DARKINT Exposure Scores in DarkOwl Vision

DARKINT Exposure tracks your organization's DARKINT score over time, based on the quantity, quality, and freshness of exposed data. Scores are generated with privacy-compliant data points, requiring only a website and email domain to calculate. Increasing scores may correlate to heightened risk profiles. Tracking scores over time, changes can indicate progress in hardening security, or alert to the presence of breaches or data leaks.

DarkOwl Vision provides the world's largest commercially-available DARKINT data collection, and the tools and services to efficiently find leaked or otherwise compromised sensitive data. Short for darknet intelligence, DARKINT encompasses actionable data from the darknet (Tor, I2P, Zeronet) and other interconnected sources (paste sites, IRC channels, ftp servers, etc).

How the DARKINT Score is Calculated

The algorithm focuses on specific DARKINT sources for unique matches on an organization's website and email domains, and adjust the results based on hackishness. Hackishness is the most critical input to the score, as it eliminates uninteresting content hits. We find it critical to differentiate between overall hits and hackish hits; simply because a piece of information is found on the darknet does not necessarily make it problematic to an organization.

- A Hackishness rating is assigned by DarkOwl Vision to every piece of content collected from the darknet, and represents how likely content could be used for criminal activity. It is based on a machine learning algorithm that considers over 100 different variables, such as patterns, metadata, or terms.

Recent results within the last 90 days are given the most weight, as recent breaches or data leaks containing an organization's proprietary information are often more useful to hackers, and potentially haven't yet been mitigated. *Note: Scores are logarithmic, meaning every point reflects almost triple the profile of a single point less.*

$$\textbf{DARKINT SCORE} = H_{90}(\ln RDS + \ln RTS) + H_{ATR}(\ln ATR)$$

- H90 = Hackishness of last 90 days results
- HATR = Hackishness of all time Data Leak results
- RDS = # results from Darknet Sites
- RTS = # results from Transitory Sites
- ATR = # results from all time Data Leak results

Viewing Scores Over Time

DARKINT scores are the first metric to measure an organization based purely on dark web intelligence. Increasing scores may correlate to heightened risk profiles.

Tracking scores over time, changes can indicate progress in hardening security, or alert to the presence of breaches or data leaks.

Scores Are:	Scores Are Not:
A point-in-time snapshot An assessment of hackish data accessible	A "risk of breach" Indicative of all risks facing an organization

Using DARKINT Exposure Scores in the UI

At initial set up in the DarkOwl Vision User Interface, scores will be generated for the previous month, and going forward, will continue to generate weekly.

Click into each score to:

- Generate a PDF an Exposure Score Report for the latest score.
- Download a CSV of all the scores and inputs that were generated overall all time.
- Click the seach buttons below Domains or Email Domains *to see the underlying results that generated the score*.