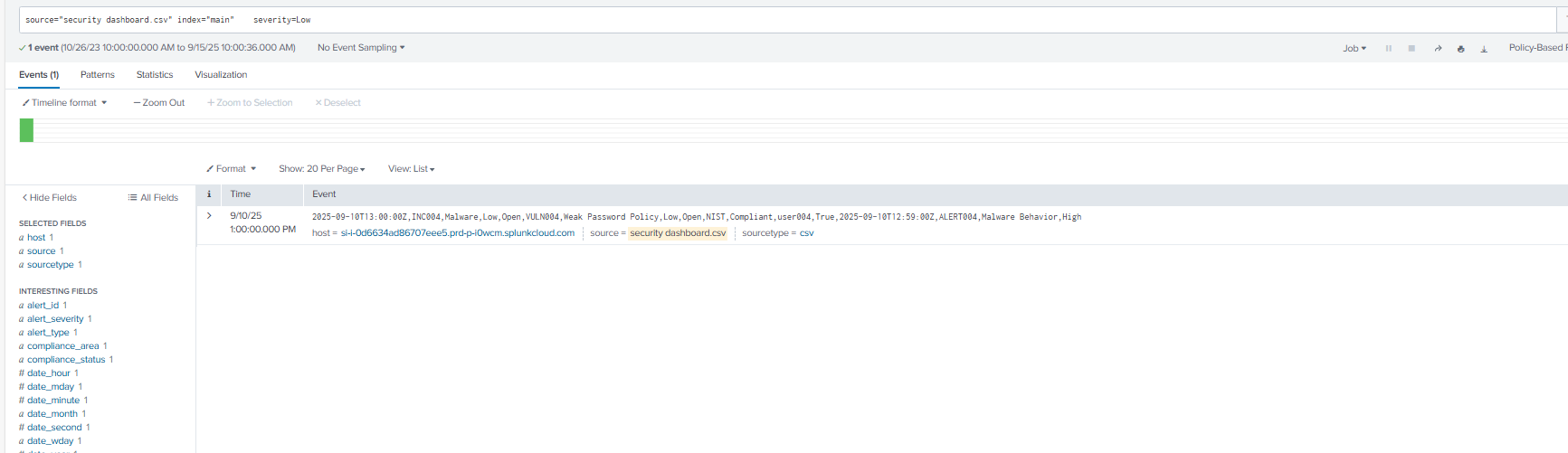
14. When i click on Critical:



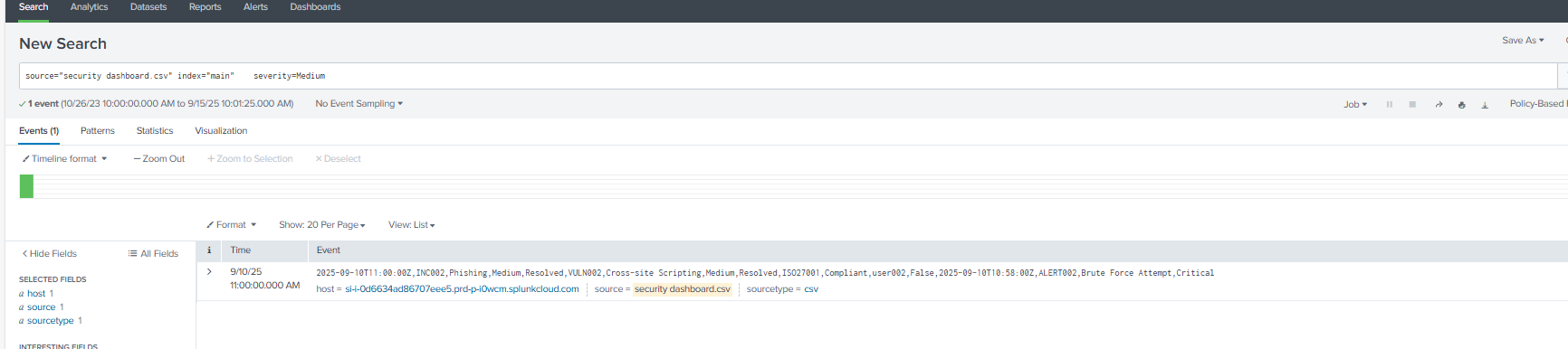
15. When i click on high:



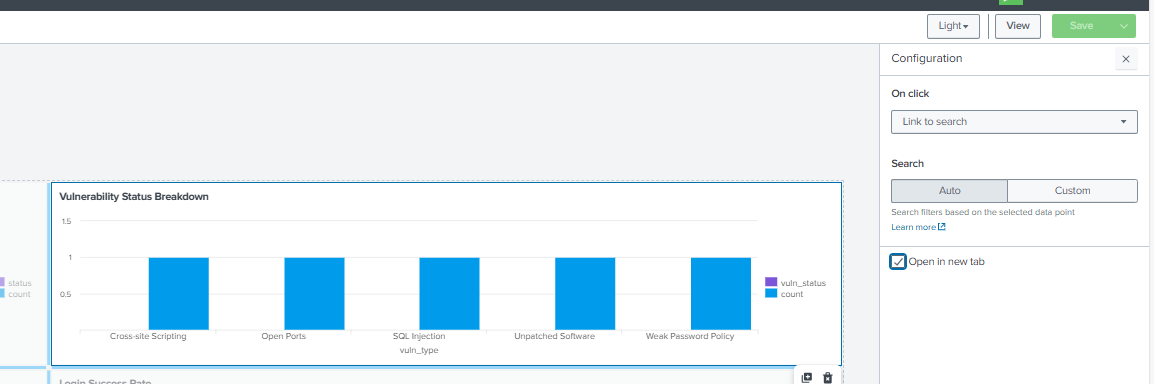
16. When i click on Low:



17. When i click on Medium:

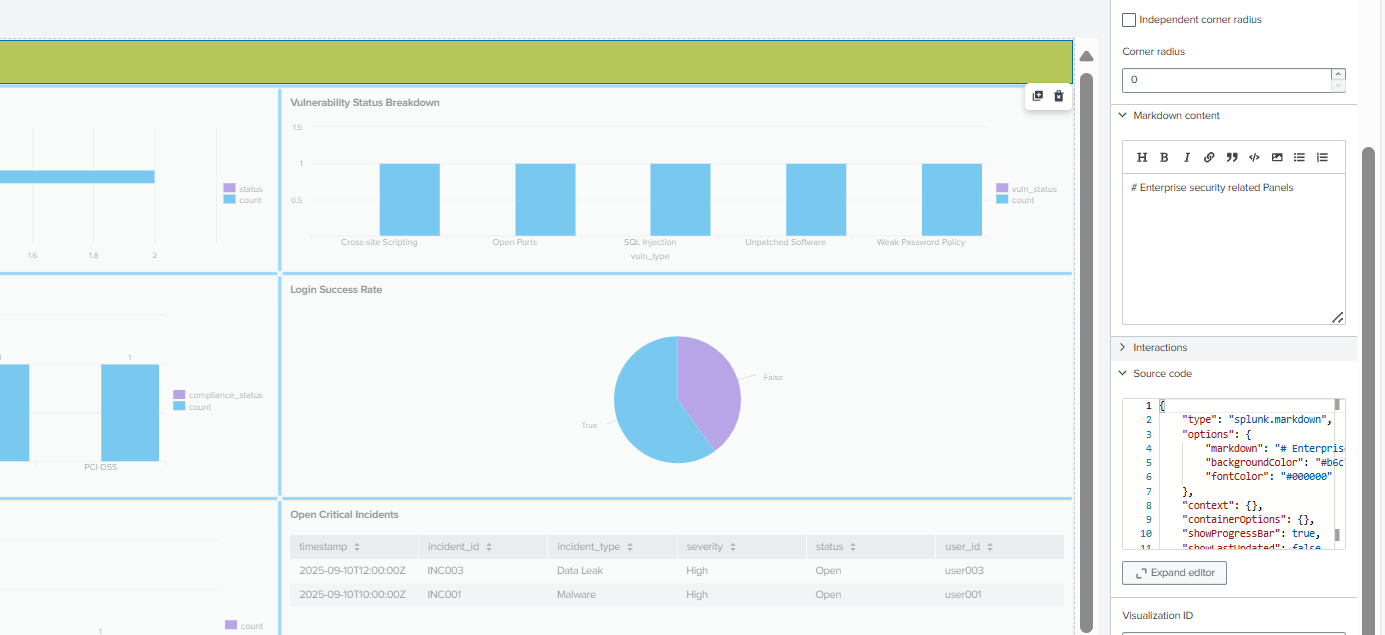


18. Configured drill down for panel2:

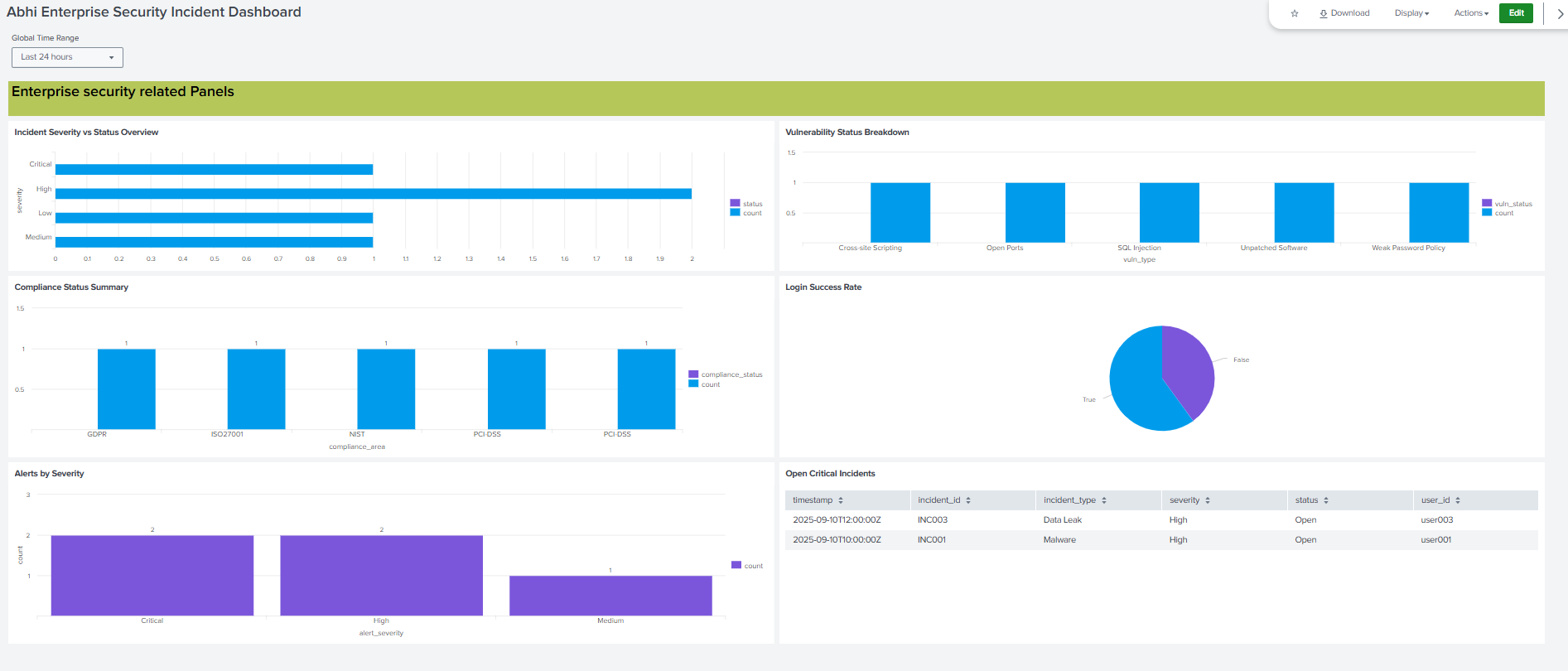


19. Configured Auto drill down -link to search to all panels.

20. Added a heading as Enterprice security related panels.



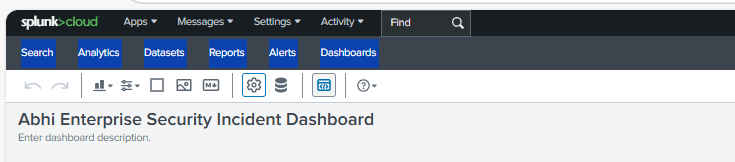
21. Dashboard:



22. Json: Actions -> Export json:

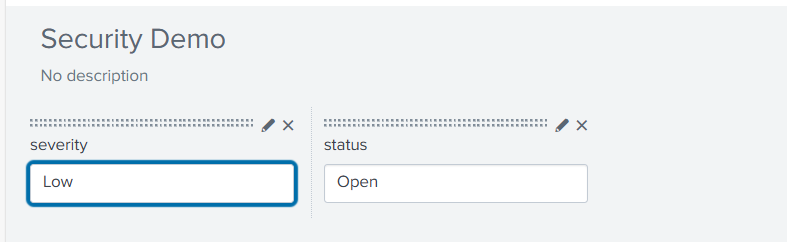
[UST-Observability/Json\_backup\_files/2\_Splunk\_security\_dashboard2.json at main · Abhiramikannan/UST-Observability](https://github.com/Abhiramikannan/UST-Observability/blob/main/Json_backup_files/2_Splunk_security_dashboard2.json)

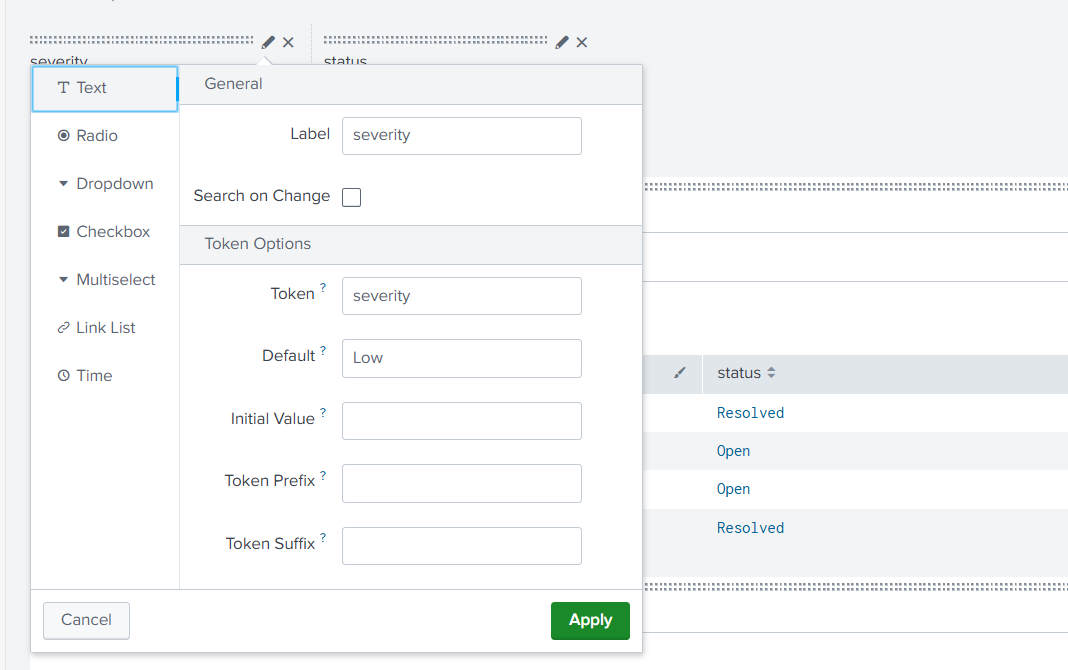
Also this option have json code: before ?

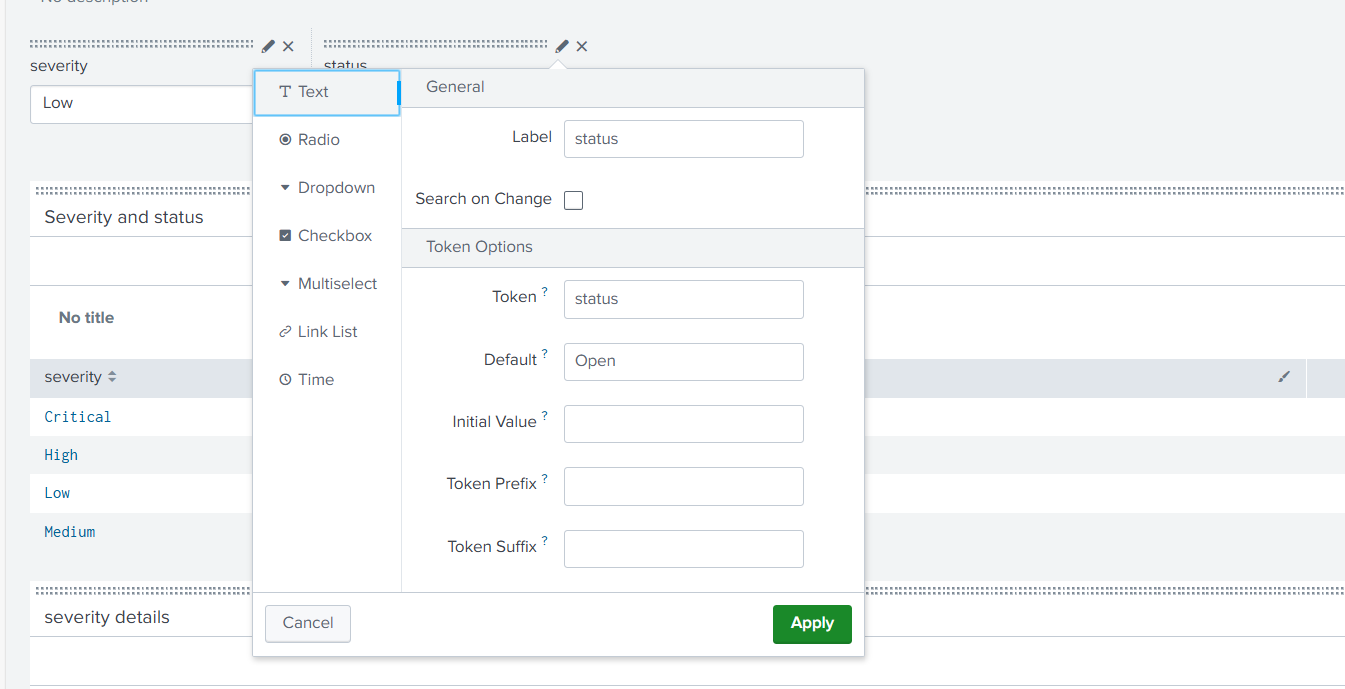


23. TRIED DRILL DOWN BY GIVING TOKEN IN CLASSIC DASHBOARD:

Add inputs:



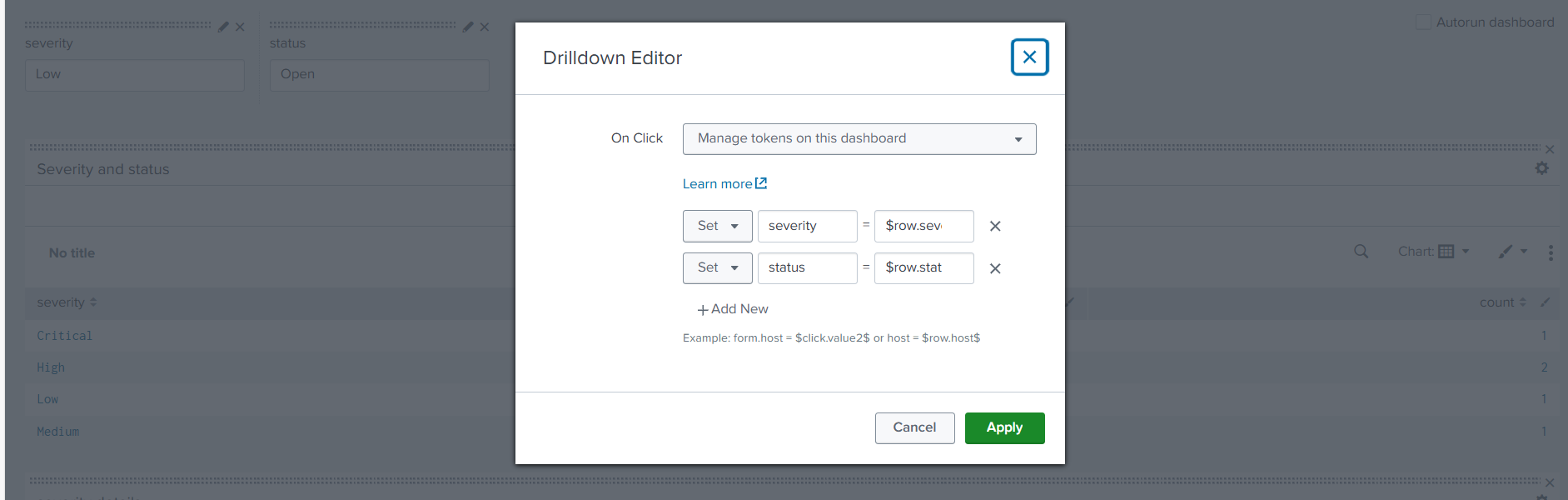




Selected the table we wanted to do drill down and gave token.

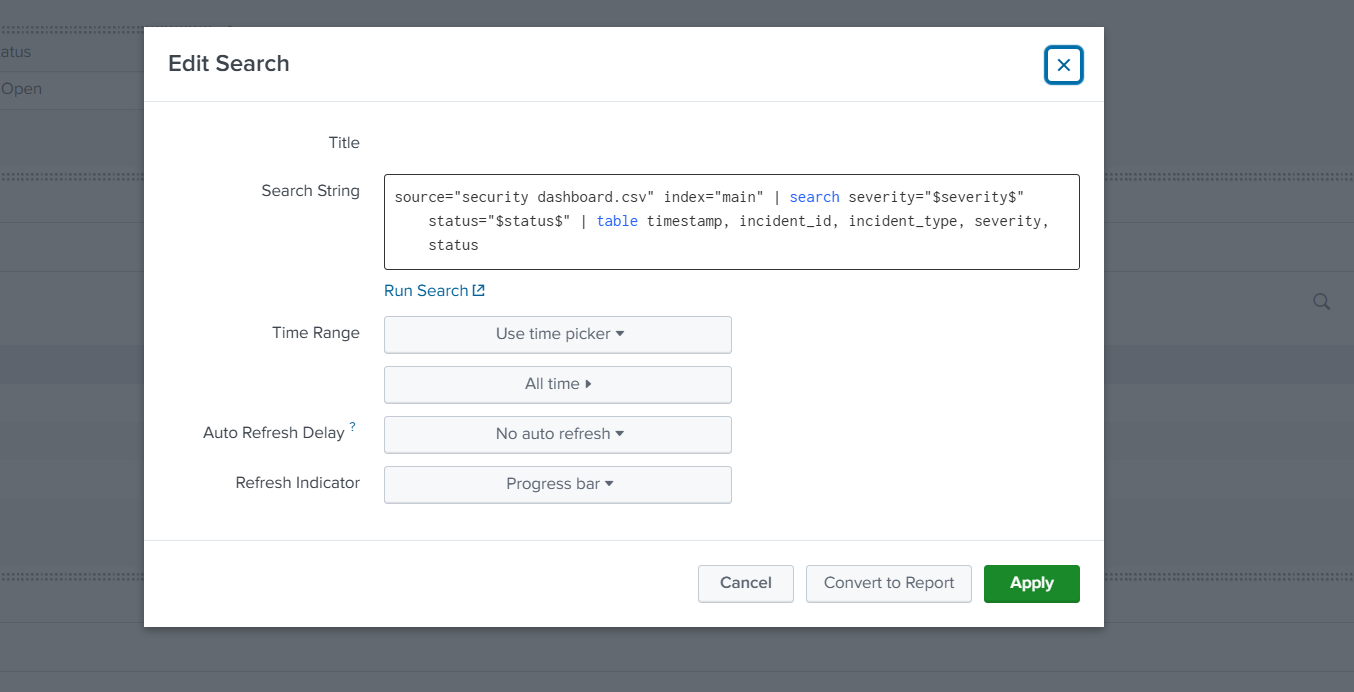
$row.severity$

$row.status$

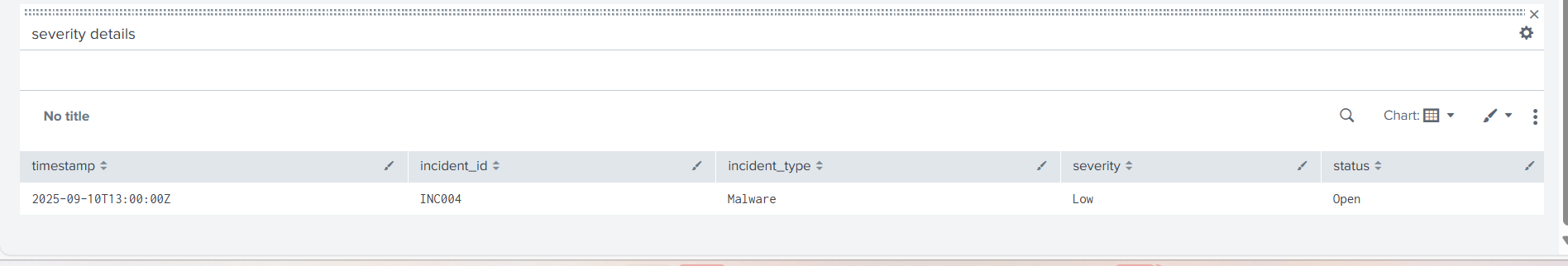


* Searched a spl in search which is fetching the proper details or not and edited the query by giving token:

source="security dashboard.csv" index="main" | search severity="$severity$" status="$status$" | table timestamp, incident\_id, incident\_type, severity, status

