

AI-Generated Incident Report

Generated: 5/18/2025 at 2:50:55 AM

Security Incident Report

Executive Summary Report: NGINX Server Anomaly Data

1. Summary Statistics

- **Total Requests:** 10,000
- **Total Alerts:** 218
- **Error Bursts:** 34
- **IP Spikes:** 91
- **Behavioral Deviations:** 93

2. Top Offending IPs

- **20.171.207.17**
 - **Flags:** [1, 3]
 - **Request Count:** 382
 - **Significance:** This IP has generated a high volume of requests, indicating potential automated activity or probing.
- **84.203.1.217**
 - **Flags:** [2]
 - **Request Count:** 244
 - **Significance:** This IP is showing signs of abnormal behavior, warranting further investigation.

3. Notable Incidents

- **Incident 1: IP Spike**
 - **IP:** 84.203.1.217
 - **Time:** 05:13–05:20
 - **Path:** /wp-cron.php
 - **Explanation:** Automated processes related to WordPress triggered a surge in traffic, potentially leading to resource exhaustion.
- **Incident 2: Error Burst**
 - **IP:** 196.251.88.242
 - **Time:** 08:49–08:50
 - **Path:** /wp-content/themes/about.php
 - **Status:** 403 Forbidden
 - **Explanation:** A potential bot was probing for vulnerabilities in theme files, suggesting a risk of exploitation.

4. Recommendations

- **Monitor Top Offenders:** Increase monitoring on the top offending IPs to assess potential threats.
- **Implement Rate Limiting:** Consider rate limiting for high-frequency requests to mitigate automated scraping.
- **Review Security Policies:** Strengthen security measures and validate current firewall rules to block suspicious traffic.
- **Conduct Vulnerability Assessment:** Regularly scan and test web applications to ensure there are no exploitable weaknesses.
- **Enhance Logging and Alerting:** Improve logging mechanisms to capture detailed traces and set up alerts for anomalies.