

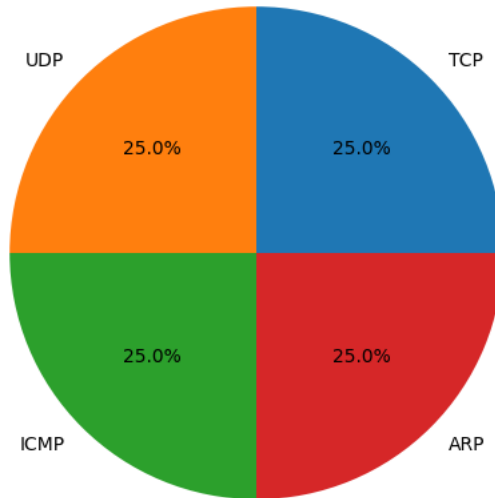
Network Security Analysis Report

AI-Powered Security Insights

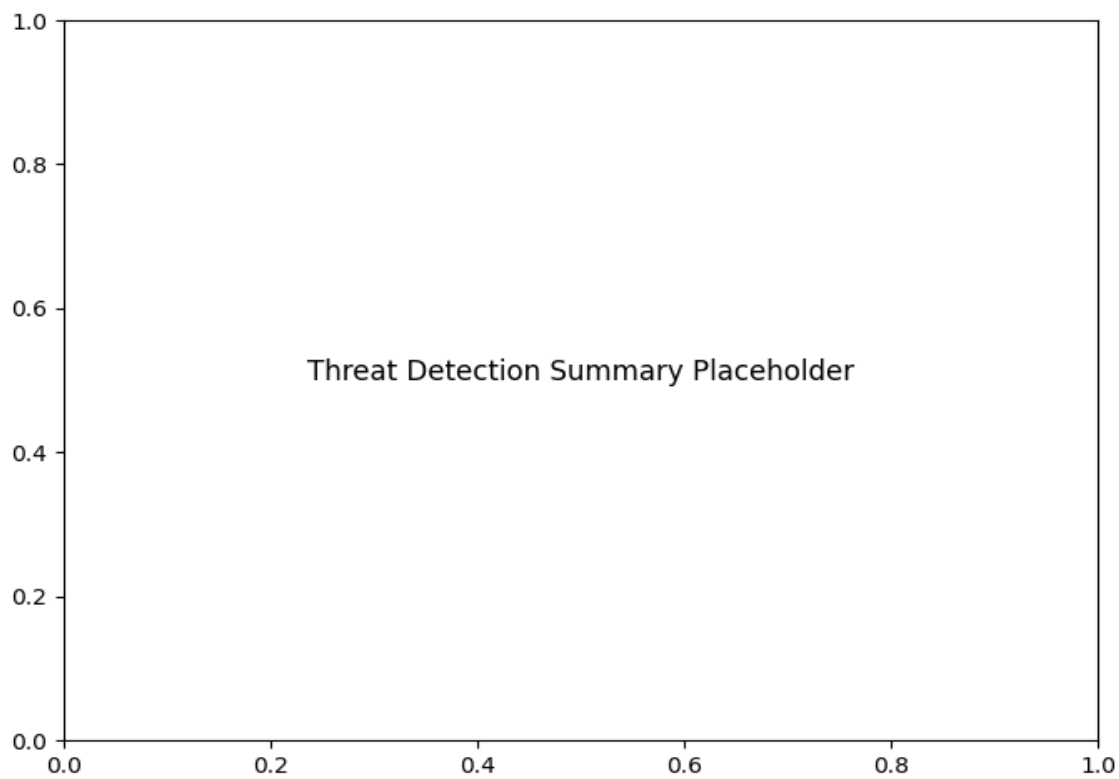
Network Traffic Analysis Security Report ## Executive Summary - **6 instances of Potential DNS tunneling** detected in analyzed traffic - All suspicious activity occurred between two internal IPs (`192.168.73.148` ↔ `192.168.73.2`) - **100% of threats leveraged UDP/DNS protocols** with no traditional attack traffic (TCP/ICMP/ARP) observed ## Risk Assessment - **Critical Risk: DNS Tunneling** Severity: ■ **High** (CWE-200) - Enables data exfiltration/command execution bypassing standard security controls - Repeated pattern (5 consecutive DNS exchanges) suggests active C2 communication - **Suspicious Host Configuration** Severity: ■ **Medium** - Internal IP (`192.168.73.148`) acting as DNS client/server simultaneously warrants investigation ## Threat Observations - **Temporal Pattern**: 5 DNS tunneling events within 7 seconds (02:02:58 - 02:03:05) - **Protocol Anomalies**: - Null source/destination ports in DNS traffic (uncommon for standard implementations) - Bi-directional UDP/DNS traffic between same endpoints (packets 159↔160, 165↔166, 167) - **Payload Characteristics**: - Missing port data suggests possible payload manipulation in DNS queries - No observed legitimate DNS traffic to external resolvers ## Recommendations 1. **Immediate Containment**: - Quarantine `192.168.73.148` for forensic analysis - Block UDP/53 traffic between internal hosts except authorized DNS servers 2. **DNS Hardening**: - Deploy **DNS filtering** (e.g., DNSSEC, TLS-enabled DNS) - Implement **DNS query rate limiting** (max 100 queries/sec per host) 3. **Threat Hunting**: - Review all DNS TXT/AAAA records from `192.168.73.148` for encoded payloads - Cross-reference with proxy logs for matching timestamp exfiltration attempts 4. **Tooling Enhancements**: - **Enable full packet capture** for DNS transactions exceeding 512 bytes - Configure SIEM alerts for DNS requests containing: - Base64-like subdomains - Uncommon record types (e.g., TXT, NULL) - Repeated failed NXDOMAIN responses

Protocol Distribution

Protocol Distribution



Threat Detection Summary



Detection Type	Count
Potential DNS tunneling detected	6