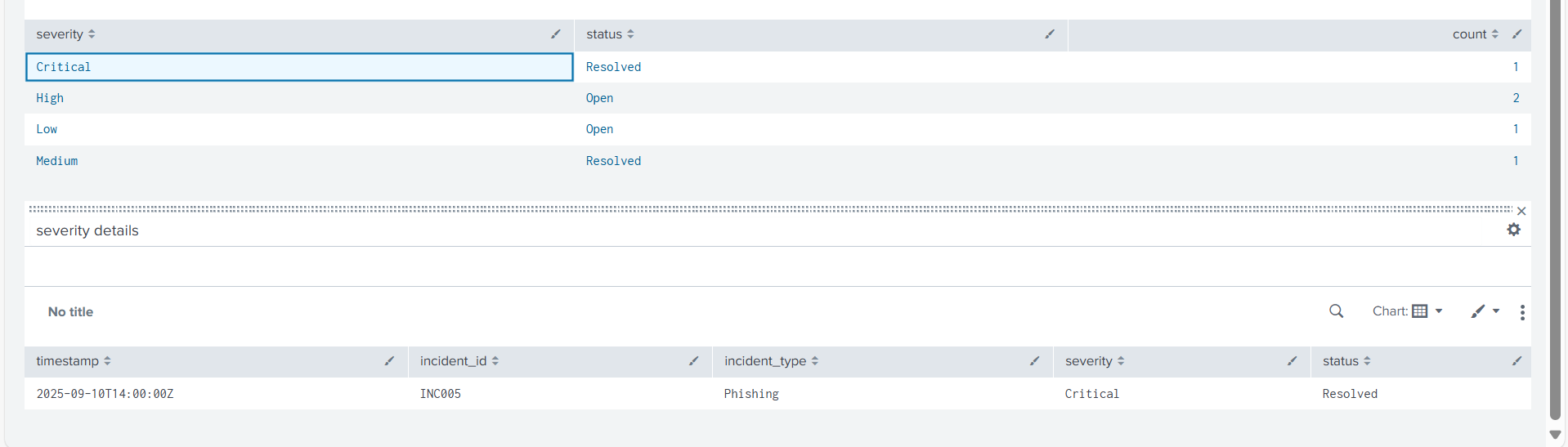


* When i select the critical,high,low,....it will display in the bottom panel where i added the query and token.

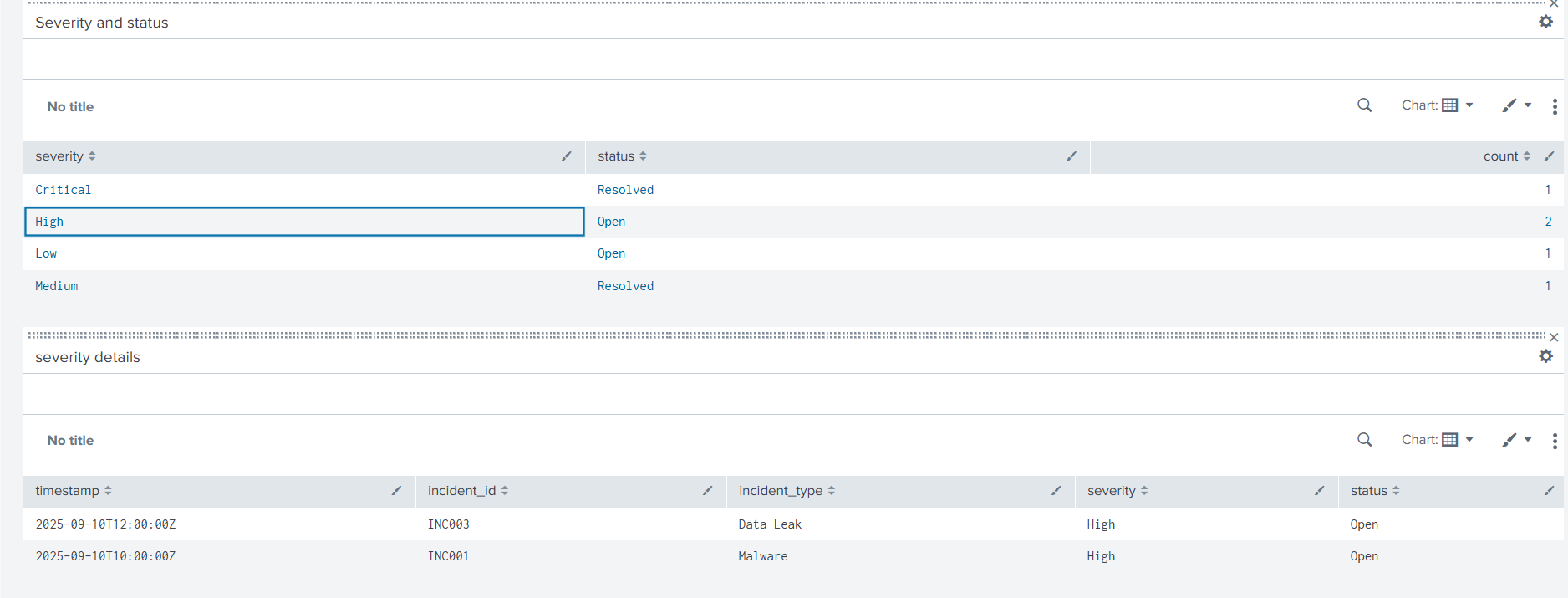


* Because of adding input on the top .. it will display defaulty everytime this severity details panel with the data of previous image i pasted here..

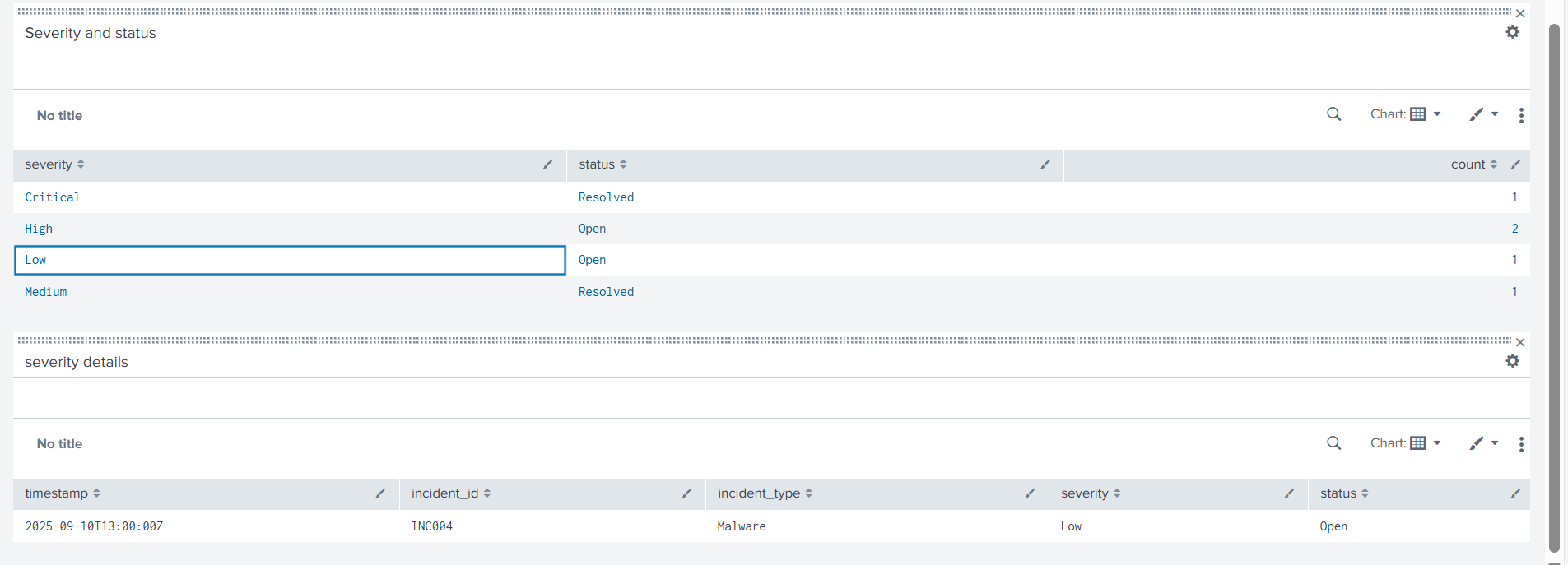
**If i click on critical:**

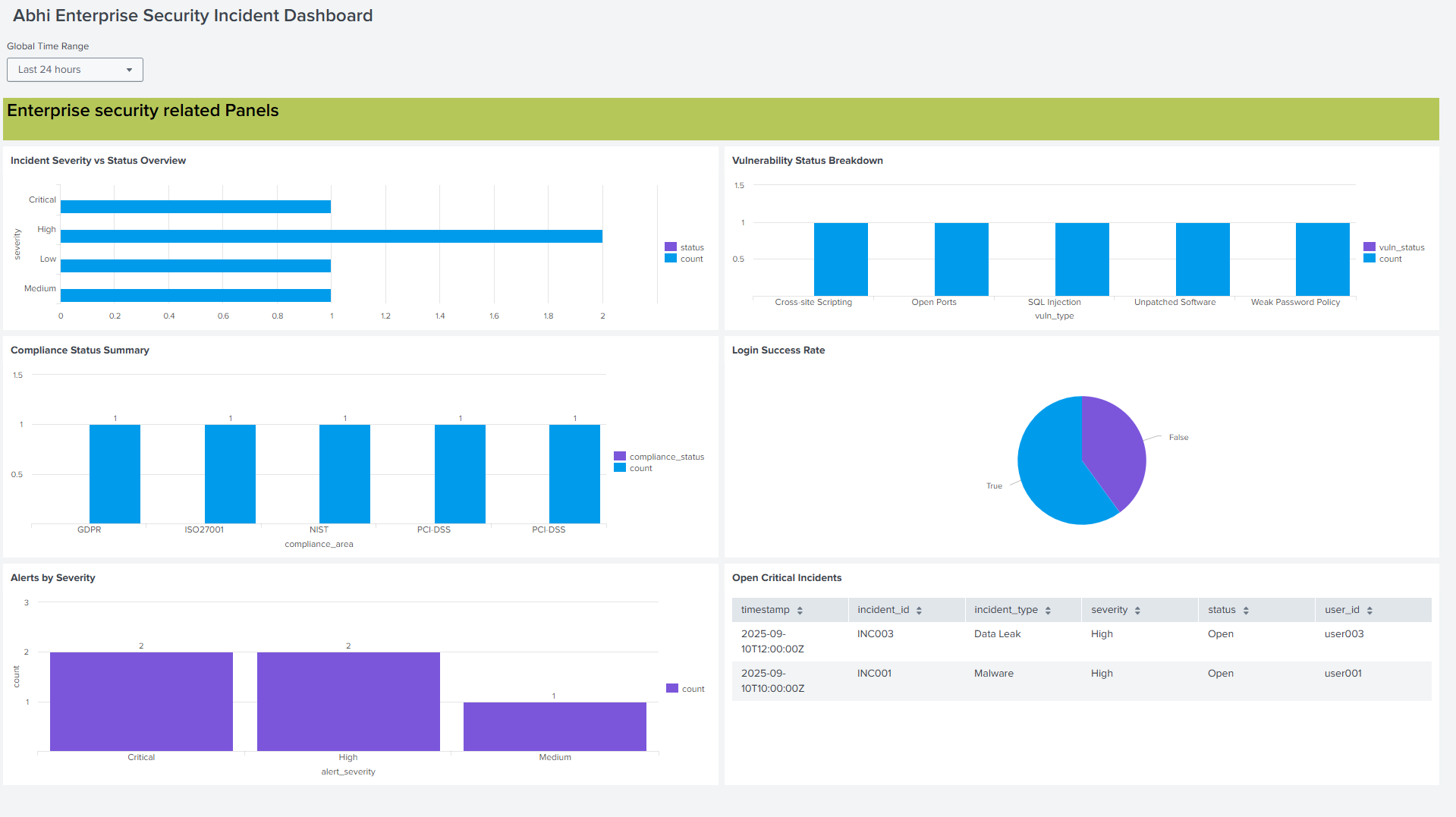


If i click on high:



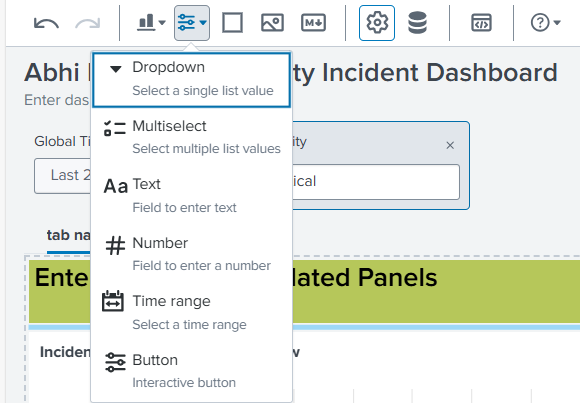
If i click on low:

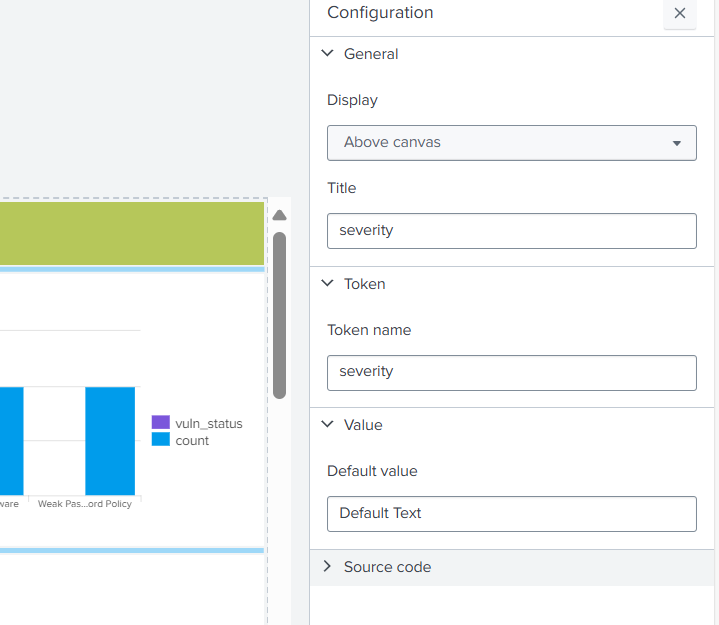




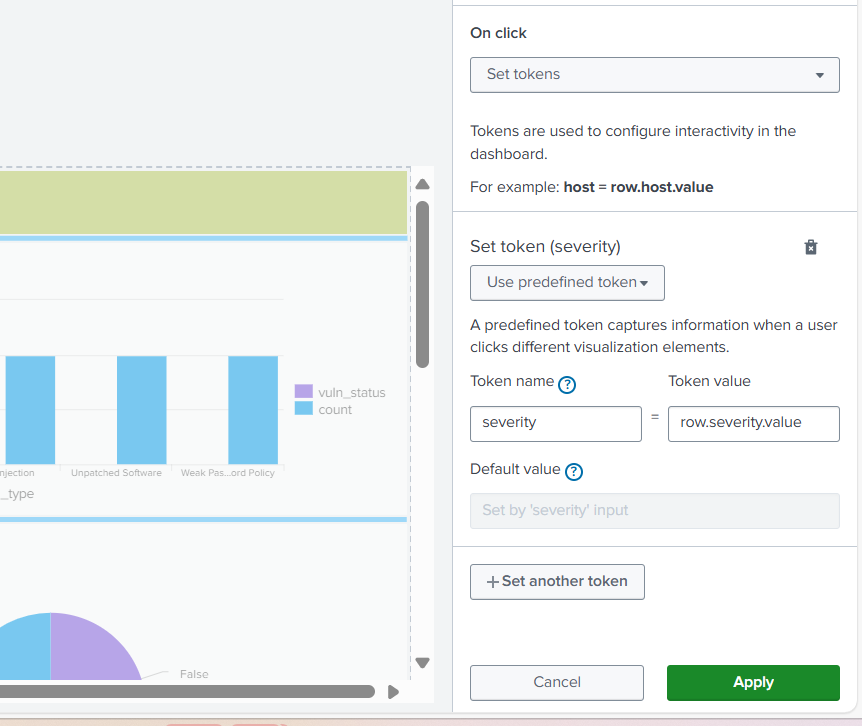
24. DRILL DOWN TO NEXT PANEL IN DASHBOARD STUDIO.

* Click on markdown in the edit and add the text(TITLE AND TOKEN as severity)





* Take panel 1 and add Token: After this when u click on critical the markdown wil change.



* Go the panel we want to redirect and edit the query. And set the query.

Datasources ->edit:

source="security dashboard.csv" index="main" | search severity="$severity$" | table timestamp, incident\_id, incident\_type, severity, status

