DATASHEET

DARK WEB MONITORING

HIGHLIGHTS

- **Risk-focussed approach to monitoring the dark web**
- **Gain instant access to hundreds of millions of indexed pages**
- **Our dedicated team of closed source analysts constantly add coverage**
- **Identify exposed credentials, fraud, insider threats, and coupon fraud**
- **Track threat actors and their campaigns**
- **Save searches, pivot on observables, and export results**

digital shadows_

DARK WEB MONITORING

The visibility needed to detect fraud and track threat actors.

The dark web is a mysterious unknown for many organizations. Unfortunately, gaining visibility into these locations is extemely challenging - it requires a knowledge of the criminal underground, logins to underground sites, and technology that's capable of monitoring these sources.

SearchLight monitors across sources where criminals are active, no matter is that is on the open, deep, or dark web. This includes continually monitoring and indexing hundreds of millions of dark web pages, pastes, criminal forums, Telegram, IRC, and I2P pages. In addition to our technology, our closed sources team works to gain new access, develop personas, build trust, and produce intelligence reports on the latest cybercriminal trends.

Even with great coverage, it's often challenging for organizations to get value from dark web sources; it's often noisy and irrelevant. That's why SearchLight looks for specific risks to your organization across the open, deep and dark web; automatically alerting you to exposed credentials and other forms of exposed data. Our team will also provide you with analysis of the latest trends in these criminal locations.

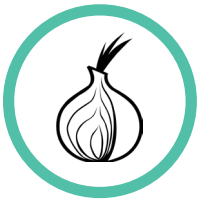
For organizations with the time and resources to conduct further research, Shadow Search provides a powerful way to search across our indexed data to track threat actors, campaigns, and identify instances of fraud.

>150M

Criminal forums and dark web pages indexed by SearchLight

SOURCE COVERAGE

The dark web is an area of the web that is only accessible with specific software, such as Tor and I2P. The increased anonymity offered by this software makes the dark web an attractive place for criminals to conduct business. The deep web can be broadly defined as anything that is not indexed by traditional search engines, and includes the dark web. Unsurprisingly, criminals also operate on the deep web,on protected forums and closed sites (indeed this is more common). To provide a comprehensive view of these locations, we continually monitor the following sources with our proprietary technology, adding approximately 1,000,000 new pages every week.



Dark web pages

Our proprietary spider crawls Tor and I2P pages, identifying new content, and sources of value.

Approximately 50 million indexed Tor and I2P pages

IRC and Telegram channels

Our technology montiors services used by groups and individuals to chat on themes ranging from threat campaigns, fraud, tactics and techniques, and technical topics.

Approximately 30 million conversations

Criminal forums

We have focused, automated custom collection on high-value forums where we identify a wide variety of activity - from exploit kits to the sale of breached data. Some of these are hosted on Tor or I2P, but many are not. Our closed sources team provide the direction and persona development to gain access to new forums.

More than 20 million indexed forums.

Paste sites

Another sources that isn't strictly limited to the dark web - there are many types of paste sites that exist across the surface and dark web. Malicious actors use these sites to share breached data and create target lists.

More than 50 million indexed pastes.

Dark web marketplaces

Specific collection for marketplaces hosted on the dark web. While marketplaces have decreased in popularity since the demise of AlphaBay and Hansa, several are still active. Previous listing can be useful as historical sources for tracking threat actors.

Approximately 1 million indexed marketplace listings.

DETECT DATA LEAKAGE, FRAUD, AND RELEVANT THREATS

Exposed Data

SearchLight detects your exposed data online when it surfaces on the dark web. This includes detecting when payment cards are traded on IRC channels, source code is offered for sales on a criminal forum, or other types of data exposure.

Counterfeits

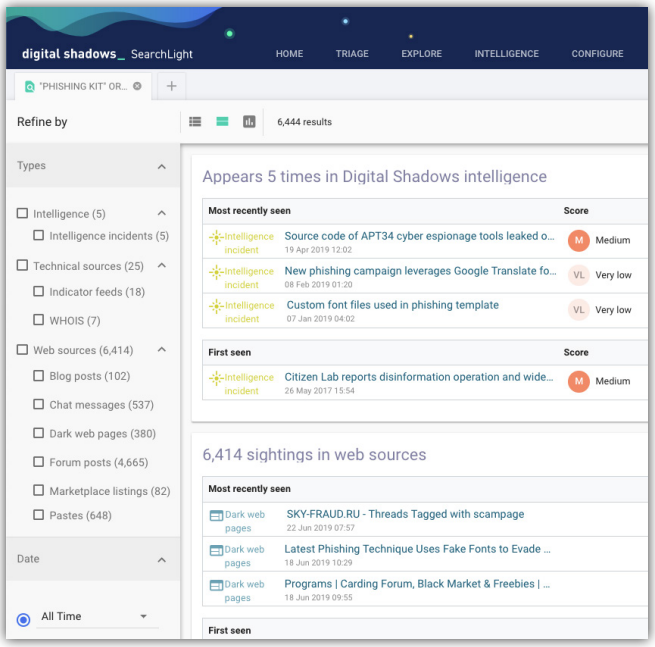
The deep and dark web have empowered the counterfeit trade - currency, coupons, vehicles, drugs, jewelry, and other knock-offs are sold on criminal locations at cheap prices. Digital Shadows identifies your products and assets being sold on these criminal locations, so you can remediate those threats before your reputation is damaged.

Detect Insider Threats

From sim-swapping to banking portal access, insiders with valuable data or privileged access are using online forums and marketplaces to find buyers, and recruit insiders from a variety of industries. Many of these criminal forums are located on the clear web, which serves as a reminder that we shouldn't hyper focus on dark web sources alone.

Investigate Tools

Attackers share and exchange a wide range of tools across the criminal underground, including phishing kits. Phishing kits are used by attackers to create a identical copies of legitimate websites that entice victims into sharing their sensitive data.



TRY FOR FREE WITHIN SEARCHLIGHT

About Digital Shadows

Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threats. Organizations can suffer regulatory fines, loss of intellectual property, and reputational damage when digital risk is left unmanaged. Digital Shadows SearchLight™ helps you minimize these risks by detecting data loss, securing your online brand, and reducing your attack surface. To learn more and get free access to SearchLight, visit www.digitalshadows.com.

digital shadows_