

# LOG-BASED SOC PLATFORM

## SECURITY INCIDENT REPORT

Incident Batch Size: 1

### Incident Summary

Time	Severity	Rule	Source IP	IOC
02/Nov/2025:12:01:02+0530	CRITICAL	SQLi - Tautology / OR 1=1	1.2.3.4	NO

### IP Intelligence & Enrichment

Primary IP	1.2.3.4
Private IP	NO
Country	AU
Region	Queensland
City	Brisbane
Organization	UNKNOWN
ASN	UNKNOWN
Source	CACHE

### Evidence Samples

1.2.3.4 - - [02/Nov/2025:12:01:02 +0530] "GET /index.php?id=1 UNION SELECT username,password FROM users HTTP/1.1" 200 512 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"