🚨 SOC ESCALATION REPORT (L1 → L2)

Incident ID: SOC-DNS-TP-001
Detected Time: <YYYY-MM-DD HH:MM>
Reported By: SOC L1 Analyst
Escalated To: SOC L2 / IR Team
Severity: 🔴 High
Status: Confirmed True Positive
Confidence: High

📌 Incident Summary

Suspicious DNS activity consistent with **DNS-based Command & Control and Data Exfiltration** detected from a single endpoint. Multiple indicators align with known DNS tunneling and beaconing behavior.

🎯 Classification

- **Attack Type:** DNS C2 / DNS Tunneling
- **Protocol:** DNS (Port 53)
- **MITRE ATT&CK:**
  - **T1071.004** – DNS-based Command & Control
  - **T1048** – Data Exfiltration Over Alternative Protocol

🚩 Key Indicators Observed

- Abnormally long DNS queries (>50 characters)
- High-frequency, periodic DNS requests (beaconing)
- Encoded/high-entropy subdomains
- DNS volume indicative of tunneling

🔍 Evidence (SIEM + Network)

- Splunk confirmed repeated long FQDN queries from same source
- Correlated alerts from single endpoint
- Packet inspection shows encoded subdomains and regular intervals
- Domain reputation: suspicious / low trust

🌐 Affected Asset

- **Source IP:** <src_ip>
- **Hostname:** <hostname>
- **Destination Domain:** <suspicious-domain>

🛑 **L1 Actions Taken**

- Blocked domain at DNS level
- Isolated affected endpoint
- Preserved logs and IOCs

🔼 **Escalation Request (L2)**

- Perform endpoint forensic analysis
- Identify malware/persistence mechanism
- Assess data exfiltration impact
- Scope hunt for similar DNS patterns across environment

📎 **IOCs**

- Domains: <domain>
- DNS Pattern: Long, encoded subdomains
- Behavior: Regular beaconing

🧠 **L1 Analyst Assessment**

Activity strongly matches **malicious DNS C2/tunneling behavior**. Confirmed true positive based on SIEM correlation, packet validation, and threat intel.

🔴 **Status:** Escalated to L2 for Incident Response