Incident Response Report

Organization Name: [Future Interns]

Prepared By: [Chandu reddy]

Date: [30-09-2025]

1. Executive Summary

This report summarizes the security incidents detected during SOC monitoring using Splunk. Logs were analyzed from authentication events, network connections, and malware alerts. Multiple suspicious activities were identified and classified based on severity.

2. Incident Details

Alert ID	Timestamp	Host	Event Type	Username	Source IP	Destination IP	Description	Severity
1	2025-09-30 09:15:23	server01	login_failed	admin	192.168.1.45	-	10 failed login attempts	High
2	2025-09-30 10:05:42	endpoint01	malware_detected	user2	198.51.100.22	-	Malware signature "Trojan.Generic" detected	High
3	2025-09-30 10:07:15	firewall01	port_scan	-	203.0.113.200	192.168.1.10	Multiple ports scanned (22,80,443)	Medium
4	2025-09-30 10:18:47	server04	network_connection	-	203.0.113.180	45.77.89.12	Outbound traffic to blacklisted IP	High

3. Incident Classification

High Severity:
- Brute-force login attempts on server01
- Malware detection on endpoint01
- Outbound connection to blacklisted IP from server04

Medium Severity:
- Port scanning attempt detected by firewall01

Low Severity:
- A few isolated failed login attempts on server03

4. Timeline of Events

- 09:15 AM: Multiple failed login attempts on server01.
- 10:05 AM: Malware detected on endpoint01.
- 10:07 AM: Port scanning activity detected targeting 192.168.1.10.
- 10:18 AM: Outbound connection from server04 to a blacklisted IP.

5. Impact Assessment

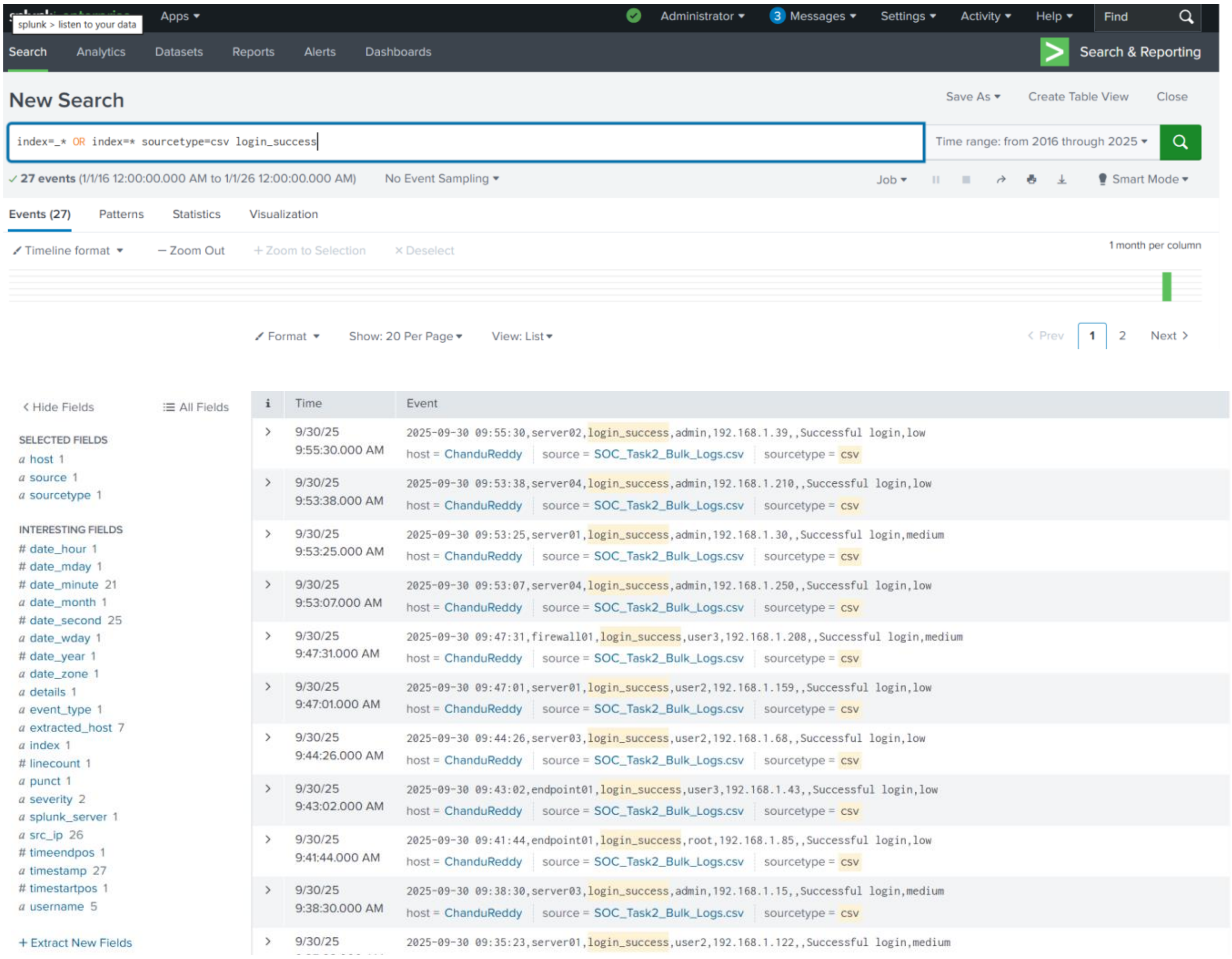
- Brute force login attempts may lead to compromised credentials.
- Malware detection indicates possible endpoint compromise.
- Port scanning is often a precursor to exploitation.
- Blacklisted IP communication suggests possible Command & Control (C2) traffic.

6. Recommended Actions

1. Lock or reset admin account credentials.
2. Isolate and scan endpoint01 for malware.
3. Block suspicious external IPs at the firewall.
4. Increase monitoring for persistence or lateral movement.
5. Educate users on phishing and account hygiene.

7. Screenshots

1.Login_Success



```
index=_* OR index=* sourcetype=csv login_success
```

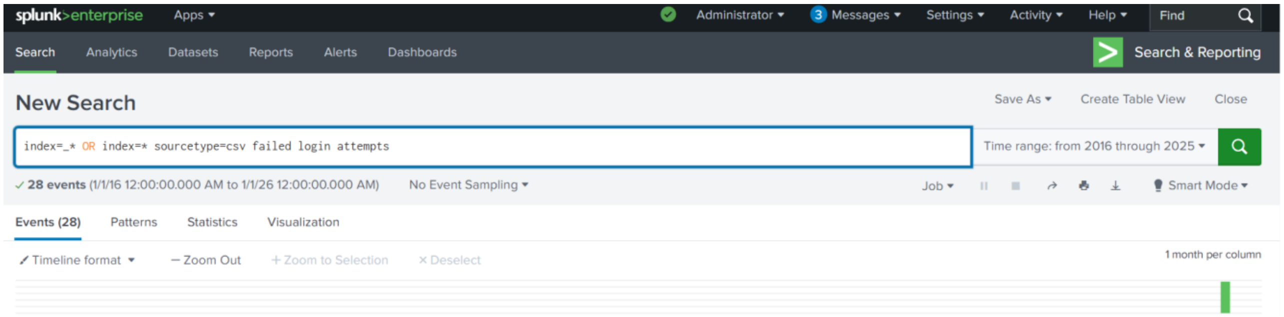
✓ 27 events (1/1/16 12:00:00.000 AM to 1/1/26 12:00:00.000 AM)   No Event Sampling

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 21
a date_month 1
# date_second 25
a date_wday 1
# date_year 1
a date_zone 1
a details 1
a event_type 1
a extracted_host 7
a index 1
# linecount 1
a punct 1
a severity 2
a splunk_server 1
a src_ip 26
# timeendpos 1
a timestamp 27
# timestartpos 1
a username 5

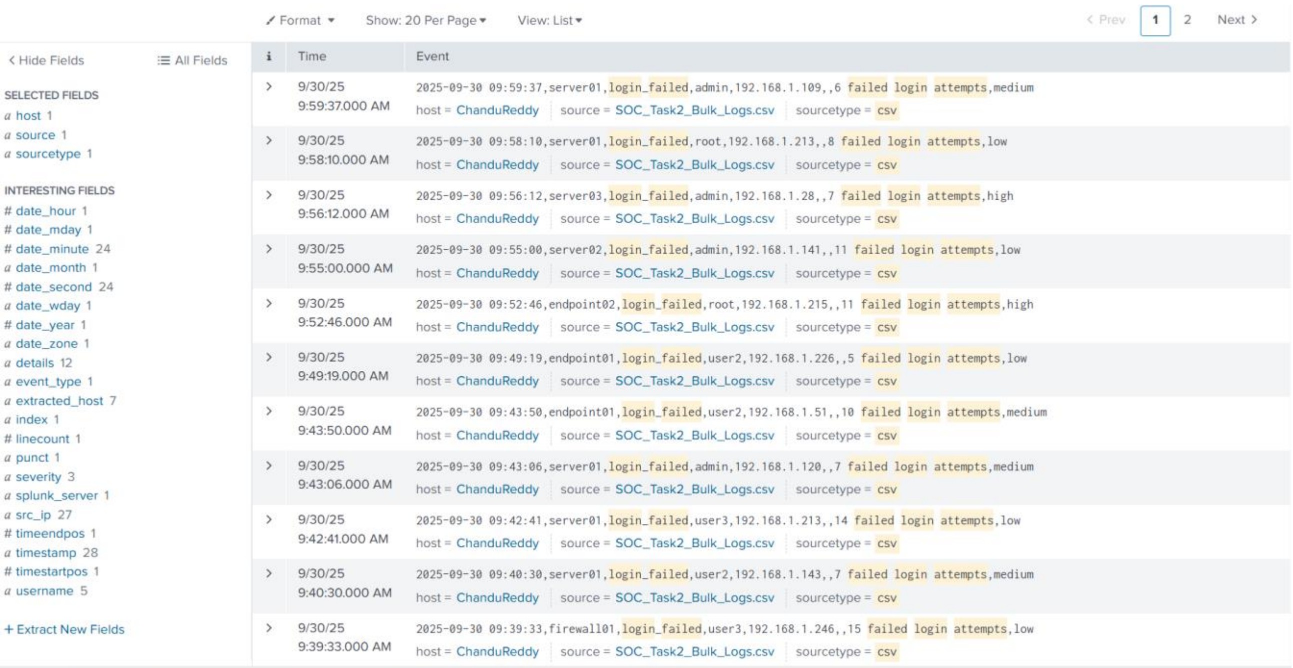
```
i  Time                  Event
>  9/30/25               2025-09-30 09:55:30,server02,login_success,admin,192.168.1.39,,Successful login,low
   9:55:30.000 AM        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
>  9/30/25               2025-09-30 09:53:38,server04,login_success,admin,192.168.1.210,,Successful login,low
   9:53:38.000 AM        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
>  9/30/25               2025-09-30 09:53:25,server01,login_success,admin,192.168.1.30,,Successful login,medium
   9:53:25.000 AM        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
>  9/30/25               2025-09-30 09:53:07,server04,login_success,admin,192.168.1.250,,Successful login,low
   9:53:07.000 AM        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
>  9/30/25               2025-09-30 09:47:31,firewall01,login_success,user3,192.168.1.208,,Successful login,medium
   9:47:31.000 AM        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
>  9/30/25               2025-09-30 09:47:01,server01,login_success,user2,192.168.1.159,,Successful login,low
   9:47:01.000 AM        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
>  9/30/25               2025-09-30 09:44:26,server03,login_success,user2,192.168.1.68,,Successful login,low
   9:44:26.000 AM        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
>  9/30/25               2025-09-30 09:43:02,endpoint01,login_success,user3,192.168.1.43,,Successful login,low
   9:43:02.000 AM        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
>  9/30/25               2025-09-30 09:41:44,endpoint01,login_success,root,192.168.1.85,,Successful login,low
   9:41:44.000 AM        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
>  9/30/25               2025-09-30 09:38:30,server03,login_success,admin,192.168.1.15,,Successful login,medium
   9:38:30.000 AM        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
>  9/30/25               2025-09-30 09:35:23,server01,login_success,user2,192.168.1.122,,Successful login,medium
```

2.Failed login attempts



```
index=_* OR index=* sourcetype=csv failed login attempts
```

✓ 28 events (1/1/16 12:00:00.000 AM to 1/1/26 12:00:00.000 AM)   No Event Sampling

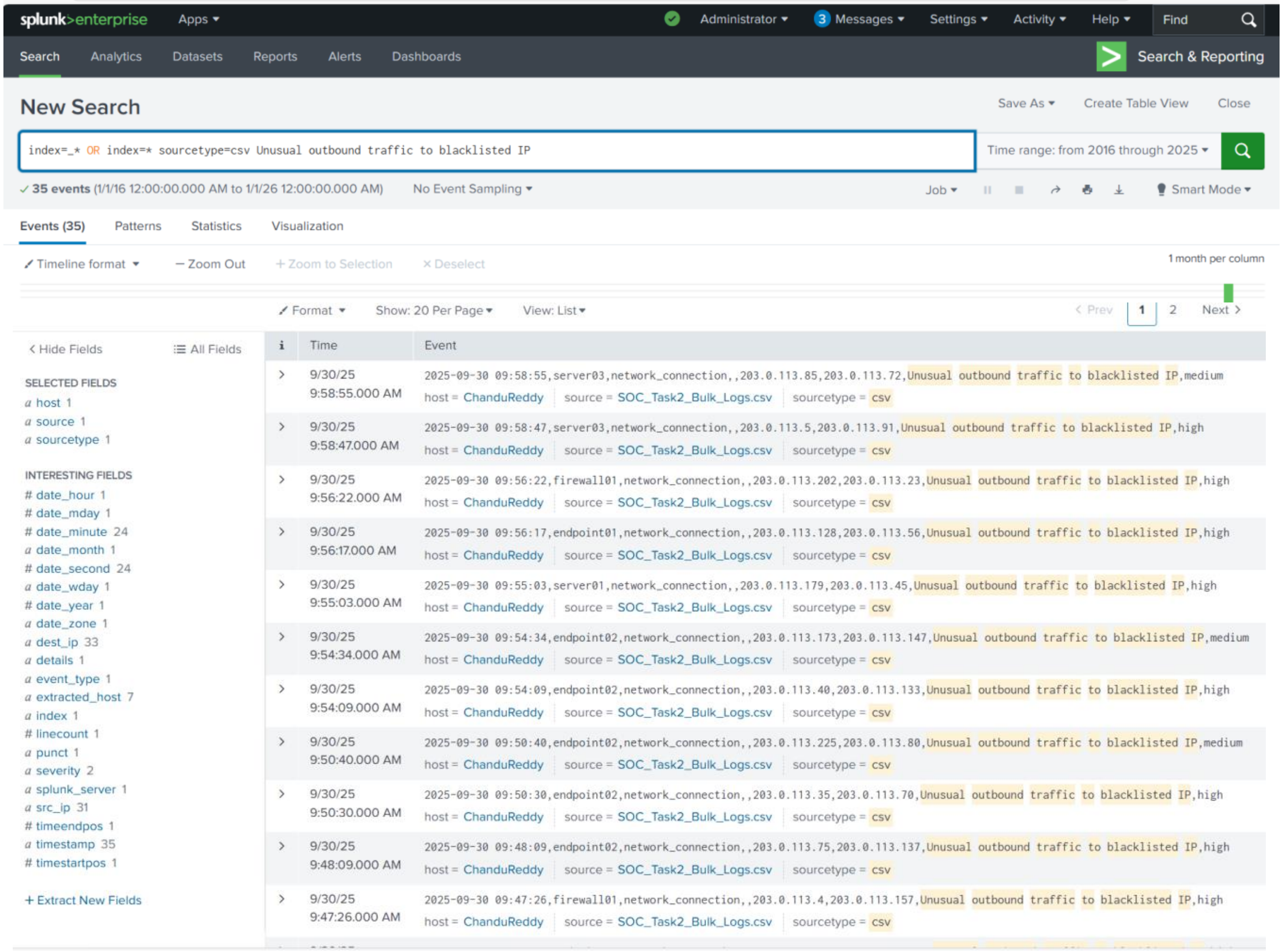


```
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 24
a date_month 1
# date_second 24
a date_wday 1
# date_year 1
a date_zone 1
a details 12
a event_type 1
a extracted_host 7
a index 1
# linecount 1
a punct 1
a severity 3
a splunk_server 1
a src_ip 27
# timeendpos 1
a timestamp 28
# timestartpos 1
a username 5
```

```
9/30/25 9:59:37.000 AM  2025-09-30 09:59:37,server01,login_failed,admin,192.168.1.109,,6 failed login attempts,medium
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:58:10.000 AM  2025-09-30 09:58:10,server01,login_failed,root,192.168.1.213,,8 failed login attempts,low
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:56:12.000 AM  2025-09-30 09:56:12,server03,login_failed,admin,192.168.1.28,,7 failed login attempts,high
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:55:00.000 AM  2025-09-30 09:55:00,server02,login_failed,admin,192.168.1.141,,11 failed login attempts,low
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:52:46.000 AM  2025-09-30 09:52:46,endpoint02,login_failed,root,192.168.1.215,,11 failed login attempts,high
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:49:19.000 AM  2025-09-30 09:49:19,endpoint01,login_failed,user2,192.168.1.226,,5 failed login attempts,low
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:43:50.000 AM  2025-09-30 09:43:50,endpoint01,login_failed,user2,192.168.1.51,,10 failed login attempts,medium
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:43:06.000 AM  2025-09-30 09:43:06,server01,login_failed,admin,192.168.1.120,,7 failed login attempts,medium
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:42:41.000 AM  2025-09-30 09:42:41,server01,login_failed,user3,192.168.1.213,,14 failed login attempts,low
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:40:30.000 AM  2025-09-30 09:40:30,server01,login_failed,user2,192.168.1.143,,7 failed login attempts,medium
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:39:33.000 AM  2025-09-30 09:39:33,firewall01,login_failed,user3,192.168.1.246,,15 failed login attempts,low
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
```

