DATASHROUD

SECURITY THROUGH OBSCURITY

DataShroud is a personal risk management tool for professionals and families. Created by experts in Open-Source Intelligence (OSINT), the tiered service reduces or eliminates your presence online and from vulnerable servers around the world.

Your usernames and passwords are important. However, your home address, your vehicle, your phone, your children's school, your vacation cabin and your assets are the fabric of your real life. Achieve security through obscurity by reducing your online footprint to zero.

We engage the same intelligence infrastructure used to find elusive individuals across the globe, then meticulously destroy the resulting data to instead help you disappear. Through thinking like a real life threat actor, we obfuscate as much data as is legally permissible to protect all your personal information to guard you against harassment, extortion and other criminal activity. When DataShroud is complete, anything related to the assignment is then purged from our own servers.

UPSTREAM INTELLIGENCE

THE PROCESS

1 BASELINE PHASE I

An Intelligence Analyst manually removes personal information from hundreds of online data aggregators, eliminating the risk a Basic Threat Actor will find a client's home, vehicle, phone, email or family relations via search engines and data aggregators.

2 BASELINE PHASE II

A holistic risk profile is created, ranking exposure at the residential, financial, communication, social media, family, travel and lifestyle levels. This risk profile is furnished to the client along with a verbal debriefing of efforts. The client may remediate some of the vulnerabilities themselves with our guidance, or elect to have them professionally purged in the Advanced Phase.

3 ADVANCED PHASE

Manual removal or obfuscation of the more advanced PII identified in Baseline Phase II. The primary goal continues to be the protection of residences and other real life items. Keen attention is also paid to travel, including hotels, rental cars, and airlines. These are popular targets of Advanced Threat Actors, particularly related to C-Suite executives and HNWIs.

4 MONITORING

In addition to traditional dark web monitoring, DataShroud monitoring ensures a consistent blackout of PII across all areas, with notifications of vulnerabilities as they are detected. Remediation efforts commence immediately. This is part software-driven, and part the active efforts of Intelligence Analysts who regularly check-up on a client's PII exposure and launch their own investigations to determine where other vulnerabilities may lie.

AREAS OF PRIMARY CONCENTRATION

- Residential addresses
- Phone numbers
- Email addresses
- Vehicle sightings and Automated License Plate Recognition (ALPR)records
- Hacked usernames and passwords
- Street-level map images of residences
- Data stored on major national background check services[1]
- Personally Identifiable Information (PII) located on 3rd party websites
- Unclaimed asset data
- Secondary & tertiary background check sites
- 2nd party website removal requests
- Online classifieds
- Real estate listings
- Online dating profiles
- Hotel and rental car records
- Airline records
- DNA profile data
- Family social media and PII
- Removal of unique vulnerabilities uncovered by Intelligence Analysts

Our goal for comprehensive DataShroud assignments is simple: once we complete our work, even we shouldn't be able to find you!

[1] Please note the complete elimination of this data can require additional levels of verification during subsequent credit applications.