LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:02:40 +0530
Severity	High
Threat Rule	Unauthorized Admin Access
Source IP	27.27.27.27
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	CN
Region	Hubei
City	Wuhan
Organization	AS4134 CHINANET-BACKBONE
ASN	UNKNOWN
Source	CACHE

Normalized Payload

```
get /admin/login http/1.1
```

Raw Log Evidence

```
27.27.27.27 - - [02/Nov/2025:12:02:40 +0530] "GET /admin/login HTTP/1.1" 200 180 "-"
"Mozilla/5.0"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated