LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Batch Size: 1

Incident Summary

Time	Severity	Rule	Source IP	IOC
02/Nov/2025:12:03:25 +0530	CRITICAL	Command Injection / Shell	36.36.36.36	NO

IP Intelligence & Enrichment

Primary IP	36.36.36.36
Private IP	NO
Country	CN
Region	Guangdong
City	Shenzhen
Organization	AS17962 ShenZhen Topway Video Communication Co. Ltd
ASN	UNKNOWN
Source	CACHE

Evidence Samples

```
36.36.36.36 - - [02/Nov/2025:12:03:25 +0530] "GET /index.php?cmd=`shutdown -h now`
HTTP/1.1" 200 34 "-" "curl/7.58.0"
```