LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:01:40 +0530
Severity	High
Threat Rule	Unauthorized Admin Access
Source IP	15.15.15.15
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	US
Region	California
City	Palo Alto
Organization	UNKNOWN
ASN	UNKNOWN
Source	CACHE

Normalized Payload

```
get /wp-admin http/1.1
```

Raw Log Evidence

```
15.15.15.15 - - [02/Nov/2025:12:01:40 +0530] "GET /wp-admin HTTP/1.1" 301 212 "-"
"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated