SOC Incident Monitoring & Response – Task 2  
Author: Bhaskar Pagadala | Date: 12th July 2025 | Tooling: Splunk Enterprise (Free/Trial), SOC\_Task2\_Sample\_Logs.txt  
  
Executive Summary  
We ingested simulated SOC logs into Splunk and performed triage across authentication, network, and malware-related events. We identified 50 suspicious activities: <brief types, e.g., brute-force login burst, malware detection, success-after-failures>. High-risk items were isolated with recommended actions (block IPs, credential resets, endpoint scans, and monitoring rules). Evidence and dashboard views are attached.

Scope

* Data source: SOC\_Task2\_Sample\_Logs.txt (uploaded via Settings > Add Data > Upload)
* Time range analyzed: <All time / specific window>
* Splunk app: Search & Reporting
* Key fields used: <src\_ip/src, user/account, host, action/EventCode, signature>

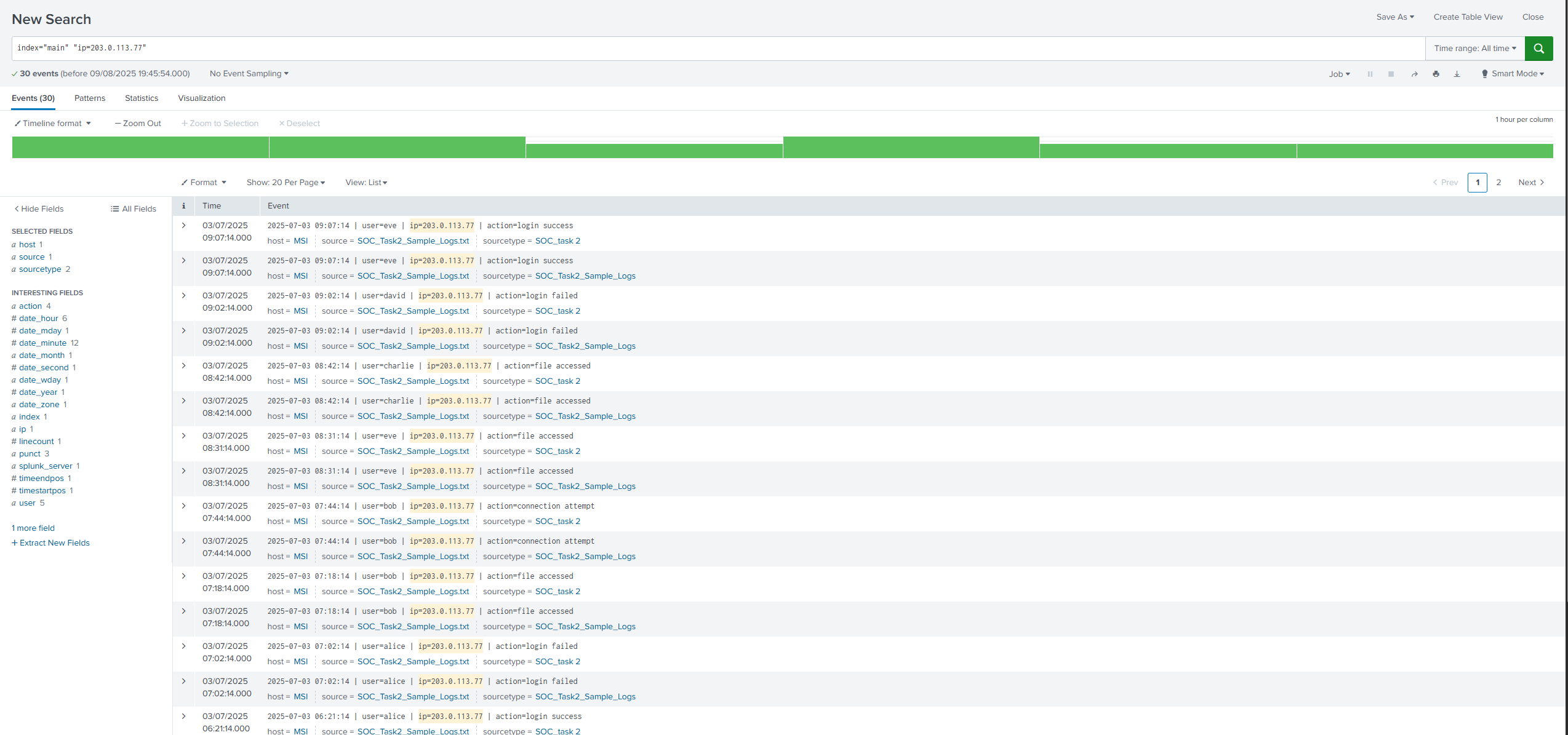
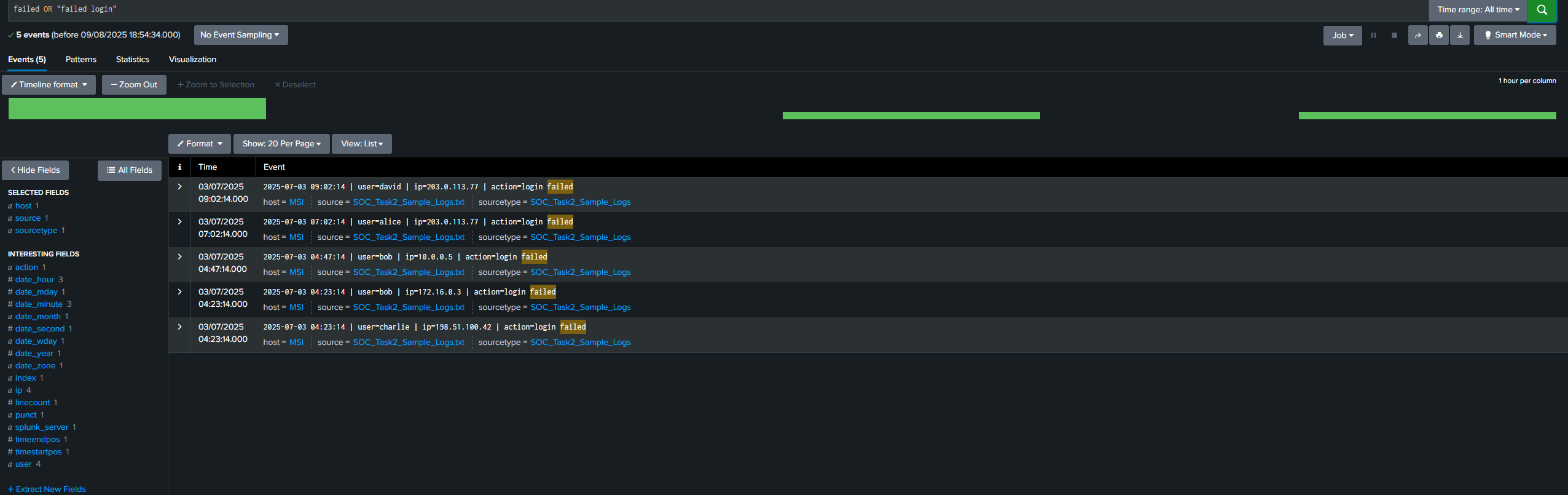
#### Methodology

