TASK:

Create a dashboard for security related metrics

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

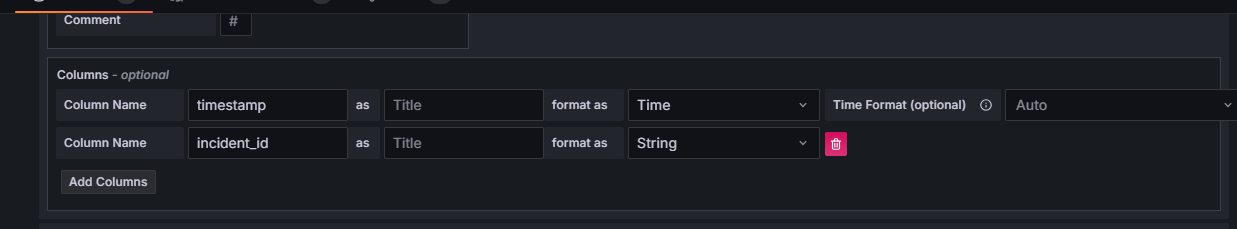
2025-09-10T12:00:00Z,INC003,Data Leak,High,Open,VULN003,Unpatched Software,Critical,Open,GDPR,Non-Compliant,user003,True,2025-09-10T11:59:00Z,ALERT003,Privilege Escalation,Medium

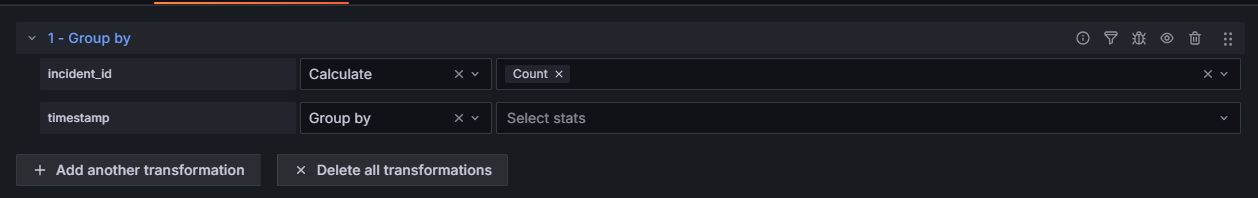
2025-09-10T13:00:00Z,INC004,Malware,Low,Open,VULN004,Weak Password Policy,Low,Open,NIST,Compliant,user004,True,2025-09-10T12:59:00Z,ALERT004,Malware Behavior,High

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

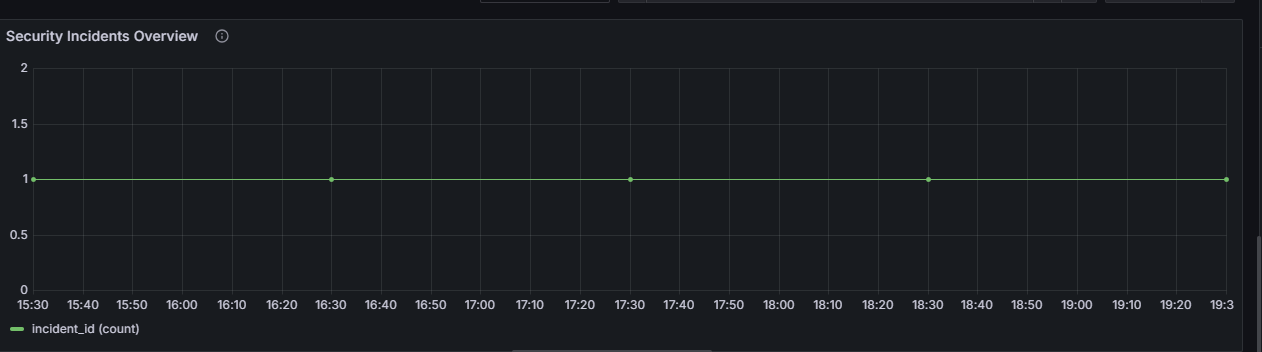
1. Panel 1 - Security Incidents Overview

Screenshots:

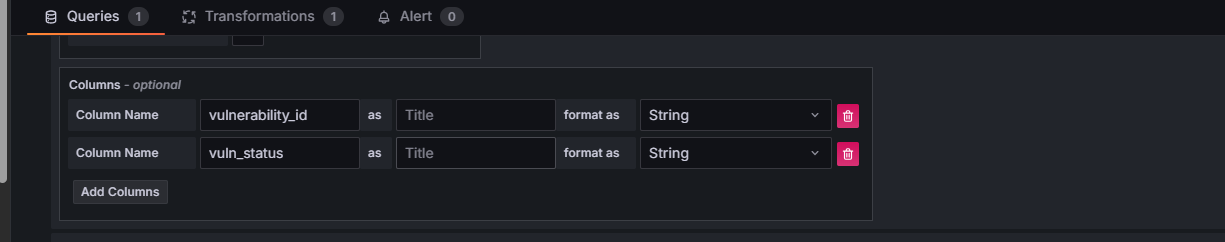


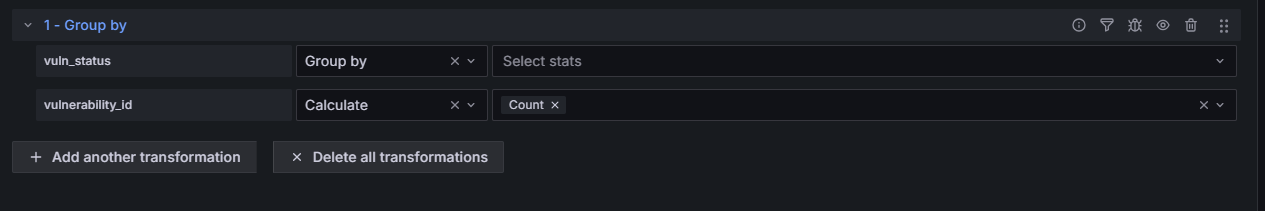


* To display a time series graph we need a time field and also a number field .
* Here timestamp is time but incident id is string.
* So timestamp can be used in a transformation of groupby.
* Then only we can use calculate for incident\_id ..to treat it as number
* So by giving count to incident\_id by using calculate: It will count the no: of incidents on that time period.
* It shows in this particular time how many incidents happened.

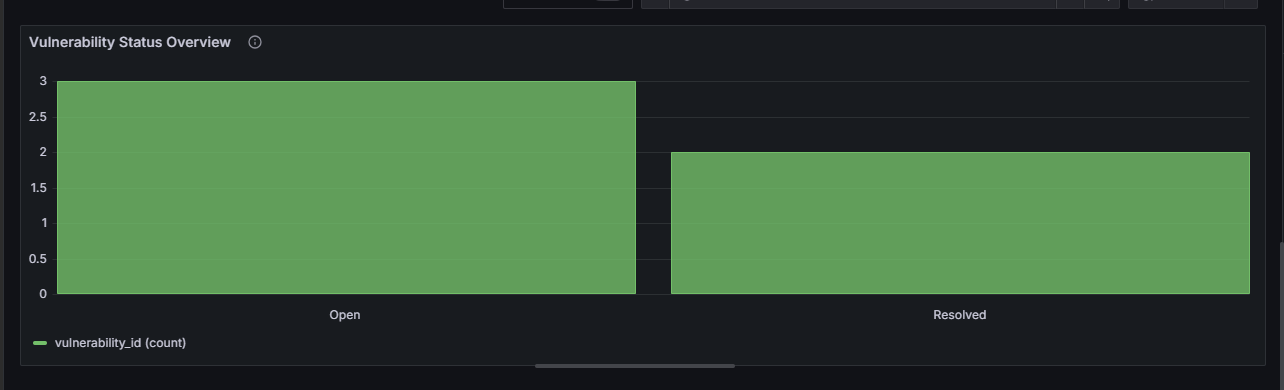


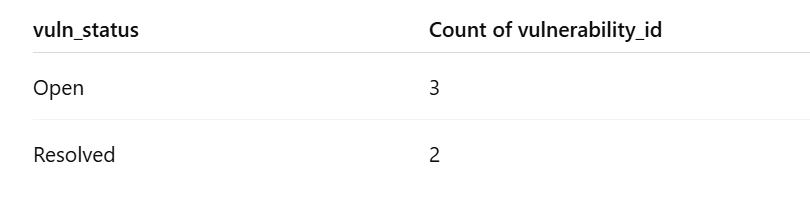
1. Panel 2 - Vulnerability Status Overview



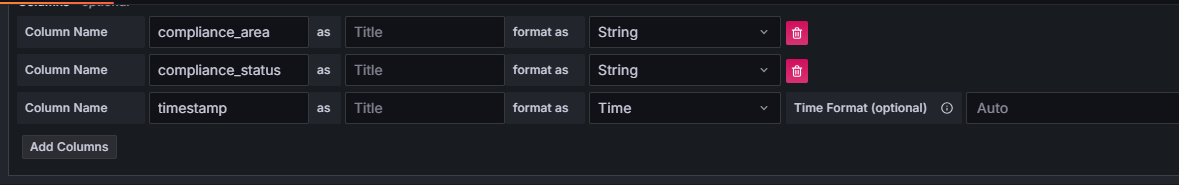


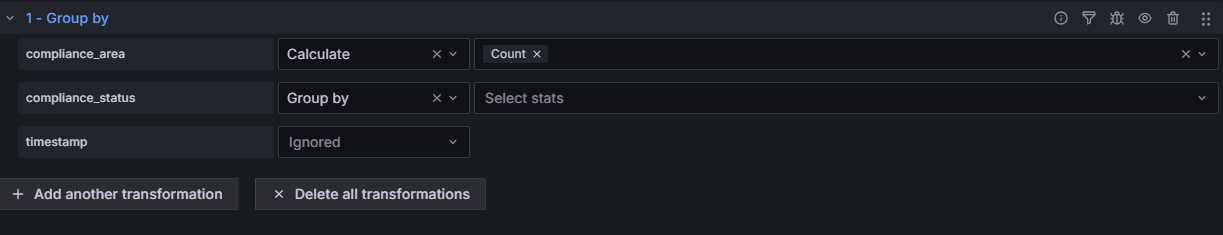
* So here also vulnerability\_id should treat as number to count the vulnerability count.
* So groupby should be used to perform count function in vulnerability\_id
* So Groupby used in vuln\_status.
* And calculate -> count performed in vulnerability\_id to calculate the count.
* It will displays the count of the open and resolved vulnerabilities in your system.

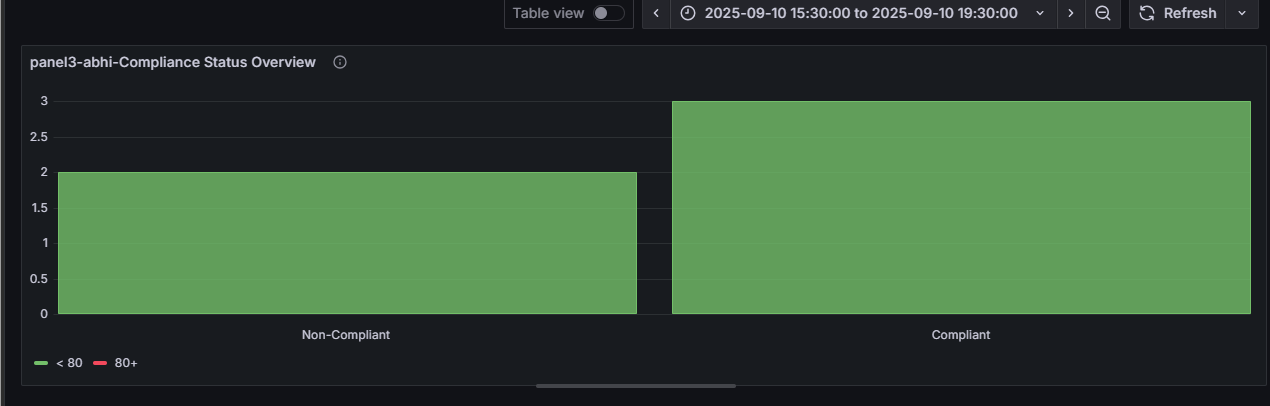




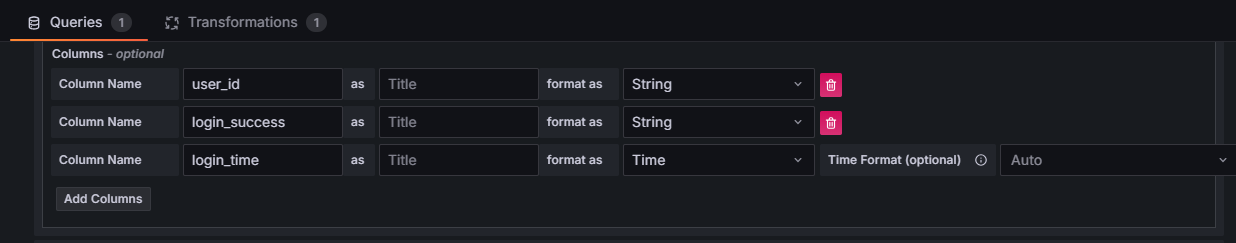
1. Panel 3 - Compliance Status Overview

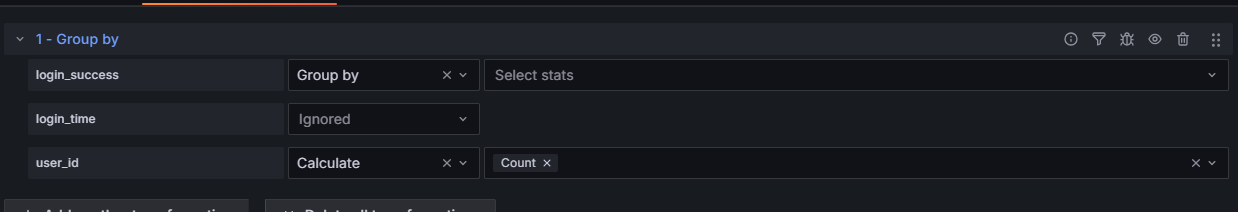


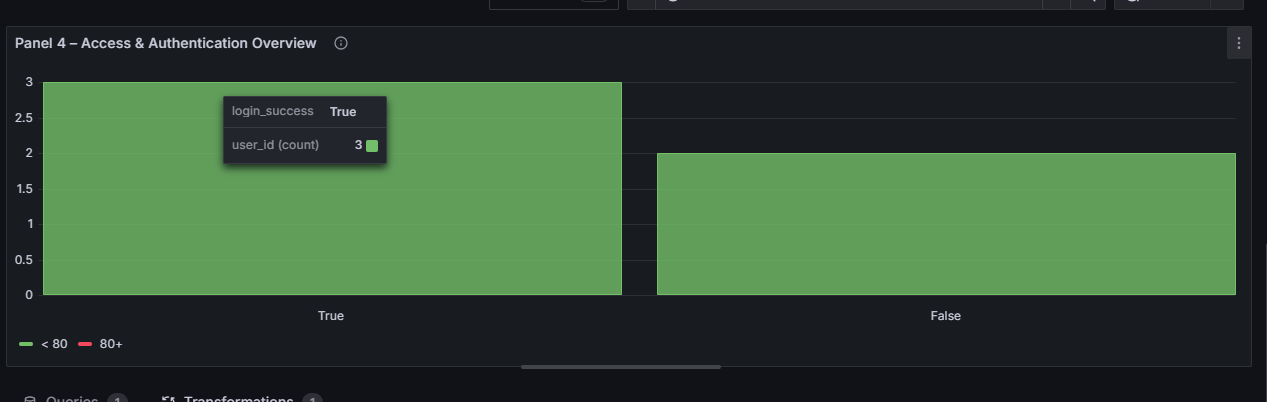




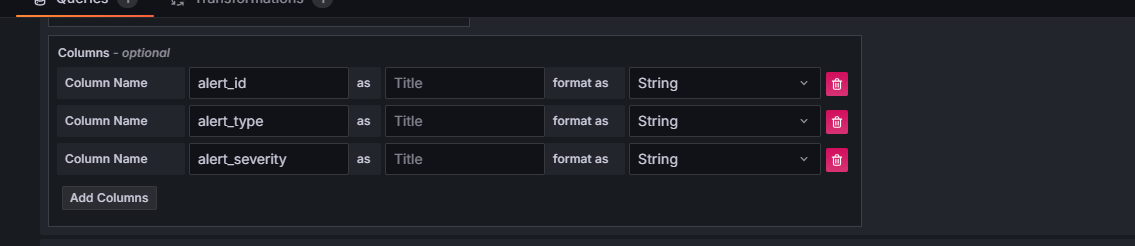
1. Panel 4 – Access & Authentication Overview

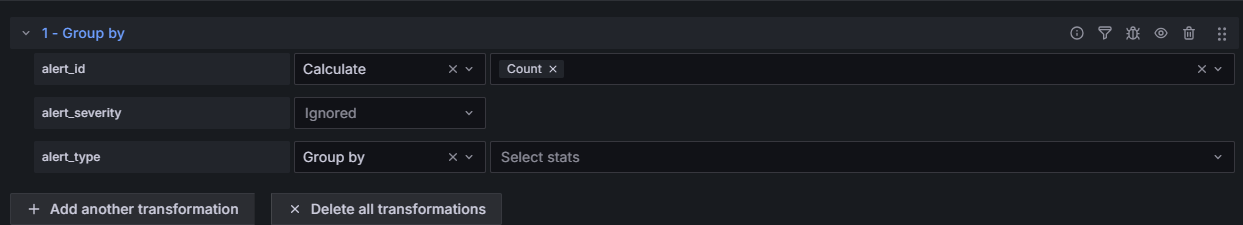


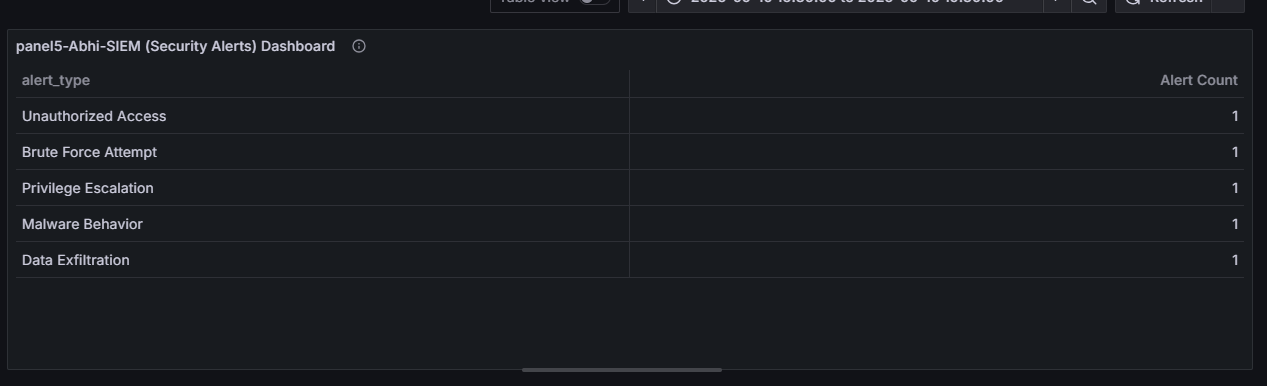


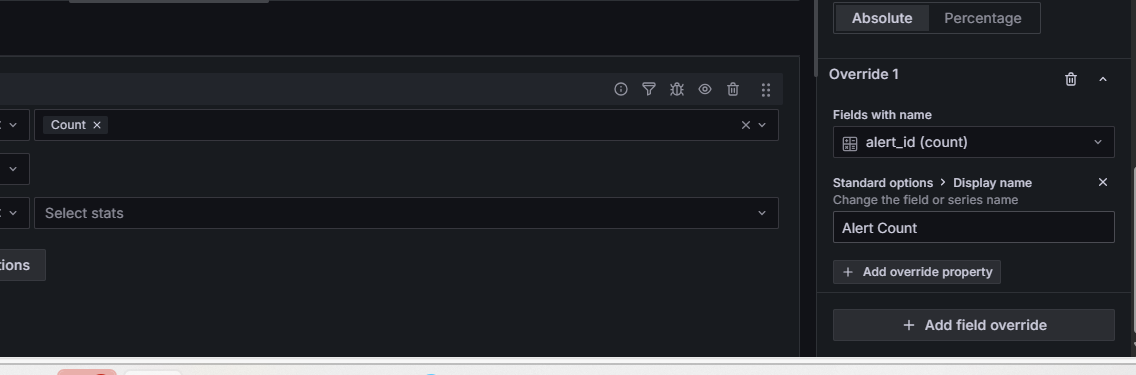


1. Panel 5 – SIEM (Security Alerts) Dashboard







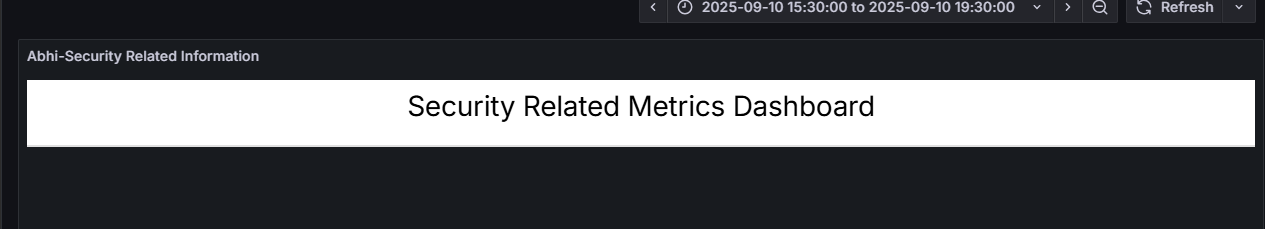


1. Heading:

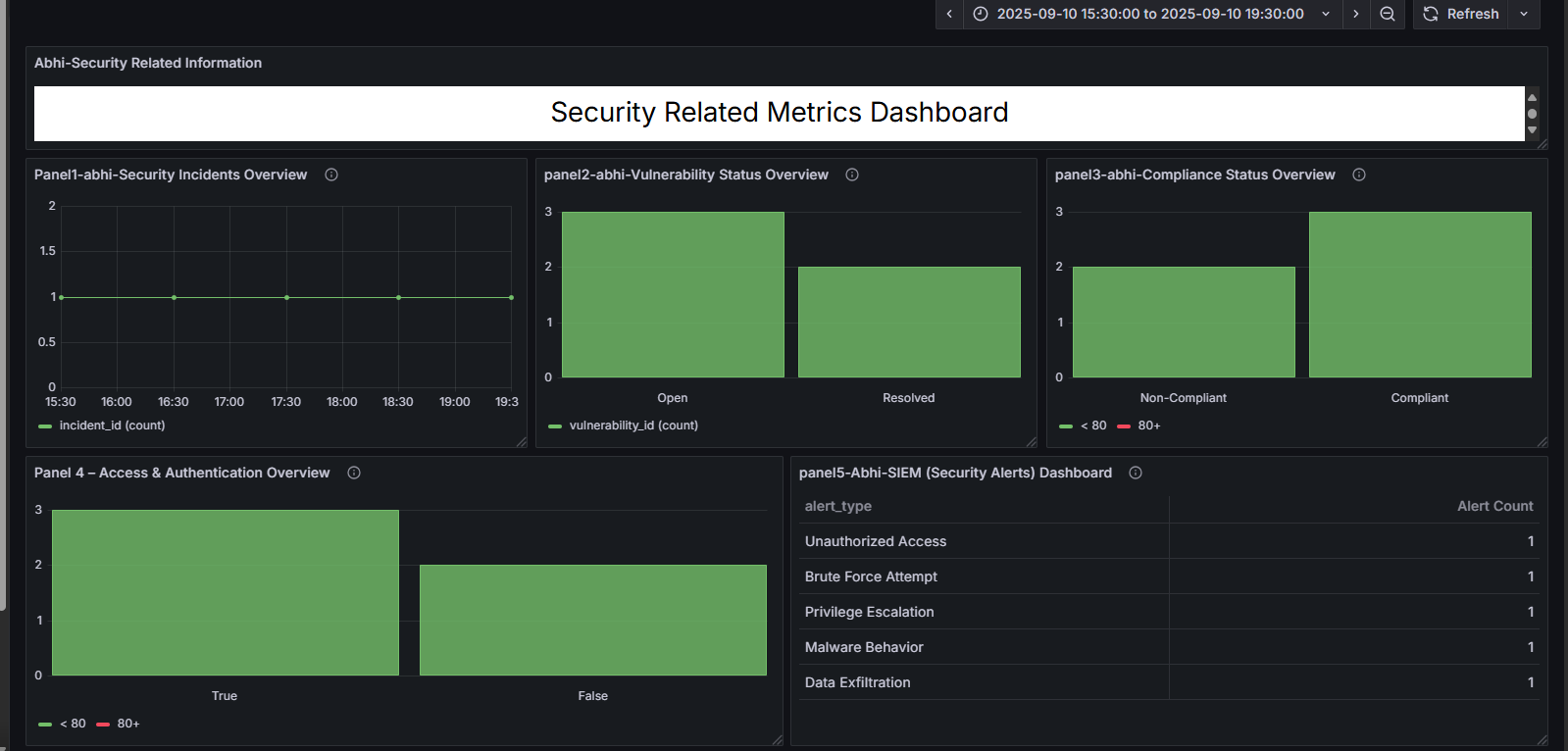
<div style="color: black; background-color: white; padding: 10px; text-align: center; border-bottom: 2px solid #E0E0E0;">

<h1>Security Related Metrics Dashboard</h1>

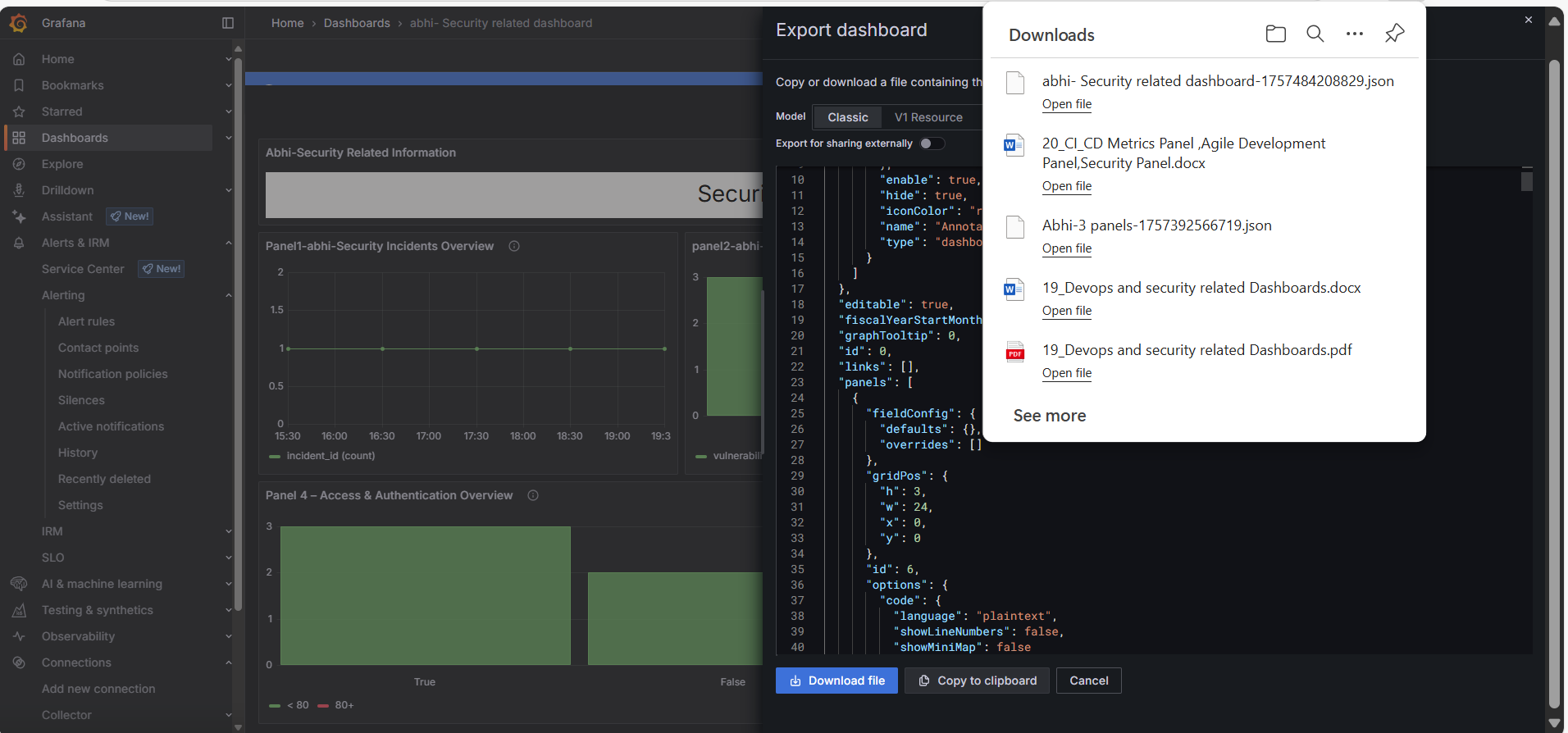
</div>

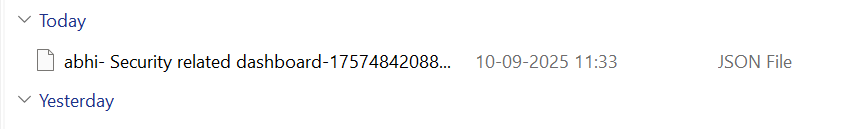


1. Dashboard:



1. Took backup:





1. Github link of backup jsonfile of this dashboard:

[UST-Observability/Json\_backup\_files/abhi- Security related dashboard-1757484208829.json at main · Abhiramikannan/UST-Observability](https://github.com/Abhiramikannan/UST-Observability/blob/main/Json_backup_files/abhi-%20Security%20related%20dashboard-1757484208829.json)