LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

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

IP Intelligence & Enrichment

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

Normalized Payload

```
get /index.php?cmd=`shutdown -h now` http/1.1
```

Raw Log Evidence

```
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"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated