LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Batch Size: 1

Incident Summary

Time	Severity	Rule	Source IP	IOC
02/Nov/2025:12:02:45 +0530	CRITICAL	Sensitive File Access	28.28.28.28	NO

IP Intelligence & Enrichment

Primary IP	28.28.28.28
Private IP	NO
Country	US
Region	Ohio
City	Columbus
Organization	AS749 United States Department of Defense (DoD)
ASN	UNKNOWN
Source	CACHE

Evidence Samples

```
28.28.28.28 - - [02/Nov/2025:12:02:45 +0530] "GET /.env HTTP/1.1" 200 102 "-"
"Mozilla/5.0"
```