2025

Security Operations Center (SOC) Task 2 Report

TASK TITLE: SECURITY ALERT MONITORING & INCIDENT RESPONSE SIMULATION

Intern Name: Jagadeesh Kommineni

Date: June 28, 2025 |

Security Operations Center (SOC) Task 2 Report

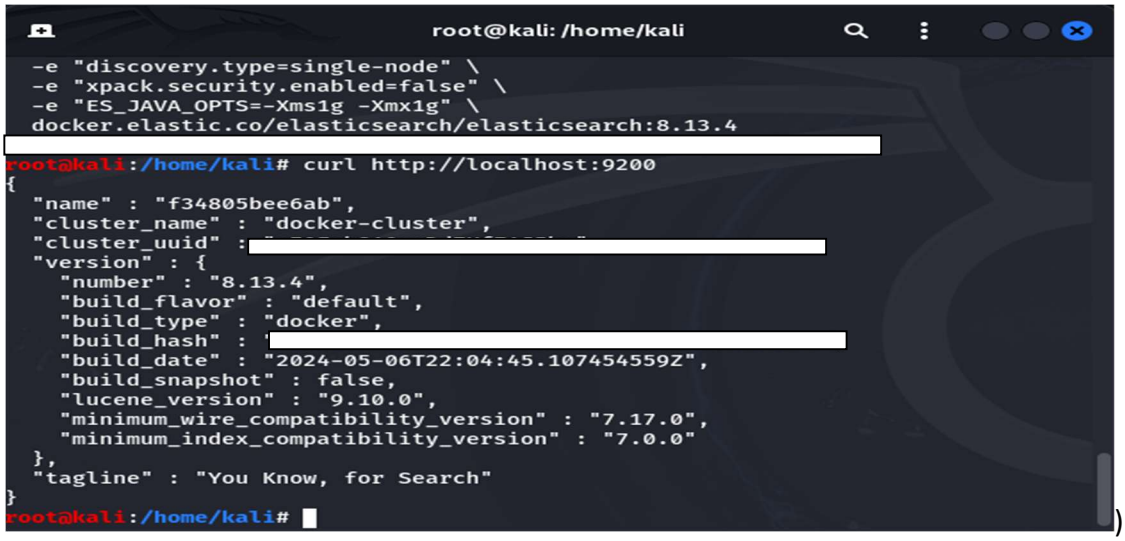
Intern Name: Jagadeesh Kommineni
Task Title: Security Alert Monitoring & Incident Response Simulation
Date: June 28, 2025

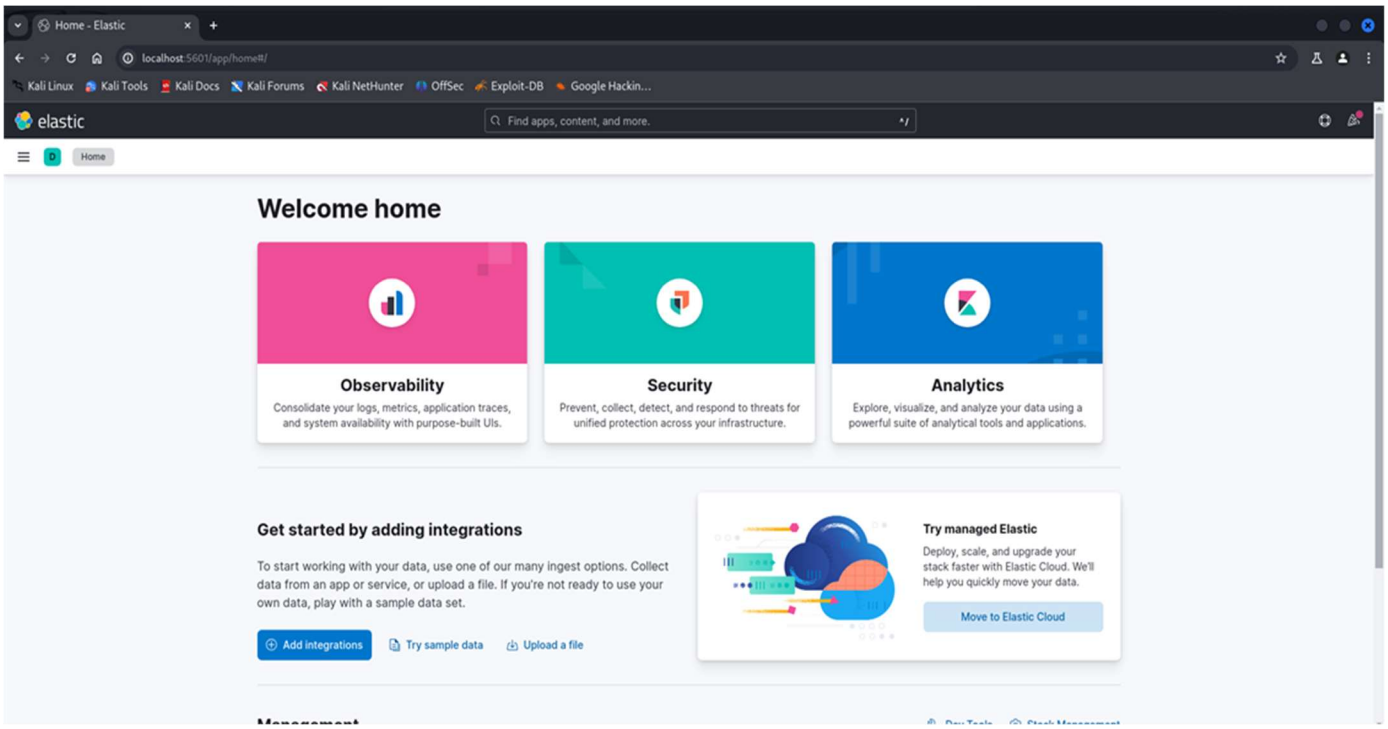
Executive Summary

This report documents a simulated engagement in the daily operations of a Security Operations Center (SOC) using Elastic Stack (ELK) to monitor, analyze, and respond to potential cybersecurity threats. The objective of this internship task was to demonstrate core SOC analyst capabilities: log ingestion, pattern recognition, alert classification, and incident response. Logs were generated across different categories — authentication, system activity, malware alerts, and network traffic — and analyzed to detect signs of compromise. The deliverable emulates how real SOC teams monitor enterprise environments, triage threats, and act to contain and mitigate security events.

Tools and Environment

- **Host OS:** Kali Linux (Rolling)
- **Virtualization:** Docker for containerized deployment
- **SIEM Platform:** Elastic Stack (Elasticsearch + Kibana)
    - **Elasticsearch:** For indexing and storing logs
    - **Kibana:** For visualization and querying
- **Data Format:** Simulated CSV file containing 1,000 logs
- **Log Categories:**
    - Authentication events (auth_success / auth_failure)
    - Malware alerts (e.g., Worms, Adware, Spyware)
    - Network traffic (source/destination IPs, ports)
    - System events (timestamps, usernames, messages

