LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Batch Size: 1

Incident Summary

Time	Severity	Rule	Source IP	IOC
02/Nov/2025:12:03:55 +0530	Critical	SQLi - Tautology / OR 1=1	42.42.42.42	NO

IP Intelligence & Enrichment

Primary IP	42.42.42.42
Private IP	NO
Country	KR
Region	Seoul
City	Seoul
Organization	AS9644 SK Telecom
ASN	UNKNOWN
Source	CACHE

Evidence Samples

```
42.42.42.42 - - [02/Nov/2025:12:03:55 +0530] "GET
/index.php?email=someone@example.com%27%20OR%20%271%27=%271 HTTP/1.1" 200 343 "-"
"sqlmap/1.6"
```