LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:04:20 +0530
Severity	High
Threat Rule	Unauthorized Admin Access
Source IP	47.47.47.47
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	US
Region	Missouri
City	Lemay
Organization	AS20115 Charter Communications LLC
ASN	UNKNOWN
Source	ipinfo.io

Normalized Payload

```
get /admin?return=https://attacker.example http/1.1
```

Raw Log Evidence

```
47.47.47.47 - - [02/Nov/2025:12:04:20 +0530] "GET /admin?return=https://attacker.example
HTTP/1.1" 302 12 "-" "Mozilla/5.0"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated