

# LOG-BASED SOC PLATFORM

## SECURITY INCIDENT REPORT

Incident Batch Size: 1

### Incident Summary

| Time                      | Severity | Rule                            | Source IP   | IOC |
|---------------------------|----------|---------------------------------|-------------|-----|
| 02/Nov/2025:12:01:20+0530 | CRITICAL | SSRF / Internal Resource Access | 11.11.11.11 | NO  |

### IP Intelligence & Enrichment

|              |   |
|--------------|---|
| Primary IP   | 11.11.11.11                                     |
| Private IP   | NO  |
| Country      | US  |
| Region       | Kansas  |
| City         | Independence                                    |
| Organization | AS749 United States Department of Defense (DoD) |
| ASN          | UNKNOWN   |
| Source       | CACHE   |

### Evidence Samples

```
11.11.11.11 - - [02/Nov/2025:12:01:20 +0530] "GET /download?file=http://127.0.0.1:8000/secret HTTP/1.1" 200 410 "-" "python-requests/2.25.1"
```