LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:02:20 +0530
Severity	Critical
Threat Rule	SQL Injection
Source IP	23.23.23.23
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	US
Region	Virginia
City	Ashburn
Organization	AS14618 Amazon.com, Inc.
ASN	UNKNOWN
Source	CACHE

Normalized Payload

```
get /index.php?name='; drop table users; -- http/1.1
```

Raw Log Evidence

```
23.23.23.23 - - [02/Nov/2025:12:02:20 +0530] "GET
/index.php?name=%27%3B+DROP+TABLE+users%3B+-- HTTP/1.1" 500 126 "-" "sqlmap/1.6.0"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated