# **INCIDENT RESPONSE REPORT**

Prepared by: Chandana Devarakonda

Date:15/8/2025

Tool Used:Kibana(Elastic stack)

Dataset:Provided simulated log files (soc-tas2-logs index)

## 1.Executive Summary

During analysis of the provided simulated log dataset in Kibana, multiple suspicious events were identified. These included unauthorized IP connections, failed logins, unusual access files and possible malware alerts. This report outlines the investigation process, findings, alerts and recommended actions.

## 2.Investigation Steps

* Opened kibana Discover view and loaded the dataset which was provided.
* Applied KQL search queries to filter events for suspicious Ips, login attempts, file access and malware alerts.
* Reviewed event details such as timestamps,IP addresses and event type.
* Caputed relevant screenshots for documentation.
* Classified incidents based in severity.

## 3.Findings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Incident ID | Description | IP Address/Event | Severity | Notes |
| 1. | Unauthorized access attempt | 10.0.0.5 | High | Unknown internal IP attempted login. |
| 2. | Multiple suspicious logins | 192.168.1.101 | High | Repeated login attempts detected. |
| 3. | External IP Connection | 172.16.0.3 | Medium | External IP not on whitelist. |
| 4. | Successful login after failed attempts | N/A | High | Possible brute-force attack succeeded. |
| 5. | File access outside work hours | N/A | Medium | Could indicate unauthorized use. |
| 6. | Malware detection alert | N/A | Critical | Requires immediate isolation and scan |

## 4.Incident Classification

* High Priority: Unauthorized internal access (10.0.0.5, 192.168.1.101, brute-force login)
* Medium Priority: External connections, unusual file access (172.16.0.3, after-hours access)
* Critical Priority: Any malware alert detected

## 5.Impact Assessment

* Confidentiality Risk: sensitive data could be accessed.
* Integrity Risk: Files or configurations may have been altered.
* Availability Risk: Malware could cause service disruption.

## 6.Recommended Response Actions

* Block suspicious IP addresses at the firewall.
* Reset passwords for affected accounts.
* Conduct malware scans on potentially compromised systems.
* Restrict file access permissions.
* Enable multi-factor authentication for all users.
* Increase log monitoring frequency.

## 7.Stakeholder communication

Subject: Security Incident Detected – Immediate action Required

Body:

Dear [Manager/Security Lead],

During log analysis in Kibana, several high-priority security events were identified. These include unauthorized IP connections, suspicious login activity, and possible malware detection. Immediate action is recommended, including blocking IPs, resetting credentials, and performing malware scans.

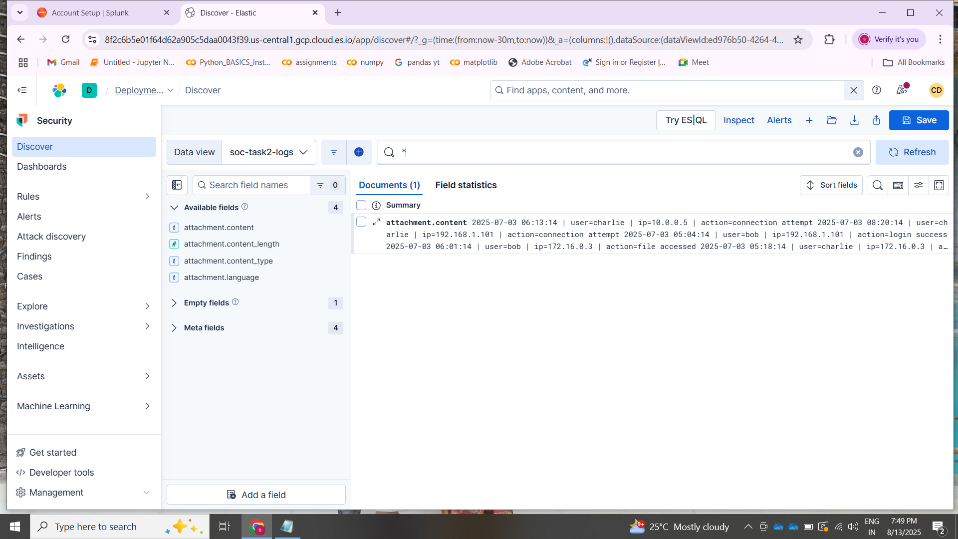
A detailed report is attached.

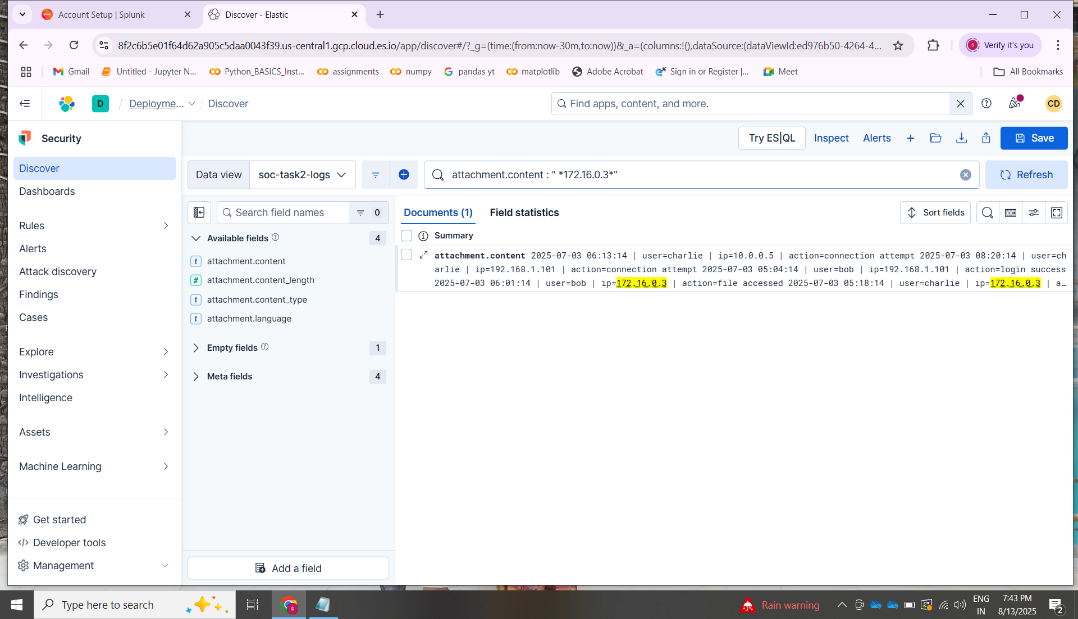
Regards,

[Chandana Devarakonda]

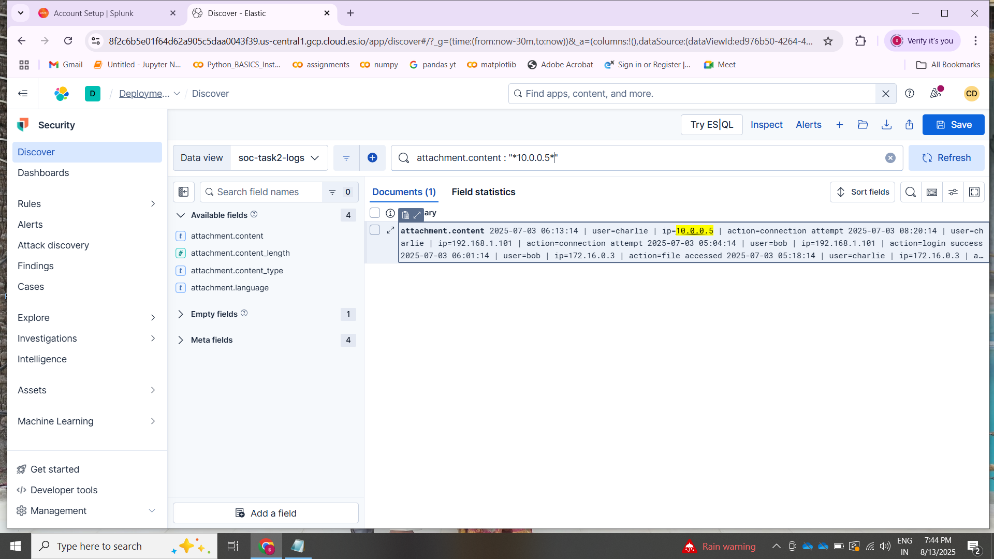
Security analyst Intern

## 8.Required Screenshots

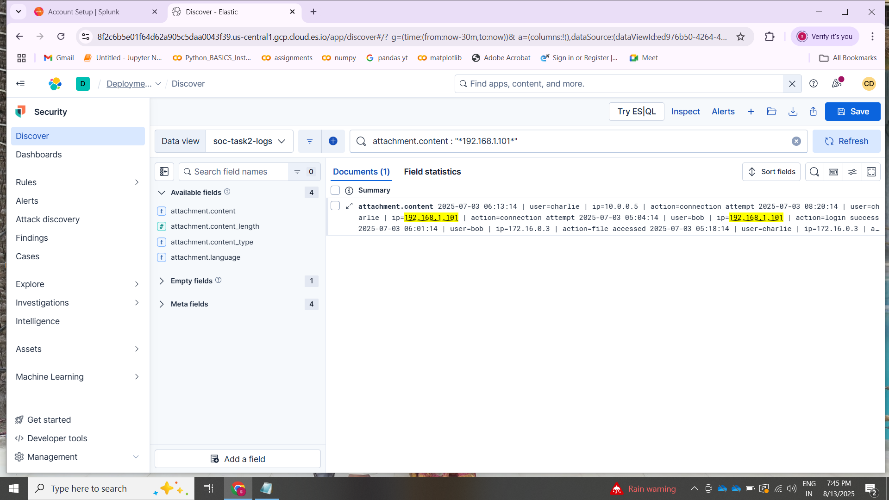
1. Discover view showing all logs (\* query)
2. Query results for IP 172.16.0.3



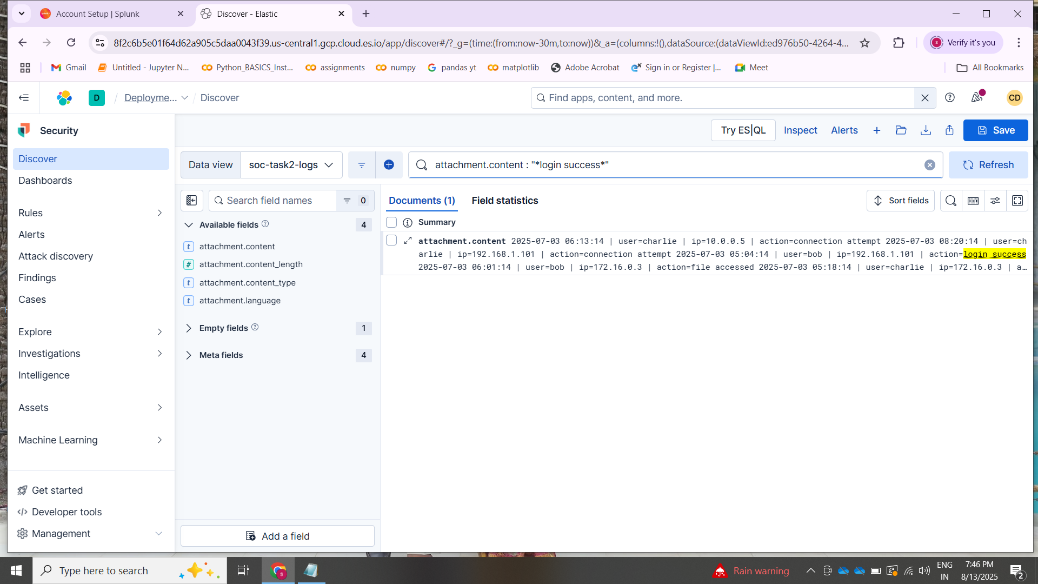
1. Query results for IP 10.0.0.5



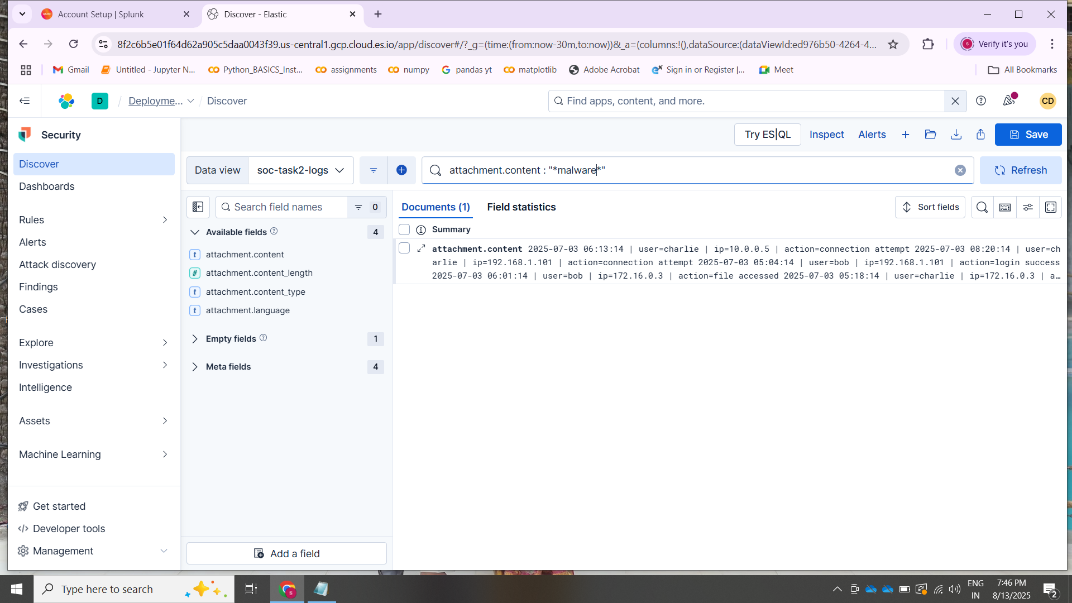
4)Query results for IP 192.168.1.101



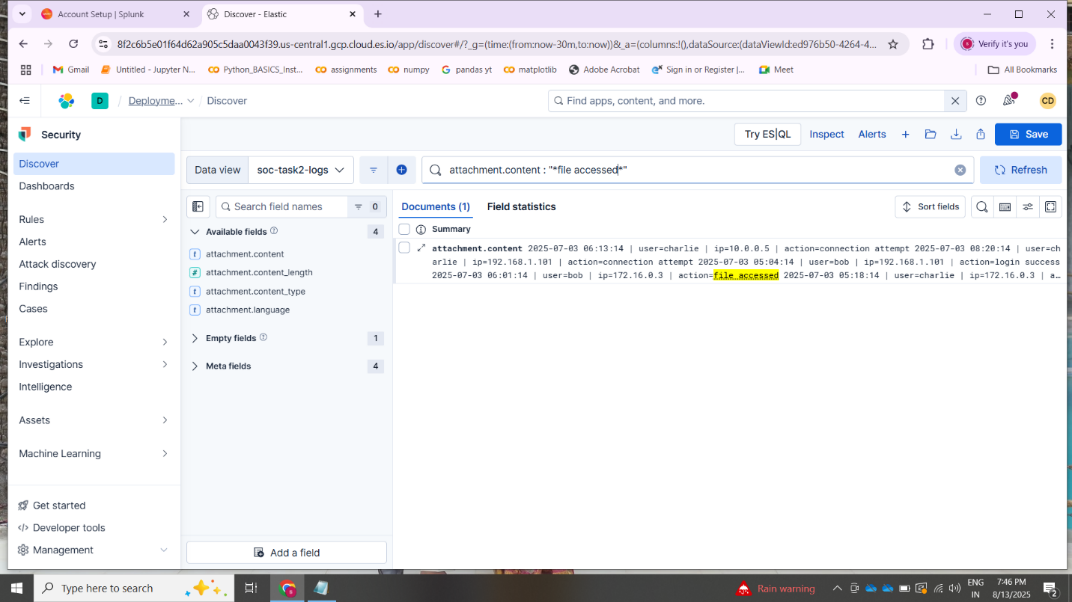
5)Successful logins



6)Malware Detection Alert (Simulated)



7) File Access events



8)Failed logins