1. Indexed logs via Splunk Add Data (Upload).
2. Verified ingestion (Data Summary, keyword searches).
3. Ran SPL triage searches:
   1. Failed login bursts:  
      failed OR "failed login" OR failure  
      | stats count by src\_ip, user  
      | sort - count
   2. Bursts over time:  
      failed OR "failed login" OR failure  
      | bin \_time span=5m  
      | stats count by \_time, src\_ip  
      | where count>=5
   3. Success after failures:  
      (failed OR failure OR "failed login" OR EventCode=4625 OR action=failure OR success OR "successful login" OR EventCode=4624 OR action=success)  
      | eval is\_fail=if(match(\_raw,"failed|failure|4625"),1,0)  
      | eval is\_succ=if(match(\_raw,"success|successful|4624"),1,0)  
      | stats sum(is\_fail) as failures sum(is\_succ) as successes by user, src\_ip  
      | where failures>=5 AND successes>0
   4. Malware detections:  
      malware OR "malware detected" OR virus  
      | stats count by host, signature, src\_ip  
      | sort - count
4. Saved key searches as Reports and added to a “SOC Task 2 Dashboard.”

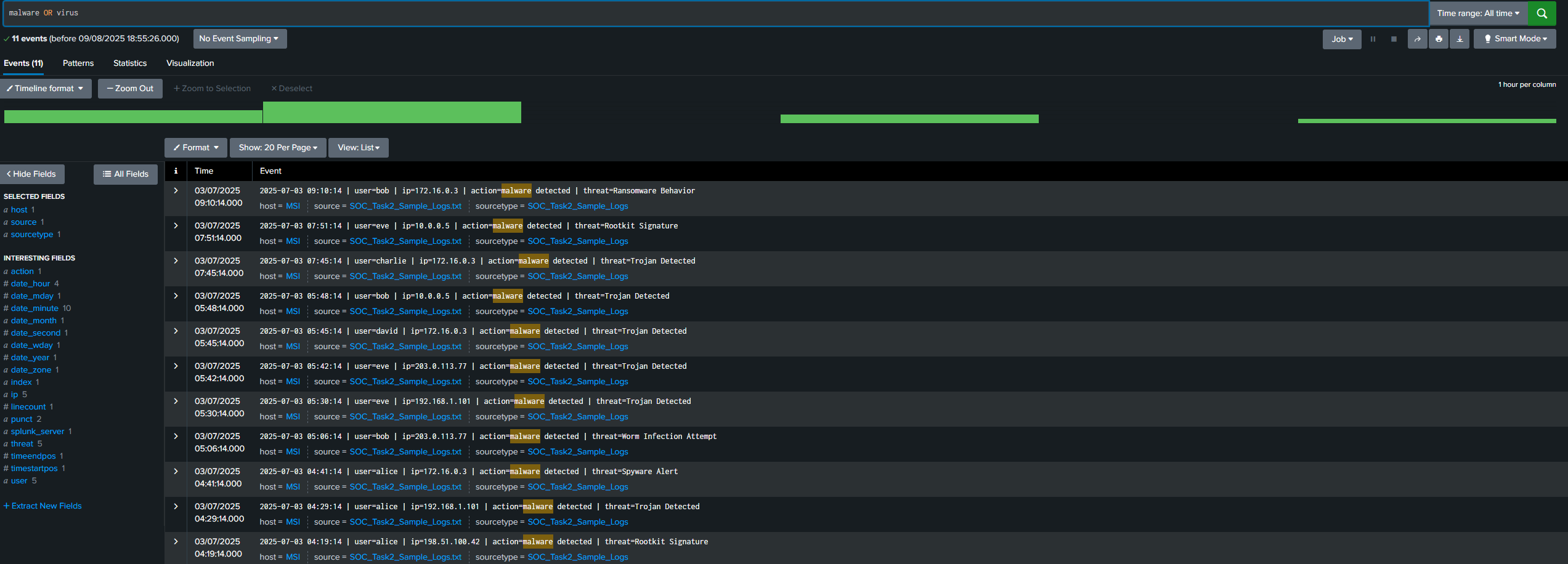
Findings Summary (Triage Table)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Incident Type | User/Host | Source IP | Severity | Evidence/Query ref |
| Failed-login burst (10 in 1 min) | user=bob | ip=203.0.113.77 | High | Search A, Panel “Failed Logins Over Time” |
| Malware alert “Trojan.Generic” | HR-WS-02 | 203.0.113.17 | High | Search D, malware table screenshot |
| Success after 6 failures | jdoe | 45.33.32.156 | Medium | Search C details |
| Unusual IP activity | <user/host> | <IP> | Medium | Search B spike |

