LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

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

IP Intelligence & Enrichment

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

Normalized Payload

```
get /index.php?email=someone@example.com' or '1'='1 http/1.1
```

Raw Log Evidence

```
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"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated