SOLUTION BRIEF

Executive Cyber Guard

Protection for Your Most Valuable Asset

In today's digital age, the ability of attackers to execute cyber attacks against a specific individual has never been easier. With phishing attacks and social engineering on the rise, almost everyone is susceptible to be targeted by an attacker.

40%

Corporate executives are among the most marked targets by hackers. In a recent study, 40% of global organizations cited their c-level executives, including the CEO, as their highest cybersecurity risk.

This can be attributed to a number of reasons:

- C-level execs own or have access to sensitive information that can be sold on the dark web and/or cause harm to the company.
- Harming a manager can lead to damage to a brand's good name, and thus cause financial damage to the organization and the manager himself.

More than ever before, the need for executive cyber protection is relevant for every company.

BlueVoyant Executive Cyber Guard helps defend against attacks targeting your executives by providing the necessary intelligence required in order to be protected in the digital age.

BlueVoyant utilizes a combination of public and proprietary data sources to monitor threat actor activity in real-time 24/7, delivering the best executive protection and unlimited removal of digital threats.

PROTECTION: IDENTIFY AND REMOVE THREATS

BlueVoyant's automated platform detects visual impersonation of the target. This platform identifies fake accounts on social media platforms using advanced algorithms with real-time monitoring of accounts. In addition, expert analysts conduct in-depth research that characterizes the digital signature of the target and enables better tracing and detection of additional accounts.

All findings are outlined in a detailed, timely report, as well as through near real-time alerts about real threats that are sent via email.

Depending on the client's services, the threats can be eliminated using the BlueVoyant 24/7 Active Unlimited Digital Takedown Service, effectively removing the fake accounts from all social networks, or simply identified for internal remediation.

PREVENTION OF FUTURE CYBER ATTACKS

Prevent future cyberattacks against your executives and the organization while identifying potential damages by detecting information leakage.

BlueVoyant provides unique threat intelligence that includes the detection of data leaks of any kind that may harm the executives or the organization, information from executives' digital accounts

that could pose a potential attack vector, and any leaks of sensitive information such as credentials, targeted personal information, and more.

BlueVoyant analysts help organizations look at executives from a cyber attacker's perspective, to allow organizations to identify upfront potential threats and cyber attack vectors ahead of the actual attack on the organization and its executives.

RECOMMENDATIONS FOR SAFER CONDUCT

Depending on your executives' personal conduct and report findings, BlueVoyant can provide practical assistance in the proper and safer management of the digital world with written recommendations that are also included in the timely report.

YOUR PEOPLE ARE YOUR GREATEST ASSET.

Locating the information necessary to target high profile individuals, their families, and their staff has never been easier. How confident are you in their protection? Ask yourself these questions to gauge your level of executive security:

Can you identify and manage threats from all the attack vectors currently available against your organization and executives?

Threat actors are continuously developing innovative and sophisticated methods of attack, and are even extending their attacks to their targets' first and second circles

of friends and colleagues in order to gain access to the original target.

Do you have the right security in place to protect your organization?

The current global median dwell time for cyber intrusion is 56 days. In order to protect an organization, it is not enough to detect an attack at the time of occurrence, as there is a great chance that the organization is already compromised. BlueVoyant analysts help organizations look at executives from a cyber attacker's perspective, to allow organizations to identify upfront potential threats and cyber attack vectors ahead of the actual attack on the organization and its executives.

About BlueVoyant

BlueVoyant is an expert-driven cybersecurity services company whose mission is to proactively defend organizations of all sizes against today's constant, sophisticated attackers and advanced threats.

Led by CEO Jim Rosenthal, BlueVoyant's highly skilled team includes former government cyber officials with extensive frontline experience in responding to advanced cyber threats on behalf of the National Security Agency, Federal Bureau of Investigation, Unit 8200 and GCHQ, together with private sector experts. BlueVoyant services utilize large real-time datasets with industry-leading analytics and technologies.

Founded in 2017 by Fortune 500 executives and former Government cyber officials and headquartered in New York City, BlueVoyant has offices in Maryland, Tel Aviv, San Francisco, London, and Latin America.

BlueVoyant®

To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**