DARKWEB ID

Dark Web ID Product Overview

Dark Web ID monitors, aggregates and alerts non-stop – 24/7, 365 days a year scouring millions of sources including botnets, criminal chat rooms, peer-to-peer networks, malicious websites and blogs, bulletin boards, illegal black market sites as well as private and public networks and forums.

Internally Managed or Fully Outsourced Monitoring & Alerting Service

Dark Web ID Monitoring & Alerting solutions provide:

- Dark Web Threat Alerting: Proactive and automated monitoring for your organizations stolen or compromised data and alerting you when data is discovered.
- Compromised Data Tracking, Incident Response Workflow & Reporting: Track and triage incidents and better manage risk within logging and reporting capabilities.
- Holistic Threat Intelligence Program Development.
- Compromised Data Trending & Peer/ Industry Benchmarking: Gain insight into your organization's current threat posture while benchmarking it against your peers and the industries that you serve.
- HR and Policy Enforcement - Cyber Education & Awareness.
- Targeted Individual and Repeat Offender Monitoring.

How We Monitor the Dark Web

We monitor the following 24/7, 365 days a year:

- Hidden Criminal Chat Rooms
- Private Websites
- Peer-to-Peer Networks
- IRC (Internet Relay Chat) Channels
- Social Media Platforms
- Black Market Sites
- 640,000+ botnets

We identify your data as it accesses criminal command-and-control servers from multiple geographies that national IP addresses cannot access.

On average, we identify and report on more than 1 million compromised IP addresses and more than 80,000 compromised emails every day.

How to Use the Actionable Intelligence Dark Web ID Provides

Internal Operations & Management

- Holistic Threat Intelligence Program Development
- Proactive & Automated Security Management
- High Value Target (HVT) Monitoring
- Targeted Individual and Repeat Offender Monitoring
- Reduce Incident Response Times
- Policy Enforcement
- Cyber Education & Awareness

Supply Chain Management

- Identify trends and potential exposure points within your supply chain
- Share threat intelligence and support corporate supply chain management and security policies

Industry Benchmarking

- Understand how your organization's threat posture compares to your industry peers and competitors

Cyber Liability Insurance

- Demonstrate a comprehensive approach to loss prevention and educate through the deployment of external security monitoring services

Manage Third Party Risk & Exposure

Better identify and mitigate your potential exposure to security incidents and data breaches originating within your supply chain, vendor, partner and customer community.

Security Threat Alerts: Identify which companies are most vulnerable to security incidents within your Supply Chain and implement applicable security precautions.

Supply Chain Cyber Policy Enforcement: Share threat intelligence and enforce stricter cyber practices within the organizations that support your operations or you do business with.

Customer Management: Better serve your customer's security posture by identifying and reporting on compromised data than can lead to unwanted access to their networks, intellectual property and potential data breaches.