Version 01/04/2023

BlueVoyant
MDR for Splunk Enterprise

Version 01/04/2023

Introduction

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

BlueVoyant Managed Detection and Response (MDR) for Splunk Enterprise (the "Service") is provided in connection with and is governed by the Client's signed Service Order/Proposal and separately signed BlueVoyant Standard Terms and Conditions (the "MSA") that explicitly authorizes the sale of managed security and consulting services. In the absence of a separate Agreement, the Services described under this Service Description will be governed by and subject to the terms and conditions of the BlueVoyant Standard Terms and Conditions ("MSA").

Description of Service

The Service consists of BlueVoyant monitoring the Client-owned Splunk Enterprise environment (the "Environment") as specified on the Service Order/Proposal and further described below. The Service provides the Client with 24 hours a day and 7 days a week ("24x7") security monitoring with detection and monitoring services, MDR support services, and access to professional services time and material services for both onboarding and ongoing support of the Environment. This Service utilizes the BlueVoyant platform (the "Platform") which includes automation, case management, and threat intelligence enrichment in conjunction with security analysts in BlueVoyant's Security Operations Centers ("SOC") and the Environment. The Client is responsible for any license, consumption fee, additional archiving, or long-term storage.

The Service will be executed according to this Service Description unless stated differently in the accompanying statement-of-work (SOW) for the following services:

The BlueVoyant Accelerator for Splunk Enterprise Platform (the "Accelerator") is a separate professional services engagement for implementation of the Platform into the Environment. This service is a one-time invoiced service. Accelerators are required for the MDR service.

MDR for Splunk Enterprise: This is an ongoing subscription for managed detection and response which includes a full-time 24x7 SOC. The details regarding this service are included below in the service features section.

Blue Voyant MDR for Splunk Enterprise Service Features

- **Security Event Monitoring:** The Service filters, normalizes, correlates, and analyzes network, user, device, and other IT and security logs, aggregating disparate data and

applying the latest detection methods to identify and respond to security events. Additionally, the BlueVoyant security operations team will proactively tune alerts respective to the Client's environment to filter out noise and false positives. If warranted to support further investigation of a Security Event, BlueVoyant SOC analysts may access the Environment via approved Identity Provider (IdP) access to perform further analysis.

- **Client Support**: Clients are provided support for break-fix issues on events that directly impact the Service or tuning of the Service, such as event flow disruption related issues related to TA's or detection content. Any enhancements, customizations, or requests deemed outside of client support activities are deferred to Professional Services.

- **Custom Support**: Clients are provided 20 hours of Splunk Professional Services to customize dashboards and alerts, and onboard additional data sources.

BlueVoyant Platform Features

- **Wavelength™ is the BlueVoyant client portal ("Wavelength™")**. A web-based portal that provides access to alerts, confirmed incidents, notes of investigations, and SOC communications (approved Client employees).
    - Dashboards: Available in Splunk, dashboards representing security insights, hygiene, and tuning are included with the service.
    - Reports: Available through Wavelength™, reports include monthly executive reports and CIS baselining.
    - Threat Intelligence Reports: Threat landscape,and intelligence summary reports are developed by BlueVoyant threat research and delivered as monthly reports.

- **Content:** The Platform will deploy and regularly update security detection algorithms ("Content"). This provides the ability to detect potential threats based on reputation by correlating data to suspicious and/or malicious Indications of Compromise. See *BlueVoyant Content* in **Scope of Service** section.

- **Security Orchestration and Automation**: There are two forms of Security Orchestration and Automation associated with BlueVoyant Services.
    - Lightspeed: Not directly visible to Clients, the BlueVoyant SOC-facing orchestration and automation system is a key component of the Platform that supports the BlueVoyant SOC. Orchestration accelerates case triage, reduces false positives, and improves mean time to resolve (MTTR).
    - Splunk Phantom: Clients are responsible for building and maintaining any Orchestration and Automation not directly provided via the Service. The Client

can leverage BlueVoyant Professional Services to assist with any SOAR based projects. Splunk Phantom or other SOAR projects will be scoped within a separate SOW.

Scope of Service

- The Service is limited to monitoring the devices & sources subscribed for service as defined in the associated Service Order/Proposal and does not include management or monitoring of any unsubscribed endpoint or intermediary log sources that have been configured to relay their logs to the Environment.
    - **BlueVoyant Content**: BlueVoyant Security Content Engineering continuously creates and deploys new and updated correlations to the Environment based on the data sources outlined in the Service Order/Proposal. As time passes and requirements change, the Client may elect to have additional Service Orders/Proposals created to onboard additional, net-new data sources. The customization required for the new development, testing, and deployment of new log sources will be done through Professional Services. Thereafter, support for the new log sources would be covered by this component of the service. Additionally, the Client may use Professional Services to request customized correlations, detections, and alerts that are deployed exclusively in the Client's environment.
    - **Client Developed Content**: The Client can develop their own reports, correlations, and alerts in the Environment. The Client can deliver the results of this content internally via email or other supported connection mechanisms, 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.

Service and Platform Requirements

Splunk Enterprise

- The Environment must meet the minimum Splunk specifications to allow for additional load and capacity.

