LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Batch Size: 1

Incident Summary

Time	Severity	Rule	Source IP	IOC
02/Nov/2025:12:03:50 +0530	High	Unauthorized Admin Access	41.41.41.41	NO

IP Intelligence & Enrichment

Primary IP	41.41.41.41
Private IP	NO
Country	EG
Region	Cairo
City	Cairo
Organization	AS8452 TE-AS
ASN	UNKNOWN
Source	CACHE

Evidence Samples

```
41.41.41.41 - - [02/Nov/2025:12:03:50 +0530] "GET /admin/ HTTP/1.1" 401 78 "-"
"nikto/2.1.6"
```

Generated by Log-Based SOC Platform | UTC 2026-01-11T06:43:17.811824