LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

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

IP Intelligence & Enrichment

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

Normalized Payload

```
get /api/lookup?url=http://169.254.169.254/latest/meta-data/ http/1.1
```

Raw Log Evidence

```
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"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Not Sent
PDF Report	Generated