

LOG-BASED SOC PLATFORM

SECURITY INCIDENT REPORT

Incident Batch Size: 1

Incident Summary

Time	Severity	Rule	Source IP	IOC
02/Nov/2025:12:02:55 +0530	Critical	Sensitive File Access	30.30.30.30	NO

IP Intelligence & Enrichment

Primary IP	30.30.30.30
Private IP	NO
Country	US
Region	Kansas
City	Independence
Organization	AS749 United States Department of Defense (DoD)
ASN	UNKNOWN
Source	CACHE

Evidence Samples

```
30.30.30.30 - - [02/Nov/2025:12:02:55 +0530] "GET /cgi-bin/../../../../etc/passwd HTTP/1.1" 200 640 "-" "libwww-perl/6.15"
```