Security Operations Center (SOC) Incident Response Report

Project: SOC Internship Task – Security Alert Monitoring
Analyst: Aditya Sutar
SIEM Tool: Elastic Security (Kibana)
Date: 10 December 2025

1. Executive Summary

During routine SIEM log monitoring, multiple security events were detected from internal systems. These events consisted of **malware infection**, **unauthorized connection attempts**, and **user login activities from internal networks**. The malware event was confirmed as a **Trojan infection on host `10.0.0.5` under user `bob`**, indicating a high-severity compromise requiring immediate containment.

2. Incident Identification

High Severity Incident:

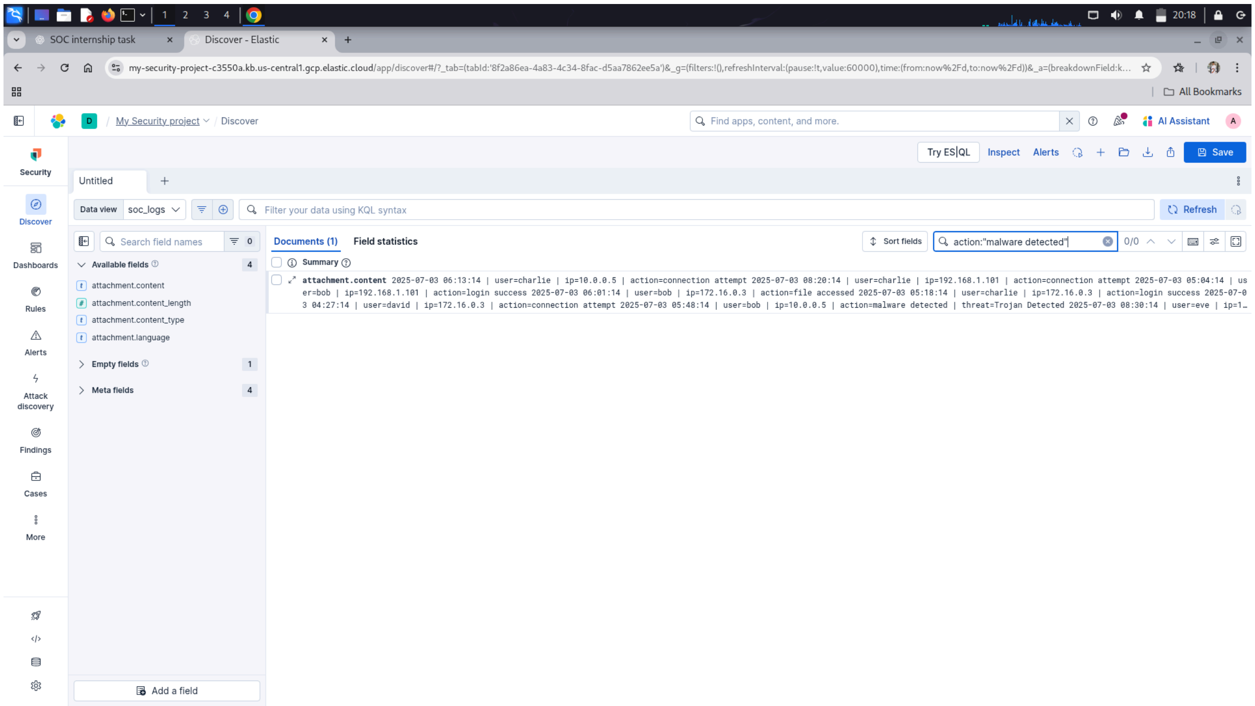
- **Action:** `malware detected`
- **Threat:** `Trojan Detected`
- **User:** `bob`
- **Host:** `10.0.0.5`
- **Description:** Indicates an active malware infection compromising system confidentiality and availability.

Medium Severity Incident:

- **Action:** `connection attempt`
- **Users:** `charlie`, `david`, etc.
- **IPs involved:** `192.168.1.101`, `172.16.0.3`, …
- **Description:** Multiple unauthorized connection attempts suggest probing or brute-force reconnaissance activity.

Low Severity Activity:

- **Action:** `login success`
- **Users:** `bob`, `charlie`
- **Description:** Login events are normal but require watchlisting in case they correspond to suspicious IPs or attempts.

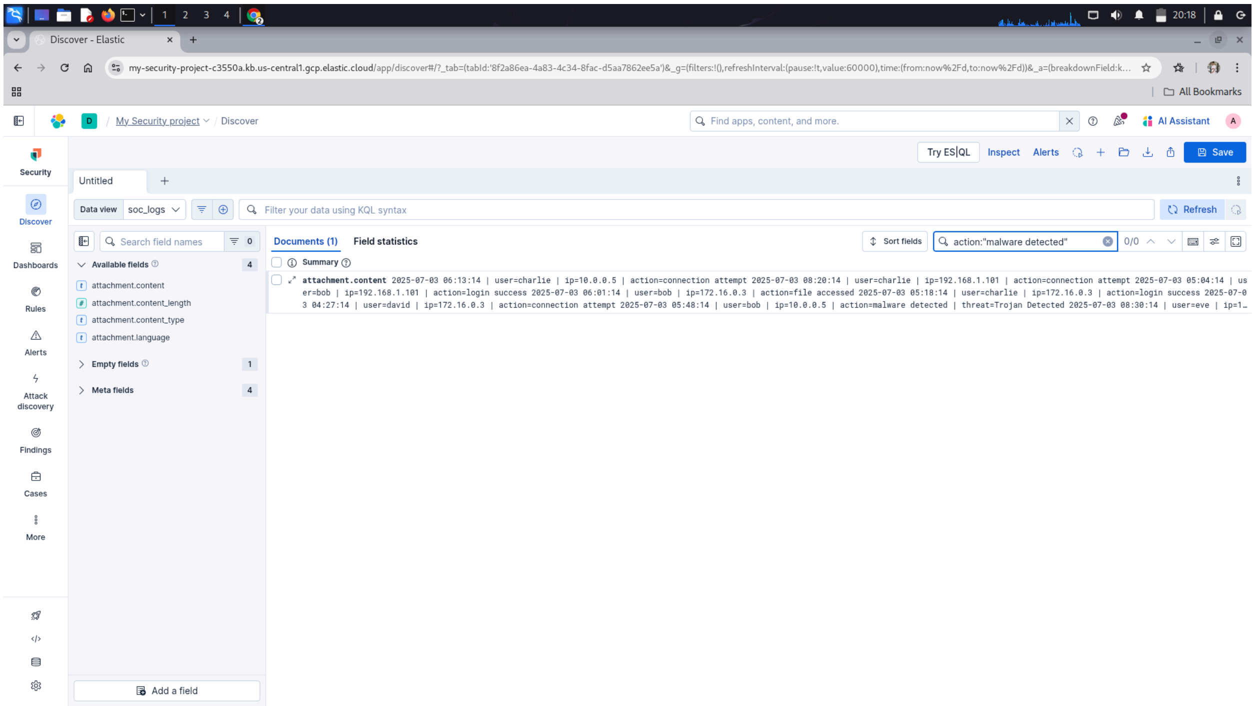

SOC internship task
Discover - Elastic
my-security-project-c3550a.kb.us-central1.gcp.elastic.cloud/app/discover#/?_tab=(tabId:'8f2a86ea-4a83-4c34-8fac-d5aa7862ee5a')&_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now%2Fd,to:now%2Fd))&_a=(breakdownField:k...
All Bookmarks
My Security project / Discover
Find apps, content, and more.
AI Assistant
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
More
Try ES|QL
Inspect
Alerts
Save
Untitled
Data view
soc_logs
Filter your data using KQL syntax
Refresh
Search field names
Available fields 4
Empty fields 1
Meta fields 4
Add a field
Documents (1)
Field statistics
Sort fields
0/0
Summary

action:"malware detected"

Available fields

- attachment.content
- attachment.content_length
- attachment.content_type
- attachment.language

```
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 | us
er=bob | ip=192.168.1.101 | action=login success 2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed 2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success 2025-07-0
3 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt 2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected 2025-07-03 08:30:14 | user=eve | ip=1…
```

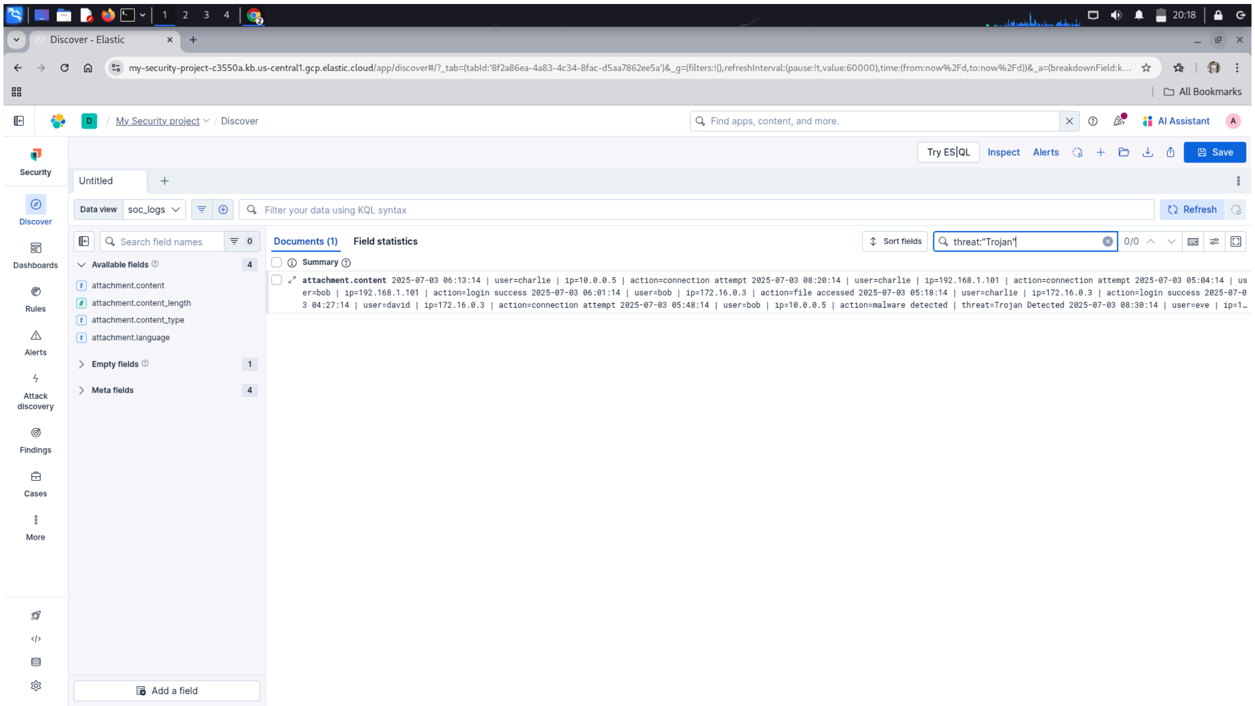

Discover - Elastic
my-security-project-c3550a.kb.us-central1.gcp.elastic.cloud/app/discover#/?_tab=(tabId:'8f2a86ea-4a83-4c34-8fac-d5aa7862ee5a')&_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now%2Fd,to:now%2Fd))&_a=(breakdownField:k...
All Bookmarks
My Security project / Discover
Find apps, content, and more.
AI Assistant
Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
More
Try ES|QL
Inspect
Alerts
Save
Untitled
Data view
soc_logs
Filter your data using KQL syntax
Refresh
Search field names
Available fields 4
Empty fields 1
Meta fields 4
Add a field
Documents (1)
Field statistics
Sort fields
0/0
Summary

action:"malware detected"

Available fields

- attachment.content
- attachment.content_length
- attachment.content_type
- attachment.language

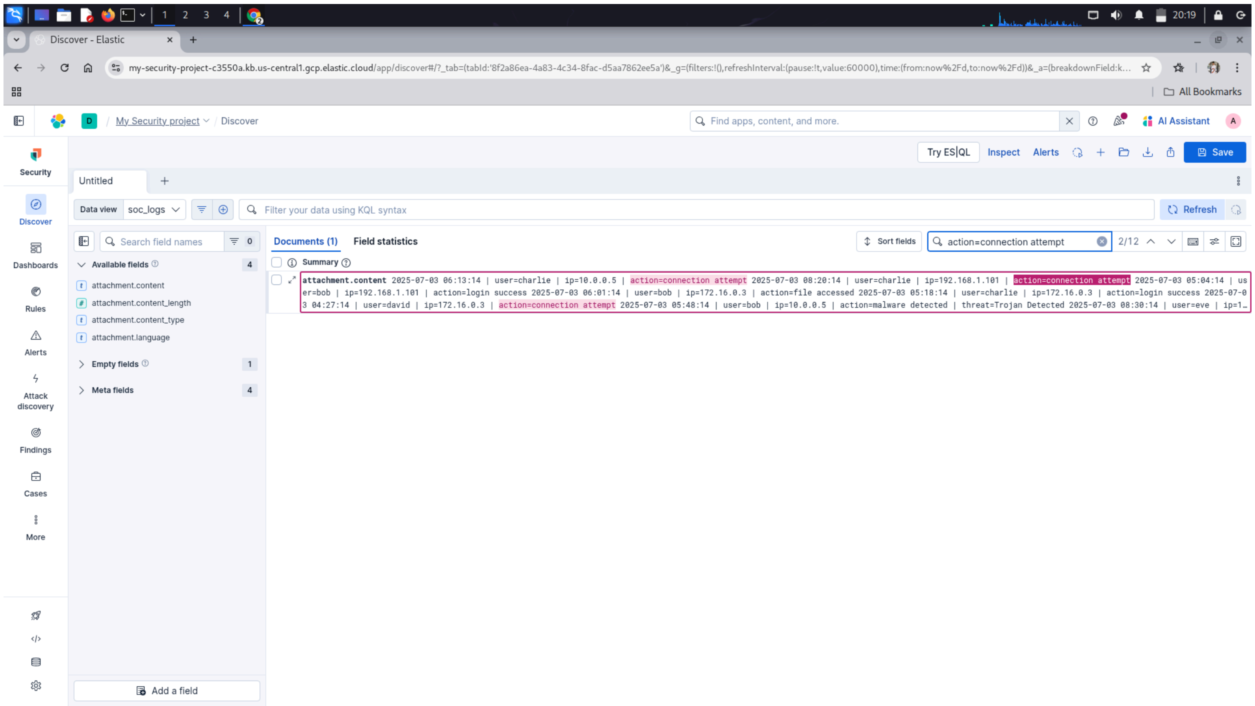
```
attachment.content 2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt 2025-07-03 05:04:14 | us
er=bob | ip=192.168.1.101 | action=login success 2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed 2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success 2025-07-0
3 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt 2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected 2025-07-03 08:30:14 | user=eve | ip=1…
```



my-security-project-c3550a.kb.us-central1.gcp.elastic.cloud/app/discover#/?_tab=(tabId:'8f2a86ea-4a83-4c34-8fac-d5aa7862ee5a')&_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now%2Fd,to:now%2Fd))&_a=(breakdownField:k…

