

LOG-BASED SOC PLATFORM SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:04:10 +0530
Severity	High
Threat Rule	XSS - Advanced Payloads
Source IP	45.45.45.45
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	CA
Region	Quebec
City	Montréal
Organization	AS5769 Videotron Ltee
ASN	UNKNOWN
Source	CACHE

Normalized Payload

```
get /?q= http/1.1
```

Raw Log Evidence

```
45.45.45.45 - - [02/Nov/2025:12:04:10 +0530] "GET /?q=%3Ciframe%20src%3D%22javascript:alert(1)%22%3E HTTP/1.1" 200 190 "-" "Mozilla/5.0"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated