# MANAGED DETECTION AND RESPONSE FOR ENDPOINT

Service Description

Subject to the terms and conditions of the Order Form and the BlueVoyant Managed Security Services Master Services Agreement, BlueVoyant will provide the managed detection and response services set forth in an Order Form and further described below to Client, at the service levels set forth below. Capitalized terms used herein but not defined shall have the meanings ascribed to such terms in the Master Services Agreement.

1. Overview: As detailed further below, BlueVoyant's managed detection and response services consist of BlueVoyant's monitoring and management of one or more advanced endpoint software deployments and performing incident response actions as needed. Monitoring the endpoints is performed 24 hours a day, 7 days a week. These services utilize the BlueVoyant platform, our cloud-based ingestion, processing, analysis, and reporting system (Platform), as well as analysts in BlueVoyant's security operations centers. Management of client systems is limited to the endpoint software agent that is installed on Client hardware. Monitoring activities include collection, storage, reporting, and Client notification of security events or device health events in accordance with specified service levels. Tools for self-service reporting and analysis are provided through Wavelength™, BlueVoyant client portal.

2. MDR Services: BlueVoyant provides two tiers of managed detection and response services:

   2.1. Managed Detection and Response (Tier 1): *Managed Detection and Response* includes managed detection and response services include MDR Services Activation, Investigation & Notification, Indicator Enrichment, Endpoint Response (excluding Remote Intrusion Response), Threat Detection (excluding Threat Hunting), Malware Prevention, Health Monitoring, and Software Upgrades (as those services are described below). Tier 1 services include access to Wavelength™, BlueVoyant's Client portal.

   2.2. Managed Detection and Response with Advanced Threat Detection (Tier 2): *Managed Detection and Response with Advanced Threat Detection* include the Managed Detection and Response services plus Threat Hunting and Remote Intrusion Response (as those services are described below), and also include access to Wavelength™, BlueVoyant's Client portal.

3. MDR Service Descriptions:

   3.1. Investigation & Notification: Once a suspicious event is detected or a prevention activity occurs, an alert is generated and a BlueVoyant security

operations center analyst will perform triage and investigation of the event to confirm true positive, benign, or false positive. Client will be notified according to the nature of the event and service-level-agreements.

3.2. Indicator Enrichment: Indicators of compromise associated with detections are automatically extracted, scored, and enriched leveraging open source and BlueVoyant proprietary threat intelligence. Enriched indicators are visible within Wavelength™ and are assigned a reputation (ex: good, suspicious, bad) and classification (ex: botnet, Zeus, crypto-miner, etc.).

3.3. Endpoint Response: BlueVoyant will take a specific set of response actions at the completion of an investigation, subject to the pre-approved actions profile established as part of MDR Services Activation (as that term is defined below).

3.3.1. Quarantine: Isolation of an endpoint so that it can no longer communicate with any other devices in the Client environment or to the Internet. BlueVoyant will move an endpoint into the quarantine state typically when there is evidence of lateral movement of an advanced threat within the Client environment or detection command-and-control (C2) software attempting to beacon to an attacker's infrastructure.

3.3.2. Delete File: BlueVoyant will delete specific files on an endpoint if a specific file is known and confirmed to be malicious. File deletion can occur in broader cases per the direction of the Client as part of policy enforcement (ex: pre-approval to delete potentially unwanted programs).

3.3.3. Whitelist: Typically performed as a response to an application that is incorrectly being blocked or terminated as malicious by the advanced endpoint software, BlueVoyant will update policies to whitelist the application for proper execution or set the correct privileges and actions it is allowed to perform. Whitelisting applications is also performed as part of MDR Services Activation in order to reduce the likelihood of unintended business disruption.

3.3.4. Monitor Only: As part of diagnosing misbehaving advanced endpoint software, a BlueVoyant security operations center analyst can move an endpoint into monitor only mode, this is done with collaboration with the Client. Monitor Only mode will direct the endpoint software not to interfere with any end user activities on the endpoint.

3.3.5. Blacklist: BlueVoyant will blacklist specific files on an endpoint if a specific file is known and confirmed to be malicious. Blacklisting a specific application either by computed hash or process name will inform the advanced endpoint software not to allow the application to run on any endpoint (that has the advanced endpoint software deployed).

3.3.6. Remote Intrusion Response: As part of an advanced investigation, BlueVoyant will use the live/real-time response capabilities in the advanced endpoint software to perform intrusion response activities

such as searching and modifying the registry, analyzing volatile memory, remote file deployment, and remote file retrieval. Remote Intrusion Response activities are subject to pre-approval guidelines set as part of MDR Services Activation.

3.4. Threat Detection: BlueVoyant will leverage the advanced endpoint software to perform detections and provide visibility to activity on the endpoint. BlueVoyant expands the default detections deployed to the advanced endpoint software utilizing proprietary intelligence, indicator enrichment, and enhanced behavioral correlations.

3.4.1. Signature Detection: BlueVoyant will use traditional anti-virus techniques to identify malicious software by the reputation of their computed hash.

3.4.1.1. BlueVoyant Signatures: BlueVoyant may detect new malware before it has been included into the signature database of advanced endpoint platforms. When this happens, BlueVoyant may deploy proprietary new signatures to the advanced endpoint software.

3.4.2. Behavioral Detection: BlueVoyant will classify activity on endpoints as distinct actions and then holistically analyzing them as part of known tactics, techniques, and procedures (TTPs) to detect patterns of adversarial behavior. Behavioral Detection enables identification of malware, not by whether it has been seen previously by detection software, but instead by how it behaves. BlueVoyant may expand on the list of known TTPs provided by the advanced endpoint software with BlueVoyant developed set of TTPs.

3.4.3. Reputational Detection: Utilizing proprietary and open source threat intelligence, BlueVoyant will detect threats based upon reputation by correlating inbound and outbound network traffic to monitor for suspicious and malicious domains and IP addresses.

3.4.4. Threat Fusion: The BlueVoyant Threat Fusion Cell is a team of cyber intelligence analysts and threat researchers focused on identifying and prioritizing information about threats using BlueVoyant proprietary and open source intelligence. The team undertakes threat hunt missions (based on the tier of service), new detection signatures, new indicators and reputation scoring.

3.5. Advanced Threat Detection: BlueVoyant's Tier 2 Managed Detection and Response includes all detection and service delivery components of Tier 1, with additional detection capabilities and techniques:

3.5.1. Anomaly Detection: BlueVoyant will perform statistical analysis of several types of endpoint metadata to identify anomalous user, process, and endpoint activity that could indicate malicious use. BlueVoyant uses

anomaly models to detect malicious activities that cannot be identified from distinct events, such as uncommon network flows, unusual authentication events and lateral movement.

3.5.2. Threat Hunting: Some advanced adversaries can evade the standard detection mechanisms of cyber security detection tools. BlueVoyant will proactively and iteratively search through events to detect and isolate advanced threats that evade existing security solutions. BlueVoyant will also conduct remote hunt missions on a regular basis that will perform manual and semi-automated activities for targeted data analysis to search for signs of advanced adversaries.

3.5.3. Forensic Artifact Analysis: BlueVoyant Threat Hunters perform advanced forensic artifact collection and analysis to triage anomalous events and determine adversary activity beyond actions captured by real-time telemetry.

3.5.4. Attacker Abuse Insights: BlueVoyant Threat Hunters continuously analyze endpoint data to identify tools, configurations, and security hygiene concerns that would benefit an adversary. BlueVoyant shares these insights via our weekly threat intelligence reporting with our clients, along with mitigation recommendations, to better prepare endpoint defenses. For any findings that can be actioned via the Endpoint Agent.

3.5.5. Ad-hoc IOC Discovery: As BlueVoyant researchers and clients identify new indicators of compromise or new attacker methodologies, BlueVoyant Threat Hunters proactively search client environments for specific network connectivity events associated with these IOCs and provide response actions and recommendations based on any findings..

3.6. Malware Prevention: BlueVoyant will utilize the advanced endpoint software to automatically prevent the execution of suspicious or known malicious software based upon detection mechanisms to prevent the outbreak or spread of malware. BlueVoyant will also administer malware prevention by blacklist policy management, delivery of unique signatures, and threat intelligence indicator matching.

3.6.1. Deny or Terminate Process: Some applications will not exhibit suspicious or malicious behaviors until after the process has been running. If an application exhibits TTP behaviors after it has run, B advanced endpoint software can terminate the application via the malware prevention blacklist. BlueVoyant can extend or manage the conditions which will cause an application to be terminated or denied.

3.6.2. Block Operation: The actions that an application can take can be controlled with a high degree of granularity, including block network connections, execution of a file-less script, invocation of a command interpreter, etc. BlueVoyant will work with the Client on what activities

are allowed by specific applications to reduce the possibility of malware, most often file-less malware, can infect the Client's environment.

3.7. Health Monitoring: BlueVoyant will monitor communication between the Platform and the advanced endpoint software vendor's infrastructure. Should the communication vendor's infrastructure become uncommunicative or unreachable, BlueVoyant will notify the vendor to take corrective action. BlueVoyant will notify the Client if the issue leads to an outage.

3.8. Software Upgrades: As software patches and upgrades are released by the third-party vendor, BlueVoyant will assess the release for security, stability, and functionality before certifying it as a supported version. BlueVoyant will work with the Client to schedule any necessary remote upgrades. Under specific circumstances, BlueVoyant may proactively reach out to the Client to request an upgrade such as if the current version has a major failure or severe vulnerability. It is Client's responsibility to maintain the current or one previously supported version.

4. Supporting Features and Teams:

4.1. Security Operations Centers (SOC): BlueVoyant's managed detection and response services are supported by BlueVoyant's SOCs, which operate 24 hours a day, 7 days a week across multiple locations.

4.2. **Wavelength™** (BlueVoyant's Client Portal): Wavelength is a web-based portal that provides real-time visibility to detected alerts, confirmed incidents, enables approved Client employees to interact with BlueVoyant's security operations center analysts, view all detected assets, and if applicable, view vulnerabilities.

4.2.1. Dashboards: Available through Wavelength™, dashboards representing a variety of content including but not limited to event volume, alert volume, detected assets, and analyst response actions.

4.2.2. Reports: Available through Wavelength™, reports include Client environment content related to alerts, incidents, indicators, assets and vulnerabilities.

If needed, the Client can request specific reporting on events be delivered as a report on an automated basis. Extensive customization of report templates and or creation of custom reports are not included in the service and can be performed on an engagement basis subject to the mutual agreement of a separate signed Statement of Work.

4.2.3. Threat Intelligence Reports: Threat landscape, sectorial, and intelligence summary reports are developed by the BlueVoyant Threat Fusion Cell.

4.3. Security Orchestration and Automation: Although not directly visible to Clients, the orchestration and automation system is a key component of the

Platform that supports the BlueVoyant SOC. Orchestration accelerates triage, reduces false positives, and improves mean time to resolve (MTTR).

4.3.1. Playbooks: BlueVoyant SOC and engineering teams have developed automations to support the Services and continue to deliver new automations. For example, an automated Emotet investigation, confirmation, and response playbook to quickly respond to specific outbreak strains.

4.4. BlueVoyant Client Experience Team: BlueVoyant's client experience team is the primary support team for the Client. The assigned Client advisor acts as the Client's consultant and enables the best experience for BlueVoyant services. The advisor will meet with the Client on a regular basis (most often monthly) to understand Client's security program goals and will advise how BlueVoyant services can best meet their needs. The advisor is also engaged in any significant security events that occur for the Client. Additionally, the advisor will deliver any requested feedback to the BlueVoyant product and service delivery teams.

5. Client Communications: Below are the standard methods for Clients to obtain information related to the Services or engage BlueVoyant staff.

5.1. **Wavelength™** (BlueVoyant Client Portal): Wavelength is the primary method for Clients to stay informed of security activity in their environment and activities of the BlueVoyant SOC. At any time, a Client end user may go to Wavelength and review any security alerts, dashboards, or reports.

5.2. Email: The Client will receive emails as a regular function of the Services. Email topics can span a wide variety of matters, but most often they relate to security investigations: notification of risk or questions on appropriate environment use or behaviors.

Clients can also initiate service change requests via email by sending an email to soc@bluevoyant.com. Upon receipt of any emails, a service request case is created and can be viewed within Wavelength.

5.3. Calling Security Operations: The BlueVoyant SOC operates 24/7 days a year and can be reached by calling 1-833-BLUEMSS or +1-833-258-3677. Only approved Client end-users will be allowed to talk with BlueVoyant SOC personnel.

6. Managed Detection and Response Service Levels

6.1. Security Monitoring: Client will receive communications to security incidents according to (a) the escalation procedures defined or in the manner pre-selected in writing by Client, either through Wavelength, email, or by telephone, and (b) the matrix below. Event classification is the process that a BlueVoyant security analyst performs an investigation to confirm the validity of an alert, impact and assigns a severity. Notification times for Client notification are measured by the

time difference between when event classification has completed and when the Client is notified. Client notification occurs after event classification in order to prevent notification for benign or false positive alerts.

| Severity | Definition | Notification Time | Notification Method |
|---|---|---|---|
| **Critical** | Events that represent an eminent threat to Client assets, including: data destruction, encryption, exfiltration, or malicious interactive attacker. | **30 minutes** of event classification completion | 1. Email<br>2. Phone Call<br>3. Wavelength |
| **High** | Events that represent a significant threat to Client assets, including: rootkits, keyloggers, or trojans, but not defined as "critical", ransomware, confirmed suspicious privilege escalation, confirmed social engineering-based attack. | **1 hour** of event classification completion | 1. Email<br>2. Phone Call<br>3. Wavelength |
| **Medium** | Events that represent a potential threat to Client assets, including: malware types that include bots or spyware, but not defined as "critical" or "high". | No Notification | Wavelength |
| **Low** | Events that represent a minimal threat to Client assets. This includes, adware or other potentially unwanted programs (PUPs). | No Notification | Wavelength |

6.2. Managed Detection and Response Service Requests: Standard service requests (applies to all non-change and non- incident tickets) submitted via Wavelength™, email, or via telephone will be subject to "acknowledgement" (either through the BlueVoyant ticketing system, email or telephonically) within

one (1) business day from the time stamp on the managed detection and response service ticket created by the Platform.

6.3. Maintenance Windows: BlueVoyant may schedule maintenance outages for BlueVoyant software which enables log collection with 24-hours' notice to designated Client contacts. Service levels shall not apply during maintenance outages and therefore are not eligible for any service level credit during these periods.

6.3.1. Emergency Maintenance: In the circumstance of immediate necessary changes, BlueVoyant may initiate an emergency maintenance window. When this situation occurs, BlueVoyant will use commercially reasonable efforts to provide notice and minimize the impact to Clients.

6.4. Client Outage: The service levels do not apply in the event of any Client-caused outage that prohibits or otherwise limits BlueVoyant from providing the managed detection and response services or otherwise delivering the service levels, including, but not limited to, Client's misconduct, negligence, inaccurate or incomplete information, modifications made to the Services, or any unauthorized modifications made to any managed hardware or software devices by Client, its employees, agents, or third parties acting on behalf of Client.

6.5. Third Party Outages: service levels are not applicable for any outages of the third-party vendor's advanced endpoint software related to the delivery of security events or alerts to the Platform.

6.6. SLA Credits: Client will receive credit for any failure by BlueVoyant to meet the service levels outlined above within thirty (30) days of notification by Client to BlueVoyant of such failure. In order for Client to receive a service level credit, the notification of the service level failure must be submitted to BlueVoyant within thirty (30) days of such service level failure occurring. BlueVoyant will research the request and respond to Client within thirty (30) days from the date of the request. The total amount credited to Client in connection with any of the above service levels in any calendar month will not exceed the monthly Services fees paid by Client for such Services. Except as otherwise expressly provided hereunder or in the BlueVoyant Managed Security Services Master Services Agreement, the foregoing service level credit(s) shall be Client's exclusive remedy for failure to meet or exceed the applicable service levels.

7. Managed Detection and Response Services Activation: Managed detection and response services activation (MDR Services Activation) consists of **three phases**: **introduction**, **provisioning**, and **tuning**. MDR Services Activation begins after a signed Order Form is received and ends with the activation of the managed detection and

response services. MDR Services Activation is dependent on a number of factors, such as the number of endpoints, central management of endpoints, the number of physical sites, the complexity of the Client's network, Client requirements, and the ability of Client to provide BlueVoyant with requested information and deployment of supporting software and configuration within a mutually agreed-upon timeframe.

7.1. Introduction Phase: The introduction phase facilitates information gathering and begins with project kickoff. During this phase there are introductions between key BlueVoyant and Client staff and Client priorities, expectations, and project timelines are established.

7.1.1. BlueVoyant Project Manager: At the beginning of Client deployment, a BlueVoyant implementation project manager will be assigned and coordinate the onboarding process. The implementation project manager will work with the Client to establish their timeline goals and what sources and devices will be onboarded in what priority and timeline and when they will move to steady-state monitoring.

7.1.2. Client Experience Team: At the beginning of Client deployment, a BlueVoyant technical account manager will be assigned to the Client. This person will work directly with the Client and will act as their main point of contact beyond direct calls to the SOC.

7.1.3. Threat Profile: In order to provide organizational specific threat intelligence, BlueVoyant will collect information about the Client to better understand potential threats. Collected information will include information about the organization's industry, segment, key employees, key systems and what types of digital assets they own including domains and IP address segments.

7.1.4. Approved Response Plan: The Client and BlueVoyant will discuss and agree upon rules of engagement for service operation e.g., response actions and policies, vulnerability scanning policies, authorized Client points of contact, and other operational considerations. Included in the response plan is the creation of the escalation procedures which defines who in the Client's organization should be contacted in the event of an incident.

7.1.4.1. Pre-approved Response Actions: A set of pre-approved response actions will be established to inform the SOC to which response actions they can perform under what conditions. For example, do not perform any response actions and only notify the Client's IT staff for specific set of business-critical assets.

7.2. Provisioning Phase: The provisioning phase is focused on deployment of the advanced endpoint software to endpoint visibility and response actions.

7.2.1. Advanced Endpoint Software: Deployment of the advanced endpoint software on the identified endpoints with Internet access to connect to the vendor infrastructure.

7.2.2. Wavelength™ User Onboarding: Client will provide a list of identified users and their email addresses for access to Wavelength™ and SOC. Client users will receive an onboarding email to access Wavelength and will configure multi-factor authentication with their device. BlueVoyant will conduct Wavelength™ training for Client users.

7.2.3. Deployment Audit: Once all advanced endpoint software has been deployed and are functioning, an audit is performed to ensure the software has been correctly deployed on all the correct systems and managed detection and response services are ready to commence. Security monitoring will begin once 80% of the target deployment has been met.

7.3. Tuning Phase: BlueVoyant will use the first 14-30 days post installation to identify a baseline of the Client environment and tune the managed detection and response services. Tuning is a process of factoring out some of the expected noise of the Client's environment and optimizing the service to provide better visibility and anomaly detection.

7.3.1. Endpoint Policy: As part of malware protection, applications may be automatically terminated or disallowed based on whether the application exhibits specific behaviors. As part of the tuning phase, any applications that are incorrectly prevented from executing will be identified and appropriately whitelisted with Client consultation. Endpoint policies will continue to be refined through steady-state operations as the Client's information technology infrastructure changes.

7.3.2. Inventory of Assets: Once the advanced endpoint software has been deployed, identification and contextualization of assets can occur. This includes the identifying "key terrain" devices and applications as well as asset tagging and assigning asset criticality.

7.4. Onsite Deployment: Should onsite installation and configuration be necessary, BlueVoyant will provide such a resource for an additional fee as well as travel and lodging expenses.

8. Client Responsibilities

8.1. Software Deployment: During the MDR Services Activation process, the Client will deploy the advanced endpoint software on identified endpoints.

8.2. Notification of Environment Changes: Client will notify BlueVoyant of any environment changes that may affect execution of the MDR Services.

8.3. Notification of User Changes: Client will notify BlueVoyant of any necessary user account changes tied to Client employee termination; this includes employees or contractors that have access to Wavelength™ or approval to contact the SOC.

8.4. Internet Access: Client is required to maintain internet connection to endpoints that are actively monitored.

8.5. Additional Remediation: During investigation of security alerts BlueVoyant may give guidance to a Client to perform specific actions in their environment in order to improve their security posture or to fully remediate an incident. Performance of these actions are the Client's responsibility.

8.6. Software Updates: Client is responsible for performing upgrades on deployed on advanced endpoint software in a timely manner.

9. Other Services & Capabilities (Not Included): Below is a list of other notable services and capabilities provided by BlueVoyant that are outside the scope of this MDR Services. These services and capabilities can be purchased alongside this MDR Services.

9.1. Detection-as-a-service: Monitoring of Client's devices and infrastructure for security and compliance.

9.2. Managed SIEM: Delivered utilizing Splunk as a best-of-breed security information and event management (SEIM) tool to monitor the Client's devices and applications. Clients have access to Splunk directly to create their own searches, correlations, searches, reports, and deploy approved add-ons.

9.3. Vulnerability Management MDR Services (VMS): Delivers vulnerability scanning, remediation tracking, active asset discovery, and reporting.

9.4. Deception: Using next-generation honey pot technology to detect advanced threats in your environment using featherweight, agentless technology.

9.5. Device Control: USB device control policy management delivered utilizing endpoint detection and response technology.

10. Out of Scope: In the event the Client requests BlueVoyant to provide additional services that are outside of the scope what is set forth in this Statement of Work, to the extent BlueVoyant is able to provide such services, the services will be mutually agreed in separate Statement of Works executed by both parties. Available additional services include:

    10.1. breach response & compromise assessment;

    10.2. forensics;

    10.3. vulnerability patching and resolution; and

    10.4. tabletop exercises;

    10.5. network architecture design;

    10.6. hardware procurement; and

    10.7. security or technology training for end users.

11. MDR Services Termination: If an Order Form including managed detection and response services is cancelled or the Agreement is terminated, the Client will have thirty (30) days from the time a cancellation request is initiated, or the Agreement has expired (whichever comes first) to request the receipt of archived data. Hourly consulting fees will apply for time spent as well as data transfer cost related to archived data. If a request is not received within the thirty (30) day period, BlueVoyant will permanently destroy all archived data pertaining to security devices no longer under a valid Order Form.

12. Additional MDR Services Terms and Conditions:

    12.1. Modify Terms: BlueVoyant reserves the right to modify the terms of this Statement of Work, including the service levels, with 30 days prior notice.

Risk Elimination: This Statement of Work provides expert security analysis and response to the Client. However, deployment of BlueVoyant managed detection and response services in a Client network does not achieve the impossible goal of risk elimination, and therefore BlueVoyant makes no guarantee that intrusion, compromises, or any other unauthorized activity will not occur on a Client network.