Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

6 instances of Potential DNS tunneling detected in analyzed traffic
Suspicious activity concentrated between two internal IP addresses (192.168.73.148 ↔ 192.168.73.2)
All malicious traffic observed exclusively via **UDP/DNS protocols**
No traditional attack patterns detected (0 TCP/ICMP/ARP attack packets)
Risk Assessment
Critical Risks (Severity: High)

DNS tunneling attempts indicating potential data exfiltration/C2 channels
Internal host compromise risk (192.168.73.148 initiating multiple DNS requests)
Lack of port information in DNS traffic obscures payload analysis
Operational Risks (Severity: Medium)

Unusually dense DNS traffic pattern (5 malicious packets within 7-second window)
Bidirectional suspicious DNS communication between internal hosts
Threat Observations

Host Communication Pattern
Repeated UDP/DNS exchanges between 192.168.73.148 (initiator) and 192.168.73.2
3 distinct request-response sequences observed in packet #159-160, #165-166, and #167

Temporal Analysis
First detection: 2009-03-26T02:02:58.910572
Last detection: 2009-03-26T02:03:05.264983 (6.35-second active window)

Protocol Anomalies
100% of malicious traffic uses UDP with embedded DNS payloads
Absence of legitimate port identifiers (null src_port/dst_port values)
Recommendations
Immediate Actions

Quarantine host 192.168.73.148 for forensic analysis
Implement DNS query filtering with **DNS firewall controls**
Block UDP port 53 traffic between internal hosts except authorized DNS servers
Technical Controls Enhancement

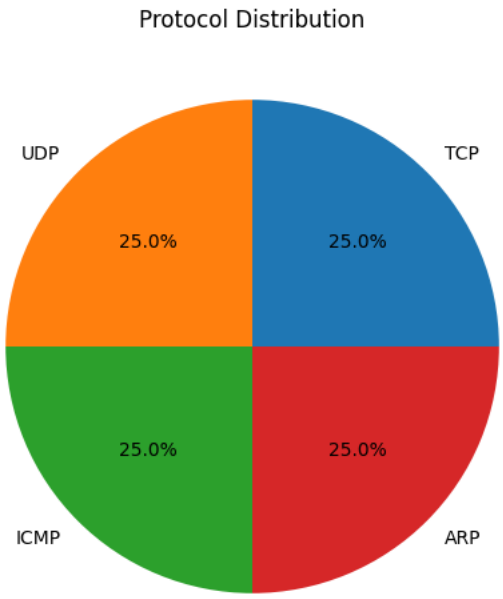
Deploy **DNS monitoring solution** with:
Payload inspection (check for base64/hex encoding in TXT records)
Query length thresholds (flag requests > 100 characters)
Uncommon subdomain detection (e.g., *.exe*..domain.com)
Policy Updates

Enforce **split-horizon DNS architecture** to separate internal/external resolution
Implement **DNSSEC** to prevent DNS cache poisoning attacks

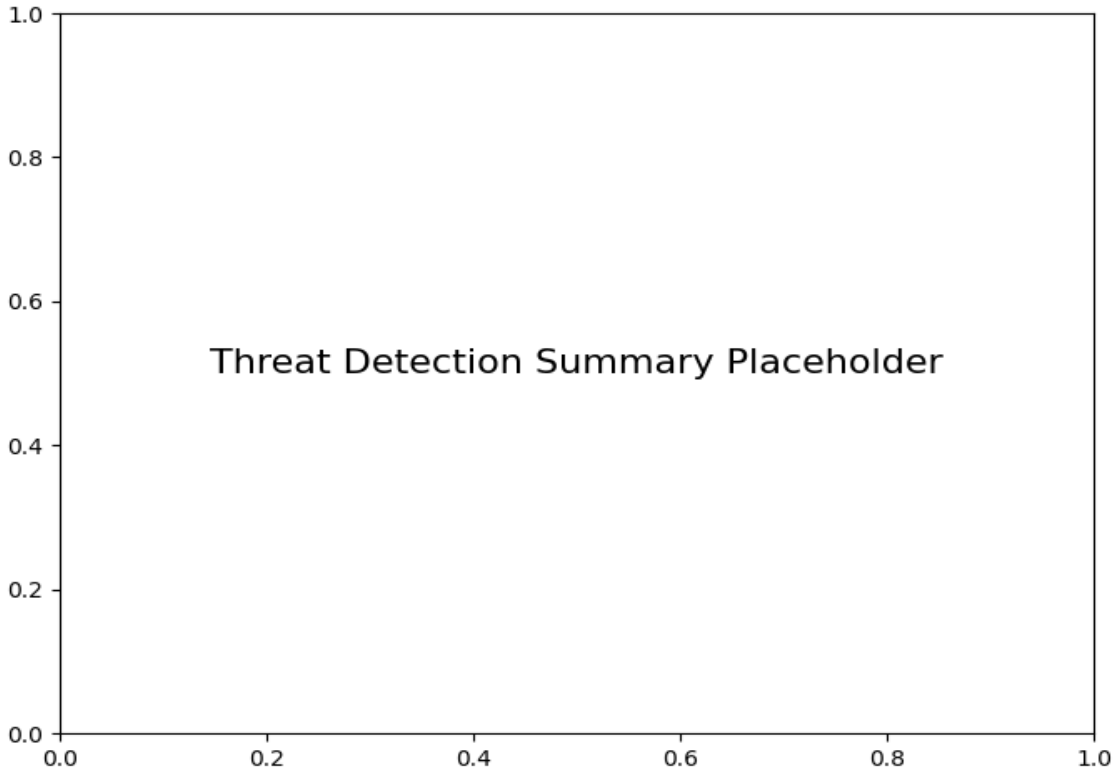
Establish baseline for normal DNS traffic patterns (volume/frequency/record types)
Investigation Priorities

Audit all services running on 192.168.73.2 (potential internal DNS resolver abuse)
Cross-correlate DNS timestamps with proxy/VPN logs for data exfiltration patterns
Conduct packet capture analysis of full DNS sessions (not just alert triggers)

Protocol Distribution



Threat Detection Summary



Detection Type	Count
Potential DNS tunneling detected	6