Domain Registration, Data Component DC0101

Archived: 2026-04-05 14:03:51 UTC

"Domain Name: Domain Registration" data component captures information about the assignment, ownership, and metadata of domain names. This information is often sourced from registries like WHOIS and includes details such as registrant names, contact information, registration dates, expiration dates, and registrar details. This data is invaluable for tracking domain ownership, detecting malicious domain registrations, and identifying trends in adversary behavior. Examples:

- Registrant Information: WHOIS lookup of example.com
- Registration and Expiration Dates: A domain registered a week before being used in phishing attacks.
- Domain Status: Status codes like clientTransferProhibited or serverHold indicate domain restrictions or potential hijacking activity.
- Name Server Information: Name servers point to a public DNS provider often associated with malicious campaigns.
- Privacy Protection: A domain uses WHOIS privacy protection to hide registrant details.

This data component can be collected through the following measures:

- WHOIS Services: Use tools or services to perform WHOIS lookups:
- WHOIS APIs: Automate domain registration lookups with APIs:
- Registrar Platforms: Directly query domain registrars (e.g., GoDaddy, Namecheap) for detailed registration data.
- Threat Intelligence Platforms: Integrate domain registration data from services like Recorded Future, RiskIQ, or PassiveTotal for enriched analysis.
