BlueVoyant

CREDENTIAL WATCHER™

THREAT ACTORS ARE HUNTING FOR YOUR FIRM'S USERNAMES, EMAILS, AND PASSWORDS ON THE DEEP AND DARK WEB - AND THEY ARE USING WHAT THEY FIND TO BREACH YOUR DEFENSES

BlueVoyant Credential Watcher limits your exposure to this attack vector helping to minimize the potential for a breach.

The "Deep Web" is the portion of the Internet that exists in places that cannot be accessed by traditional search engines. The "Dark Web" is any web-like network that uses proprietary protocols or requires special software to access. Threat Actors routinely search for your employees' usernames and passwords in these environments in an attempt to use that information to compromise and breach your organization.

Employees that reuse passwords in their personal and professional lives pose an increased risk. If that password and individual have been compromised elsewhere, this data can be easily exploited by threat actors within your network.

BlueVoyant helps to reduce this risk by informing our clients when we see exposed credentials. This encourages and reinforces better password management procedures and in turn helps to avoid breaches.

BlueVoyant

CREDENTIAL WATCHER™

KEY CAPABILITIES

EXPOSURE BASELINE

At the outset of our engagement, BlueVoyant will prepare a baseline report that details all exposed credentials related to your corporate email domains. Many firms assume that their existing password reset policies are sufficient for protecting their organization. It is our experience that this is not true, which is why we always revalidate baseline accounts. Without revalidation, overhang exposure risks will continue from noncompliant users. BlueVoyant provides IT with the data needed to perform checks that ensure no compromised passwords remain in use.

MONTHLY EXPOSURE UPDATE

BlueVoyant's data breach monitoring team will continue to collect additional data and perform analytics to determine if there are additional account credentials exposed. The monthly update report will include a list of all newly known accounts that have been compromised.

AD HOC ALERTS

In the event BlueVoyant discovers a major data breach that impacts your firm, an ad hoc alert will be issued before the monthly report to ensure that your firm is aware of the exposure and can take the appropriate immediate actions, such as password resets and account lockouts.

ABOUT BLUEVOYANT

BlueVoyant is an analytic-driven cybersecurity company whose mission is to protect organizations of all sizes against agile and well-financed cyber attackers. Founded and led by experts in the cyber security and government security sectors, BlueVoyant's offerings are built with real-world insight and applicability, plus an eye on the threat horizon.

Through our Advanced Threat Intelligence, Managed Security Services, and Incident Response Services, we excel in intelligence gathering, cyber security defense, detection of attacks and response coupled with remediation.

Our SOCs around the world keep us on top of developing and established threat actors and the well-financed tools they are developing to out-smart traditional security measures. Our 24/7 SOCs, offices around the world, and our security analytics platform position us to best help our customers defend against emerging cyber threats.

Discover the BlueVoyant Difference
Visit www.bluevoyant.com
Follow us on linkedin.com/company/bluevoyant
Secure your business now, contact@bluevoyant.com