LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:03:10 +0530
Severity	Critical
Threat Rule	Sensitive File Access
Source IP	33.33.33.33
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 /search?q=../../etc/passwd http/1.1
```

Raw Log Evidence

```
33.33.33.33 - - [02/Nov/2025:12:03:10 +0530] "GET /search?q=%2e%2e%2f%2e%2e%2fetc%2fpasswd
HTTP/1.1" 200 842 "-" "Mozilla/5.0"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated