

LOG-BASED SOC PLATFORM

SECURITY INCIDENT REPORT

Incident Batch Size: 1

Incident Summary

Time	Severity	Rule	Source IP	IOC
09/Jan/2026:12:10:21+0000	Critical	SQL Injection	192.0.2.45	NO

IP Intelligence & Enrichment

Primary IP	192.0.2.45
Private IP	YES
Country	UNKNOWN
Region	UNKNOWN
City	UNKNOWN
Organization	Private / Internal Network
ASN	UNKNOWN
Source	LOCAL

Evidence Samples

```
192.0.2.45 - - [09/Jan/2026:12:10:21 +0000] "GET /login.php?username=admin' OR '1'='1'-- HTTP/1.1" 200 532
```