NISOS

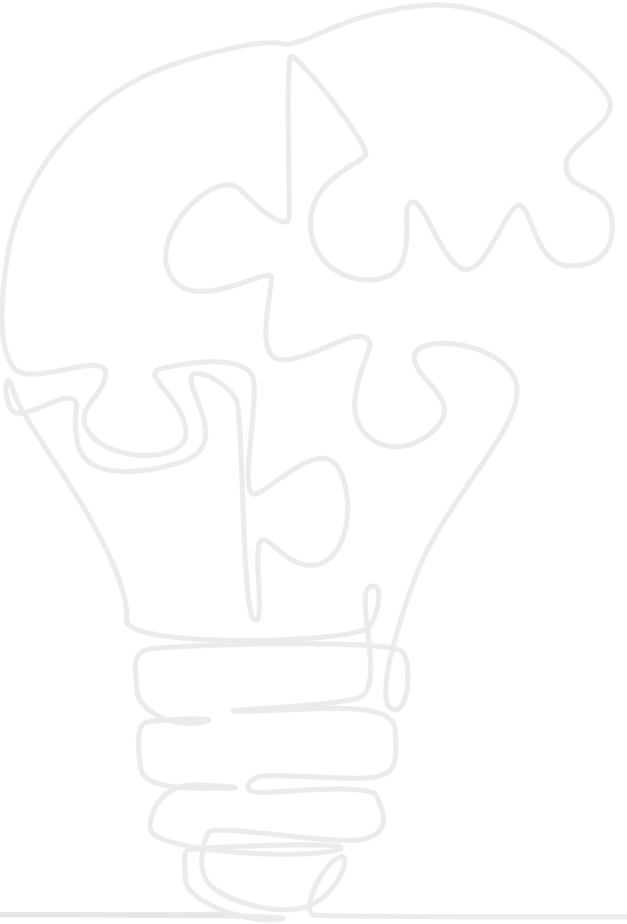
Capability Brief

Nisos Intelligence Database (NID)

Curated Collection of Difficult-to-Access and Sensitive Data from the Open, Deep, and Dark Web to Enable Actionable Intelligence for Nisos Operators

Nisos enhances security programs by collecting and operationalizing data from various sources to inform cyber security operations, improve defenses, disrupt attacks, and stop adversaries.

Nisos draws upon its lawfully-obtained collection of sensitive and difficult-to-access datasets, including breach data compilations and dark web hacked data.



Aggregating Open Source Data

Our recommendations are informed by the footprint of data that exists in the open, deep and dark web that internal security teams may not have the operating protocols, appetite, or sophistication to safely navigate. Common data sources within the Nisos Intelligence Data Set include hard targets, such as:

- Russia
- China
- Iran
- India
- Ukraine
- Turkey
- Qatar
- Georgia
- Mexico
- Nigeria
- Bulgaria
- ...and more

We Collect and Leverage Data From:

Hard target government personnel records, customs data, vehicle, and driver records

Foreign and extremist social media data

Credential pairs, emails, passwords, phone numbers, and other sources of PII tied to data breaches

Foreign bank data, credit records, business registration data, and flight manifests

Foreign phone and internet usage records

Foreign legal and business documents

Our Approach

STEP 1: COLLECT

When breached or leaked data sets become available on the deep, dark, and open web, Nisos operators engage with data brokers who have access to that information and lawfully obtain that data to enhance the NID. In addition, we take client specific information (like domains) and query public datasets of known breaches, identifying and acquiring additional data sets relevant to our clients.

Bringing these datasets to Nisos' protected servers has several advantages; as we are able to control ETL and other enrichment actions to deliver data in an easy-to-use interface that ensures scalability and maximum use by Nisos operators. This allows us to research while not leaving a digital trail of input search terms on unverified sites.

STEP 2: VERIFY

Nisos evaluates the authenticity and accuracy of the acquired dataset. The longer a dataset has been public prior to collection increases the possibility the data may have been manipulated or corrupted. For example, we have observed datasets that have been edited; PII no longer correlating to the correct username or password. We also engage with online data brokers who may have original copies.

After we conduct an initial triage to determine the dataset's authenticity, we search password hashes against publicly available hash databases. We then run the remaining hashes not found in those databases through an internal cracking rig with a 60-70% rate of cracking success.

STEP 3: ANALYZE

Data must be analyzed for structure before it can be extracted for enrichment. Structures vary from CSV, SQL dump, JSON, to raw text. Sometimes files need to be broken into different segments depending on the schema and format of the file collected (mixed CSV, SQL, JSON, Postgres, PDF, etc.). It is critical to standardize data structure to maximize its utility.

STEP 4: ENRICH

We utilize entity recognition to identify enrichable selectors, such as phone numbers and email addresses. We then cross reference these selectors against a variety of subscription datasets and our internal platform to validate or add additional data points. Data points can include name, address, carrier or ID to the associated email or phone number. We also conduct email and username correlations to social media platform look-ups to identify potential username reuse. Password reset analysis is also used to retrieve additional metadata and provide confirmation of associated accounts with the corresponding phone numbers/email addresses.

STEP 5: SEARCH

After enrichment, Nisos operators extract, transform, and load data into a queryable format for searches, including advanced wildcard searches (querying on partial email address, phone number, etc). Further, we apply automation scripts to provide candidates for fragmented selectors . Results automatically return from the datasets that have high confidence matches to the fragmented selector. We use this information to notify clients about breach credentials and provide clues for attribution.

STEP 6: CROSS REFERENCE

Many times during investigations, we cross reference the several data sets to bring additional context with leads derived from the Nisos Intelligence Data. These data sets include:

Network & Telephony

- Anonymous Infrastructure
- DNS and WHOIS
- Internet Netflow (90%+ of IPV4)
- Mobile and IP Geolocation
- Threat Feeds

Web & Social

- Deep and Dark Web
- Foreign Media
- Historical Web Content
- Open Web
- Social Media

Human

- Closed Forum
- Deep and Dark Web

Media

- Domestic News
- Foreign Media

Adversaries

- Activist
- Disinformation
- E-Crime
- Nation State
- Political

Breach

- 20+ billion records of legally acquired datasets including PII, selectors, and information/credentials

Businesses

- Business Registrations
- Corporate Filings
- Corporate Profiles
- Public Records

Persons & Groups

- Biographical
- Civil and Criminal Actions
- Email and Identity
- Investigative Databases
- Public Records

Our Differentiator

Nisos is able to deliver insights other threat intelligence and cybersecurity services cannot because of our access to secure and protected information. Using sensitive data sets would not be possible without close coordination with legal counsel. We operate under strict guidelines regarding the collection, maintenance, and use of the intelligence gathered.

While these datasets may reside on open, deep, or dark web locations, once we become the custodians of these datasets, we safely and securely store and utilize the data to help our clients understand threats, exposure, and potential attribution.

Nisos can help enhance your security program with lawfully-obtained data so that you can improve your security posture and take action against sophisticated adversaries.