Vulnerability Management Services

BlueVoyant

BlueVoyant

INTRODUCTION

"The latest industry reports estimate that 92 percent of attacks originate from spear-phishing, where employees unwittingly click on malicious malware. No company is immune from a smart threat actor with spoofing capabilities, but BlueVoyant helps reduce your risk of cyber attack and is here to remediate attacks that have already occurred through our layered security protection products and services."

Milan Patel, Chief Client Officer

OUR SERVICES

Threat Intelligence

Managed Security Services

Professional Services

About BlueVoyant

A first-things-first cybersecurity company focused on delivering best-of-breed technology and outstanding customer service to businesses around the world. We believe in the democratization of cybersecurity - offering robust solutions and tools to businesses previously ignored and underserved. Through our advanced Threat Intelligence, Managed Security Services, and Incident Response services, we excel in intelligence gathering, cybersecurity defense, and detection of attacks with response coupled with remediation. With global SOCs, we are prepared to protect the world over from well-financed threat actors and their newest tools of attack. Learn more at www.bluevoyant.com

BlueVoyant

Vulnerability Management Services

Democratized Cybersecurity

BlueVoyant Vulnerability Management Service (VMS) delivers vulnerability assessments of your environment to let you know where there are weaknesses that threat actors could potentially exploit.

From missing updates and patches to software bugs and operating design flaws, weaknesses in your system leave you open to possible risk. BlueVoyant VMS offers automated, recurring vulnerability scanning utilizing the BlueVoyant technology platform in conjunction with a team of elite, highly-certified security analysts to help you catalogue and prioritize vulnerabilities within your system.

BlueVoyant accomplishes this by installing a software appliance on your endpoints in order to perform the vulnerability assessments.

VMS is an additional layer of protection that we offer to current BlueVoyant Managed Security Services clients. Your vulnerability assessments will inform and improve the quality of your current BlueVoyant service protection.

We offer three tiers of the VMS service exclusively to our MDR+, DaaS℠ and Managed SIEM clients: Vulnerability Import, Internal Scanning, and Full Service Scanning.

Vulnerability Import, the first service tier, works with you to enable the automatic import of vulnerabilities into the BlueVoyant platform utilizing support third-party vendor assessment software. Vulnerabilities will be visible to the expert analysts in the Security Operations Center.

Internal Scanning, our second tier, expands upon the first tier by deploying the BlueVoyant Virtual Appliances and conducting vulnerability assessments and asset discovery internally in your environment.

Full VMS, our third and most comprehensive tier, combines all the service features and most notably adds external scanning.

Wavelength™, the BlueVoyant client portal gives you visibility into your network vulnerabilities and allows you to track them and generate reports. It is a feature of all three tiers of service.

Failure to patch a vulnerability discovered in March allowed attackers to access **143 Million** Equifax customer records in May, 2017.

Equifax Officially Has No Excuse Wired Magazine 9-14-2017

SERVICE OVERVIEW

Vulnerability Assessment: VMS works to perform a variety of vulnerability assessments utilizing best-of-breed vulnerability detection software to discover well known weaknesses in software. It provides recommendations for managing or resolving the vulnerabilities through Wavelength™, the BlueVoyant client portal, and custom reports.

Scanning: Scans will be conducted on a regular basis at weekly, monthly, or quarterly intervals. External scanning includes the detection of vulnerabilities that are exposed beyond your network perimeter and are therefore visible and possibly exploitable by attackers. Internal scanning includes vulnerabilities within your organization that may not be externally facing but could be exploitable by attackers within the environment. BlueVoyant can also conduct on-demand vulnerability scans on a need basis.

Assets: Asset Discovery: as part of the service, you can request BlueVoyant to conduct regular asset scanning to identify new devices in the environment or to update any identifying information on previously detected assets such as hostname or IP address. Asset Prioritization: Through the Wavelength™ , the BlueVoyant Portal, you can assign criticality to asset records to indicate which assets are most important in the environment. Asset Tagging: Through Wavelength™ you can apply “tags” to asset records. This enables grouping of assets to support dashboards and reports.

Vulnerability Verification: By comparing new vulnerability scan results against previously identified vulnerabilities our experts determine which vulnerabilities have been appropriately remediated. Vulnerabilities remain in an active state within the client portal until a vulnerability scan occurs, rather than when a patch or upgrade was applied, in order to confirm any remediations.

Policy Selection: As part of Service Activation, BlueVoyant staff will work with you to understand what your compliance and risk goals are to help you select one of the approximate twenty (20) vulnerability scan policies.

Vulnerability Tracking: Through Wavelength™, you are able to see all active vulnerabilities that have been detected. These vulnerabilities are mapped to asset records which are mapped to any security alerts or incidents (detected through other BlueVoyant Managed Security Services) to support traceability of the activity of assets and vulnerabilities.

Software Upgrades: As software patches, upgrades, and new vulnerability signatures are released for the supporting vulnerability assessment software BlueVoyant will assess the release for security, stability, and functionality before certifying it as a supported version. BlueVoyant will perform software upgrades automatically for deployments leveraging the BlueVoyant virtual appliance.

FEATURES

Vulnerability Management Services are supported by expert analysts who operate 24/7 across multiple locations and within 2 global Security Operations Centers (SOCs). Certifications held by the team include SANS GIAC, EC-Council, and ISC-2, as well as others.

Wavelength™, the BlueVoyant client portal is a web-based portal that provides real-time visibility into detected alerts, confirmed incidents, all detected assets, and vulnerabilities. Locate dashboards representing a variety of content including but not limited to event volume, alert volume, detected assets, and analyst response actions inside Wavelength™.

Access vulnerability reports containing content such as new and resolved vulnerabilities and high-risk vulnerabilities on critical assets through Wavelength™.

Orchestration and automation, a key component of the technology platform, synchronizes security tools and helps maintain the proper balance of machine automation and human intervention. Orchestration and automation accelerates triage, reduces false positives, and improves mean time to resolve (MTTR).

BlueVoyant SOC and engineering teams have developed automations to support Managed Detection and Response and continue to deliver new automations. For example, an automated Emotet investigation, confirmation, and response playbook exist to quickly respond to specific outbreak strains.

The Client Experience team is your primary support team. Your advisor will meet with you on a regular basis (most often monthly) to understand your security program goals and will advise how BlueVoyant services can best meet your needs.

GETTING STARTED

During Introduction, key BlueVoyant and enterprise staff will engage you to learn your priorities, expectations, and deadlines. You will meet your BlueVoyant Project Manager as well as the Client Experience Team. The Client Experience team is your primary support team. Your advisor will meet with you on a regular basis (most often monthly) to understand your security program goals, to offer advice, and to help you select BlueVoyant services to best meet your security needs.

BlueVoyant works with you to understand your network environment and the best deployment locations for BlueVoyant virtual appliances to ensure proper vulnerability assessment coverage. Our team will work with you to understand your risk and compliance goals and select the best vulnerability scan policies and scan frequency to meet those vulnerability assessment needs. During the introduction phase, you will identify infrastructure that is hosted with a cloud provider and BlueVoyant will work with you to obtain prior approval for the scan frequency of that infrastructure.

Introduction

Facilitates information gathering and begins with project kickoff.

Provisioning

Deploys software, sets configurations, and establishes connections.

Tuning

Establishes the baseline of activities and highlights anomalies.

Your Client Experience Team

Client Advisor

The Client Experience Team is your primary support resource. You will be assigned an advisor who will act as your consultant and will enable the best experience interacting with BlueVoyant services. Your advisor will meet with you regularly to understand the goals of your security program and track results. Your advisor will also engage with you should you have any significant security events occur.

Implementation Project Manager

At the beginning of your VMS deployment, a BlueVoyant Implementation Project Manager will be assigned to you to assist you through the onboarding process. The Implementation Project Manager will help you establish timeline goals and select sources and devices that will be onboarded with the appropriate priority that aligns with your goals.

GETTING STARTED

The Provisioning Phase focuses on the deployment of software to enable log collection and the configuration of devices and applications to deliver logs to the BlueVoyant Technology Platform for storage and analysis. This phase includes the installation of BlueVoyant virtual appliances and connectivity of BlueVoyant virtual appliances. You will also gain access to the client portal, Wavelength™ and we will configure multi-factor authentication which will be followed by training for client users. Security monitoring will begin once 80% of the target deployment has been met and an audit has been performed to ensure software has been properly deployed.

During Tuning, we establish the baseline of activities and highlights anomalies. Once the BlueVoyant virtual appliances have been deployed, the environment will be scanned to detect all assets. The asset list will be reviewed with you. This includes the identifying "Key Terrain" devices and applications as well as asset tagging and assigning asset criticality.

LAYERED SECURITY

Robust, Relevant, and Right-Sized Cybersecurity Options for Businesses of All Sizes

As part of our commitment to democratizing cybersecurity, BlueVoyant's services are designed to be mutually reinforcing, but do provide significant value as stand alone solutions.

Many clients choose additional services that are designed to work together to enhance and strengthen their security posture; this decision is generally based upon the size and expertise level of their IT staff.

Additional Managed Security Services Available:

Managed Detection and Response (MDR+)

Our Managed Detection and Response (MDR) service is the foundation of a robust cybersecurity program. Adding additional layers of protection as your need grows helps reduce risk to your enterprise.

Detection-as-a-Service℠

Collects logs from applications and on-premise and/or cloud infrastructure to enable advanced threat detection. BlueVoyant leverages proprietary, open-source, and dark web intelligence to expedite triage and enrich investigations conducted by the SOC.

Managed SIEM

Maximize existing platform investments with access to a BlueVoyant hosted Splunk® Enterprise environment that will enable hands-on access to data and a team to help you perform searches, develop correlations, and execute analyses.

The average cost top companies spend on a malware attack is $2.4 million -Accenture, 2017

Malware and web-based attacks are the two most costly attack types -Accenture, 2017

In 2017, 2.7 billion records were stolen, or twice as many as were stolen in 2016 -Wipro, 2018

87% of surveyed CEOs are investing in cybersecurity to build trust with clients -PwC, 2018