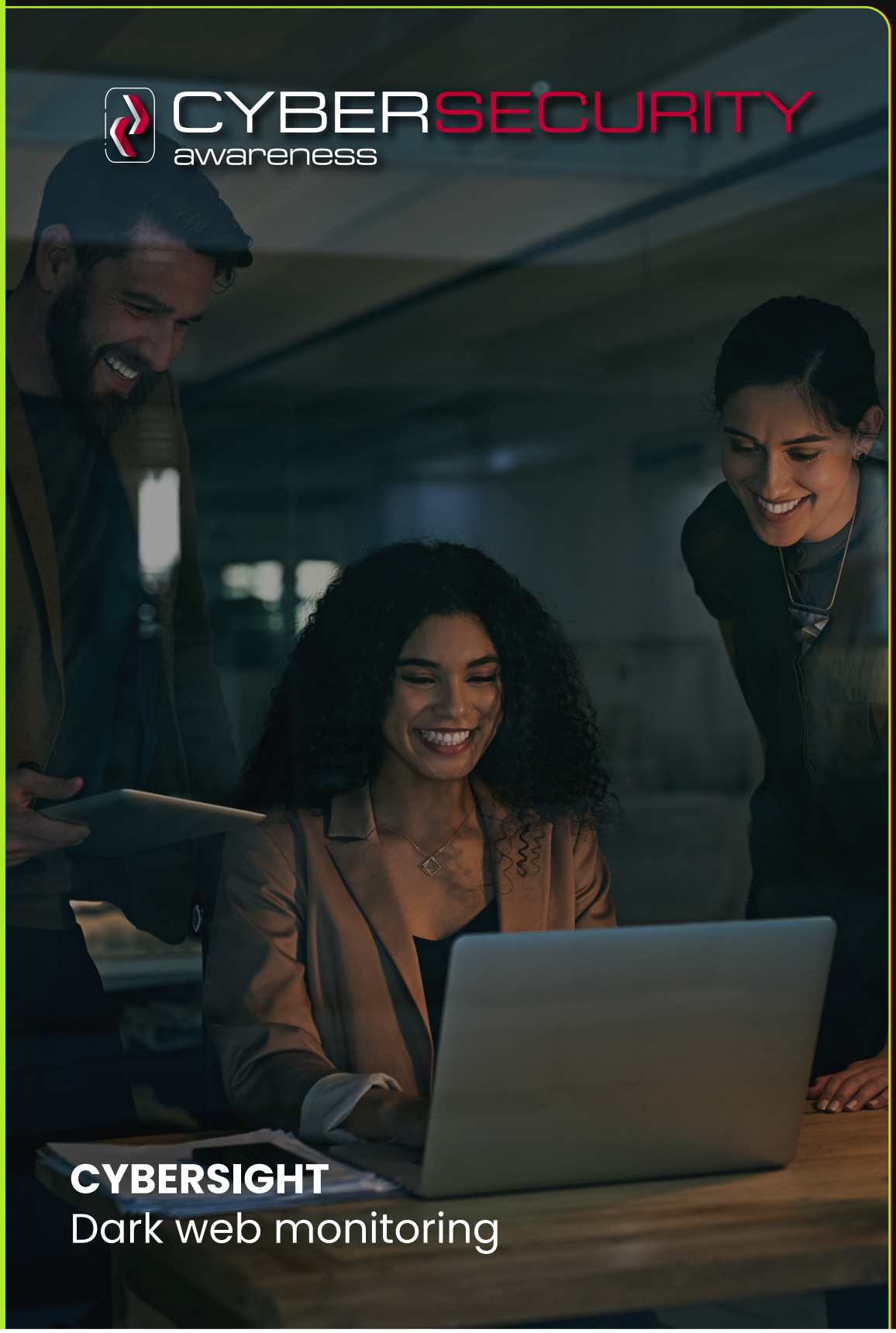


How many of your organisation's credentials have already been compromised?

Our leading CyberSIGHT dark web monitoring service will report your historical breaches, but most importantly will alert you to new breaches when they happen so you can prevent costly cyber attacks.

A Dark and Dangerous Place

The Dark Web is made up of digital communities that sit on top of the Internet, and while there are legitimate purposes to the Dark Web, it is estimated that over 50% of all sites on the Dark Web are used for criminal activities, including the disclosure and sale of digital credentials.

Far too often, companies that have had their credentials compromised and sold on the Dark Web but don't know about it. Stolen credentials lead to costly data breaches and enable cyber attacks.

81%

of hacking-related breaches leverage either stolen and/or weak passwords.

How does this happen?

When sites and online services used by your employees experience a data breach, your business credentials including usernames and passwords are leaked, obtained by cybercriminals, and made readily available on the Dark Web.

Even your employees being breached on personal sites can significantly damage your organisation because all employees typically use the same usernames and passwords across both personal and work sites and applications.

47%

of people say that they use the same usernames and passwords across multiple sites and applications.

Protect your organisation

By utilising CyberSIGHT, a combination of human and sophisticated Dark Web intelligence with search capabilities, you are able to identify, analyse and proactively monitor for your organisation's compromised employee and customer data.

Using our recommendations and advice, you are able to remediate security gaps and weak points around credential breaches.

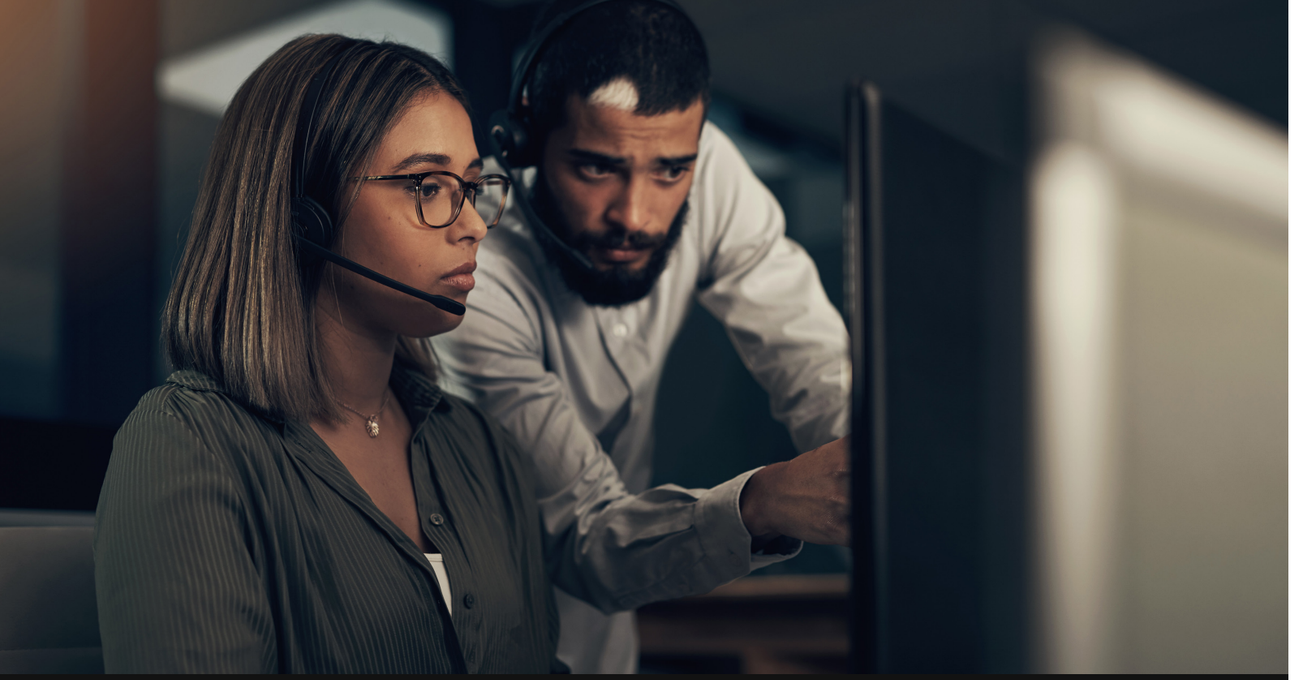
How it works

Prevent
Receive breach alerts, monthly reports and ongoinging remediation asice to significantly reduce the risk of breach from stolen credential within your organisation.

