LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:01:50 +0530
Severity	Critical
Threat Rule	Sensitive File Access
Source IP	17.17.17.17
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	US
Region	California
City	Cupertino
Organization	AS714 Apple Inc.
ASN	UNKNOWN
Source	CACHE

Normalized Payload

```
get /.git/config http/1.1
```

Raw Log Evidence

```
17.17.17.17 - - [02/Nov/2025:12:01:50 +0530] "GET /.git/config HTTP/1.1" 200 450 "-"
"Masscan/1.6.0"
```

Response Actions

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