

# LOG-BASED SOC PLATFORM

## SECURITY INCIDENT REPORT

Incident Batch Size: 1

### Incident Summary

Time	Severity	Rule	Source IP	IOC
02/Nov/2025:12:01:07+0530	Critical	Sensitive File Access	9.9.9.9	NO

### IP Intelligence & Enrichment

Primary IP	9.9.9.9
Private IP	NO
Country	US
Region	Virginia
City	Ashburn
Organization	AS19281 Quad9
ASN	UNKNOWN
Source	CACHE

### Evidence Samples

```
9.9.9.9 - - [02/Nov/2025:12:01:07 +0530] "GET /profile.php?user=../../../../etc/passwd HTTP/1.1" 200 842 "-" "curl/7.68.0"
```