

LOG-BASED SOC PLATFORM

SECURITY INCIDENT REPORT

Incident Batch Size: 1

Incident Summary

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

IP Intelligence & Enrichment

| | |
|--------------|---|
| Primary IP | 49.49.49.49 |
| Private IP | NO |
| Country | TH |
| Region | Nonthaburi |
| City | Mueang Nonthaburi |
| Organization | AS45758 Triple T Broadband Public Company Limited |
| ASN | UNKNOWN |
| Source | CACHE |

Evidence Samples

```
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"
```