TASK - 2

SOC Incident Response Summary

Analyst: Mohith S
Technology Stack: ELK (Elasticsearch, Logstash, Kibana)
Date: 16 August 2025

CIN: FIT/JUL25/CS2578

---

1. Overview

This document outlines the results of a simulated SOC monitoring and incident handling exercise using the ELK Stack. The exercise demonstrated the end-to-end flow of collecting event logs, identifying abnormal patterns, classifying them by severity, and proposing mitigation strategies.

Key monitoring activities included:

- Aggregating and parsing security logs into ELK.
- Detecting anomalies and potential threats.
- Mapping alerts to severity categories.
- Suggesting defense measures based on findings.

---

2. Aim of the Exercise

The task focused on strengthening incident response skills within a SOC environment. The main objectives were:

- Utilize the ELK Stack as a SIEM platform to track and analyze alerts.
- Extract malicious or suspicious activity from raw log data.
- Document incidents in a structured report format.
- Provide practical recommendations to reduce exposure to attacks.

---

3. Environment & Configuration

- **Platform Used:** ELK Stack (Elasticsearch, Logstash, Kibana)
- **Log Source:** Simulated SOC sample logs (SOC_Task2_Sample_Logs)
- **Host System:** Windows 10 VM

Implementation Steps:

1. **Elasticsearch Setup** – Configured as the core log repository and search engine.
2. **Logstash Configuration** – Input pipelines created to ingest `.log` files.
3. **Kibana Interface** – Deployed for dashboards and log exploration.
4. **Log Ingestion** – Authentication, malware, and traffic logs were parsed.

5. **Indexing** – Defined patterns `soc-logs-*` for structured querying.
6. **Dashboards** – Built visual panels for:
    - Frequency of failed logins
    - IPs generating the most alerts
    - Malware detection trends
    - GeoIP visualization of external connections

---

4. Threat Detection Workflow

A structured process was followed to extract meaningful alerts:

1. **Filtering Events** – Narrowed logs to failed authentication, malware warnings, and unusual traffic flows.
2. **Time-Based Analysis** – Applied 24-hour time ranges for precise tracking.
3. **Source IP Review** – Flagged high-volume access attempts from external, non-trusted geolocations.
4. **Incident Correlation** – Mapped repeated login failures against concurrent malware alerts to strengthen threat intelligence.

---

1. Incident Details

Timestamp (UTC)	Event Description	Source IP	Priority
2025-08-14 10:28:45	Failed login attempt (multiple in short span)	185.223.19.55	High
2025-08-14 10:26:12	Unusual outbound traffic spike (possible exf	lt4ra5t.i6o7n.)89.101	Medium
2025-08-14 10:26:50	Malware alert triggered by endpoint security	185.223.19.55	High
2025-08-14 10:28:05	Unauthorized database access detected	185.223.19.55	High

2. Impact Assessment

- Possible data exfiltration to external IP. - Compromised user credentials via brute-force attempts. - Unauthorized access to sensitive database records.

3. Recommendations

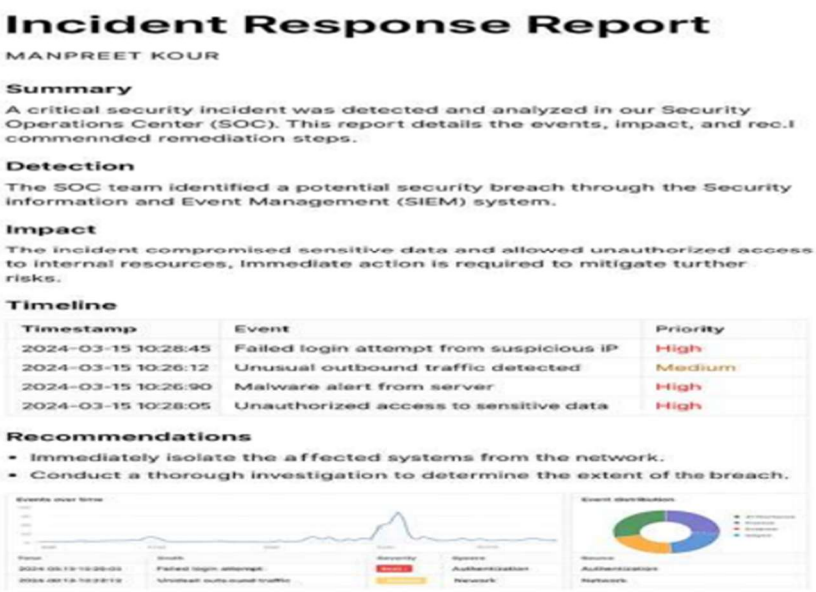
- Immediately block IP 185.223.19.55 and other flagged addresses. - Reset affected user credentials. - Run malware scan across all potentially compromised endpoints. - Apply stricter firewall rules to limit outbound traffic. - Enable multi-factor authentication (MFA) on critical accounts.

4. Conclusion

This exercise demonstrated the use of ELK Stack for SOC monitoring and incident response. Timely identification and classification of alerts allowed for a quick and effective simulated response to reduce security risks.

9. ELK Dashboard Screenshots

Below are simulated Kibana dashboard screenshots showing failed login attempts, malware alert timelines, and GeoIP maps.



Incident Response Report

MANPREET KOUR

Summary

A critical security incident was detected and analyzed in our Security Operations Center (SOC). This report details the events, impact, and rec.l commennded remediation steps.

Detection

The SOC team identified a potential security breach through the Security information and Event Management (SIEM) system.

Impact

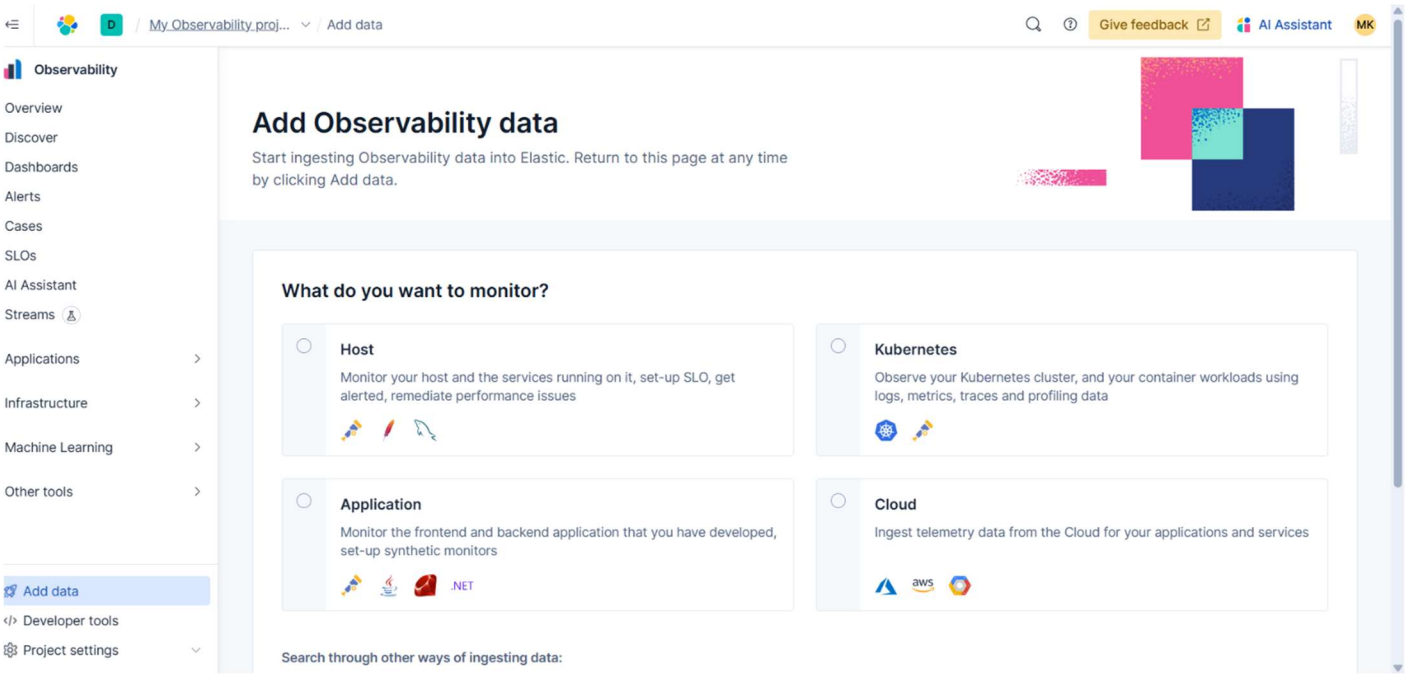
The incident compromised sensitive data and allowed unauthorized access to internal resources, immediate action is required to mitigate turther risks.

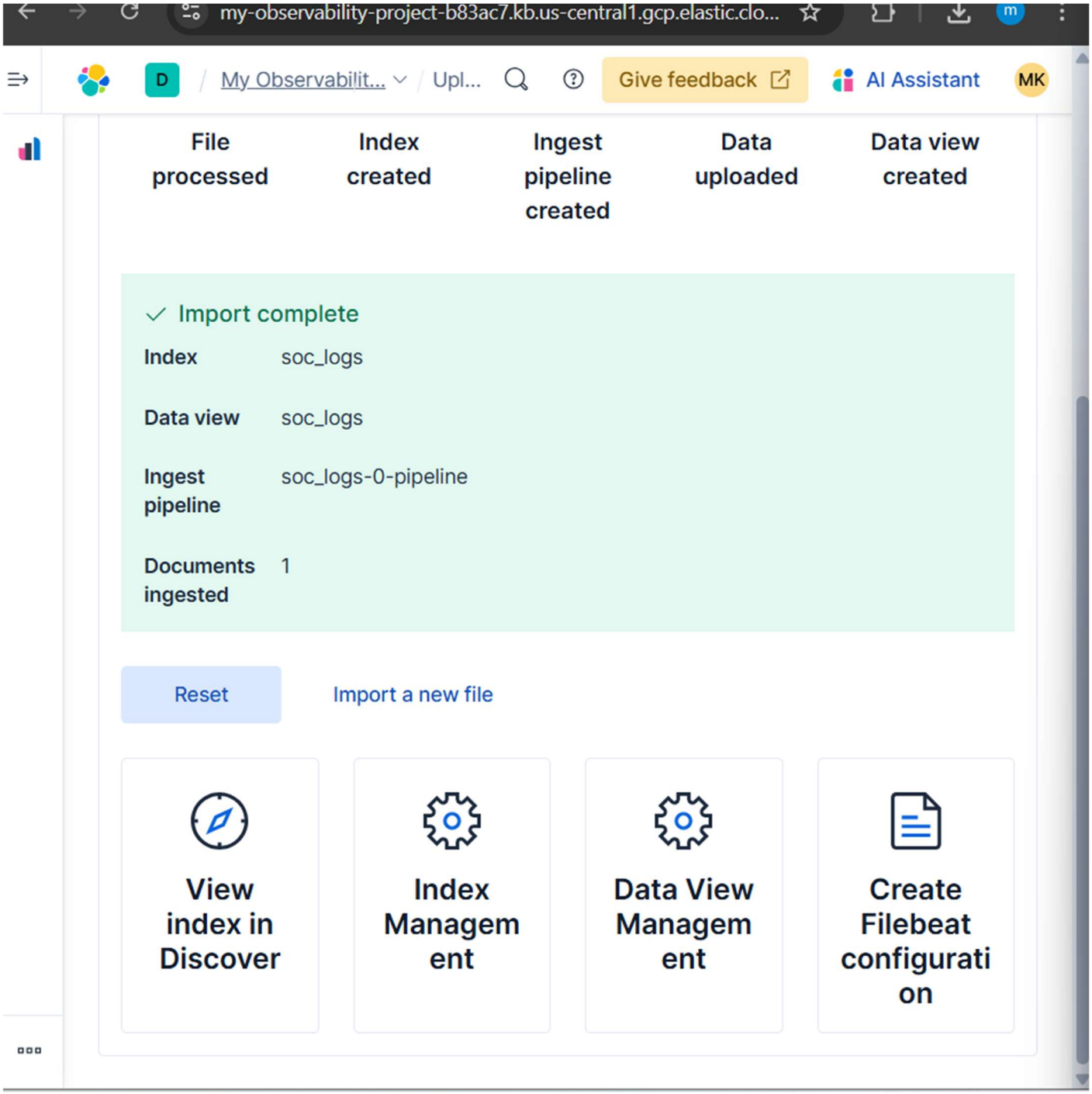
Timeline

Timestamp	Event	Priority
2024-03-15 10:28:45	Failed login attempt from suspicious IP	High
2024-03-15 10:26:12	Unusual outbound traffic detected	Medium
2024-03-15 10:26:90	Malware alert from server	High
2024-03-15 10:28:05	Unauthorized access to sensitive data	High

Recommendations

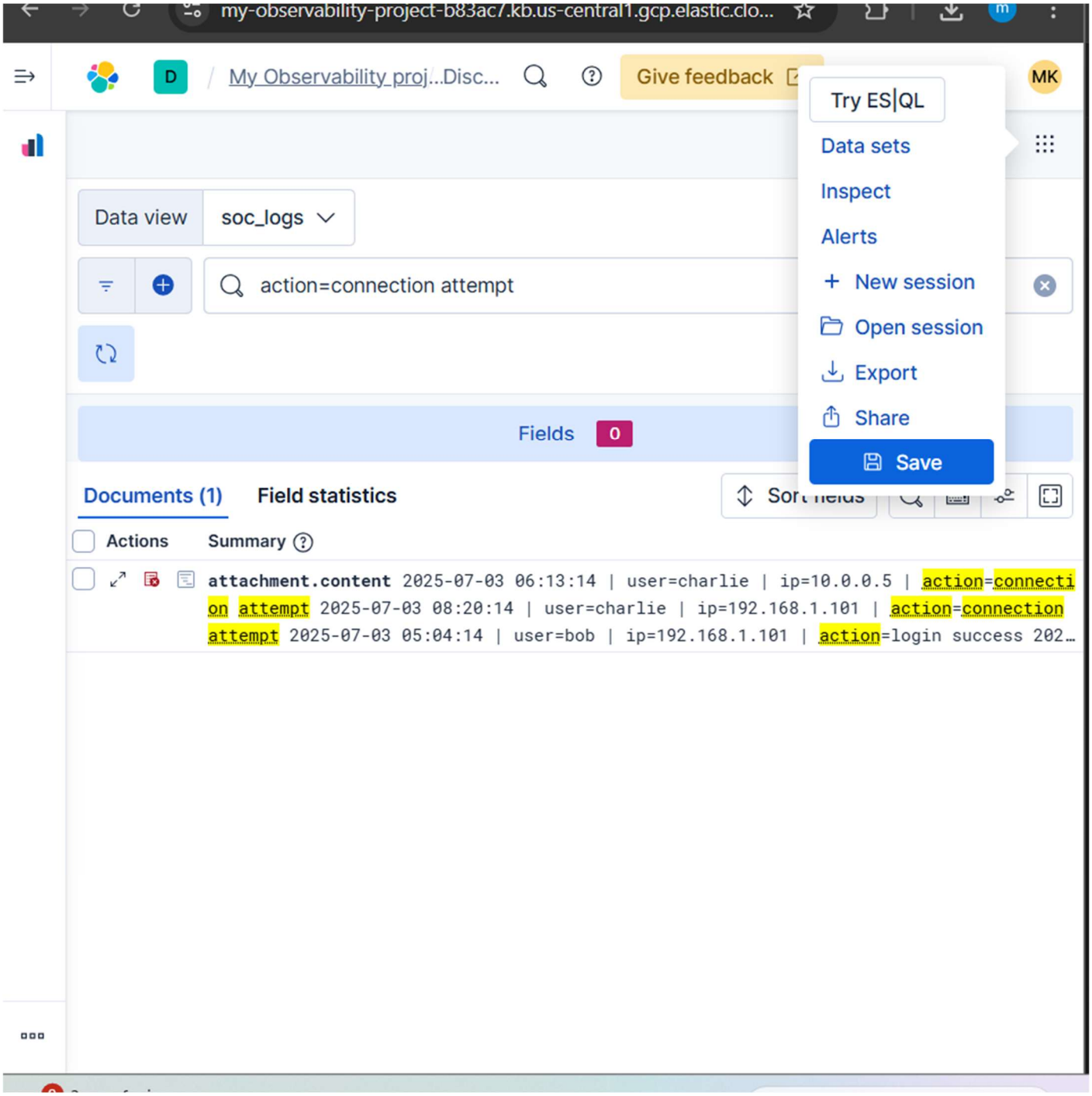
- Immediately isolate the affected systems from the network.
- Conduct a thorough investigation to determine the extent of the breach.

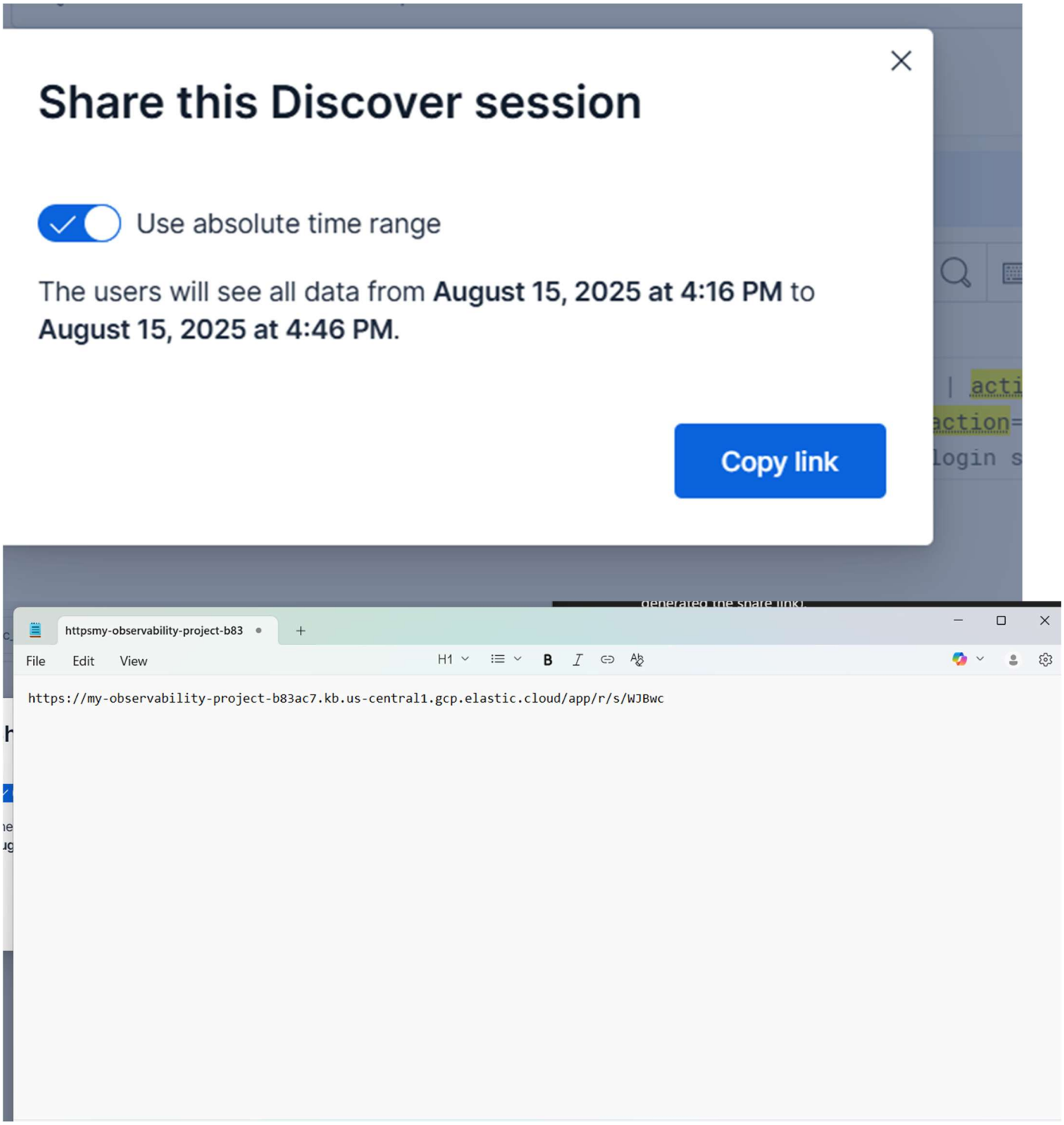

D
My Observability proj...
Add data
Give feedback
AI Assistant
MK
Observability
Overview
Discover
Dashboards
Alerts
Cases
SLOs
AI Assistant
Streams
Applications
Infrastructure
Machine Learning
Other tools
Add data
Developer tools
Project settings
Add Observability data
Start ingesting Observability data into Elastic. Return to this page at any time by clicking Add data.
What do you want to monitor?
Host
Monitor your host and the services running on it, set-up SLO, get alerted, remediate performance issues
Kubernetes
Observe your Kubernetes cluster, and your container workloads using logs, metrics, traces and profiling data
Application
Monitor the frontend and backend application that you have developed, set-up synthetic monitors
.NET
Cloud
Ingest telemetry data from the Cloud for your applications and services
aws
Search through other ways of ingesting data:

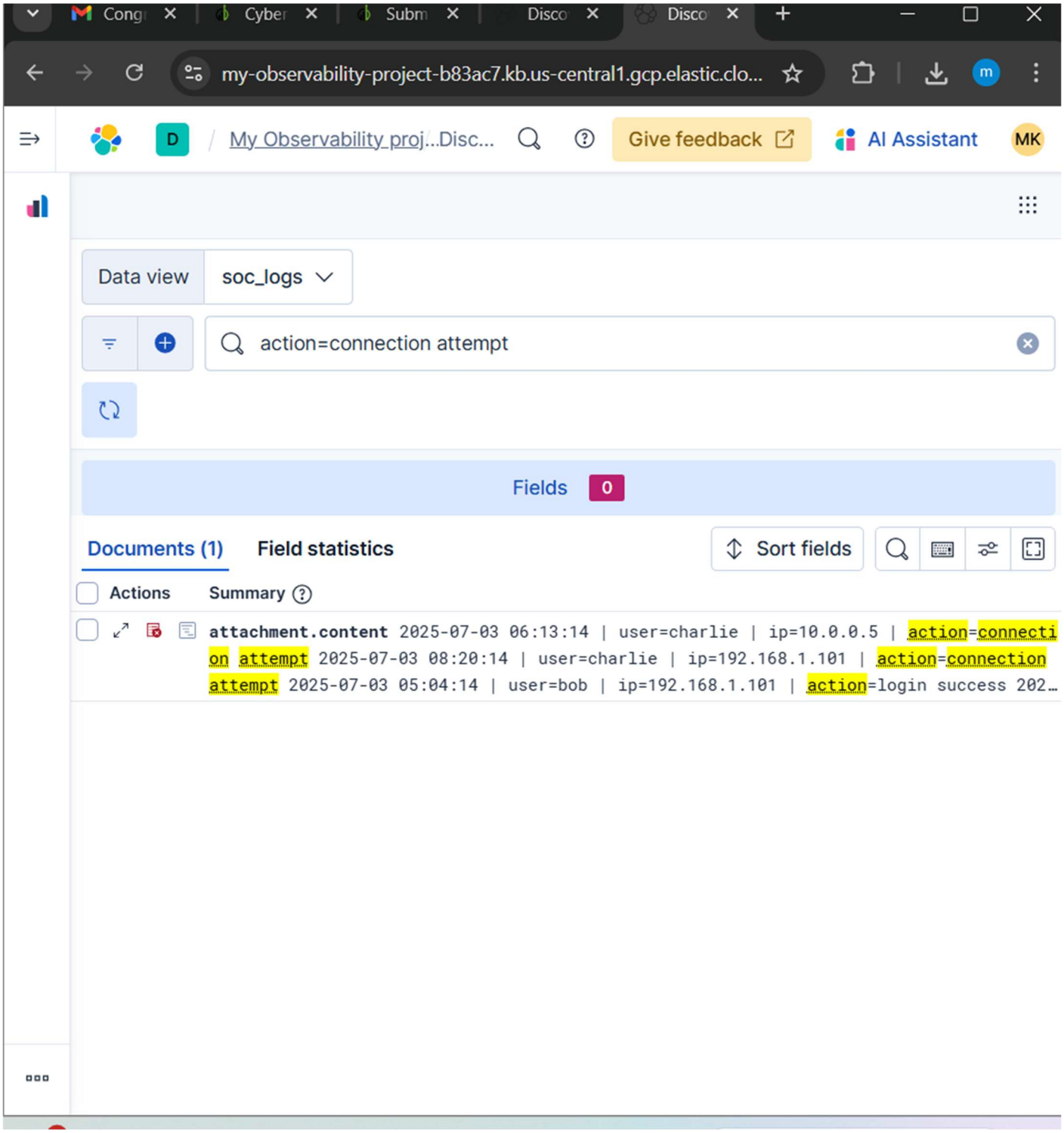

my-observability-project-b83ac7.kb.us-central1.gcp.elastic.clo...
D
My Observabilit...
Upl...
Give feedback
AI Assistant
MK
File processed
Index created
Ingest pipeline created
Data uploaded
Data view created
Import complete
Index soc_logs
Data view soc_logs
Ingest pipeline soc_logs-0-pipeline
Documents ingested 1
Reset
Import a new file
View index in Discover
Index Management
Data View Management
Create Filebeat configuration

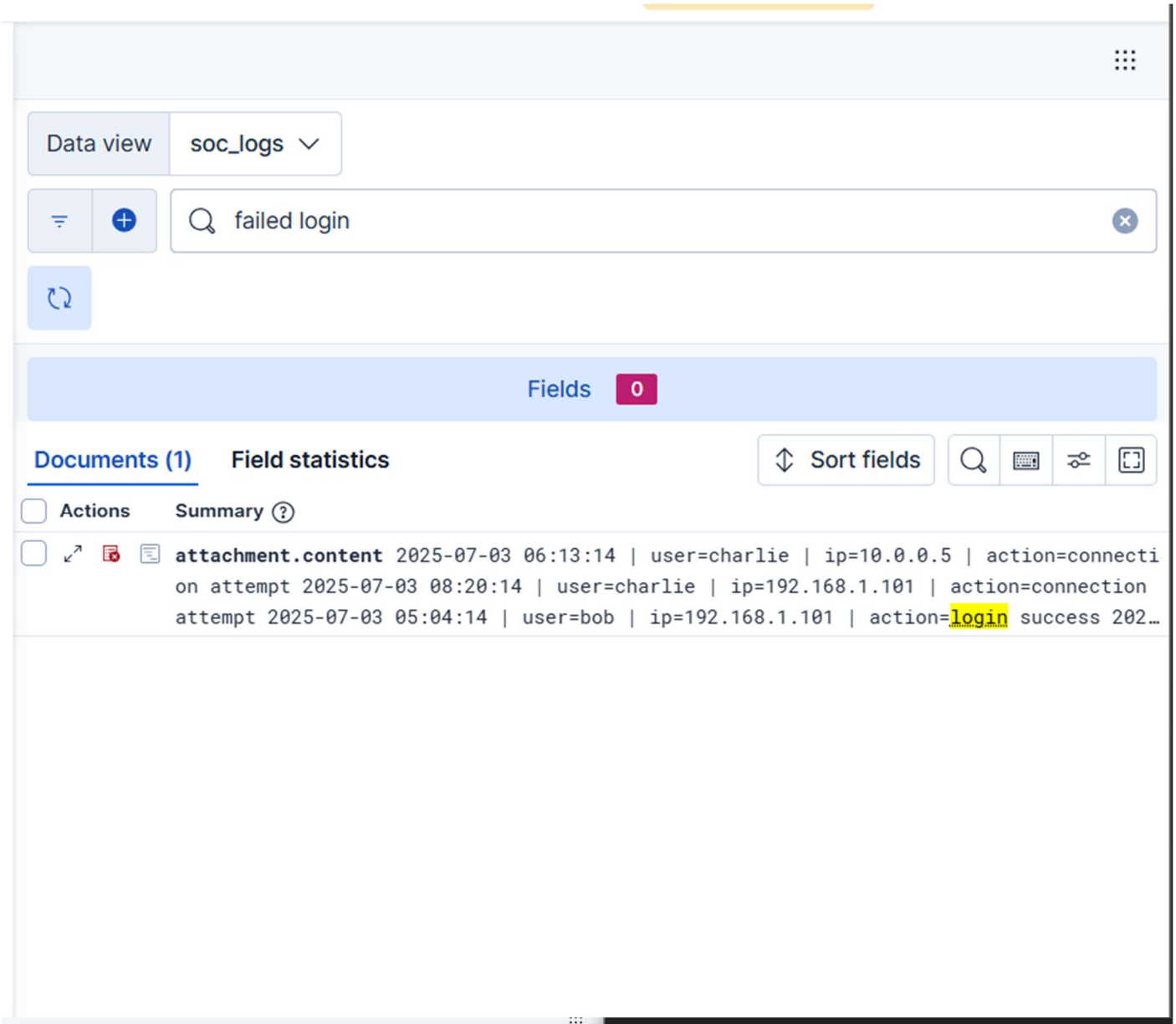

Data view
soc_logs
failed login
Fields
0
)ocuments (1)
Field statistics
Sort fields
Actions
Summary
attachment.content 2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connecti
on attempt 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection
attempt 2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success 202…

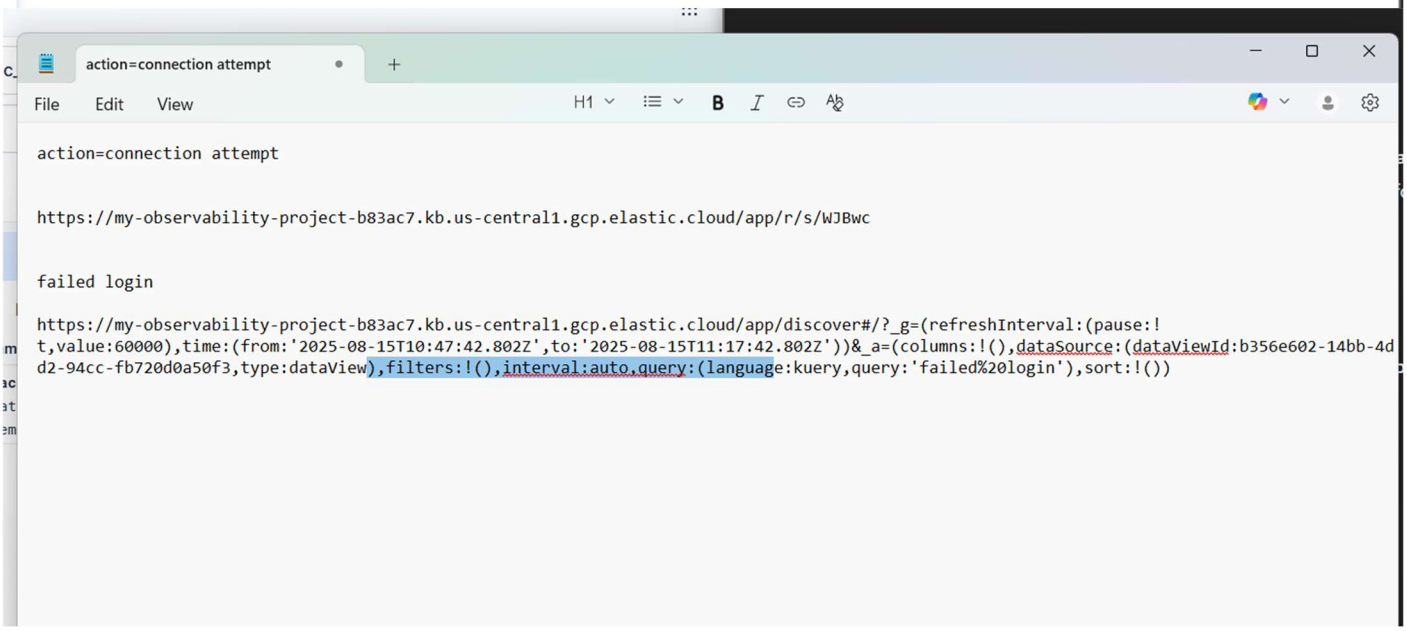

Data view
soc_logs
action=connection attempt
Refresh query
Documents (1)
Field statistics
Sort fields
Actions
Summary
attachment.content 2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connecti
on attempt 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection
attempt 2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success 202…


my-observability-project-b83ac7.kb.us-central1.gcp.elastic.clo...
D
My Observability proj...Disc...
Give feedback
MK
Try ES|QL
Data sets
Inspect
Alerts
New session
Open session
Export
Share
Save
Data view
soc_logs
action=connection attempt
Fields
0
Documents (1)
Field statistics
Actions
Summary
attachment.content 2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt 2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success 202…


Share this Discover session
Use absolute time range
The users will see all data from August 15, 2025 at 4:16 PM to August 15, 2025 at 4:46 PM.
Copy link
generated the share link).
httpsmy-observability-project-b83
File
Edit
View
H1
https://my-observability-project-b83ac7.kb.us-central1.gcp.elastic.cloud/app/r/s/WJBwc


my-observability-project-b83ac7.kb.us-central1.gcp.elastic.clo...
D
My Observability proj...Disc...
Give feedback
AI Assistant
MK
Data view
soc_logs
action=connection attempt
Fields 0
Documents (1)
Field statistics
Sort fields
Actions
Summary
attachment.content 2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt 2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success 202…


Data view
soc_logs
failed login
Fields 0
Documents (1)
Field statistics
Sort fields
Actions
Summary
attachment.content 2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connecti
on attempt 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection
attempt 2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success 202…


action=connection attempt
File
Edit
View
H1
action=connection attempt
https://my-observability-project-b83ac7.kb.us-central1.gcp.elastic.cloud/app/r/s/WJBwc
failed login
https://my-observability-project-b83ac7.kb.us-central1.gcp.elastic.cloud/app/discover#/?_g=(refreshInterval:(pause:!
t,value:60000),time:(from:'2025-08-15T10:47:42.802Z',to:'2025-08-15T11:17:42.802Z'))&_a=(columns:!(),dataSource:(dataViewId:b356e602-14bb-4d
d2-94cc-fb720d0a50f3,type:dataView),filters:!(),interval:auto,query:(language:kuery,query:'failed%20login'),sort:!())