LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:02:50 +0530
Severity	Critical
Threat Rule	SQLi - Tautology / OR 1=1
Source IP	29.29.29.29
IOC Confirmed	NO

IP Intelligence & Enrichment

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

Normalized Payload

```
get /pay?acc=1234' or '1'='1 http/1.1
```

Raw Log Evidence

```
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"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated