LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

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

IP Intelligence & Enrichment

Private IP	NO
Country	EG
Region	Cairo
City	Cairo
Organization	AS8452 TE-AS
ASN	UNKNOWN
Source	ipinfo.io

Normalized Payload

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

Raw Log Evidence

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

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated