

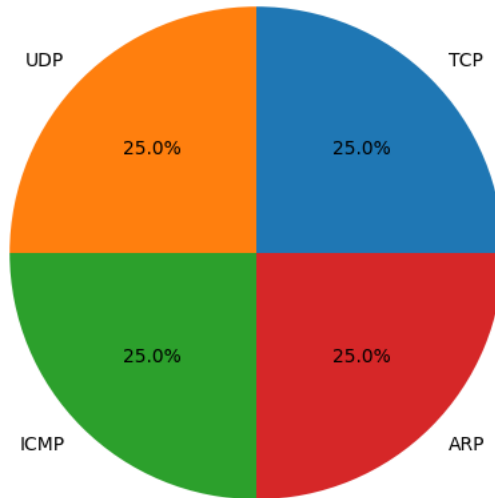
Network Security Analysis Report

AI-Powered Security Insights

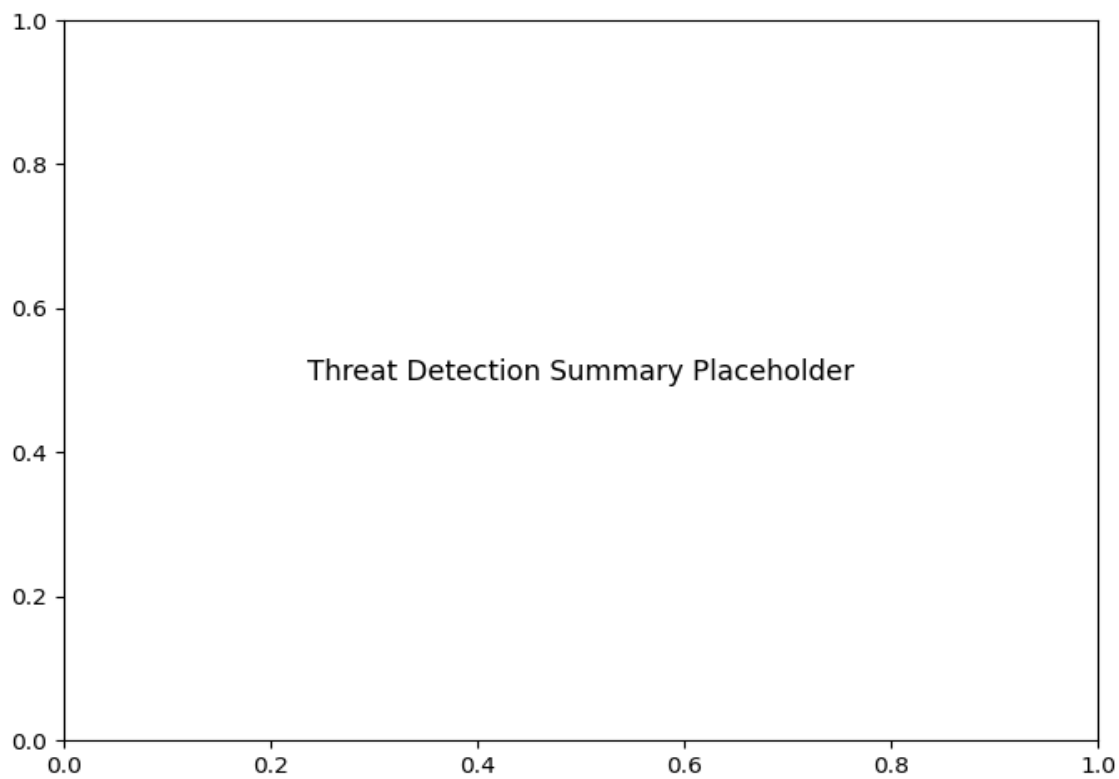
``markdown Executive Summary **6 instances of Potential DNS tunneling** detected in analyzed traffic (100% of alerts) Suspicious activity concentrated between two internal IPs: 192.168.73.148 (source) and 192.168.73.2 (destination) All malicious traffic uses **UDP/DNS protocols** with no traditional attack packets (TCP/ICMP/ARP) observed Risk Assessment Critical Risks **DNS tunneling exploitation**: High severity (CWE-300). Enables data exfiltration/C2 channels bypassing traditional security controls. **Internal host compromise**: Repeated bidirectional DNS traffic between 192.168.73.148 and 192.168.73.2 suggests **potential lateral movement**. Operational Risks **Lack of DNS traffic monitoring**: No apparent controls to detect/block abnormal DNS payload patterns **Sensor data discrepancy**: Attack stats report 0 UDP packets despite 5 UDP-based threats in top_threats list Threat Observations **Pattern Analysis**: 5 consecutive DNS tunneling attempts between 2009-03-26T02:02:58 and 02:03:05 (7-second window) Bidirectional communication (packets 159↔160, 165↔166, 167) indicates **protocol handshaking** **Technical Anomalies**: Null port numbers in DNS traffic (standard DNS uses UDP/53) Absence of legitimate DNS server IPs in communications High frequency of DNS requests (6 events) from internal IP to internal IP Recommendations Immediate Actions **Quarantine 192.168.73.148**: Investigate for installed tunneling tools (e.g., DNSCat2, Iodine) **Implement DNS filtering**: Block TXT/NULL/CNAME record types except from authorized DNS servers Enforce maximum DNS query length (e.g., 100 bytes) **Validate sensor configurations**: Resolve UDP packet counting discrepancy between attack_stats and top_threats data Long-Term Controls Deploy **DNS firewall solutions** (e.g., Cisco Umbrella, Infoblox) with tunneling detection capabilities Establish **network segmentation policies** to restrict internal host-to-host DNS communications Enable **DNS query logging** with payload inspection for all critical subnets

Protocol Distribution

Protocol Distribution



Threat Detection Summary



Detection Type	Count
Potential DNS tunneling detected	6