LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:04:30 +0530
Severity	Critical
Threat Rule	Command Injection / Shell
Source IP	49.49.49.49
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	TH
Region	Nonthaburi
City	Mueang Nonthaburi
Organization	AS45758 Triple T Broadband Public Company Limited
ASN	UNKNOWN
Source	CACHE

Normalized Payload

```
get /cgi-bin/test.cgi?cmd=uname -a; id http/1.1
```

Raw Log Evidence

```
49.49.49.49 - - [02/Nov/2025:12:04:30 +0530] "GET /cgi-bin/test.cgi?cmd=uname -a; id
HTTP/1.1" 200 123 "-" "libwww-perl/6.02"
```

Response Actions

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