3. Unusual outbound traffic to blacklisted IP



New Search

```
index=_* OR index=* sourcetype=csv Unusual outbound traffic to blacklisted IP
```

Time range: from 2016 through 2025

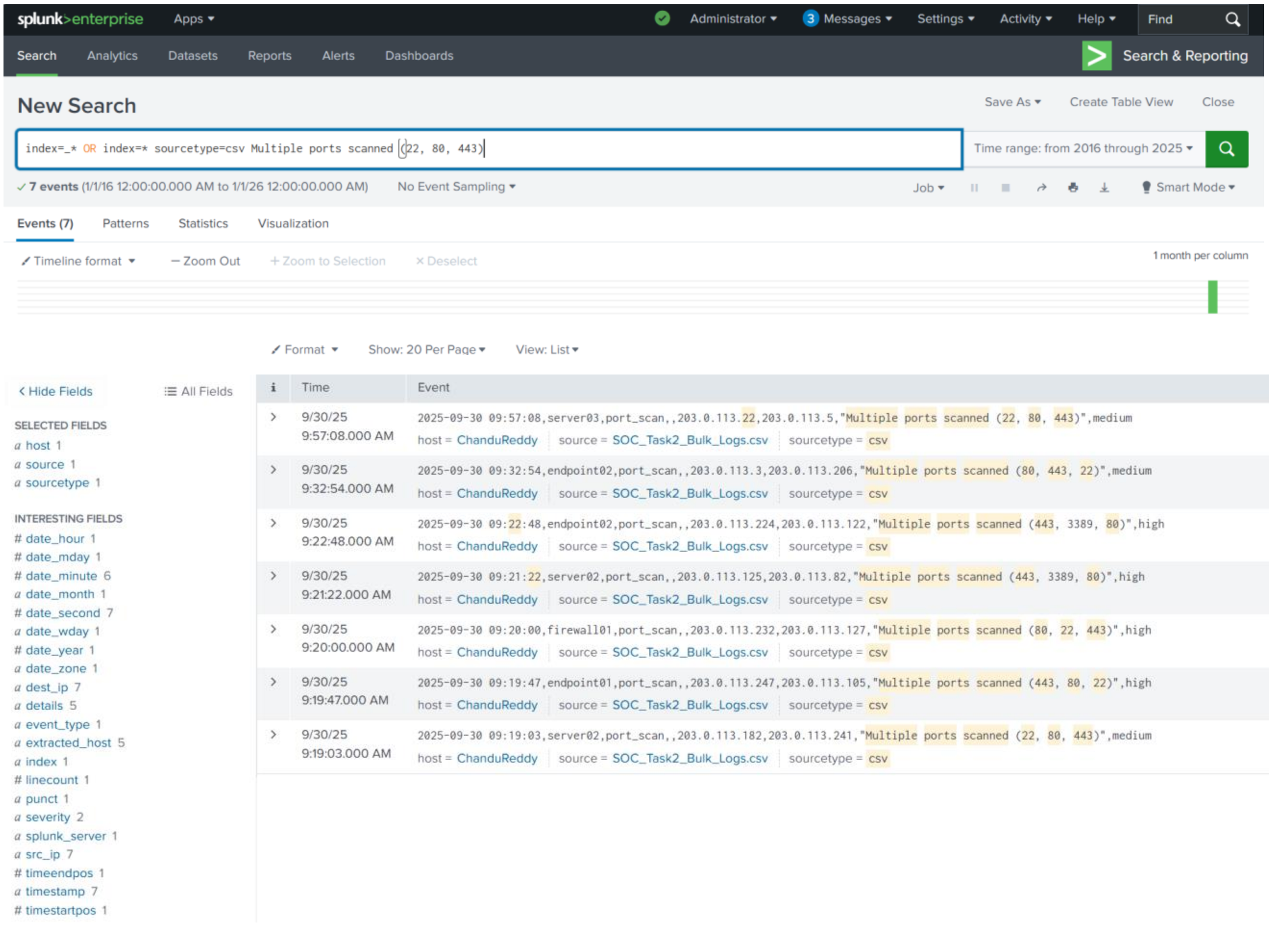
✓ 35 events (1/1/16 12:00:00.000 AM to 1/1/26 12:00:00.000 AM) No Event Sampling

```
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 24
a date_month 1
# date_second 24
a date_wday 1
# date_year 1
a date_zone 1
a dest_ip 33
a details 1
a event_type 1
a extracted_host 7
a index 1
# linecount 1
a punct 1
a severity 2
a splunk_server 1
a src_ip 31
# timeendpos 1
a timestamp 35
# timestartpos 1
```

```
9/30/25 9:58:55.000 AM  2025-09-30 09:58:55,server03,network_connection,,203.0.113.85,203.0.113.72,Unusual outbound traffic to blacklisted IP,medium
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:58:47.000 AM  2025-09-30 09:58:47,server03,network_connection,,203.0.113.5,203.0.113.91,Unusual outbound traffic to blacklisted IP,high
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:56:22.000 AM  2025-09-30 09:56:22,firewall01,network_connection,,203.0.113.202,203.0.113.23,Unusual outbound traffic to blacklisted IP,high
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:56:17.000 AM  2025-09-30 09:56:17,endpoint01,network_connection,,203.0.113.128,203.0.113.56,Unusual outbound traffic to blacklisted IP,high
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:55:03.000 AM  2025-09-30 09:55:03,server01,network_connection,,203.0.113.179,203.0.113.45,Unusual outbound traffic to blacklisted IP,high
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:54:34.000 AM  2025-09-30 09:54:34,endpoint02,network_connection,,203.0.113.173,203.0.113.147,Unusual outbound traffic to blacklisted IP,medium
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:54:09.000 AM  2025-09-30 09:54:09,endpoint02,network_connection,,203.0.113.40,203.0.113.133,Unusual outbound traffic to blacklisted IP,high
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:50:40.000 AM  2025-09-30 09:50:40,endpoint02,network_connection,,203.0.113.225,203.0.113.80,Unusual outbound traffic to blacklisted IP,medium
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:50:30.000 AM  2025-09-30 09:50:30,endpoint02,network_connection,,203.0.113.35,203.0.113.70,Unusual outbound traffic to blacklisted IP,high
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:48:09.000 AM  2025-09-30 09:48:09,endpoint02,network_connection,,203.0.113.75,203.0.113.137,Unusual outbound traffic to blacklisted IP,high
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:47:26.000 AM  2025-09-30 09:47:26,firewall01,network_connection,,203.0.113.4,203.0.113.157,Unusual outbound traffic to blacklisted IP,high
                        host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
```

