Introduction to Threat Hunting

Step By Step Guides

How to Filter DNS traffic to find malicious queries

1. In wireshark click the search bar at the top
2. Type “dns.flags.response == 0” into the search bar to remove dns responses and leave only queries
3. Press enter or the arrow to the right of the search bar.
4. Look for suspicious and/or malicious activity within the displayed queries

How to Detect Data Exfiltration (tcp and frame.len > 1000)

1. In wireshark click the search bar
2. Type “tcp && frame.len > 1000 &&” to filter tcp frames that are greater than 1000 bytes
3. Look at the IP addresses and port numbers of packets and look for any suspicious IP addresses or port numbers

How to identity C2 beaconing activity

Screenshots