LOG-BASED SOC PLATFORM
SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:01:20 +0530
Severity	Critical
Threat Rule	SSRF / Internal Resource Access
Source IP	11.11.11.11
IOC Confirmed	NO

IP Intelligence & Enrichment

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

Normalized Payload

```
get /download?file=http://127.0.0.1:8000/secret http/1.1
```

Raw Log Evidence

```
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"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated