BlueVoyant

EXTERNAL THREAT HUNTING

PROACTIVE IDENTIFICATION OF THREATS OUTSIDE OF YOUR PERIMETER

Organizations concerned about cybersecurity understand that they need to be ardent when it comes to identifying and mitigating threats. As a result, they are investing in data sources, tools, and people.

Unfortunately, these defenses are often focused either on events inside the perimeter, or are passive in nature, which can mean that emerging threats, such as large scale malware campaigns and attacks targeting a specific organization, its leadership and employees, or its vendor ecosystem can go undetected.

BlueVoyant can help. Using an unparalleled combination of data, analytics, and skilled staff, BlueVoyant is capable of identifying both general and specific external threats, providing organizations with the type of early warnings that can help dramatically improve cybersecurity.

METHODOLOGY

BlueVoyant has developed a business-driven methodology for external threat identification that produces actionable results:

Risk-Based Intelligence Strategy: we work with our clients to identify key areas where external threats could negatively impact their business, taking into account geographic, sector-specific, and client-specific information.

Data Curation: we implement the agreed threat hunting strategy by proactively accessing and feeding various data (including data from the dark, deep, and open web) into our threat hunting platform.

Identification of Threats: data from our global sources is processed and correlated automatically and threat indicators are reviewed and rated by our experienced analysts.

Severity-Based Triage: where identified threats require additional information, our analysts will expand the threat hunting strategy or proactively expand sources coverage, providing organizations with the right context.

CAPABILITIES

- Full external threat identification capabilities covering people, sources, and technology.
- Strategic threat discovery, focusing on generating actionable and tailored intelligence based on specific business needs.
- Access to open, deep, and dark web, including instant messaging.
- Ability to uncover “below the surface” threats through untraceable proactive interactions with threat actors.
- Access to global data for detecting indications of compromise.
- Expertise in a variety of use cases including: data leakage, payment fraud, online fraud, vulnerabilities prioritization, identity theft, insiders, and phishing.
- Dedicated analyst and quick response to RFIs
- Web portal for day-to-day findings and communications.

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, cybersecurity 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 positions us to best help our customers defend against emerging cyber threats.

Discover the BlueVoyant Difference

www.bluevoyant.com | contact@bluevoyant.com

07222019