

# LOG-BASED SOC PLATFORM

## SECURITY INCIDENT REPORT

Incident Batch Size: 1

### Incident Summary

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

### IP Intelligence & Enrichment

Primary IP	25.25.25.25
Private IP	NO
Country	GB
Region	England
City	London
Organization	AS209242 Cloudflare London, LLC
ASN	UNKNOWN
Source	CACHE

### Evidence Samples

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"