

# LOG-BASED SOC PLATFORM

## SECURITY INCIDENT REPORT

Incident Batch Size: 1

### Incident Summary

Time	Severity	Rule	Source IP	IOC
02/Nov/2025:12:02:10 +0530	Medium	IDOR / Object Access Violation	21.21.21.21	NO

### IP Intelligence & Enrichment

Primary IP	21.21.21.21
Private IP	NO
Country	US
Region	Ohio
City	Columbus
Organization	AS749 United States Department of Defense (DoD)
ASN	UNKNOWN
Source	CACHE

### Evidence Samples

```
21.21.21.21 - - [02/Nov/2025:12:02:10 +0530] "GET /api/lookup?url=http://169.254.169.254/latest/meta-data/ HTTP/1.1" 200 200 "-" "python-requests/2.26.0"
```