threat:"Trojan" 0/0

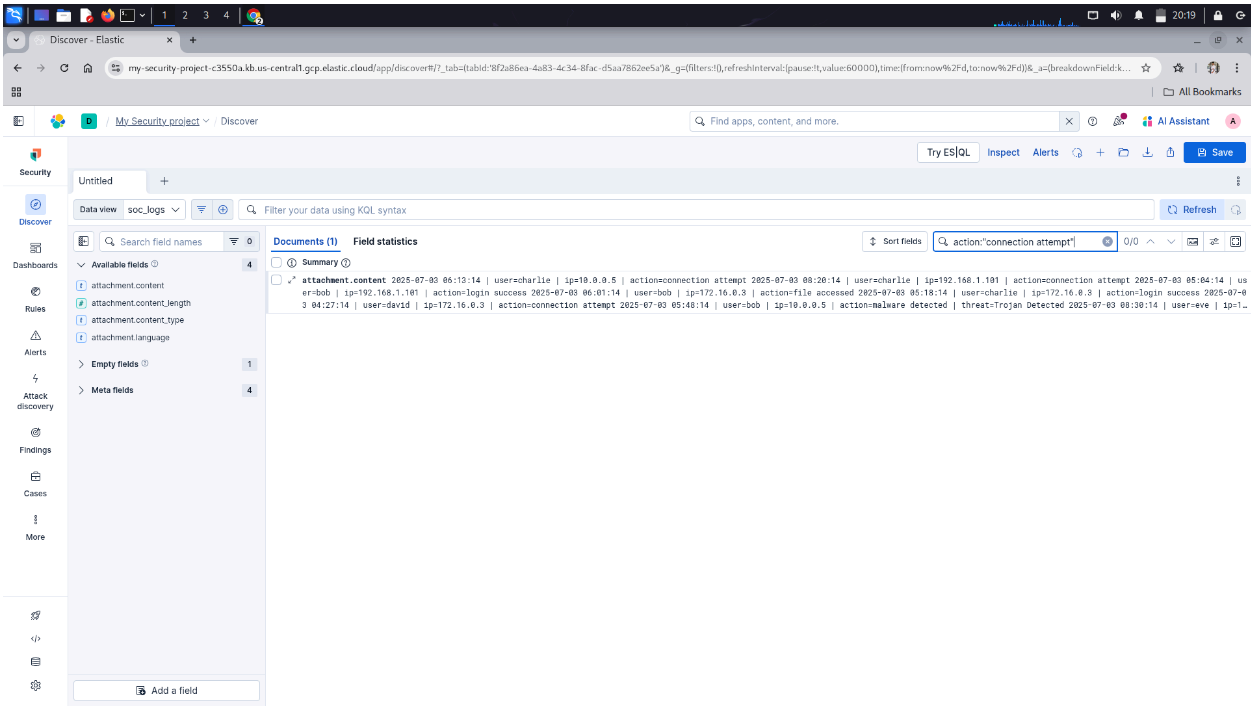
```
attachment.content 2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt 2025-07-03 05:04:14 | us
er=bob | ip=192.168.1.101 | action=login success 2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed 2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success 2025-07-0
3 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt 2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected 2025-07-03 08:30:14 | user=eve | ip=1…
```



my-security-project-c3550a.kb.us-central1.gcp.elastic.cloud/app/discover#/?_tab=(tabId:'8f2a86ea-4a83-4c34-8fac-d5aa7862ee5a')&_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now%2Fd,to:now%2Fd))&_a=(breakdownField:k…

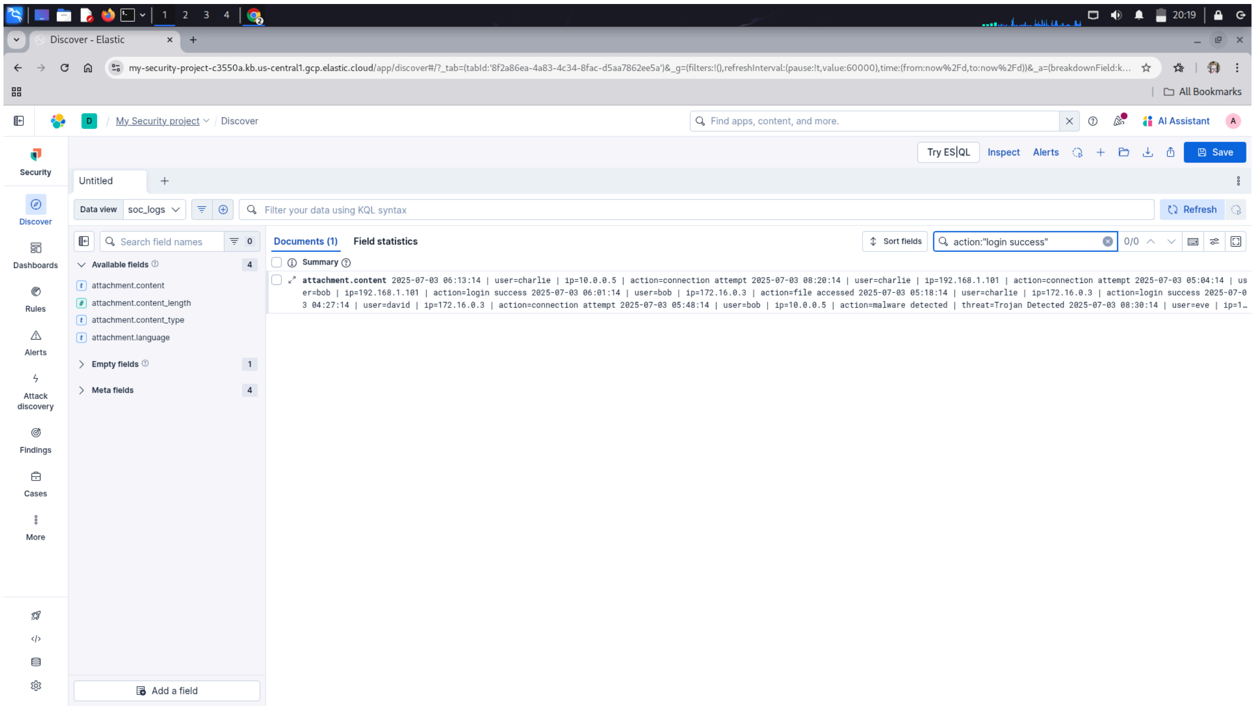
action=connection attempt 2/12

```
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 | us
er=bob | ip=192.168.1.101 | action=login success 2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed 2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success 2025-07-0
3 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt 2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected 2025-07-03 08:30:14 | user=eve | ip=1…
```



action:"connection attempt"

```
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 | us
er=bob | ip=192.168.1.101 | action=login success 2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed 2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success 2025-07-0
3 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt 2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected 2025-07-03 08:30:14 | user=eve | ip=1…
```



action:"login success"

```
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 | us
er=bob | ip=192.168.1.101 | action=login success 2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed 2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success 2025-07-0
3 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt 2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected 2025-07-03 08:30:14 | user=eve | ip=1…
```

3. Incident Timeline

Time	Event
06:13	Connection attempt from user charlie
06:01	Login success by user bob
05:18	File access by user charlie
05:48	Connection attempt by user david
08:30	**Malware Detected — Trojan — Host 10.0.0.5 under bob**

4. Impact Assessment

- **Malware Impact:** Trojan infection can lead to credential theft, system corruption, data exfiltration, or internal lateral movement.
- **Connection Attempts Impact:** Possible reconnaissance/brute force activity indicating attempts to gain unauthorized access.
- **Login Activity Impact:** Legitimate login but could relate to active lateral spread if malware gains persistence.

5. Root Cause Analysis

The malware detection event on host `10.0.0.5` indicates:

- Possible malicious file execution
- Lack of endpoint security scanning
- Potential inbound infection via internal file access

Repeated **connection attempts** show:

- Internal probing by multiple users/IPs
- Weak network segmentation
- Absence of access rate limiting

6. Severity Classification

Alert Type	Host/User	Severity	Rationale
Trojan Malware Detected	bob / 10.0.0.5	**High**	Active compromise requiring isolation
Unauthorized Connection Attempts	charlie/david / 192.168.1.101 / 172.16.0.3	**Medium**	Exploitation or brute-force exploration
Login Success Events	bob/charlie	**Low**	Normal, but required monitoring for correlation

7. Remediation Recommendations

For Malware

Immediately isolate host `10.0.0.5` from network
Run full endpoint anti-malware scan
Remove Trojan and reset compromised credentials
Patch OS and validate persistence mechanisms
Monitor for lateral movement

For Unauthorized Access Attempts

Block suspicious internal traffic at firewall
Enforce network segmentation
Monitor failed/connection attempts for escalation
Lock out accounts after repeated attempts

For Login Activity

Monitor logins from same accounts post-infection
Require MFA for access to critical systems
Review user access privileges

8. Conclusion

The SOC monitoring successfully identified a **critical Trojan malware incident** alongside related network probing. Prompt containment and continuous monitoring are necessary to protect internal assets. All findings were derived using SIEM log investigations inside Elastic Discover.