LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:01:35 +0530
Severity	High
Threat Rule	Unauthorized Admin Access
Source IP	14.14.14.14
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	JP
Region	Nagano
City	Matsumoto
Organization	AS131927 TV Matsumoto Cablevision
ASN	UNKNOWN
Source	CACHE

Normalized Payload

```
get /admin.php http/1.1
```

Raw Log Evidence

```
14.14.14.14 - - [02/Nov/2025:12:01:35 +0530] "GET /admin.php HTTP/1.1" 403 62 "-"
"sqlmap/1.5.5#stable"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Not Sent
PDF Report	Generated