

# LOG-BASED SOC PLATFORM

## SECURITY INCIDENT REPORT

Incident Batch Size: 1

### Incident Summary

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

### IP Intelligence & Enrichment

Primary IP	16.16.16.16
Private IP	NO
Country	SE
Region	Stockholm
City	Stockholm
Organization	AS16509 Amazon.com, Inc.
ASN	UNKNOWN
Source	CACHE

### Evidence Samples

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