Passive DNS, Data Component DC0096

Archived: 2026-04-05 14:14:12 UTC

"Domain Name: Passive DNS" captures logged historical and real-time domain name system (DNS) data. This includes records of domain-to-IP address resolutions over time, enabling analysts to track the evolution of domain infrastructure, uncover historical patterns of use, and detect malicious activities tied to domains and their associated IP addresses. Examples:

- Historical Resolutions
- Shared IP Usage
- Temporal Patterns
- Malicious Domain Clustering
- Historical Lookback

This data component can be collected through the following measures:

- Passive DNS Platforms: Use platforms that specialize in passive DNS collection and analysis:
- Tools: Farsight DNSDB, RiskIQ PassiveTotal, PassiveDNS.
- Threat Intelligence Feeds: Integrate passive DNS data from commercial or open-source threat intelligence providers.
- Custom DNS Collectors: Deploy custom tools to capture DNS traffic at the network level for analysis.
- Cloud DNS Services: Leverage cloud DNS services (e.g., AWS Route 53, Azure DNS) that maintain DNS query logs.
