MANAGED SIEM

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 SIEM (the "Service") consists of BlueVoyant's monitoring of the contracted Client-owned 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").

   Management activities include Service implementation, configuration changes necessary for the successful provision of the Service, 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 WavelengthTM, the BlueVoyant Client Portal ("Wavelength").

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 (as specified on the Service Order) to enable collection of logs for security event monitoring. Logs are aggregated and stored within the BlueVoyant Platform from many sources including endpoint (workstations, laptops, servers, etc.),

network, applications, and cloud infrastructure. See Section 6 below for a detailed description of Log Collection.

3.2. Security Event Monitoring: 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. Reputational Detection: Utilizing BlueVoyant proprietary and open source threat intelligence, the Service detects potential threats based on reputation by correlating inbound and outbound network traffic to suspicious and/or malicious domains or IP address.

3.2.2. 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.

3.2.3. Managed Detection and Response (Separate): If a client has also purchased a separate BlueVoyant Managed Detection and Response (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 Managed Detection and Response managed service is defined in a separate service description.

3.2.4. 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 WavelengthTM 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 appliances 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.

3.4. Log Retention & Archiving:BlueVoyant stores s of searchable data in the hosted environment by default. After 30 days, data is archived (non-searchable) and no longer available for on-demand searches, correlations, or on-demand reporting. Extending the period of searchable data is available at additional cost. Archived data can be retrieved and delivered to clients per written request with associated retrieval fees. All Managed SIEM customers receive a minimum of one year (365 days) of data retention by default.

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. Splunk Enterprise: The Service is supported by a dedicated, single-tenant deployment of Splunk Enterprise to a specified number of client employees who will be granted access to the Splunk Enterprise application.

4.2.1. Licensing: BlueVoyant acquires a subscription for Splunk Enterprise on the Client’s behalf, based on daily data ingest volume. This volume is determined by the log source types and quantity provided during the sales scoping process, and is confirmed during Service Activation. Daily data volumes that exceeds what is quoted during scoping is subject to additional fees.

4.2.2. Splunk Enterprise Infrastructure: BlueVoyant will host the supporting Splunk Enterprise instance within the BlueVoyant Platform, and will configure and maintain on the Client’s behalf. Client will not have access to the supporting BlueVoyant Platform, platform infrastructure or any underlying configurations. BlueVoyant will manage these on the client’s behalf.

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.

4.3.1. Dashboards: Available through WavelengthTM, 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. Security Orchestration and Automation: Although not directly visible to clients, the 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 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 (typically 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.

4.6. SIEM Support Expert: As part of the service, the client will have access to SIEM 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. SIEM Support Expert requests can be created via a service request. or via your BlueVoyant Client Experience Team advisor.

4.6.1. Scope of Requests: The scope that the SIEM Concierge Specialist will support includes (but is not limited to) development of customized dashboards, widgets, reports, alerts based on event and/or available threat intelligence data, and informal user training of the SIEM software.

4.6.2. Limitations: All Concierge requests are subject to the technical and contractual limitations of the SIEM Software as provided by Splunk ("the Vendor"). All Concierge requests are subject to review and approval by BlueVoyant. SCSs 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 SCS completion of SIEM Concierge requests.

4.6.3. Billing: All Managed SIEM customers receive an initial pool of forty (40) hours of SIEM Concierge 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. SIEM Concierge does 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 the primary 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. BlueVoyant Collector: The BlueVoyant collector 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 collector.

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

6.3. Cloud/SaaS Platforms: The BlueVoyant platform is able to communicate directly via API with most cloud-based technologies and services for log ingestion, such as Microsoft Office365, and Google GSuite.. Client is responsible for providing and maintaining API credentials for BlueVoyant. Contact your sales representative for a list of supported services.

6.4. Minimum Collection Sources: In order to provide the best detection and highest quality service, there is a minimum set of four (4) 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. Network Perimeter Visibility: Visibility of network traffic entering or leaving the environment, typically provided via Firewall or Next-Generation Firewall or equivalent within a cloud environment.

6.4.2. 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.

6.4.3. 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.

6.4.4. 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).

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. Non-Security Data: Client may elect during the scoping phase to send non-security related log data to the SIEM Cluster, such as performance, transactional, or internal health monitoring data. Client is able to write their own dashboards, alerts, or reports against this data, but BlueVoyant will not monitor, report, or action against it. Non-security data applies against daily ingest volume for pricing and software subscription purposes.

6.7. 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.

6.7.1. Unapproved Sources: Sources that have been configured to relay their logs to a BlueVoyant collector or agent but are not defined in the Service Order 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 the unapproved source.

7. Correlations & Detections

7.1. Managed Threat Correlations As part of the Service, BlueVoyant Engineering implements and delivers new correlations. Client may use available SIEM

Concierge hours to request customized correlations, detections, and alerts that are deployed exclusively in the client's environment.

7.2. Client Developed Threat Correlations: Client 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.

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.

1. Email 2. Phone Call 3. BlueVoyant
Customer Portal

High

30 minutes

of event classification

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. Email 2. Phone Call 3. BlueVoyant
Customer Portal

Medium

1 hour

of event classification

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

Events that represent a minimal threat to client assets. This includes, adware or other potentially unwanted programs (PUPs). Low

BlueVoyant

No
Notification
No
Notification

Customer Portal

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. Maintenance Windows: BlueVoyant may schedule maintenance outages for BlueVoyant software which enables log collection 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.

8.3.1. 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.

8.4. 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.

8.5. 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 BlueVoyant platform.

8.6. 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 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 Experience 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 the Security Operations Center.

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 BlueVoyant platform for storage and analysis.

9.2.1. BlueVoyant Collector:Provisioning of client equipment and installation of the BlueVoyant collectors based upon agreed upon locations for collection for specific devices. Client would enable connectivity of BlueVoyant collectors to the remote BlueVoyant platform. BlueVoyant will provide minimum system requirements for hosting the BlueVoyant Collector software

9.2.2. BlueVoyant Agents: Deployment of the BlueVoyant agents to identified endpoints and servers to enable log collection. Client would enable connectivity of BlueVoyant agents to the remote BlueVoyant platform.

9.2.3. 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 collector for log collection.

9.2.4. Wavelength^{TM} 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.

9.2.5. 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; this includes a review of daily log volume ingestion to ensure the Splunk license sized during scoping is sufficient.

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, reports, dashboards, 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. Exclusions. Client may not modify any searches, reports or alerts with a “BV_” or “BV-” prefix. This indicates BlueVoyant-specific content that is required for SOC Operations.

10.2. Right of Review.BlueVoyant has the right to review and terminate all searches, reports, and dashboards created by Client if we determine (in our full discretion) that any of these are causing significant, negative impact on system performance or BlueVoyant monitoring capabilities. In the event that this occurs, BlueVoyant will inform Client of the removed or terminated content at our discretion..

10.3. Prohibited Changes: Client may not, at any time, modify or change any other aspect of the Splunk environment, with the exception of those items listed in 12.1, without review and approval from The BlueVoyant SOC.

11. SIEM Architecture & Content: BlueVoyant builds each Client’s SIEM infrastructure (or “SIEM Cluster”) to custom specifications as captured during the scoping process. It is important that the Client provides accurate information on current log sources as well as future growth in order to ensure the infrastructure and software subscriptions are sized appropriately. The Client may incur additional costs if the information provided during the scoping process is inaccurate or incomplete.

11.1. Data Structures & Schema: BlueVoyant will design the data structure & schema to following the Splunk Common Information Model (“CIM”). This best-practice method ensures optimal performance, data viability, and supports BlueVoyant's Proprietary Content

11.2. 3rd Party Applications: BlueVoyant will install, configure, log management software applications, modules, and technology addons in the SIEM Platform on Client's behalf. These software applications must be approved by the Vendor's software distribution platform and will be installed from the Vendor's software distribution platform. The software may be installed with or without custom modifications as required by BlueVoyant. If the requested application may incur additional fees, BlueVoyant will communicate and get client acceptance of these fees before installation

11.3. 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. Migration from an Existing Client Splunk Deployment For clients with an existing, operational installation of Splunk software, BlueVoyant will provide an evaluation, analysis, and cost estimate to migrate the existing installation. This engagement will occur with the Professional Services team under a separate statement of work

The initial phase of a migration project ("Health Check") will review existing architecture, use-cases, sourcetype data ingestion, and other technical requirements to ensure proper steady-state operations post-migration. Following the Health Check, BlueVoyant will perform a migration of the Splunk application stack and relevant data to ensure access to historical data and all client-owned Splunk application components as specified by the health check. A health check review is required prior to any migration project.

12.1. Health Check: The health check will consist of five (5) phases which BlueVoyant will conduct over the course of five (5) days (note: a separate statement of work is required for each Health Check):

12.1.1. Discovery**:** Environment Discussion, Architecture Review, Apps, User base and usage, internal use cases

12.1.2. Server Config and Health**:** Server Config, System resource utilization, Splunk configuration and consistency, review installed apps, review Splunk internal errors and messages

12.1.3. Data Review: Index sizing and configuration, forwarder health review, data feed review field extraction and data model review

12.1.4. Search Performance: Data Model Completion and scheduling, catalog of schedule searches, overall search performance analysis, identify long running expensive/ searches

12.1.5. Wrap up: Review, Roles and Access, Create Architecture diagram, as well and artifacts from the discovery phase, Identify areas for remediation.

And includes the following assumptions:

12.1.6. Client shall provide environment access suitable for completing this work

12.1.7. Client will provide a point of contact for the Consultant resource to work with

12.1.8. Client is responsible for all infrastructure and underlying dependencies for the Splunk environment

12.1.9. Client resource(s) with appropriate knowledge of requirements and resources will be made available during the project

12.1.10. Client resource(s) with Splunk functional and domain knowledge are available for feedback and consultation during the project.

13. Migration of Existing Detection as a Service to BlueVoyant Managed SIEM:

Migration from Detection as a Service (DaaS) to Managed SIEM will require a scope validation for all data sources and use-cases, followed by execution of a new Service Order.

After order execution and scope validation are complete, the client’s Managed SIEM environment will be provisioned and any data migration will be completed followed by initiation of the Service Activation.

14. Client Responsibilities

14.1. 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.

14.2. 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.

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

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

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

14.6. 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.

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

15. 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.

15.1. 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.

15.2. Detection-as-a-Services (DaaS): Delivered utilizing a shared-tenant Splunk environment as a best-of-breed Security Information and Event Management tool to monitor the Client’s devices and applications at the lowest possible cost. Clients do not have access to Splunk directly, but can request reports with specific parameters on-demand via support requests.

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

16. 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.

16.1. Breach Response & Compromise Assessment

16.2. Forensics

16.3. Vulnerability Patching and Resolution

16.4. Tabletop Exercises

16.5. Network architecture design

16.6. Hardware procurement

16.7. Security or Technology Training for End Users

16.8. Security Risk or Compliance Consulting

17. 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.

18. Additional Service Terms and Conditions:

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

18.2. 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.