DETECTION AS A SERVICE℠

Statement of Work

Subject to the terms and conditions of the Order Form and the BlueVoyant Managed Security Services Master Services Agreement, BlueVoyant will provide the detection 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. Service Overview: BlueVoyant's monitoring of pre-agreed network security device(s) (Devices) and application(s) (Applications), and provides Client with real-time, security event analysis across monitored security and critical infrastructure 24 hours a day, 7 days a week. The service utilizes the BlueVoyant platform, our cloud-based ingestion, processing, analysis, and reporting system (Platform) as well as analysts in BlueVoyant's security operations centers.

   Implementation and configuration changes necessary for provisioning of software agents are included in the services, as are (1) vendor software updates in line with the BlueVoyant software update policy , and (2) 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's client portal.

2. Service Feature:

   2.1. Log Collection: Software agents will be deployed on Devices to enable collection of logs for security event monitoring. Using BlueVoyant Virtual Appliances (described below), logs are aggregated and stored within Platform from the Devices and Applications.

   2.2. Security Event Monitoring: Process of detecting threats in the environment and performing security investigations 24/7.

      2.2.1. Threat Detection: Filters, normalization, correlation, and data analysis will be applied to identify anomalous, suspicious, or malicious behaviors indicative of threats in the monitored environment. Threat detection occurs through threat detection methods, including but not limited to signature, behavioral, and cross-source correlations.

2.2.2. Reputational Detection: A notable detection method, reputation detection occurs by utilizing proprietary and open source threat intelligence, BlueVoyant will identify threats based upon reputation by correlating inbound and outbound threat intelligence with network traffic to monitor for suspicious and malicious domains and IP address.

2.2.3. Investigation & Notification: Once a suspicious event is detected or an automatic prevention activity occurs, an alert is generated and a BlueVoyant security operations center analyst will investigate the event to determine whether or not there is a true positive, benign, or false positive. Client will be notified according to the nature of the event and service-level-agreements.

2.2.4. Managed Detection and Response (Separate): If a client has also purchased managed detection and response (services from BlueVoyant, then the BlueVoyant security analyst will also undertake response activities on the endpoint as a result of the investigation if applicable and appropriate. *[BlueVoyant's Managed detection and response managed services are described in BlueVoyant's Managed Detection and Response Statement of Work]*.

2.2.5. Indicator Enrichment: Indicators of compromise associated with detections within the monitored environment 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.).

2.3. Health Monitoring: BlueVoyant will monitor installed endpoint agent communications using the Platform. Should agents become uncommunicative and unreachable, BlueVoyant will notify the Client and assist with troubleshooting. BlueVoyant will monitor log sources that are within the scope of service and will generate an alert when a log source's output has not been received in a specified interval.

2.4. Log Retention & Archiving: All log data collected from Devices and Applications will be retained by BlueVoyant for a period of 30 days for security event analysis and retained in archive storage for a period of one year or as specified in the service order. Logs older than 30 days can be retrieved and delivered to Client upon written request, for an additional retrieval fee.

3. Supporting Features and Teams

3.1. Security Operations Center (SOC): The Service is supported by the BlueVoyant Security Operations Center which operates 24 hours a day, 7 days a week, and across multiple locations.

3.2. **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.

1.1.1. 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.

3.2.1. 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 agreement of a separate signed Statement of Work.

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

3.3. BlueVoyant Virtual Appliance: The BlueVoyant virtual appliance is a software package that enables log collection from external sources and delivers it to the BlueVoyant platform. It enables log collection and monitoring for devices and systems in which deployment of a log collection agent is not possible, such as a router or firewall. Most often devices are configured to deliver Syslog content to a BlueVoyant virtual appliance.

3.4. Collection Agents: Collection agents are software that are installed directly on client endpoints and servers to enable log collection and delivery to the BlueVoyant platform.

3.5. 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).

3.5.1. 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.

1.1. BlueVoyant Client Experience Team: The 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.

4. Client Communications: Below is the standard methods that the Service enables for the client to obtain information related to the Service or engage BlueVoyant staff.

4.1. **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.

4.2. Email: T The client will receive Emails as a regular function of the Service. 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.

4.3. 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 the BlueVoyant Customer Portal.

4.4. 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.

5. Log Collection Sources

5.1. Minimum Collection Sources: In order to provide adequate detection and highest quality service, there are a minimum set of log collection source types that must be monitored. BlueVoyant reserves the right to refuse service and is unable to meet service level agreements if any of these sources are not included as part of the agreed monitored sources:

5.1.1. Network Perimeter Visibility: Visibility of network traffic entering or leaving the environment, which typically provided by means of access to a Client's firewalls or next-generation firewalls or equivalent within a cloud environment.

5.1.2. Advanced Endpoint Visibility: Comprehensive visibility of activities occurring on the client's endpoints including behavioral detections. Visibility can be provided either through Bluevoyant's managed detection

and response services (available separately), or by means of allowing BlueVoyant access to Clients' deployed next-generation anti-virus agents or Client's deployed endpoint detection and response agents.

5.1.3. User Authentication & Access: Visibility to users and user accessed systems typically provided through Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP) server or 3rd party federated login provider.

5.1.4. Dynamic Host Configuration Protocol (DHCP): Access to DHCP logs to enable understanding of assets in the environment using IP resolution. Alternatives to DHCP log collection can be substituted if it provides full asset visibility (such as Cloud IaaS).

5.2. Non-standard Sources: BlueVoyant will provide a set of correlations and detections for commonly supported sources and platforms. For nonstandard log sources, BlueVoyant may require its consultants or engineers to work with Client to understand the Client's log source(s), important event criteria, and any custom reporting or real-time alerting requirements. The scope of this analysis will be set out in a separate mutually agreed signed statement of work as this work is separate and distinct from the efforts of the deployment engineers described below and specifically excluded from the Services.

5.3. Correlation Development: BlueVoyant Engineering implements and delivers new correlations on a regular basis; Client requests for new correlations are prioritized by BlueVoyant's product management process. If Client has urgent correlations that it would like BlueVoyant to prioritize, The scope of this analysis will be set out in a separate mutually agreed signed statement of work.

5.4. Scope of Service: The Service is limited to monitoring the devices & sources subscribed for service as defined in the associated Service Order and does not include management or monitoring of any unsubscribed end-point or intermediary log sources.

5.4.1. Unapproved Sources: Sources that have been configured to relay their logs to a BlueVoyant but are Devices or Applications are deemed as "unapproved". Log collection from unapproved sources may be blocked by BlueVoyant and a Client may receive charges related to the monitoring of unapproved sources.

6. Service Level Agreements

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	Agreement	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	1. Email 2. Phone Call 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	1. Email 2. Phone Call 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. Service Requests: Standard service requests (applies to all non-change and non-incident tickets) submitted via WavelengthTM, 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 Service Outage: The service levels do not apply in the event of any Client-caused Service outage that prohibits or otherwise limits BlueVoyant from providing the Service or otherwise delivering 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 Outage: For log collection of third-party sources such as Software-as-a-Service or Cloud Infrastructure providers, SLAs are not applicable for any outages of the third party in which related to the delivery of their logs to the Platform.

6.6. SLA Credits: Client will receive credit for any failure by BlueVoyant to meet the SLAs outlined above within thirty (30) days of notification by Client to BlueVoyant of such SLA failure. In order for Client to receive an SLA credit, the notification of the SLA failure must be submitted to BlueVoyant within thirty (30) days of such SLA 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 SLAs in any calendar month will not exceed the monthly Service fees paid by Client for such Service. Except as otherwise expressly provided hereunder or in the BlueVoyant Detection-as-a-Service 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. Service Activation: Service activation ("Service Activation") consists of **three phases**: **introduction**, **provisioning**, and **tuning**. Service Activation begins once the signed Service Order is received and ends with the activation of the Service. Service Activation is dependent on a number of factors, such as the number of log collection sources, 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. BlueVoyant does not provide SLAs for completing Service Activation within a specified period of time.

7.1. Introduction Phase: The introduction phase facilitates information gathering and begins with project kickoff. During the 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

7.2. Provisioning Phase: The provisioning phase is focused on deployment of software to enable log collection and the configuration of devices and applications to deliver logs to the BlueVoyant platform for storage and analysis.

7.2.1. BlueVoyant Virtual Appliance: Provisioning of client equipment and installation of BlueVoyant virtual appliances at agreed upon locations for collection of logs for specific devices. Client would enable connectivity of BlueVoyant virtual appliances to the Platform. BlueVoyant will provide minimum system requirements for hosting BlueVoyant virtual appliance software.

7.2.2. Software Agents: : Deployment of software agents to identified endpoints and servers to enable log collection. Client would enable connectivity of software agents to the Platform. .

7.2.3. Source Configuration: Configuration of devices and applications to enable collection of logs. This most often includes configuration of network devices such as firewalls to direct syslog content to a BlueVoyant Virtual Appliance for log collection.

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

7.2.5. Log Collection Audit: Once all collection software has been deployed and sources have been appropriately configured to enable detection, an audit is performed to ensure the Service is ready to commence.

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 Service. 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. Inventory of Assets: Once the collection and agent 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 service activation process, the client will deploy BlueVoyant Virtual Appliances and software agents where appropriate to enable collection of logs and appropriate environment visibility. Additionally, the client will support configuration of devices and applications for collection where necessary; for example, configuring their firewall to direct changes over syslog

8.2. Source Configuration: Client is responsible for configuring all log sources so that logs are appropriately sent to the agents and log collection devices. This includes, but is not limited to, any intermediary log sources. If changes to Client's existing network architecture are required for Service implementation, BlueVoyant will communicate these changes to Client

8.3. Notification of Environment Changes: Client will notify BlueVoyant of any environment changes that may affect execution of the Service.

8.4. 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 WavelengthTM or approval to contact the SOC.

8.5. Internet Access: Client is required to maintain Internet connection to all systems that are performing log collection.

8.6. Additional Remediation: During investigation of security alerts the BlueVoyant Security Operation Center 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

8.7. PII Obfuscation: Client is responsible for filtering all data delivered to BlueVoyant for Personally Identifiable Information (PII), credit card information, or other protected content

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 Service. These services and capabilities can be purchased alongside this Service. .

9.1. Managed Detection and Response (MDR): Advanced detection of threats against the client's endpoints with supporting response action including process termination, whitelisting, blacklisting, and quarantining.

9.2. Managed SIEM: Delivered utilizing Splunk as a best-of-breed Security Information and Event Management tool to monitor the Client's devices and applications. Clients have access to Splunk directly to create their own searches and correlations.

9.3. Vulnerability Management Service (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.

10. Out of Scope: The parties agree that services, deliverables and equipment not listed in the applicable Service Order (as agreed to by the parties) are out of scope and are not part of this Agreement. In the event the client requests BlueVoyant to provide serves that are outside of the scope of this Schedule, to the extent BlueVoyant is able to provide such services, the services will be detailed in a statement of work executed by both parties

10.1. Breach Response & Compromise Assessment

10.2. Forensics

10.3. Vulnerability Patching and Resolution

10.4. Tabletop Exercises

10.5. Network architecture design

10.6. Hardware procurement

10.7. Security or Technology Training for End Users

11. Service Termination: If the Service Order with BlueVoyant 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 all time spent restoring the 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 Service Order or Agreement..

12. Additional Service 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.

12.2. Risk Elimination: This Statement of Work provides expert security analysis to the Client. However, deployment of BlueVoyant Detection-as-Service 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.