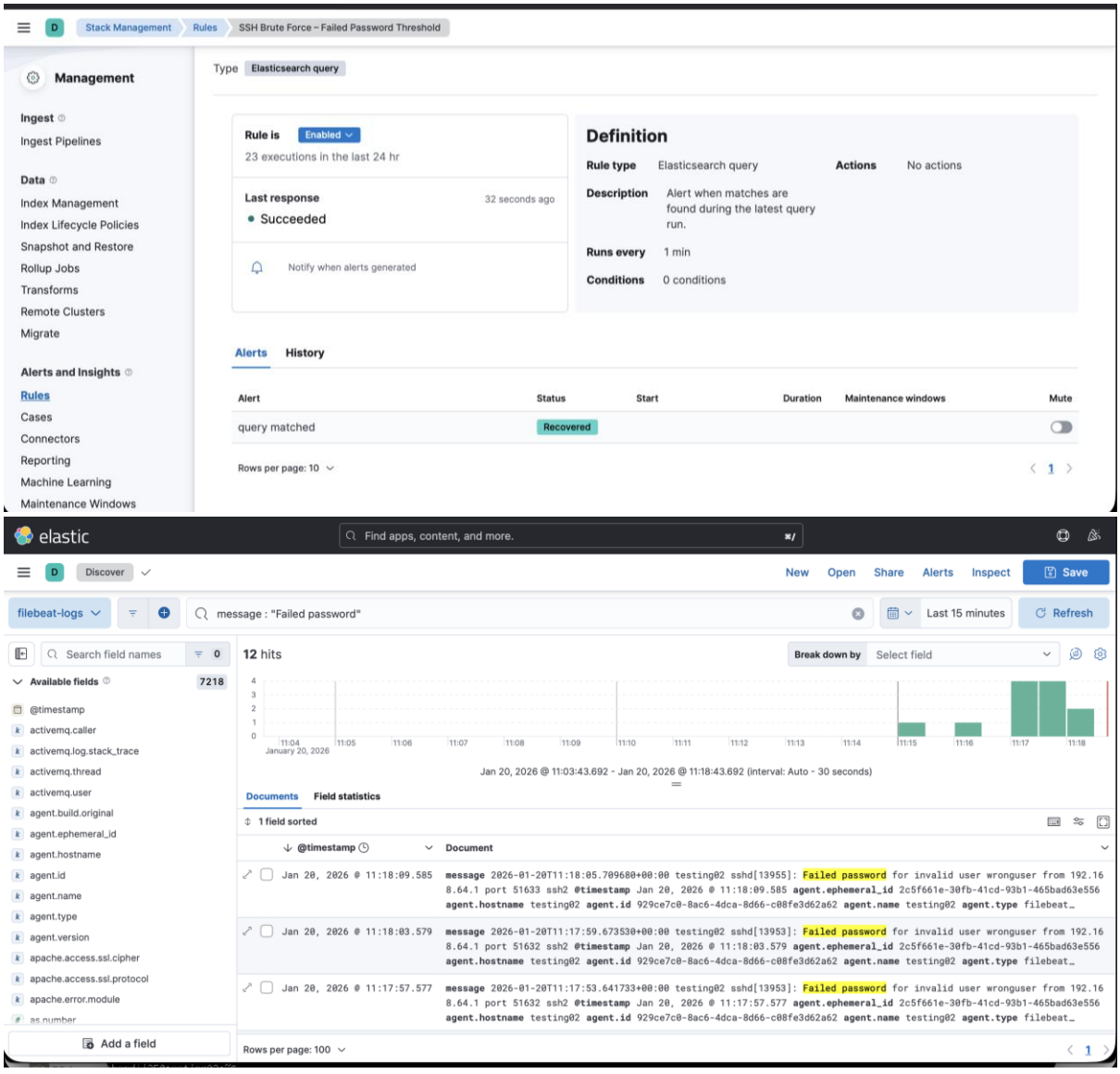
Incident Title: SSH Brute Force Failed Password Threshold
Severity: Medium
Detection Source: Elastic SIEM rule (Elasticsearch query on filebeat-logs)

Affected Host: testing02

Time Window: January 20, 2026 ~11:17–11:18 (approx.)



Observed Activity:
Multiple failed SSH authentication attempts targeting the user wronguser were observed on host testing02. A total of 12 failed login attempts occurred within a short time window, consistent with brute-force behavior.

Source:
Source IP identified from raw log messages in /var/log/auth.log (not parsed into structured fields by Filebeat).

Impact:
No successful authentication was observed. The attack did not result in account compromise.

Evidence:

- Multiple message: "Failed password" events in Kibana Discover
- Elastic rule triggered and later recovered once activity stopped

Recommended Response:

- Block offending source IP at firewall or network layer
- Enable fail2ban to rate-limit SSH authentication attempts
- Disable password-based SSH authentication and enforce key-based access
- Review SSH configuration and user access controls