

# LOG-BASED SOC PLATFORM

## SECURITY INCIDENT REPORT

### Incident Summary

|               |                                |
|---------------|--------------------------------|
| Incident Time | 02/Nov/2025:12:01:55 +0530     |
| Severity      | Medium                         |
| Threat Rule   | IDOR / Object Access Violation |
| Source IP     | 18.18.18.18                    |
| IOC Confirmed | NO                             |

### IP Intelligence & Enrichment

|              |   |
|--------------|---|
| Private IP   | NO  |
| Country      | US  |
| Region       | Massachusetts                             |
| City         | Boston                                    |
| Organization | AS3 Massachusetts Institute of Technology |
| ASN          | UNKNOWN                                   |
| Source       | CACHE                                     |

### Normalized Payload

get /product?id=1 or 1=1 http/1.1

### Raw Log Evidence

18.18.18.18 - - [02/Nov/2025:12:01:55 +0530] "GET /product?id=1%20OR%201=1 HTTP/1.1" 200 398 "-" "Mozilla/5.0"

### Response Actions

|                 |                    |
|-----------------|--------------------|
| Firewall Action | No Firewall Action |
| Email Alert     | Sent               |
| PDF Report      | Generated          |