LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:01:45 +0530
Severity	Critical
Threat Rule	Sensitive File Access
Source IP	16.16.16.16
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	SE
Region	Stockholm
City	Stockholm
Organization	AS16509 Amazon.com, Inc.
ASN	UNKNOWN
Source	ipinfo.io

Normalized Payload

```
get /config.php.bak http/1.1
```

Raw Log Evidence

```
16.16.16.16 - - [02/Nov/2025:12:01:45 +0530] "GET /config.php.bak HTTP/1.1" 200 1204 "-"
"Mozilla/5.0"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated