

# LOG-BASED SOC PLATFORM SECURITY INCIDENT REPORT

## Incident Summary

Incident Time	02/Nov/2025:12:02:30 +0530
Severity	High
Threat Rule	XSS - Advanced Payloads
Source IP	25.25.25.25
IOC Confirmed	NO

## IP Intelligence & Enrichment

Private IP	NO
Country	GB
Region	England
City	London
Organization	AS209242 Cloudflare London, LLC
ASN	UNKNOWN
Source	CACHE

## Normalized Payload

```
get /?search= http/1.1
```

## Raw Log Evidence

```
25.25.25.25 - - [02/Nov/2025:12:02:30 +0530] "GET /?search=%3Csvg%20onload%3Dalert(1)%3E HTTP/1.1" 200 256 "-" "Mozilla/5.0"
```

## Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated