MDR for Azure Sentinel

Service Description

1. Description of Service: This Service Description and Service Level Agreement ("Service Description") describes the Service (as defined below) being provided to you ("Customer", "Client", or "you") by BlueVoyant executed by Client for the purchase of this Service.

   This Service is provided in connection with Client's signed Service Order and separate signed master services agreement that explicitly authorizes the sale of managed security and consulting services. In the absence of either a master services agreement or security services schedule, the Services described under this Service Description will be governed by and subject to the terms and conditions of the BlueVoyant Master Services Agreement ("MSA").

2. Service Overview: BlueVoyant Managed Azure Sentinel (the "Service") consists of BlueVoyant's monitoring of the contracted Client-owned Azure Sentinel environment and related security device(s) ("Devices") and application(s) ("Applications") as specified on the Service Order. It provides Client with near real-time, security event analysis across Client's security and critical infrastructure 24 hours a day, 7 days a week per the terms of this Service Description. This Service utilizes the BlueVoyant platform ("The Platform") in conjunction with analysts in BlueVoyant's Security Operations Centers ("SOC") and the Client's Azure Sentinel instance. Client is responsible for any license and consumption fees for their Azure environment including fees associated with Microsoft Azure Sentinel and supporting components.

   Management activities include Service implementation, configuration changes necessary for the successful provision of the Service, tuning the Azure instance efficiency & cost optimization, as well as vendor software updates in line with the BlueVoyant software update policy described in this Service Description. Monitoring activities include collection, storage, reporting, and Client notification of security events or device health events in accordance to Service Level Agreements. Tools for self-service reporting and analysis are provided through Wavelength™, the BlueVoyant Client Portal ("Wavelength") as well as through Azure Sentinel.

3. Service Features

   3.1. Log Collection: Depending on the scope of the client's environment, software agents will be deployed by Client on contracted Client-owned devices or

work-loads (as specified on the Service Order) to enable collection of logs for security event monitoring. Logs are aggregated and stored within the Client's Microsoft Azure environment, which the Client pays all associated fees including, but not limited to ingestion, storage, and compute.

3.1.1. Microsoft Native Sources: Azure Sentinel includes a number of connectors & capabilities for ingesting data from native Microsoft solutions including, but not limited to Microsoft 365 Defender (formerly Microsoft Threat Protection), Microsoft 365 sources (including Office 365), Azure AD, Microsoft Defender for Identity (formerly Azure ATP), Microsoft Cloud App Security, Azure SQL, Azure WAF and more. Data from Microsoft native sources are ingested leveraging service-to-service integration directly within Microsoft Azure. The Service leverages these sources for service to service integration into Azure directly.

3.1.2. External Sources: For non-native Microsoft sources, the Service will leverage Azure Sentinel APIs to ingest logs from sources IT and Security devices and applications such as firewalls, UTMs, IDS/IPS, SaaS applications, or any security relativent source. The service includes building and maintaining security relevant data connectors (and an external collector as needed) to enable log collection from these sources thus enabling threat detection across the Client's Collector broader environment. Building and maintaining custom client and/or non-relevant data connectors for the client is out-of-scope for the Service.

3.1.3. Data Normalization: In order to make proper use of the logs for security monitoring and threat detection, the logs will be normalized into a format to enable the Service. This is a prerequisite to enable BlueVoyant's threat detection methods, correlations, and models.

3.1.4. Log Reduction: As part of the deployment and implementation process, logs are reviewed and tuned to maximize security value relative to log ingestion costs. Often the log reduction process produces material cost savings to the client. As data collectors and data ingestion is maintained, log reduction and optimization is continued through the length of Service.

3.2. Security Event Monitoring & Threat Detection: Filters, normalization, correlation, and data analysis will be applied to identify potentially anomalous, suspicious, or malicious behaviors indicative of threats in the client's environment.

3.2.1. Investigation & Notification: Once a suspicious event is detected, an alert is generated and a BlueVoyant security analyst will perform triage and investigation of the event to confirm true-positive, benign, or false-positive. The client will be notified according to the nature of the event and service-level-agreements. When security cases are handled by the Security Operations team, this information is synchronized with the Client's Azure tenant for Client visibility.

3.2.2. Endpoint MDR (Separate): If a client has also purchased a separate BlueVoyant Endpoint MDR managed service, then the BlueVoyant security analyst will perform response activities on the endpoint as a result of the investigation if applicable and appropriate. *The Endpoint MDR managed service is defined in a separate service description.*

3.2.3. Indicator Enrichment: Indicators of Compromise ("IoCs") associated with detections are automatically extracted, scored, and enriched leveraging open source and BlueVoyant proprietary threat intelligence. Enriched IoCs are visible within Wavelength™ and are assigned a reputation (ex: Good, Suspicious, Bad) and classification (ex: botnet, Zeus, crypto-miner, etc.).

3.3. Health Monitoring: If BlueVoyant detects that agents and/or log collection sources become uncommunicative or unreachable or output has not been received from log sources that are within the scope of service, BlueVoyant will notify the Client and assist with troubleshooting.

4. Supporting Features and Teams

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

4.2. Azure Sentinel: Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. The tool supports the collection, correlation of data to enable threat detection and investigation for the BlueVoyant Security Operations Center.

4.2.1. Azure Sentinel Infrastructure: The collection, storage, and computation of the Azure Sentinel component will be hosted in the client's Azure instance/tenant.

4.2.2. Azure Sentinel SOAR: Azure Sentinel SOAR (leveraging Azure Logic Apps) is a useful component in performing automation within the Azure environment, especially tied to security incident automation. BlueVoyant will deploy and maintain a set of standard playbooks within the client's Azure environment to support the Service and provide key automations

including consumption reporting delivered through emails. The Client can build their own automations within the Sentinel platform or request custom playbooks through the BlueVoyant Sentinel Support Engineer (see below)..

4.3. Wavelength, BlueVoyant Customer Portal: The BlueVoyant Client Portal is a web-based portal that provides real-time visibility to alerts, confirmed incidents, SOC communications (approved client employees) and to view detected assets and vulnerabilities. Wavelength supplements the client's Azure Sentinel platform for Service visibility; Azure Sentinel is the client's primary method for Service and security program monitoring.

4.3.1. 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.

4.3.2. Reports: Available through Wavelength, reports include client environment content related to alerts, incidents, indicators, assets and vulnerabilities.

4.3.3. Threat Intelligence Reports: Threat landscape, sectorial, and intelligence summary reports are developed by BlueVoyant threat research and delivered as reports on a monthly basis.

4.4. BlueVoyant Orchestration and Automation: Although not directly visible to clients, BlueVoyant's internal orchestration and automation system is a key component of the BlueVoyant platform that supports the BlueVoyant Security Operations Center. Orchestration accelerates triage, reduces false positives, and improves mean time to resolve (MTTR).

4.5. BlueVoyant Client Success Team: The Client Success team is the primary support team for the client. The assigned Security 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 (typically monthly) to understand the 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.

4.6. Sentinel Support Expert: As part of the service, the client will have access to Sentinel Support Experts ("SSE"), a billed service for the creation of customized content. Billable hours are determined by "work effort", or the time it takes a SSE to build, test, and deploy the requested content to your environment. Sentinel Support Expert requests can be created via a service request or via your assigned Security Advisor. Supporting, maintaining, and tuning data sources to enable Service operation is included in the service, SSE work is intended only for custom client requested content. BlueVoyant has the right to refuse development of custom content for the Client based upon the effort or scope of the request.

4.6.1. Scope of Requests: The scope that the Sentinel Support Specialist will support includes (but is not limited to) development of customized dashboards, widgets, reports, alerts rules, playbooks based on event and/or available threat intelligence data, and informal user training of the Sentinel software. Alert tuning is included in the service by default; no Sentinel Support is required for tuning requests.

4.6.2. Limitations: All Support requests are subject to the technical and contractual limitations of the Azure Sentinel software as provided by Microsoft ("the Vendor"). All content requests are subject to review and approval by BlueVoyant. SSEs will spend no more than 2 hours per day with Client, to a maximum of 10 hours in a given business week. Due to the highly customized and dynamic nature of the Concierge service, there is no SLA for SSEs completion of concierge requests.

4.6.3. Billing: All Managed Azure Sentinel customers receive an initial pool of forty (40) hours of support experts' time to be used over the duration of the Service period. Additional hours can be purchased through your sales representative or the Client Experience Team. Any Concierge services provided during the Service Activation process are not counted against the pool.

4.6.4. Exclusions. Sentinel Support Experts do not fulfill requests for security consulting, posturing, incident response/remediation, legal, or audit support. Please contact your Client Experience Team advisor to direct these types of requests to the appropriate channels. For incident response, please email incident@bluevoyant.com (24/7) or call 646-558-0052 (8am-5pm EST)

4.6.5. Tracking: SSEs will record and report on hours on a weekly basis to Client as incurred, along with an email summary of work performed.

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

5.1. BlueVoyant Customer Portal: The BlueVoyant Customer Portal ("Wavelength") is a supporting method for clients to stay informed of security activity in their environment and activities of the BlueVoyant Security Operations Center. At any time, a client end user may go to the BlueVoyant Customer Portal and review any security alerts, dashboards, or reports.

5.2. Email: 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.

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.

5.3. Calling Security Operations: The BlueVoyant Security Operations Center (SOC) is available 24/7/365 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 Security Operations and will be authenticated when their call is received.

6. Log Collection

6.1. Syslog Collection: BlueVoyant may leverage Syslog as a method to collect logs from devices and systems in which APIs or an agent deployment for log collect is impractical such as a router or firewall. The Client is responsible for Syslog daemon deployment and management. BlueVoyant will notify the Client and assist with troubleshooting if an outage of the Syslog daemon is detected.

6.2. Collection Agents: Optionally, BlueVoyant agents may be installed directly on client endpoints and servers to enable log collection and delivery to the Client's Azure Sentinel instance. In some cases, specific third-party collectors (ex: Microsoft Monitoring Agent) would be delivered in-lieu of or included as a component in the BlueVoyant agent.

6.3. Cloud/SaaS Platforms: Log collection from cloud technologies or applications, such as Google GSuite, are integrated with Azure Sentinel through API by leveraging data connectors (provided by BlueVoyant or third-parties). Client is responsible for providing and maintaining API credentials for BlueVoyant.

6.4. Minimum Collection Sources: In order to provide the best detection and highest quality service, there is a minimum set of three (3) log collection source-types that must be monitored across the scoped environment. BlueVoyant reserves the right to refuse service and is unable to meet service level agreements if these sources are not included as part of the set of monitored sources in the associated service order.

6.4.1. Advanced Endpoint Visibility: Comprehensive visibility of activities occurring on the client's endpoints including behavioral detections. Visibility can be provided either through the BlueVoyant Managed Detection and Response (MDR) service, deployed Next-Generation Anti-Virus agents or deployed Endpoint Detection and Response agents.

6.4.2. User Authentication & Access: Visibility to users and user accessed systems typically provided through Azure Active Directory.

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

6.4.4. Network Perimeter Visibility: Not required but highly encouraged, provided access to log data associated with visibility of network traffic entering or leaving the client's on-premise environment, typically provided via Firewall or Next-Generation Firewall or equivalent within a cloud environment.

6.5. 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 signed Statement of Work ("SOW"). This consulting work is separate and distinct from the efforts of the deployment engineers described below.

6.6. Scope of Service: Although Azure Sentinel can collect many sources, standard or custom, 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 ingested source into the Azure Sentinel environment. The Azure environment is owned by the client and the client can configure the environment to ingest any data source they prefer, without support from BlueVoyant. For example, the client could configure a VOIP telephony system to ingest non-security logs into Azure; monitoring, alerting, and investigating any alerts for this source would be out of scope.

6.6.1. Unapproved Sources: Only data sources that have been included in the associated Service Order are allowed to be relayed to BlueVoyant collectors or agents. The client may receive additional charges related to the monitoring of any unapproved sources that are processed for monitoring by BlueVoyant. The client can leverage non-BlueVoyant technology for ingestion into their Azure infrastructure through separate ingestion methods. For example, if the client directs a syslog feed for an OT device that is not in the Service Order that is processed by BlueVoyant's ingestion pipeline, the client may receive additional charges., but not before notification from BlueVoyant to review additional ingestion and root cause of additional alerts.

7. Correlations & Detections

7.1. Managed Threat Correlations As part of the Service, BlueVoyant Security Content Engineering creates and delivers new correlations. The Client may use available Sentinel Concierge hours to request customized correlations, detections, and alerts that are deployed exclusively in the client's environment.

7.2. Client Developed Threat Correlations: Clients are able to develop their own reports, correlations, and alerts. The client can deliver the results of this content internally via email or other supported connection mechanism, but this content cannot be delivered to or actioned upon by the BlueVoyant SOC. The client can request the addition of correlations that the BlueVoyant SOC will monitor; upon review, the BlueVoyant SOC may add the correlation to the standard set of correlations.

8. Service Level Agreements

8.1. Security Event Monitoring: The Client shall receive a communication (according to the escalation procedures defined or in the manner pre-selected in writing by Customer, either through the Portal, email, or by telephone) to security incidents according to the matrix below. Event classification is measured by the time that an analyst has completed their investigation in order to prevent notification for benign or false positive alerts.

Severity	Definition	Agreement	Notification Method
Critical	Events that represent an imminent threat to client assets, including data destruction, encryption, exfiltration, or compromise by malware or malicious attacker.	**30 minutes** of event classification	1. Email 2. Phone Call 3. BlueVoyant Customer Portal / Azure Sentinel
High	Events that represent a significant threat to client assets, including rootkits, keyloggers, or trojans, but not defined as "critical", confirmed suspicious privilege escalation, confirmed social engineering-based attack.	**1 hour** of event classification	1. Email 2. Phone Call 3. BlueVoyant Customer Portal / Azure Sentinel

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	BlueVoyant Customer Portal / Azure Sentinel
Low	Events that represent a minimal threat to client assets. This including adware or other potentially unwanted programs (PUPs).	No Notification	BlueVoyant Customer Portal/ Azure Sentinel

8.2. Service Requests: Standard service requests (applies to all non-change and non- incident tickets) submitted via the Portal, Email, or via telephone will be subject to "acknowledgement" (either through the BlueVoyant ticketing system, email or telephonically) within one (1) hour from the time stamp on the Service Request ticket created by the BlueVoyant Platform.

8.3. Health Outages: Client notification of critical service outages affecting security monitoring of the client's environment. This SLA is notification of the client via email within four (4) hours of creation of a health incident alert. This SLA excludes low volume data sources in which detecting outage relative to baselines may not be accurate.

8.4. Maintenance Windows: BlueVoyant may schedule maintenance outages for BlueVoyant software which enables log collection (typically for collecting on-premise data sources) with 24-hours' notice to designated Client contacts. SLAs shall not apply during maintenance outages and therefore are not eligible for any SLA credit during these periods.

8.4.1. 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.

8.5. Client Service Outage: The SLAs shall not apply in the event of any Client-caused Service outage that prohibits or otherwise limits BlueVoyant from providing the Service, delivering the SLAs, 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.

8.6. 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 BlueVoyant platform or the Clients Microsoft Azure Instance.

8.7. 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 MSA, the foregoing SLA credit(s) shall be Client's exclusive remedy for failure to meet or exceed the foregoing SLAs.

9. 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.

9.1. 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.

9.1.1. 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.

9.1.2. Client Experience Team: At the beginning of client deployment, a BlueVoyant Client Success Advisor 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/from the Security Operations Center tied to security incidents.

9.1.3. Threat Profile: In order to provide organizational specific threat intelligence, BlueVoyant will collect information about the company 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.

9.1.4. 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.

9.2. 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 Client's Microsoft Azure Sentinel instance for storage and analysis.

9.2.1. Deploy Sentinel Instance: Client will grant BlueVoyant contributor access to their Azure instance in order to properly deploy and configure their Azure Sentinel instance.

9.2.2. Configure Lighthouse: Enable BlueVoyant Azure Lighthouse access. Azure Lighthouse is a key component to enable BlueVoyant to perform service activities in the environment. During the provisioning phase, the BlueVoyant Implementation team will work with the Client to properly onboard into Azure Lighthouse through various methods: marketplace, CLI, or other methods.

9.2.3. Deploy Security Content: During the provisioning phase, security content will be deployed to the Client's Azure Sentinel instance including, but not limited to correlations, workbooks, data connectors, and playbooks.

9.2.4. Source Configuration: Configuration of devices and applications to enable collection of logs. This often includes configuration of network devices such as firewalls to direct Syslog content to a BlueVoyant collector for log collection.

9.2.5. Log Reduction & Alert Tuning: During provisioning, logs are reviewed and tuned to maximize security value relative to log ingestion costs. Often the log reduction process produces material cost savings to the client. As data collectors and data ingestion is maintained, log reduction and optimization is continued through the length of Service.

9.2.6. 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.

9.2.7. 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.

9.3. 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.

9.3.1. 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.

9.4. 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.

10. Allowed Modifications: Client is able to create or modify searches, correlations, reports, workbooks, and alerts at any time without approval or notification to BlueVoyant; provided these changes do not impact BlueVoyant Monitoring. (see "Right of Review").

10.1. Right of Review. BlueVoyant has the right to modify client content that may cause negative impact on BlueVoyant monitoring capabilities. In the event that this occurs, BlueVoyant will inform Client of the removed or modified content.

10.2. Exclusions. Client may not modify any correlations, reports, workbooks, or alerts that have been marked as enabling the monitoring service including, but not limited to the content with the following designations: "BV_" or "BV-" or "MS" or

"SSC" prefix or suffix.. These markers indicate BlueVoyant-specific content that is required for SOC Operations.

11. Proprietary Content: BlueVoyant's customized correlations, data analysis methods, alerting schema, threat intelligence and reporting templates are considered the intellectual property of BlueVoyant. Unauthorized use, distribution, or reverse engineering is strictly forbidden.

12. Client Responsibilities

12.1. Software Deployment: During the service activation process, the client will deploy BlueVoyant Collector and Agent software 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.

12.2. Azure Resource Management: Client is responsible for providing stable access to Azure Sentinel instance including application of Azure Resource Management (ARM) templates, also known as Azure Lighthouse, in order to provision access for BlueVoyant Security Operations and Support. This will include, at minimum, access to Azure Sentinel, Azure Log Analytics, and Azure Logic Apps. BlueVoyant will provide the documentation necessary for completing this action.

12.3. Azure Sentinel Access: Client is responsible for applying Azure Resource Management (ARM) templates, also known as Azure Lighthouse, in order to provision access for BlueVoyant Security Operations and Support. This will include, at minimum, access to Azure Sentinel, Azure Log Analytics, and Azure Logic Apps. BlueVoyant will provide the documentation necessary for completing this action.

12.4. Digital Partner of Record: Client is responsible to add BlueVoyant as DPOR (Digital Partner of Record for Microsoft visibility and support.

12.5. Log Retention & Archiving: Client is responsible for managing their log archiving process through Microsoft Azure.

12.6. 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.

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

12.8. 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 the BlueVoyant client portal or approval to contact the Security Operations Center.

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

12.10. 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.

12.11. PII Obfuscation: Client is responsible for filtering all data delivered to BlueVoyant for Personally Identifiable Information (PII) or credit card information

13. 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.

13.1. 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.

13.2. Vulnerability Management Service (VMS): Delivers vulnerability scanning, remediation tracking, active asset discovery, and reporting.

13.3. Microsoft Threat Protection (MTP) security services: Any installation, configuration, tune-up and integration with Azure Sentinel of any MTP services

14. 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.

14.1. Breach Response & Compromise Assessment

14.2. Forensics

14.3. Vulnerability Patching and Resolution

14.4. Tabletop Exercises

14.5. Network architecture design

14.6. Hardware procurement

14.7. Security or Technology Training for End Users

14.8. Security Risk or Compliance Consulting

15. 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.

16. Additional Service Terms and Conditions:

16.1. Modify Terms: BlueVoyant reserves the right to modify the terms of this Service Description, including the SLAs, with 30 days prior notice.

16.2. Risk Elimination: This provides expert security analysis to the Client. However, deployment of BlueVoyant 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.