4.Multiple ports scanned (22, 80, 443)



New Search

```
index=_* OR index=* sourcetype=csv Multiple ports scanned (22, 80, 443)
```

Time range: from 2016 through 2025

✓ 7 events (1/1/16 12:00:00.000 AM to 1/1/26 12:00:00.000 AM) No Event Sampling

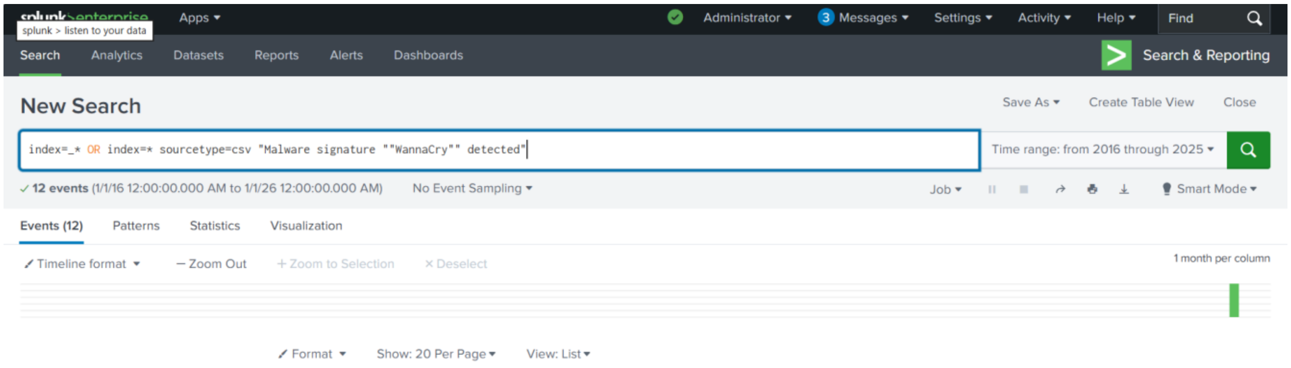
Events (7) Patterns Statistics Visualization

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 6
a date_month 1
# date_second 7
a date_wday 1
# date_year 1
a date_zone 1
a dest_ip 7
a details 5
a event_type 1
a extracted_host 5
a index 1
# linecount 1
a punct 1
a severity 2
a splunk_server 1
a src_ip 7
# timeendpos 1
a timestamp 7
# timestartpos 1

i	Time	Event
>	9/30/25 9:57:08.000 AM	2025-09-30 09:57:08,server03,port_scan,,203.0.113.22,203.0.113.5,"Multiple ports scanned (22, 80, 443)",medium host = ChanduReddy source = SOC_Task2_Bulk_Logs.csv sourcetype = csv
>	9/30/25 9:32:54.000 AM	2025-09-30 09:32:54,endpoint02,port_scan,,203.0.113.3,203.0.113.206,"Multiple ports scanned (80, 443, 22)",medium host = ChanduReddy source = SOC_Task2_Bulk_Logs.csv sourcetype = csv
>	9/30/25 9:22:48.000 AM	2025-09-30 09:22:48,endpoint02,port_scan,,203.0.113.224,203.0.113.122,"Multiple ports scanned (443, 3389, 80)",high host = ChanduReddy source = SOC_Task2_Bulk_Logs.csv sourcetype = csv
>	9/30/25 9:21:22.000 AM	2025-09-30 09:21:22,server02,port_scan,,203.0.113.125,203.0.113.82,"Multiple ports scanned (443, 3389, 80)",high host = ChanduReddy source = SOC_Task2_Bulk_Logs.csv sourcetype = csv
>	9/30/25 9:20:00.000 AM	2025-09-30 09:20:00,firewall01,port_scan,,203.0.113.232,203.0.113.127,"Multiple ports scanned (80, 22, 443)",high host = ChanduReddy source = SOC_Task2_Bulk_Logs.csv sourcetype = csv
>	9/30/25 9:19:47.000 AM	2025-09-30 09:19:47,endpoint01,port_scan,,203.0.113.247,203.0.113.105,"Multiple ports scanned (443, 80, 22)",high host = ChanduReddy source = SOC_Task2_Bulk_Logs.csv sourcetype = csv
>	9/30/25 9:19:03.000 AM	2025-09-30 09:19:03,server02,port_scan,,203.0.113.182,203.0.113.241,"Multiple ports scanned (22, 80, 443)",medium host = ChanduReddy source = SOC_Task2_Bulk_Logs.csv sourcetype = csv

5."Malware signature ""WannaCry"" detected"



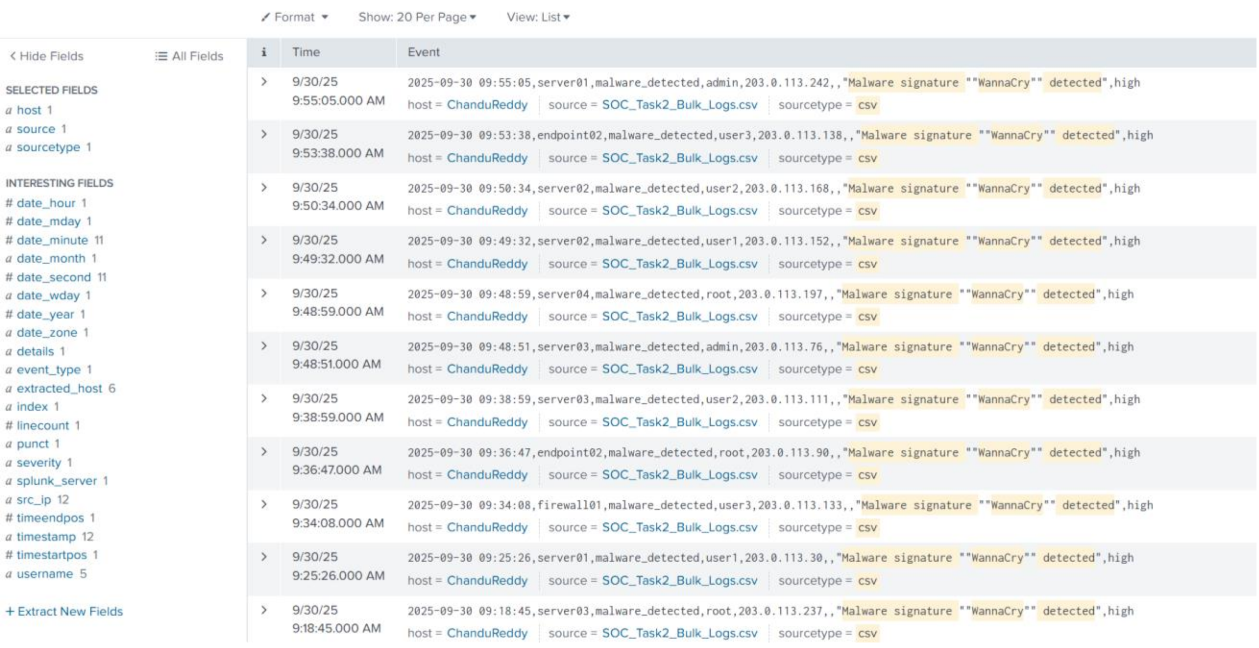
New Search

```
index=_* OR index=* sourcetype=csv "Malware signature ""WannaCry"" detected"
```

Time range: from 2016 through 2025

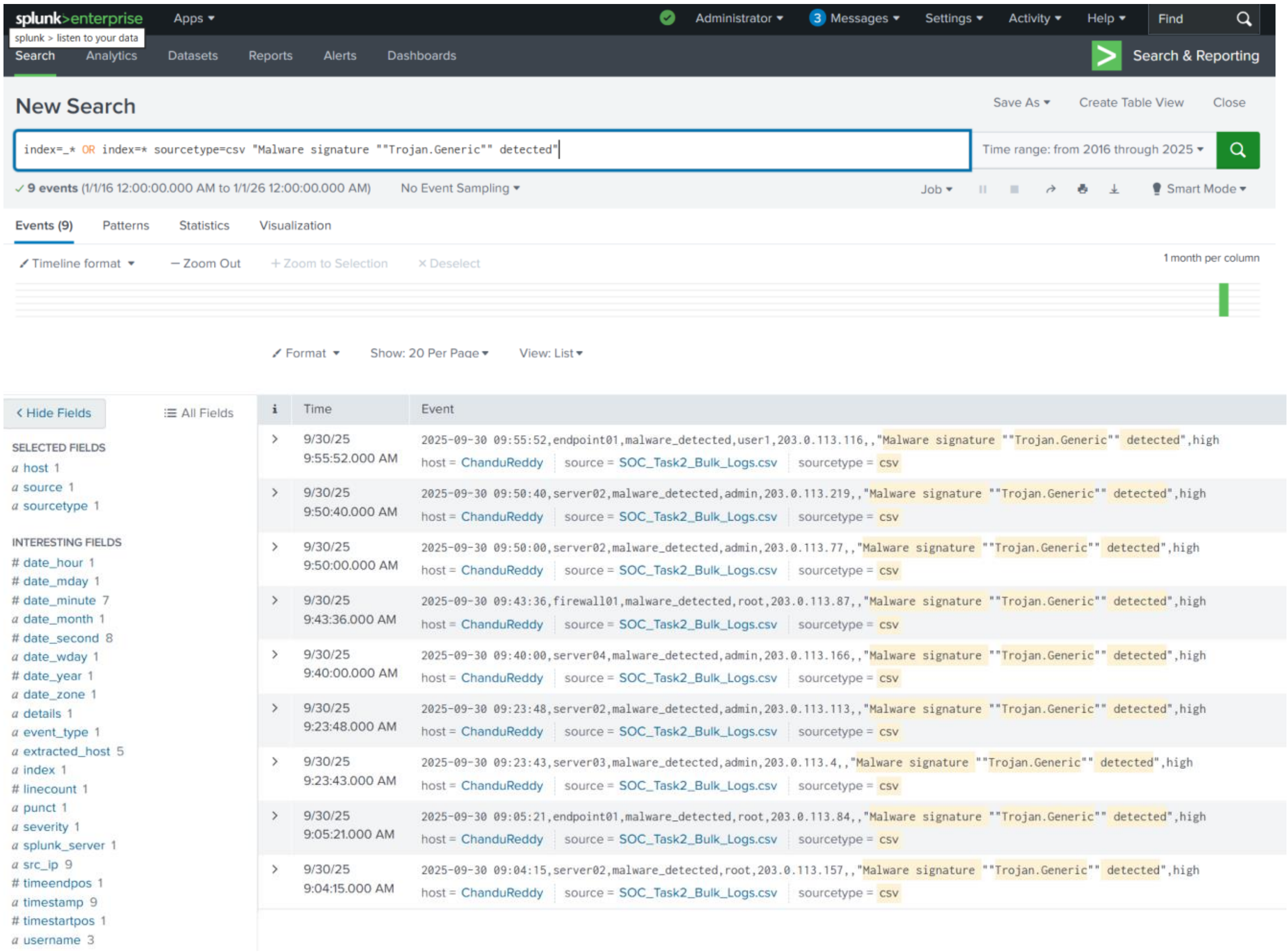
✓ 12 events (1/1/16 12:00:00.000 AM to 1/1/26 12:00:00.000 AM) No Event Sampling

