LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:02:55 +0530
Severity	Critical
Threat Rule	Sensitive File Access
Source IP	30.30.30.30
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	US
Region	Kansas
City	Independence
Organization	AS749 United States Department of Defense (DoD)
ASN	UNKNOWN
Source	ipinfo.io

Normalized Payload

```
get /cgi-bin/../../../../etc/passwd http/1.1
```

Raw Log Evidence

```
30.30.30.30 - - [02/Nov/2025:12:02:55 +0530] "GET /cgi-bin/../../../../etc/passwd
HTTP/1.1" 200 640 "-" "libwww-perl/6.15"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated