LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:01:05 +0530
Severity	High
Threat Rule	XSS
Source IP	5.6.7.8
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	DE
Region	Hamburg
City	Hamburg
Organization	AS6805 Telefonica Germany GmbH & Co.OHG
ASN	UNKNOWN
Source	CACHE

Normalized Payload

```
get /search?q=alert(1) http/1.1
```

Raw Log Evidence

```
5.6.7.8 - - [02/Nov/2025:12:01:05 +0530] "GET /search?q=alert(1) HTTP/1.1" 200 310 "-"
"Mozilla/5.0 (X11; Linux x86_64)"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated