Managed Detection & Response

BlueVoyant

BlueVoyant

INTRODUCTION

"Business disruption is a major concern of both large and small enterprises today. As the world of cyber criminals continues to grow, companies will continue to deploy more and more defenses and layers of protection to defend themselves from losses. No single form of defense is sufficient - you have to take a multi-layered approach."

Jim Rosenthal, CEO | Former Chief Operating Officer of Morgan Stanley. Past Chairman of the Securities Industry and Financial Markets Association and its Cybersecurity Committee

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 Professional 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

Managed Detection & Response

Democratized Cybersecurity

BlueVoyant democratizes next-generation cybersecurity by creating services for small-to-mid-sized businesses that offer the same level of protection enjoyed by large enterprises at a fraction of the cost.

Managed Detection and Response (MDR+) from BlueVoyant consists of monitoring and management of endpoint software deployments and the performance of incident response actions as needed. Monitoring Services include 24/7 collection, storage, reporting, and client notification of security events and device health events.

This service is supported by the BlueVoyant technology platform, a cloud-based ingestion, processing, and analysis system. This web-based platform generates reports based on the alerts that are analyzed by experts in BlueVoyant's geographically diverse security operations centers (SOCs).

Managed Detection and Response includes a proven implementation methodology and tools for simple reporting and analysis that are provided through Wavelength™, BlueVoyant's client portal.

MDR+ can be tailored to fit your needs with additional services like custom advanced threat detection.

Security Monitoring

Event classification is part of the process that BlueVoyant analysts perform when investigating security alerts. Depending on the severity, clients will be notified by email, phone call, or through the client portal.

LOW → **MEDIUM** → **HIGH** → **CRITICAL**

Minimal Threat
adware or other potentially unwanted programs (PUPs).

Potential Threat
malware bots or spyware that do not pose immediate risk to your network.

Significant Threat
rootkits, keyloggers, trojans, ransomware, confirmed suspicious privilege escalation, confirmed social engineering-based attack.

Imminent Threat
data destruction, encryption, exfiltration, or malicious interactive attackers.

OVERVIEW

Services Activation

Advanced endpoint software will be deployed. Client applications will be whitelisted to reduce the likelihood of unintended business disruption. Remote intrusion response activities pre-approval guidelines will be established.

Investigation and Notification

When a suspicious event is detected or an automatic prevention activity occurs, an alert is generated and a security operations center analyst will investigate to determine whether or not there is a true positive, benign, or false positive and the client will be notified.

Indicator Enrichment

Indicators of compromise associated with detections within the monitored environment are automatically extracted, scored, and enriched, leveraging open source and proprietary Threat Intelligence. Enriched indicators, assigned a reputation and classification, are visible within Wavelength™.

Endpoint Response

BlueVoyant will take a specific set of actions at the completion of an investigation: quarantine, delete, whitelist, monitor, or blacklist. Depending on your services, if an advanced investigation with live/real-time response is needed, BlueVoyant may perform remote intrusion response activities.

Threat Detection

Advanced endpoint software will be used to expand enrichment and enhanced behavioral correlations. Depending on your services, BlueVoyant will proactively and iteratively search through events to detect and isolate advanced threats that evade existing security solutions.

Malware Prevention

Deployed endpoint software will automatically prevent the execution of suspicious or known malicious software, often preventing the outbreak or spread of malware. Through blacklist policy management, delivery of unique signatures and threat intelligence indicator matching, BlueVoyant can deny, terminate and block operations remotely.

Health Monitoring

BlueVoyant will monitor installed endpoint agent communications using the technology platform. BlueVoyant will monitor log sources and will generate an alert when a log source's output has not been received in a specified interval.

Outage Prevention

All third-party vendor patches and upgrades will be assessed for their security, stability, and functionality by BlueVoyant prior to client deployment to ensure they are supported and won't cause outages.

FEATURES

Managed Detection and Response is supported by expert analysts operate 24 hours a day, 7 days a week, across multiple locations within the Security Operations Centers (SOCs). Certifications held by the team include SANS GIAC, EC-Council, and ISC-2, as well as others.

Our experts leverage Wavelength™, BlueVoyant's client portal, to provide real-time visibility into detected alerts and to confirm incidents. This web-based portal enables approved client employees to interact with BlueVoyant's security operations center analysts, view all detected assets, and if applicable, view vulnerabilities.

Dashboards, representing a variety of content such as event volume, alert volume, detected assets, and analyst response actions provide a snapshot of real-time security posture. Reports are available through Wavelength™ and include client environment content related to alerts, incidents, indicators, assets, and vulnerabilities.

We offer custom FFIEC and NCUA-ACET automations to assist financial institutions manage the growing number of security compliance management challenges adversely impacting compliance.

The mandatory risk assessments and compliance reports can be burdensome, but BlueVoyant has automated many of the FFIEC and NCUA-ACET compliance controls to reduce the time-intensive reporting process that is crucial.

Updates on the threat landscape, sectorial, and intelligence summary reports are developed by the BlueVoyant Threat Fusion Cell - an elite team of cyber intelligence analysts and threat researchers focused on identifying and prioritizing information about threats using BlueVoyant proprietary and open source intelligence.

Orchestration and automation is a key component of our technology platform; it allows the BlueVoyant SOC to accelerate triage, reduce false positives, and improve 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.

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. We will establish your threat profile, which helps us identify potential threats. We will create a pre-approved response plan as well as a list of pre-approved response actions that will be used to inform the SOC which response actions they may perform under what conditions.

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 MDR+ 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.

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.

GETTING STARTED

During Tuning, BlueVoyant will use the first 14-30 days post installation to identify a baseline of the environment and familiarize ourselves with your technology set and its alerts. Tuning is a process of factoring out some of the expected noise of the client's environment and optimizing our service to provide better visibility and anomaly detection. We will develop endpoint policies to help with whitelisting applications which will be refined through steady-state operations as your IT infrastructure changes.

Once the advanced endpoint software on the identified endpoints has been deployed onto your environment, identification and contextualization of assets can occur. This includes identifying "key terrain" devices and applications, as well as tagging assets and assigning asset criticality.

Service Tier Comparison

Managed Detection and Response	MDR+	MDR+ with Advanced Threat Hunting
MDR+ Service Activation	✓	✓
Investigation & Notification	✓	✓
Indicator Enrichment	✓	✓
Endpoint Response	✓	✓
Threat Detection	✓	✓
Malware Prevention	✓	✓
Health Monitoring	✓	✓
Software Upgrades	✓	✓
Access to Wavelength™	✓	✓
Threat Hunting		✓
Remote Intrusion Response		✓

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.

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.

Additional Managed Security Services Available:

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.

Vulnerability Management Services

Takes the guesswork out of identifying potential weaknesses such as missing patches, malware, and misconfigurations. Vulnerability Management Services help organizations prioritize vulnerabilities so that they can reduce risk.

73% of breaches are perpetrated by outsiders

60% of breaches are conducted by organized crime

92% of breaches originated through email

Companies that contained a breach in under 30 days saved over **$1M USD**

Ponemon Institute 2018 Cost of a Data Breach Study sponsored by IBM