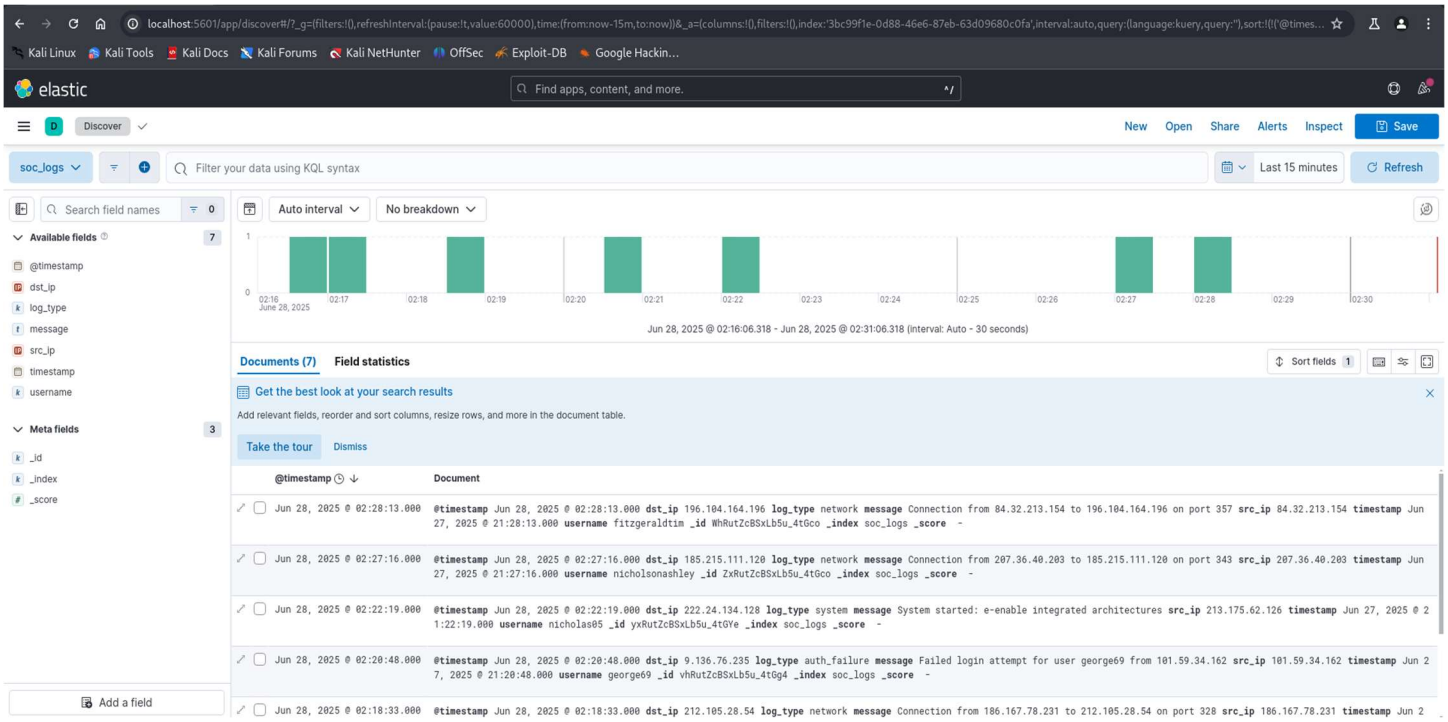


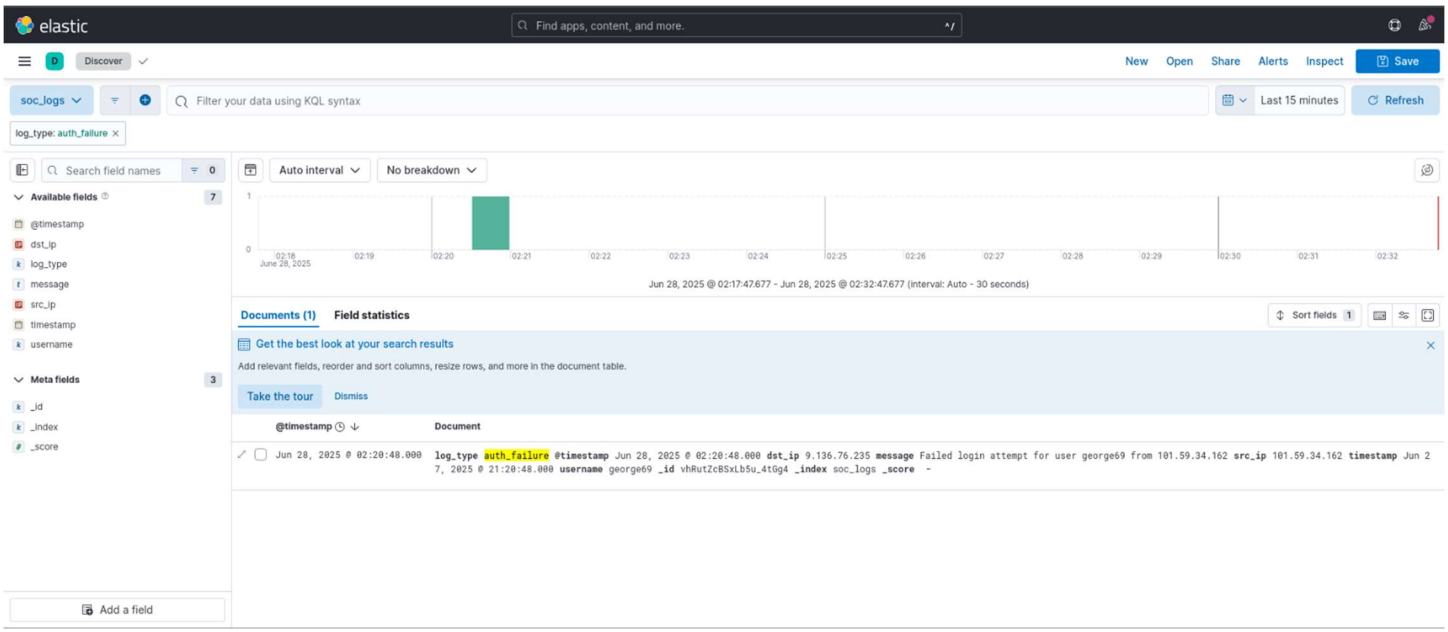


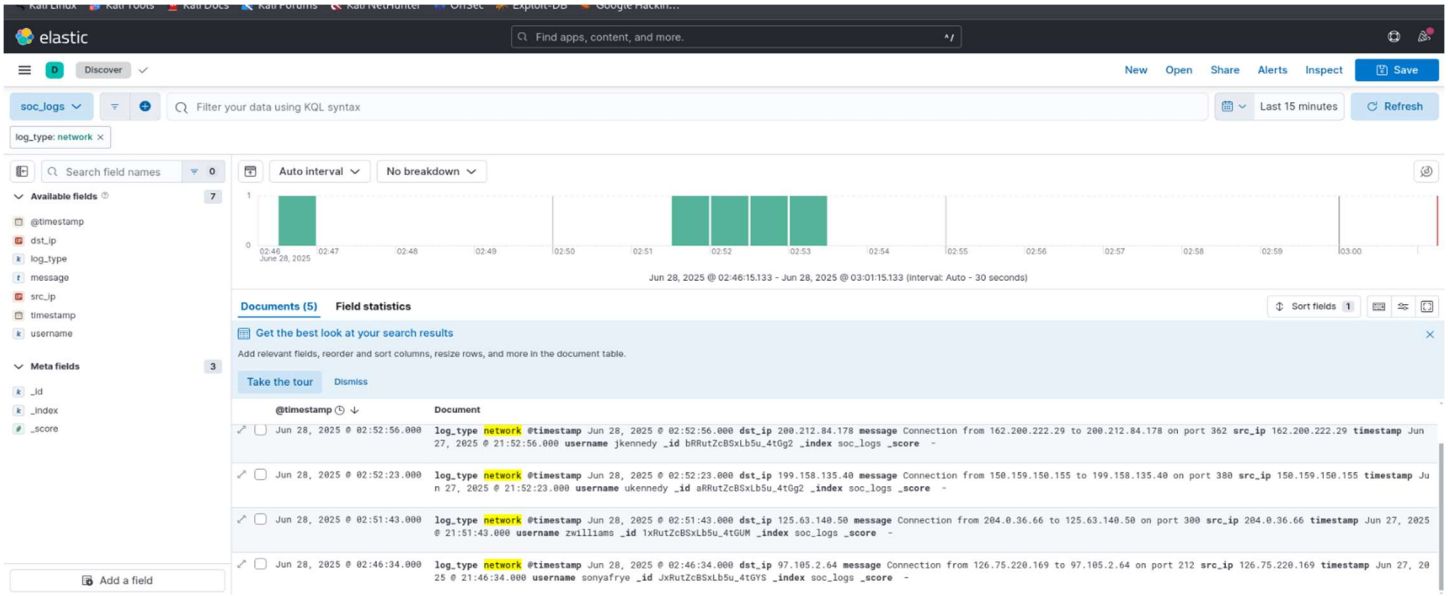
Key Findings (Alert Classification Table)

Timestamp	Alert Type	Message	Severity	Notes
2025-06-28 02:20:48	Failed Login	Failed login for user george69 from `101.59.34.162`	High	Repeated attempts likely indicate brute-force activity
2025-06-28 02:34:51	Malware Alert	Malware detected: Worm on host `167.212.30.96`	High	Worms can propagate rapidly, risk lateral movement
2025-06-28 02:33:10	Malware Alert	Malware detected: Adware on host `207.52.45.170`	Medium	Lower risk, but could lead to privacy violations
2025-06-28 02:33:02	Malware Alert	Malware detected: Spyware on host `207.177.251.213`	High	Spyware may result in data exfiltration
2025-06-28 02:28:13	Network Traffic	Repeated connections from `84.32.213.154` to multiple endpoints	High	Pattern consistent with network scanning or reconnaissance
2025-06-28 02:27:16	Network Traffic	Repeated connection from `207.36.40.203` to `185.215.111.120`	High	Indicates targeting of specific asset
2025-06-28 02:28:13	Targeted Host	Destination `196.104.164.196` hit repeatedly	High	May indicate asset under active attack

Timestamp	Alert Type	Message	Severity	Notes
2025-06-28 02:35:19	Successful Login	Login for user `bridgetlee` from `216.164.73.143`	Low	Normal activity; tracked for audit trail
2025-06-28 02:46:34	Network Traffic	Connection from `126.75.220.169` to `97.105.2.64` on port 212	Medium	Non-standard port activity, possible probing
2025-06-28 02:51:43	Network Traffic	Connection from `204.0.36.66` to `125.63.140.50` on port 300	Medium	Suspicious port activity from uncommon IP
2025-06-28 02:52:23	Network Traffic	Connection from `150.159.150.155` to `199.158.135.40` on port 380	Medium	Mid-level recon attempt, frequency low
2025-06-28 02:52:56	Network Traffic	Connection from `162.200.222.29` to `200.212.84.178` on port 362	Medium	Emerging pattern of network mapping
2025-06-28 02:53:26	Network Traffic	Connection from `178.149.122.154` to `204.71.223.240` on port 418	Medium	Possibly active scan with varied port usage



