

LOG-BASED SOC PLATFORM SECURITY INCIDENT REPORT

Incident Batch Size: 1

Incident Summary

| Time | Severity | Rule | Source IP | IOC |
|----------------------------|----------|---------------------------|-------------|-----|
| 02/Nov/2025:12:02:40 +0530 | High | Unauthorized Admin Access | 27.27.27.27 | NO |

IP Intelligence & Enrichment

| | |
|--------------|--------------------------|
| Primary IP | 27.27.27.27 |
| Private IP | NO |
| Country | CN |
| Region | Hubei |
| City | Wuhan |
| Organization | AS4134 CHINANET-BACKBONE |
| ASN | UNKNOWN |
| Source | CACHE |

Evidence Samples

```
27.27.27.27 - - [02/Nov/2025:12:02:40 +0530] "GET /admin/login HTTP/1.1" 200 180 "-" "Mozilla/5.0"
```

Generated by Log-Based SOC Platform | UTC 2026-01-11T06:43:17.698767