

LOG-BASED SOC PLATFORM

SECURITY INCIDENT REPORT

Incident Batch Size: 1

Incident Summary

Time	Severity	Rule	Source IP	IOC
02/Nov/2025:12:03:03 +0530	Critical	Sensitive File Access	33.33.33.33	NO

IP Intelligence & Enrichment

Primary IP	33.33.33.33
Private IP	NO
Country	US
Region	Ohio
City	Columbus
Organization	AS749 United States Department of Defense (DoD)
ASN	UNKNOWN
Source	CACHE

Evidence Samples

33.33.33.33 - - [02/Nov/2025:12:03:10 +0530] "GET /search?q=%2e%2e%2f%2e%2e%2fetc%2fpasswd HTTP/1.1" 200 842 "-" "Mozilla/5.0"