DARK WEB MONITORING

A Scary Place For Scary People

The dark web is filled with stolen intellectual property, PII, PHI, and leaked credentials. As a haven for criminal activity, it's highly utilized for cybercrime but, unfortunately, it's also well protected.

In reality, the dark web is difficult, even for security professionals, to traverse. Shrouded in secrecy, operating on referral networks, and paid access, even getting to the *real* auctions and forums isn't easy. We have you covered.

Your New Dark Web Data Team

Here's a breakdown of the collection tools and monitoring team and reporting:

Criminal Intelligence Team (CIT)

Fluent in over 35 languages, including many Eastern European dialects, our CIT has infiltrated and scraped a massive collection of data from both the dark and surface (Internet) webs.

Threat Intelligence Platform (TIP)

From the efforts of our CIT, we have amassed a large (and quickly searchable) data lake that is continually collecting new data from known black market sites, auctions, forums, and real-time messaging services used by threat actors for communications.

Reporting

Be in-the-know with custom reporting from this service. Real-time alerting of data breaches can also be enabled for your organization and executives. Think Google Alerts for the dark web.

What we look for:

Initial Access Brokers (IABs)

Sell compromised credentials of an organization.

Data Dumps

Exfiltrated data usually makes its way to breach sites for sale.

Executive Alerting

Monitors the dark web and breach sites for keywords relating your executive leadership team.

Get Started

Ready to see what's out there? Contact us today for a quick consultation and list of monitoring options.

info@sevnx.com

484.989.0911

ACHIEVE BETTER CYBERSECURITY