DNS Log-based Command and Control Tunnel Detection and Prevention System Design

Overview

With this microservice-based design, the system can ingest continuous DNS logs, run real-time anomaly detection, leverage historical data for large-window analysis, integrate dynamic threat intelligence, generate timely alerts, and provide a central dashboard for situational awareness—while also contributing discovered threats back to the broader cybersecurity community.

Note: The microservices are grouped by a Tier in which they will be primarily operating.