Events (12) Patterns Statistics Visualization



```
9/30/25 9:55:05.000 AM  2025-09-30 09:55:05,server01,malware_detected,admin,203.0.113.242,,"Malware signature ""WannaCry"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:53:38.000 AM  2025-09-30 09:53:38,endpoint02,malware_detected,user3,203.0.113.138,,"Malware signature ""WannaCry"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:50:34.000 AM  2025-09-30 09:50:34,server02,malware_detected,user2,203.0.113.168,,"Malware signature ""WannaCry"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:49:32.000 AM  2025-09-30 09:49:32,server02,malware_detected,user1,203.0.113.152,,"Malware signature ""WannaCry"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:48:59.000 AM  2025-09-30 09:48:59,server04,malware_detected,root,203.0.113.197,,"Malware signature ""WannaCry"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:48:51.000 AM  2025-09-30 09:48:51,server03,malware_detected,admin,203.0.113.76,,"Malware signature ""WannaCry"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:38:59.000 AM  2025-09-30 09:38:59,server03,malware_detected,user2,203.0.113.111,,"Malware signature ""WannaCry"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:36:47.000 AM  2025-09-30 09:36:47,endpoint02,malware_detected,root,203.0.113.90,,"Malware signature ""WannaCry"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:34:08.000 AM  2025-09-30 09:34:08,firewall01,malware_detected,user3,203.0.113.133,,"Malware signature ""WannaCry"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:25:26.000 AM  2025-09-30 09:25:26,server01,malware_detected,user1,203.0.113.30,,"Malware signature ""WannaCry"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:18:45.000 AM  2025-09-30 09:18:45,server03,malware_detected,root,203.0.113.237,,"Malware signature ""WannaCry"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
```

6."Malware signature ""Trojan.Generic"" detected"



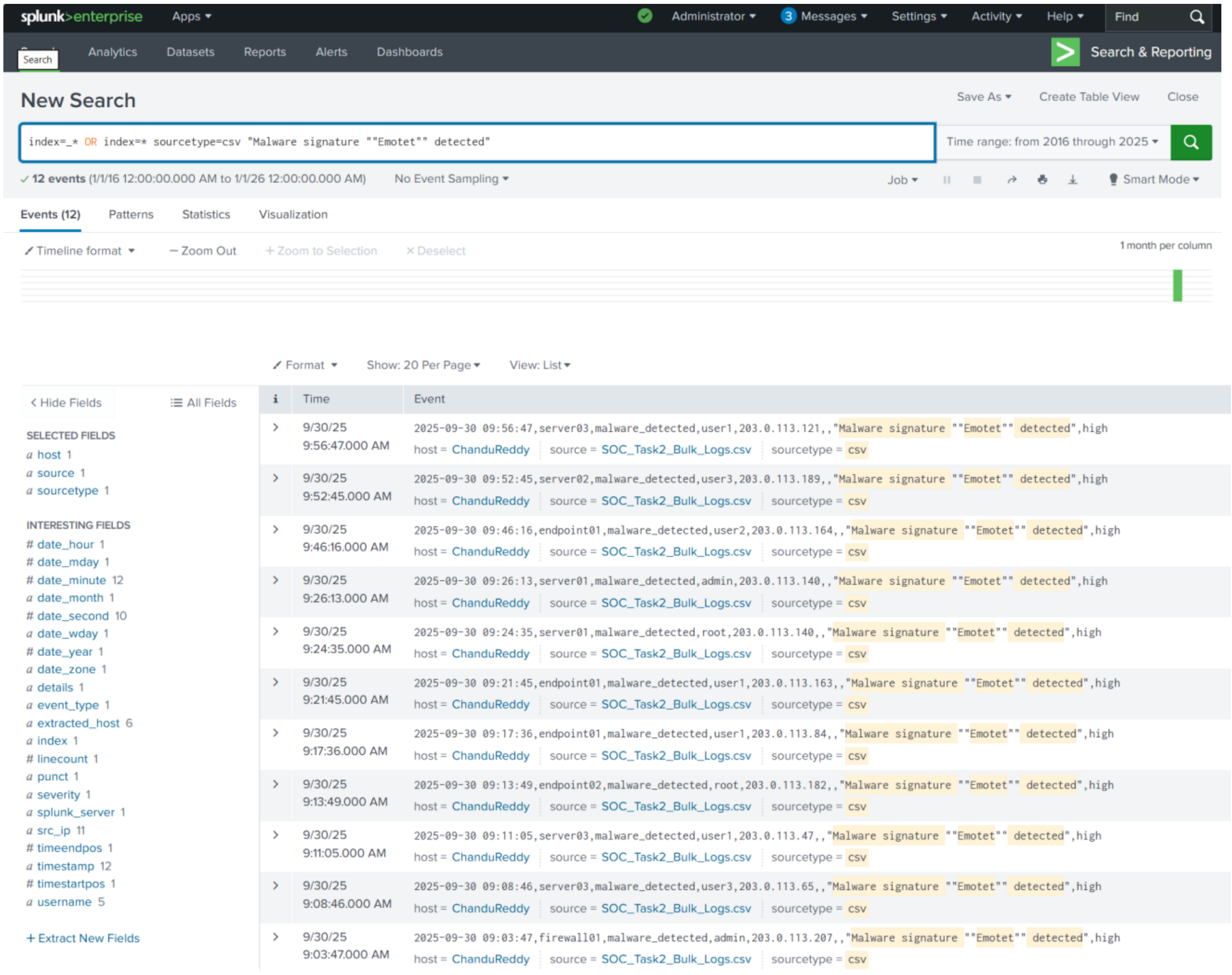
```
index=_* OR index=* sourcetype=csv "Malware signature ""Trojan.Generic"" detected"
```

Time range: from 2016 through 2025

✓ 9 events (1/1/16 12:00:00.000 AM to 1/1/26 12:00:00.000 AM)   No Event Sampling

```
9/30/25 9:55:52.000 AM  2025-09-30 09:55:52,endpoint01,malware_detected,user1,203.0.113.116,,"Malware signature ""Trojan.Generic"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:50:40.000 AM  2025-09-30 09:50:40,server02,malware_detected,admin,203.0.113.219,,"Malware signature ""Trojan.Generic"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:50:00.000 AM  2025-09-30 09:50:00,server02,malware_detected,admin,203.0.113.77,,"Malware signature ""Trojan.Generic"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:43:36.000 AM  2025-09-30 09:43:36,firewall01,malware_detected,root,203.0.113.87,,"Malware signature ""Trojan.Generic"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:40:00.000 AM  2025-09-30 09:40:00,server04,malware_detected,admin,203.0.113.166,,"Malware signature ""Trojan.Generic"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:23:48.000 AM  2025-09-30 09:23:48,server02,malware_detected,admin,203.0.113.113,,"Malware signature ""Trojan.Generic"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:23:43.000 AM  2025-09-30 09:23:43,server03,malware_detected,admin,203.0.113.4,,"Malware signature ""Trojan.Generic"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:05:21.000 AM  2025-09-30 09:05:21,endpoint01,malware_detected,root,203.0.113.84,,"Malware signature ""Trojan.Generic"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
9/30/25 9:04:15.000 AM  2025-09-30 09:04:15,server02,malware_detected,root,203.0.113.157,,"Malware signature ""Trojan.Generic"" detected",high
                        host = ChanduReddy   source = SOC_Task2_Bulk_Logs.csv   sourcetype = csv
```

7. "Malware signature ""Emotet"" detected"



```
index=_* OR index=* sourcetype=csv "Malware signature ""Emotet"" detected"
```

✓ 12 events (1/1/16 12:00:00.000 AM to 1/1/26 12:00:00.000 AM)

```
Time                   Event
9/30/25 9:56:47.000 AM 2025-09-30 09:56:47,server03,malware_detected,user1,203.0.113.121,,"Malware signature ""Emotet"" detected",high
                       host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:52:45.000 AM 2025-09-30 09:52:45,server02,malware_detected,user3,203.0.113.189,,"Malware signature ""Emotet"" detected",high
                       host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:46:16.000 AM 2025-09-30 09:46:16,endpoint01,malware_detected,user2,203.0.113.164,,"Malware signature ""Emotet"" detected",high
                       host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:26:13.000 AM 2025-09-30 09:26:13,server01,malware_detected,admin,203.0.113.140,,"Malware signature ""Emotet"" detected",high
                       host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:24:35.000 AM 2025-09-30 09:24:35,server01,malware_detected,root,203.0.113.140,,"Malware signature ""Emotet"" detected",high
                       host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:21:45.000 AM 2025-09-30 09:21:45,endpoint01,malware_detected,user1,203.0.113.163,,"Malware signature ""Emotet"" detected",high
                       host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:17:36.000 AM 2025-09-30 09:17:36,endpoint01,malware_detected,user1,203.0.113.84,,"Malware signature ""Emotet"" detected",high
                       host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:13:49.000 AM 2025-09-30 09:13:49,endpoint02,malware_detected,root,203.0.113.182,,"Malware signature ""Emotet"" detected",high
                       host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:11:05.000 AM 2025-09-30 09:11:05,server03,malware_detected,user1,203.0.113.47,,"Malware signature ""Emotet"" detected",high
                       host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:08:46.000 AM 2025-09-30 09:08:46,server03,malware_detected,user3,203.0.113.65,,"Malware signature ""Emotet"" detected",high
                       host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
9/30/25 9:03:47.000 AM 2025-09-30 09:03:47,firewall01,malware_detected,admin,203.0.113.207,,"Malware signature ""Emotet"" detected",high
                       host = ChanduReddy | source = SOC_Task2_Bulk_Logs.csv | sourcetype = csv
```

8. Communication to Management

(chandureddy9101@gmail.com)

Subject: Security Incident Report

During SOC monitoring, several high-severity alerts were detected:
- Brute-force login attempts on server01
- Malware activity on endpoint01
- Outbound traffic to a blacklisted IP

Immediate response actions have been initiated, including account lockout, IP blocking, and malware isolation. Further monitoring is ongoing.

Best Regards,
[Chandu reddy]