Report
Receive full reports on your corporate domains, breaking down which e-mail accounts have had credential breached, the source of the breach, what passwords were stolen and any PII that has been lost.

Monitor
Receive 24/7 monitoring on your coporate domains to find any credential breaches. CyberSight spots indursty patterns long beofre they become trends.

Remediate
Advise employees who have had credentials breached to update their passwords to critical buisness sites and applications. Review your existing infrastructure for Multi-factor authentication, password managers and staff awareness.



Key Benefits of CyberSIGHT

- Stay on top of your Dark Web exposure
- Free Dark Web scan to get started
- Breach Alerts
- Monthly Reports
- 24 x 7 | 365 Assurance
- Breach Location/Source
- Lost Passwords and PII
- Executive Monitoring

Why choose us?

- Fully Managed Service
- Very Low Cost
- Assured Remediation Advice
- Industry Experience

CyberSight - FAQs

What is the Dark Web?
The Dark Web is a hidden universe contained within the “Deep Web”- a sublayer of the Internet that is hidden from conventional search engines. Search engines like Google, BING and Yahoo only search .04% of the indexed or “surface” Internet. The other 99.96% of the Web consists of databases, private academic and government networks, and the Dark Web.

The Dark Web is estimated at 550 times larger than the surface Web and growing. Because you can operate anonymously, the Dark Web holds a wealth of stolen data and illegal activity.

How are the stolen or exposed credentials found on the dark web?
CyberSIGHT focuses on cyber threats that are specific to our clients’ environments. We monitor the Dark Web and the criminal hacker underground for exposure of our clients’ credentials to malicious individuals. We accomplish this by looking specifically for our clients’ top level email domains. When a credential is identified, we harvest it.

While we harvest data from typical hacker sites like Pastebin, a lot of our data originates from sites that require credibility or a membership within the hacker community to enter. To that end, we monitor over 500 distinct Internet relay chatroom (IRC) channels, 600,000 private Websites, 600 twitter feeds, and execute 10,000 refined queries daily.

Where do we find data?

- **Dark Web Chatroom:** compromised data discovered in a hidden IRC;
- **Hacking Site:** compromised data exposed on a hacked Website or data dump site;
- **Hidden Theft Forum:** compromised data published within a hacking forum or community;
- **P2P File Leak:** compromised data leaked from a Peer-to-Peer file sharing program or network;
- **Social Media Post:** compromised data posted on a social media platform;
- **C2 Server/Malware:** compromised data harvested through botnets or on a command and control (C2) server.

FAQs

How was the data stolen or compromised?

- Tested: the compromised data was tested to determine if it is live/active;
- Sample: the compromised data was posted to prove its validity;
- Keylogged or Phished: the compromised data was entered into a fictitious website or extracted through software designed to steal PII;
- 3rd Party Breach: the compromised data was exposed as part of a company's internal data breach or on a 3rd party Website;
- Accidental Exposure: the compromised data was accidentally shared on a Web, social media, or Peer- to-Peer site;
- Malicious / Doxed: the compromised data was intentionally broadcast to expose PII.

How does CyberSIGHT help protect my organisation?
Our service is designed to help both public and private sector organisations detect and mitigate cyber threats that leverage stolen email addresses and passwords.

CyberSIGHT leverages a combination of human and artificial intelligence that scours botnets, criminal chat rooms, blogs, websites and bulletin boards, Peer to Peer networks, forums, private networks, and other blackmarket sites 24/7, 365 days a year to identify stolen credentials and other personally identifiable information (PII).

Does the Identification of my Organisations Exposed Credentials mean that we are being Targeted by Hackers?
While we can't say definitively that the data we've discovered has already been used to exploit your organisation, the fact that we are able to identify this data should be very concerning.

Organisations should consult their internal or external IT and/or security teams to determine if they have suffered a cyber incident or data breach.

Get in touch

sales@cybersecurityawareness.co.uk

01256 379977

cybersecurityawareness.co.uk