

# LOG-BASED SOC PLATFORM

## SECURITY INCIDENT REPORT

### Incident Summary

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

### IP Intelligence & Enrichment

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

### Normalized Payload

get /index.php?id=1 union select username,password from users http/1.1

### Raw Log Evidence

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)"

### Response Actions

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