SOC Investigation #5 — Temporal Analysis of Brute Force Attack (Low & Slow Pattern)

Executive Summary

This investigation focuses on the temporal behavior of failed authentication attempts in the 'big.log' file. Analysis reveals a clear pattern of automated brute-force activity, distributed uniformly across more than one hundred minutes. The attacker adjusts the frequency of failed attempts over time, indicating rate-limiting evasion typically seen in low-and-slow credential attacks. **Key Findings**

- 190 total authentication failures detected.
- Activity spans minutes 1 through 100 with no gaps.
- Phase 1: 3 attempts/minute (aggressive attack).
- Phase 2: 2 attempts/minute (reduced pace).
- Phase 3: 1 attempt/minute (stealth mode).
- The attacker demonstrates adaptation — a hallmark of automated brute-force tools.

Temporal Pattern Analysis

The distribution of authentication failures is incompatible with human behavior. No user would sustain evenly distributed login attempts across 100 consecutive minutes. Instead, this timeline aligns with brute-force frameworks that implement dynamic slowing after a threshold of failures, preventing blocking or alerting. **Conclusion**

The failed authentication activity in 'big.log' constitutes a coordinated automated attack. Its adaptive rate, sustained duration, and structured minute-by-minute distribution confirm a low-and-slow brute-force pattern. Immediate action is recommended: block the attacking IP (203.0.113.10), correlate with other alerts, and evaluate endpoint or network logs for potential compromise attempts.