SOC ESCALATION REPORT (L1 → L2)

Alert Name: Excessive HTTP 404 Errors – Possible Web Scanning
Severity: Medium
Date/Time: 12-Jan-2026 | 14:20 IST
Detected By: Splunk SIEM
Source: HTTP Logs (index=main sourcetype=http)

➢ **L1 Analysis Summary:-**

- Detected high volume of HTTP 404 responses from a single source IP
- **Source IP**: 192.168.1.45
- Total 404 requests: 137 within 10 minutes
- Targeted multiple different URLs, indicating directory enumeration / scanning

➢ **Initial Assessment:-**

- Activity consistent with web reconnaissance
- No successful exploitation observed
- No impact to production services at this time

➢ **Evidence:-**

- Splunk SPL used:

```
index=main sourcetype=http
| where status=404
| stats count by src_ip
| where count > 100
```

➢ **Escalation Reason**

- Repeated abnormal behavior exceeding baseline thresholds
- Requires deeper investigation and possible blocking action

🔄 **Recommended L2 Actions**

- Validate IP against threat intelligence
- Check WAF / firewall logs for related activity
- Consider temporary IP blocking if activity continues

Status: Escalated to L2
Escalated By: SOC L1 Analyst