LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:02:45 +0530
Severity	Critical
Threat Rule	Sensitive File Access
Source IP	28.28.28.28
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	ipinfo.io

Normalized Payload

```
get /.env http/1.1
```

Raw Log Evidence

```
28.28.28.28 - - [02/Nov/2025:12:02:45 +0530] "GET /.env HTTP/1.1" 200 102 "-"
"Mozilla/5.0"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated