

# LOG-BASED SOC PLATFORM

## SECURITY INCIDENT REPORT

Incident Batch Size: 1

### Incident Summary

| Time                      | Severity | Rule                      | Source IP   | IOC |
|---------------------------|----------|---------------------------|-------------|-----|
| 02/Nov/2025:12:04:20+0530 | High     | Unauthorized Admin Access | 47.47.47.47 | NO  |

### IP Intelligence & Enrichment

|              |                                    |
|--------------|------------------------------------|
| Primary IP   | 47.47.47.47                        |
| Private IP   | NO                                 |
| Country      | US                                 |
| Region       | Missouri                           |
| City         | Lemay                              |
| Organization | AS20115 Charter Communications LLC |
| ASN          | UNKNOWN                            |
| Source       | CACHE                              |

### Evidence Samples

47.47.47.47 - - [02/Nov/2025:12:04:20 +0530] "GET /admin?return=https://attacker.example HTTP/1.1" 302 12 "-" "Mozilla/5.0"