INSIGHTLOG SECURITY REPORT

Generated on: 2025-11-19 23:27:01

This document summarizes log activity, alerts, correlations,
and anomalies detected by the InsightLog monitoring engine.

Executive Summary

The following report provides an overview of log activity, detected threats, and correlated events captured by the InsightLog engine.

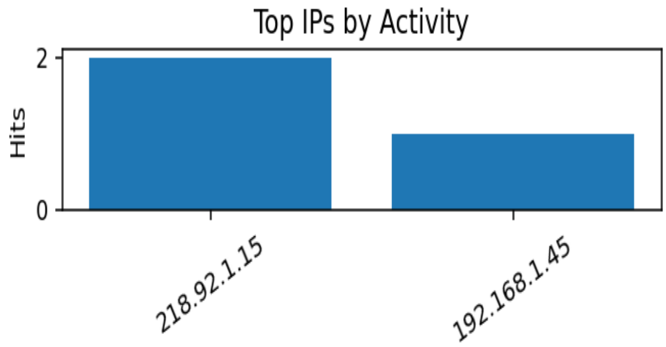
Activity Statistics

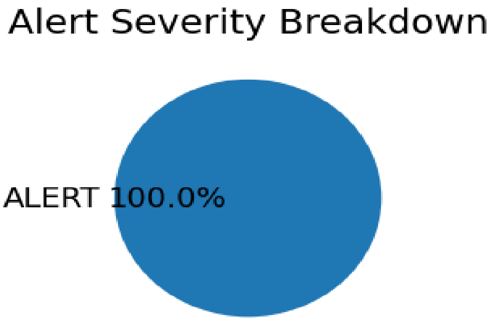
Total Records: 6

Total Alerts: 2

Correlation Events: 0

Visual Analytics





Security Alerts

Severity	Type	Message
ALERT	per_ip	Rule failed_login by_ip >= 1 ALERT triggered for 218.92.1.15 (coun
ALERT	global	Rule failed_login >= 1 ALERT triggered globally (count=2)

Correlation Events

No correlation events detected.

Attack Timeline

```
2025-10-28T06:25:01+00:00  |  INFO  |  (root) CMD (test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily ))
2025-10-28T06:25:05+00:00  |  INFO  |  Accepted publickey for ubuntu from 192.168.1.45 port 50222 ssh2: RSA SHA256:y5+
2025-10-28T06:25:05+00:00  |  INFO  |  pam_unix(sshd:session): session opened for user ubuntu by (uid=0)
2025-10-28T06:25:15+00:00  |  INFO  |    ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/cat /va
2025-10-28T10:15:22+00:00  |  ALERT  |  Invalid user admin from 218.92.1.15 port 44212
2025-10-28T10:15:24+00:00  |  ALERT  |  Failed password for invalid user admin from 218.92.1.15 port 44212 ssh2
2025-10-28T10:15:24+00:00  |  ALERT  |  Rule failed_login by_ip >= 1 ALERT triggered for 218.92.1.15 (count=2)
2025-11-19T17:54:29.491326+00:00  |  ALERT  |  Rule failed_login >= 1 ALERT triggered globally (count=2)
```