# LOG-BASED SOC PLATFORM
# SECURITY INCIDENT REPORT

Incident Batch Size: 1

## Incident Summary

| Time | Severity | Rule | Source IP | IOC |
|------|----------|------|-----------|-----|
| 02/Nov/2025:12:02:50 +0530 | Notice | SQLi - Tautology / OR 1=1 | 29.29.29.29 | NO |

## IP Intelligence & Enrichment

| | |
|------|------|
| **Primary IP** | 29.29.29.29 |
| **Private IP** | NO |
| **Country** | US |
| **Region** | Kansas |
| **City** | Independence |
| **Organization** | AS749 United States Department of Defense (DoD) |
| **ASN** | UNKNOWN |
| **Source** | CACHE |

## Evidence Samples

```
29.29.29.29 - - [02/Nov/2025:12:02:50 +0530] "GET /pay?acc=1234' OR '1'='1 HTTP/1.1"
200 333 "-" "Mozilla/5.0"
```