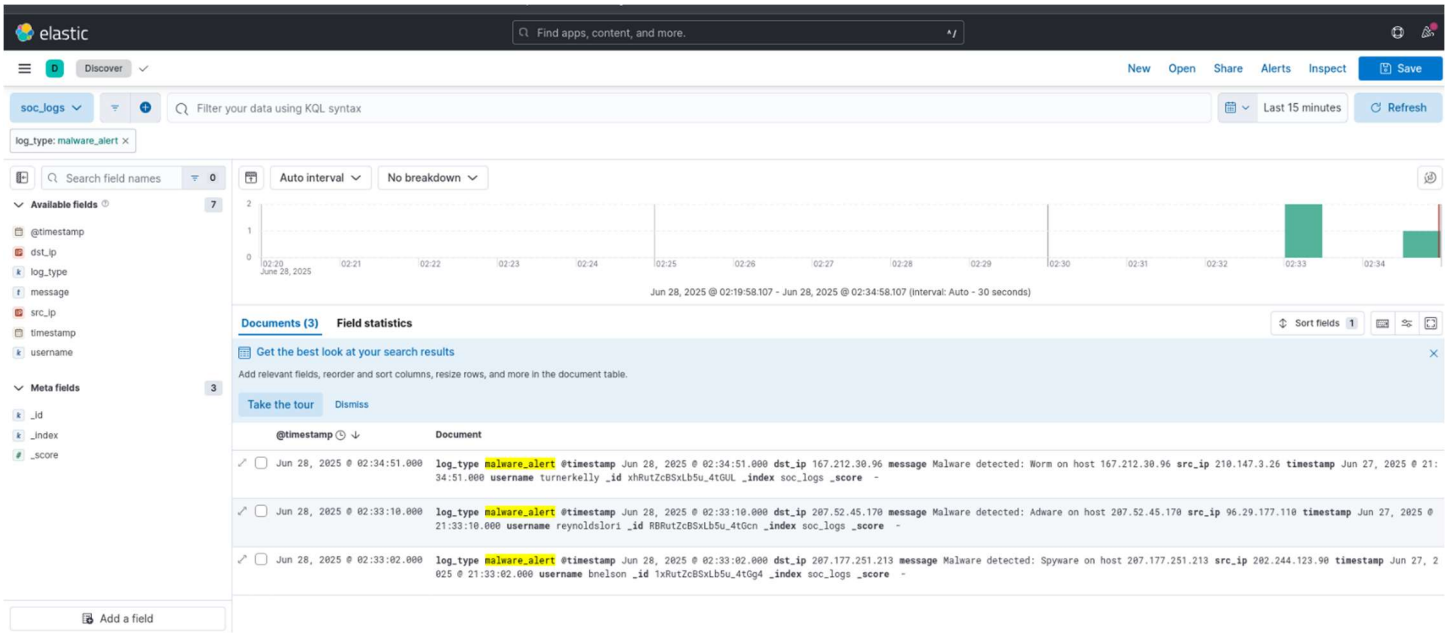




Detailed Threat Analysis

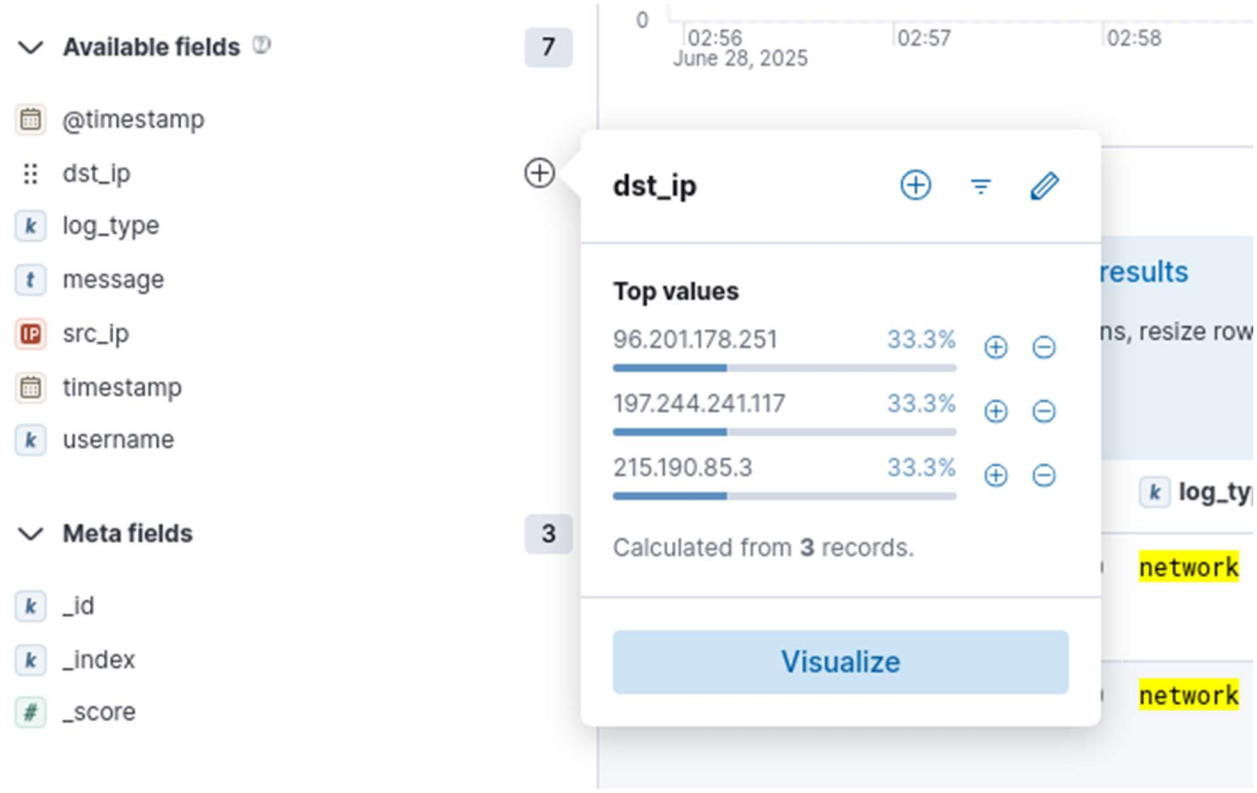
- **Authentication Threats:**
    - Detected failed login attempts from untrusted external IP addresses. The user george69 experienced repeated failed authentication, which may indicate an ongoing brute-force or credential stuffing attack. This kind of attack typically leverages automated tools to guess user passwords.

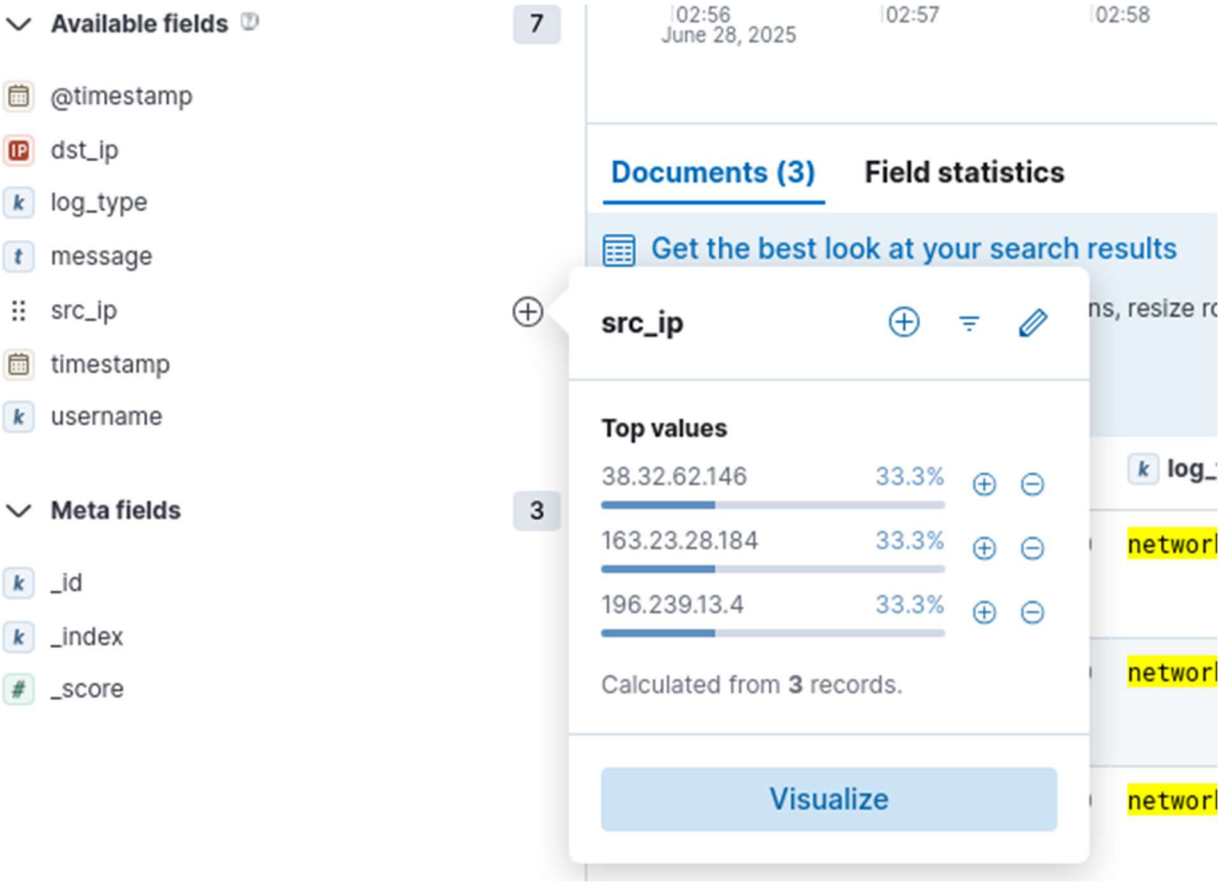
- **Malware Alerts:**
    - Three malware detections observed:
        - **Worm:** Self-propagating across the network — requires immediate isolation.
        - **Spyware:** May silently monitor and transmit user data to malicious actors.
        - **Adware:** Though lower in severity, persistent adware often opens a door for more serious payloads.



