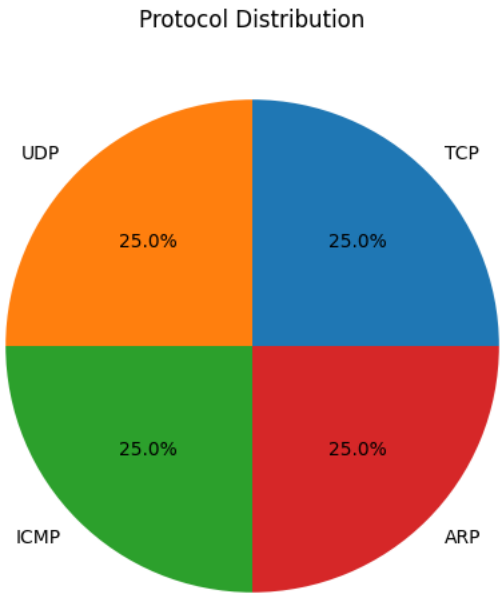
Network Security Analysis Report

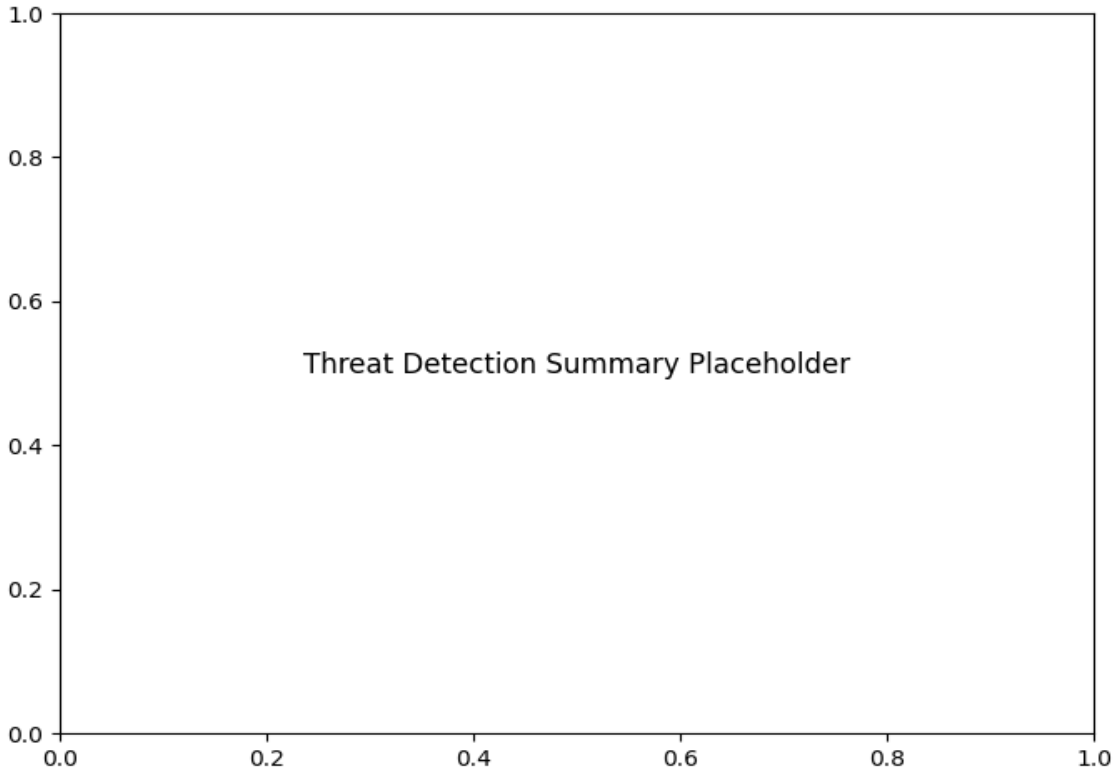
AI-Powered Security Insights

Network Traffic Analysis Security Report ## Executive Summary - **6 instances of Potential DNS tunneling** detected in network traffic analysis - Primary risk vector identified in UDP/DNS communications between internal hosts - No observed TCP/ICMP/ARP-based attacks in current dataset - Suspicious activity concentrated between `192.168.73.148` and `192.168.73.2` ## Risk Assessment - **Critical Risk: DNS Tunneling Attempts** **Severity: High** - 100% of detected threats involve DNS protocol manipulation - Potential data exfiltration or command-and-control channel establishment - **Internal Host Compromise** **Severity: Medium** - Suspicious bidirectional communication between internal IP addresses - All detections involve local network assets (`192.168.73.0/24`) ## Threat Observations - **Protocol Analysis**: - 100% of malicious packets use UDP/DNS combination - Zero detected attacks via TCP/ICMP/ARP protocols - **Temporal Pattern**: - Cluster of 5 DNS tunneling events within 6-second window - Initial detection at `2009-03-26T02:02:58.910572` - **Traffic Characteristics**: - Bidirectional communication pattern (packets 159→160, 165→166) - Consistent absence of port data in DNS transactions - Repeated query-response behavior between same endpoints - **Host Behavior**: - `192.168.73.148` initiates 3 tunneling attempts - `192.168.73.2` responds to tunneling attempts while generating 2 suspicious requests ## Recommendations - **DNS Security Measures**: - **Implement DNS query filtering** to block non-standard record types - Enforce DNS payload size restrictions (max 512 bytes for UDP) - Deploy DNS logging with anomaly detection capabilities - **Host Investigation**: - **Immediate forensic analysis** of `192.168.73.148` and `192.168.73.2` - Review DNS client configurations on affected hosts - Validate legitimate DNS requirements for critical systems - **Network Controls**: - **Implement egress filtering** for DNS traffic to external resolvers - Enforce DNSSEC validation for all DNS transactions - Segment internal DNS servers from general workstation traffic - **Monitoring Enhancements**: - Create baseline of normal DNS activity patterns - Implement alerts for repeated DNS queries to same domain - Monitor TXT/ANY record type usage exceeding threshold - **Policy Updates**: - **Restrict DNS resolver privileges** to authorized servers only - Implement application whitelisting for DNS client software - Establish protocol-specific firewall rules for DNS port 53 usage

Protocol Distribution



Threat Detection Summary



Detection Type	Count
Potential DNS tunneling detected	6