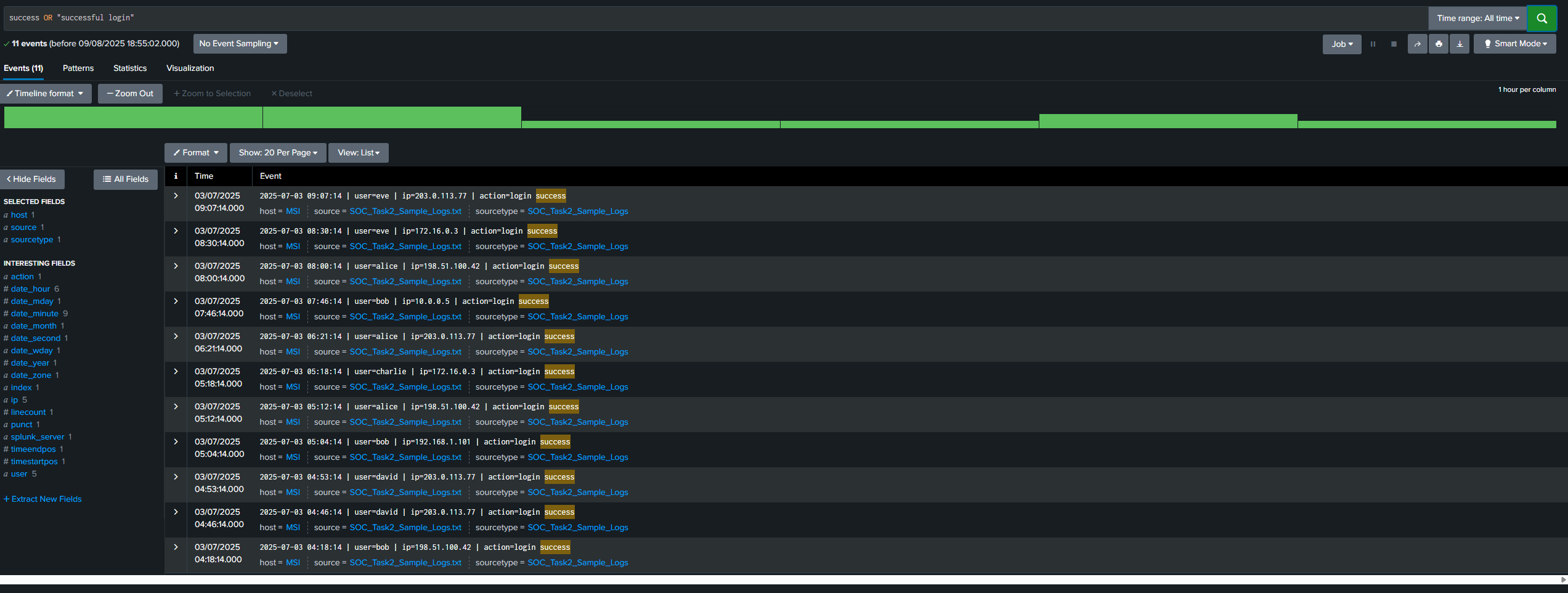
Detailed Incident Analysis  
Incident 1: Failed-login burst from ip=203.0.113.77 against admin (High)

* What we saw: 12 failures within 1 minute; pattern consistent with brute force/credential stuffing.
* Evidence: SPL Search A table; time-series spike (Dashboard Panel: Failed Logins Over Time).
* 
* Impact: Risk of account compromise; potential lateral movement if admin creds are exposed.
* Recommended actions:
  + Block ip=203.0.113.77 at WAF/firewall; add rate limiting on auth endpoints.
  + Force password reset on admin; enable/verify MFA.
  + Add detection rule: alert on ≥5 failures in 5 minutes per IP/user.

Incident 2: Malware detection “Trojan.Generic” on HR-WS-02 (High)

* What we saw: AV flagged malware signature on host HR-WS-02.
* Evidence: Malware query results with host/signature. 
* Impact: Potential data exfiltration or persistence on endpoint; user data at risk.
* Recommended actions:
  + Isolate HR-WS-02 from network; run full AV/EDR scan and quarantine/clean.
  + Review autoruns, scheduled tasks, startup items.
  + Hunt for same hash/signature across environment; patch and review USB/email vectors.

Incident 3: Successful login after multiple failures for user jdoe from 45.33.32.156 (Medium)

* What we saw: 6 failed attempts followed by a success from same IP within 10 minutes.
* Evidence: Search C summary table. 
* Impact: Possible credential stuffing success; account integrity uncertain.
* Recommended actions:
  + Reset jdoe password; require MFA enrollment if not already.
  + Geolocation/IP reputation check; consider conditional access policies.
  + Monitor subsequent activity on jdoe (downloads, privilege changes).

#### Additional Observations

* <e.g., minor anomalies / off-hours logins marked Low severity>

#### Dashboards

* SOC Task 2 Dashboard panels:
  + Failed Logins Over Time (line chart)
  + Top Source IPs for Failures (bar)
  + Malware Detections by Host/Signature (table/bar)

Conclusion  
We detected and triaged <X> suspicious events with two high-priority items requiring immediate response. Implementing blocking rules, MFA enforcement, endpoint isolation/scanning, and basic SIEM detection content will reduce risk and improve time-to-detect.

Appendix

* Key SPL Queries (as listed above)