Network Traffic Analysis:

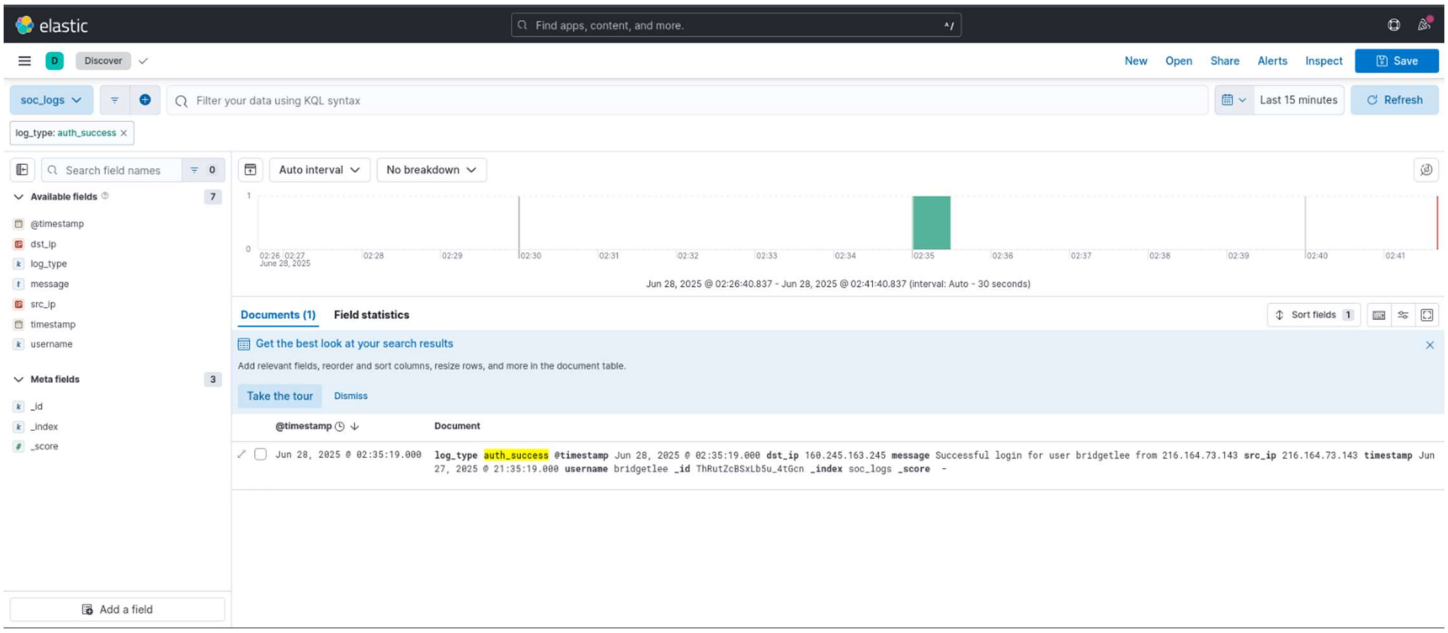
- Two source IPs (84.32.213.154, 207.36.40.203) accounted for 100% of observed external connections. This behavior is highly anomalous and may represent port scanning or command-and-control beaconing.
- Traffic was observed on non-standard ports (357, 343), further indicating reconnaissance behavior and evasion of default firewall policies.
- Targeted destination IPs (185.215.111.120, 196.104.164.196) received multiple connection attempts, suggesting these may be critical systems under active targeting.


Available fields
7
@timestamp
dst_ip
log_type
message
src_ip
timestamp
username
Meta fields
3
_id
_index
_score
0
02:56
June 28, 2025
02:57
02:58
dst_ip
Top values
96.201.178.251 33.3%
197.244.241.117 33.3%
215.190.85.3 33.3%
Calculated from 3 records.
Visualize
results
ns, resize row
log_ty
network
network


Available fields
7
@timestamp
dst_ip
log_type
message
src_ip
timestamp
username
Meta fields
3
_id
_index
_score
02:56
June 28, 2025
02:57
02:58
Documents (3)
Field statistics
Get the best look at your search results
src_ip
Top values
38.32.62.146 33.3%
163.23.28.184 33.3%
196.239.13.4 33.3%
Calculated from 3 records.
Visualize
log_
networ
networ
networ

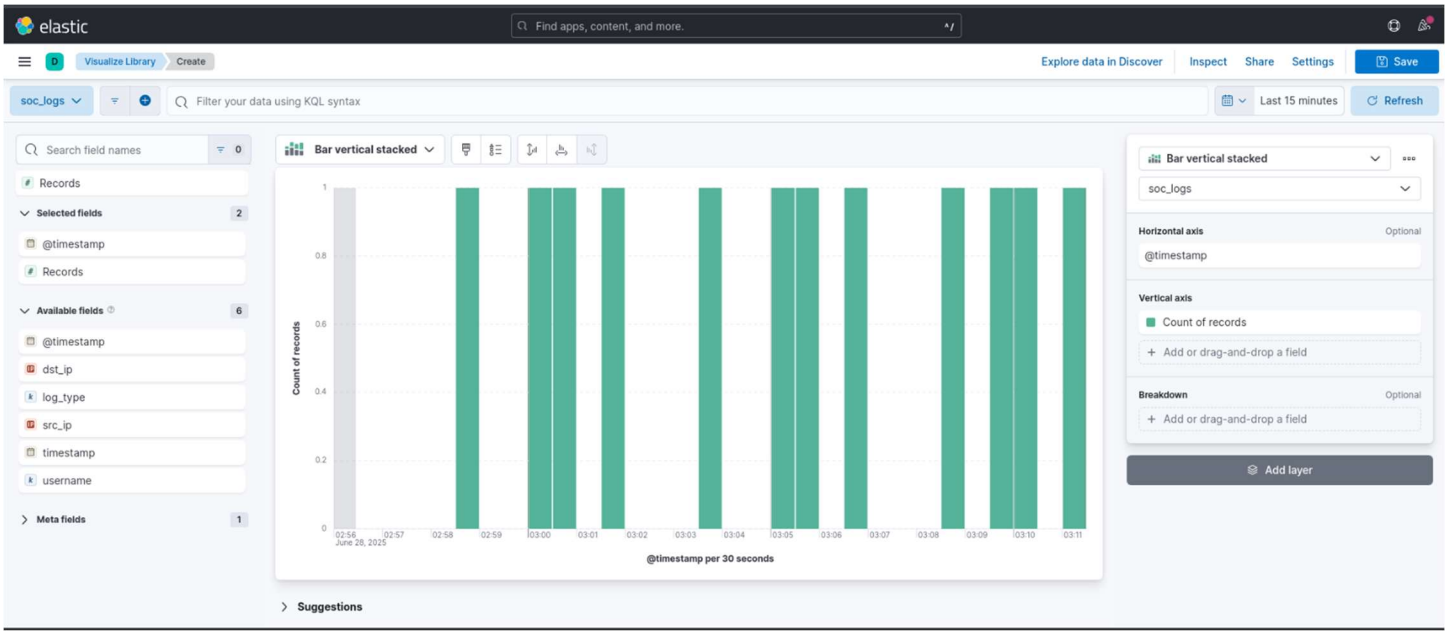
Authentication Success Review:

- Only one successful login was detected (bridgetlee from 216.164.73.143) with no correlation to prior alerts. However, this login should still be verified against user access policy and geolocation consistency.



Timeline of Events

Time (UTC)	Event Description
02:20:48	Brute-force login attempt detected
02:27 - 02:28	Multiple network connections from external IPs
02:33 - 02:34	Multiple malware types detected across different hosts
02:35	Legitimate login for user bridgetlee recorded



Threat Impact & Risk Evaluation

- **Impact Level:** High — Active brute-force attempts, malware infections, and targeted reconnaissance indicate a potentially compromised perimeter.
- **Risk to Business Continuity:**
    - Data exfiltration risk due to spyware
    - Lateral movement risk via worm
    - Unauthorized access risk due to credential attacks
- **Security Posture Recommendation:** Immediate containment, policy review, and broader log correlation needed.

Recommended Mitigation Actions

1. **Block malicious IPs:** Implement firewall rules to deny traffic from 101.59.34.162, 84.32.213.154, 207.36.40.203
2. **Endpoint Isolation:** Quarantine hosts showing malware alerts (167.212.30.96, 207.52.45.170, 207.177.251.213)
3. **Credential Audit:** Force password reset for affected users; enable login alerts
4. **Enable MFA:** Apply multi-factor authentication to all external-facing services
5. **Log Correlation:** Cross-reference logs with threat intelligence feeds
6. **Update SIEM Alerts:** Add detection rules for brute-force patterns and port scans

📧 Email Template

Subject: High-Priority Security Incident Report – Immediate SOC Attention Required

Dear IT Security Lead,

As part of a structured SOC analysis exercise, several high-risk alerts were discovered in system logs, including:

- Multiple failed login attempts likely indicating a brute-force attack
- Detection of Worm, Spyware, and Adware malware across three internal hosts
- Network scanning and reconnaissance behavior from suspicious external IPs
- Potential targeting of high-value systems based on repeated destination IP analysis

Action is advised immediately to contain and mitigate these threats. Please initiate a full incident response review.

Sincerely,
Jagadeesh Kommineni
cyber security intern, Future Interns
