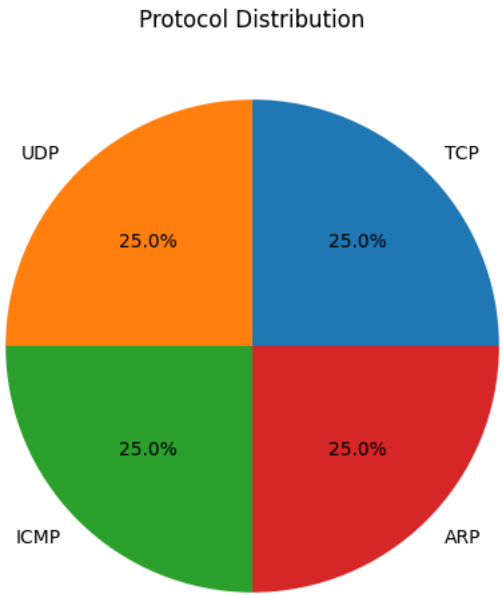
Network Security Analysis Report

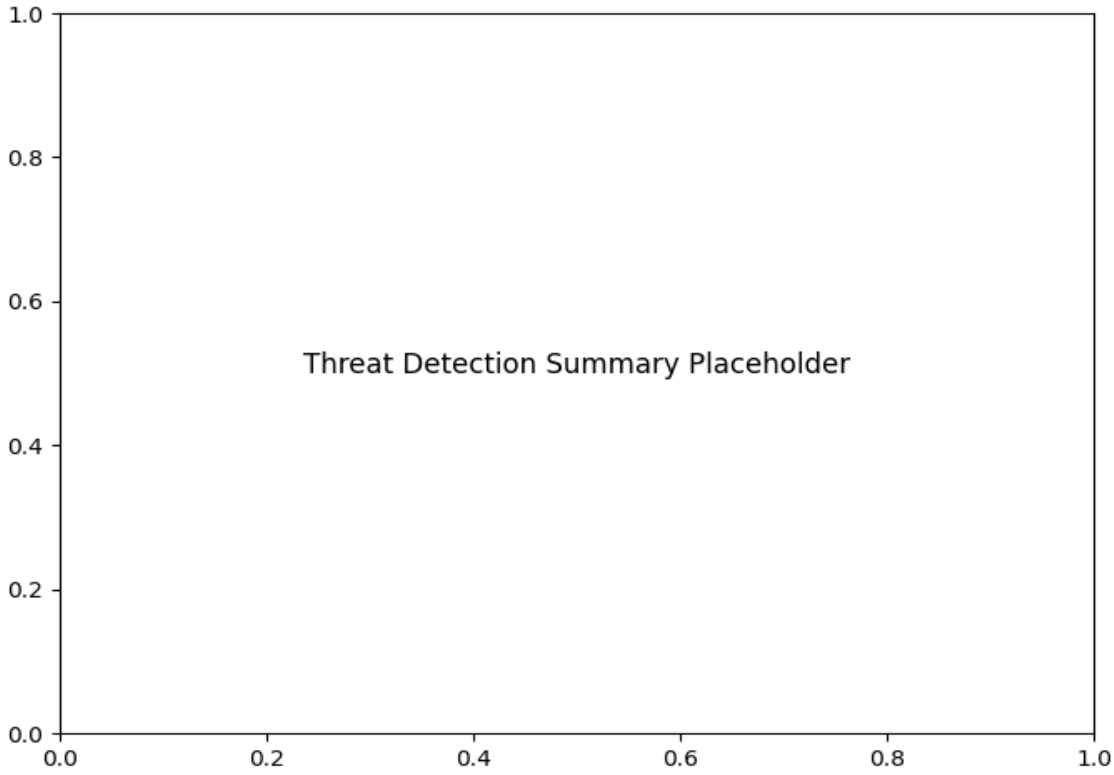
AI-Powered Security Insights

Network Traffic Analysis Security Report Executive Summary **6 instances of Potential DNS tunneling** detected in analyzed traffic (100% of flagged anomalies) All malicious activity concentrated between two internal IPs (192.168.73.148 ↔ 192.168.73.2) using UDP/DNS protocols No observed TCP, ICMP, ARP, or conventional UDP attack patterns Risk Assessment Critical Risks **DNS tunneling (Severity: Critical)** - Consistent pattern of bidirectional DNS/UDP traffic between internal hosts matches data exfiltration/covert channel signatures **Internal host compromise (Severity: High)** - Suspicious activity between 192.168.73.148 (client) and 192.168.73.2 (likely DNS server) suggests potential lateral movement Contextual Observations Zero detections of traditional network attacks (SYN floods, ICMP abuse, ARP spoofing) 100% of top threats involve DNS protocol abuse Threat Observations **Pattern Analysis** 5 consecutive DNS/UDP transactions within 7 seconds (Packets #159-167) Bidirectional traffic pattern: Initial query from .148 → .2, followed by immediate response Null port numbers suggest possible protocol manipulation or misconfigured logging **Key Artifacts** Primary source: 192.168.73.148 (3 outbound requests) Consistent DNS response host: 192.168.73.2 Timestamp clustering: All events occurred within 02:02:58 - 02:03:05 timeframe **Statistical Highlights** 100% of detected threats leverage UDP/DNS combination 0% traditional attack payloads observed (TCP/UDP flood attempts, etc.) Recommendations Immediate Actions **Quarantine 192.168.73.148** for forensic analysis - observed behavior matches Stage 2 compromise indicators **Implement DNS query filtering** with: Domain whitelisting for internal DNS servers Payload size restrictions (block >512 byte DNS packets) TXT/ANY record request monitoring Technical Controls Deploy **DNS traffic analysis tools** (e.g., DNSTwist, dnsmeter) to baseline normal activity **Enable DNS logging** with mandatory port enforcement (UDP 53 only) Implement **network segmentation** to restrict direct host-to-host DNS communication Policy Enhancements **Update IDS/IPS rulesets** to detect DNS tunneling techniques: High entropy subdomains Excessive NULL/TXT records Uncommon record type proliferation **Conduct DNS security audit** focusing on: Zone transfer restrictions Recursive query permissions Cache snooping protections

Protocol Distribution



Threat Detection Summary



Detection Type	Count
Potential DNS tunneling detected	6