    - **Licensing:** The Client must supply their own Splunk Enterprise license. The license must allow for adequate capacity for BlueVoyant to perform the Services.

    - **MDR Search Head:** The Client will host a Splunk Enterprise MDR Search Head ("MDR SH") peered to and capable of searching applicable data in the Environment. The minimum hardware requirements are:
        - 16 physical CPU cores, or 32 vCPU at 2Ghz or greater speed per core.
        - 16GB RAM
        - 200GB SSD Storage with minimum of 1200 IOPS.
        - The ability to install Cloudflare.
        - Firewall rules are required to establish Zero-trust connectivity
        - This is subject to change based on the environment analysis from the Accelerator engagement.

    - **Access:** The Service requires the Client to provide access to the Environment via secure means. Secure Zero-Trust tunneling is used to connect the SOC and Platform to the MDR Search Head only to run detections and investigate BlueVoyant created detections.
        - Personnel Access: The Service requires integrations of BlueVoyant Single Sign On and Multi-factor Authentication (MFA). The Accelerator will assist with the setup and configuration to ensure Client Role Based Access Controls (RBAC) are adhered to.
        - Client Access: Client access can be provided via LDAP configurations. Clients will receive read-only access to all BlueVoyant security content and data normalization. The Accelerator will support access configuration.
        - Platform Access: The Platform will access the MDR SH through two required service accounts. Authentication will be performed by Java Web Tokens (JWT) and tokens are refreshed every 30 days.

    - **Fundamental Data Sources.** Fundamental data sources support the Services Content feature. BlueVoyant has categorized five (5) Fundamental Data Sources

to ensure the most effective coverage possible. The following categories apply as Fundamental Data Sources.

- Network: Visibility of network traffic entering or leaving the environment, both on-premises and cloud. Sources include Firewalls (North-South Traffic Only), Web Proxy, and Domain Name Services.
- Authentication: Visibility to users and the systems in which they access typically are generated from centralized access such as Active Directory, Single Sign On (SSO), and Virtual Private Network (VPN) solutions.
- Cloud: Cloud based telemetry around workload processes and configurations are provided through AWS Cloudwatch, GuardDuty, Azure Event Hub, Azure Audit, and GCP Audit logs.
- Email: Metadata and filtering data around O365, Exchange, Google Web Apps including through third party systems such as Proofpoint.
- Endpoint: Visibility of endpoint activities occurring on the Client's endpoints including IoC and behavioral detections. This is provided by third party products such as Micorsoft Defender, Crowdstrike, and SentinelOne.
    1. Visibility can be provided by the Client's existing endpoint security solution provided it has an API or the ability to provide logs.

Security Event Monitoring

- The Client shall receive communication (according to the escalation procedures defined or in the manner pre-selected in writing by the Customer), either through Wavelength™, Email, or by telephone to security incidents according to the matrix below. Incident classification is the process that a BlueVoyant security analyst performs an investigation to confirm the validity of an alert, impact, and assign a severity. Notification times for Client notification are measured by the time difference between when incident classification has been 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 Levels

Severity	Definition	Agreement Notification Method
Critical	Events that represent an imminent threat to Client assets, including data destruction, encryption, exfiltration, or malicious interactive attacker.	30 minutes Email of event Phone Call Wavelength™ classification
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 Email of event Phone Call Wavelength™ classification

Medium Low	Events that represent a potential threat to Client assets, including malware types that include bots or spyware, but not defined as “critical” or “high”. Events that represent a minimal threat to Client assets. This includes adware or other potentially unwanted programs (PUPs).	Notification Wavelength™

- **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.
- **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 the Client.
- **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, software (including Splunk Enterprise), or devices by Client, its employees, agents, or third parties acting on behalf of the Client.
    - Where a Client-caused service outage degrades the Security Event Monitoring portion of the Service, any actions requiring the review of historical data during the time of the outage will be deferred to Professional Services. This includes requests such as data backfill, bad data recovery, and re-running correlations.
- **Third-Party Outage**: For log collection of third-party sources such as Software-as-a-Service or Cloud Infrastructure providers, including Splunk Enterprise Platform, SLAs are not applicable for any outages of the third party related to the delivery of their logs to the Platform. Any actions requiring the review of historical data during the time of the outage will be deferred to Professional Services. This includes requests such as data backfill, bad data recovery, and re-running correlations.
- **SLA Credits**: The 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 the 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 the Client within thirty (30) days from the date of the request. The total amount credited to the Client in connection with any of the above SLAs in any calendar month will not exceed the monthly Service fees paid by the Client for such Service. Except as otherwise expressly provided hereunder or in the MSA, the foregoing SLA credit(s) shall be the Client's exclusive remedy for failure to meet or exceed the foregoing SLAs.

Supporting Team Definition

- **Security Operations Center (SOC):** BlueVoyant's managed detection and response service is delivered through a cloud-native SOC, which operates 24 hours a day, 7 days a week. The BlueVoyant SOC is SOC II TYPE II certified and staffed with security experts with technical certifications including, but not limited to, Splunk certifications, SANS (GCFA, GCFE, CDIA, GCIA, GCIH), and CISSP.

- **Threat Fusion Cell (TFC):** The BlueVoyant Threat Fusion Cell (TFC) is a dedicated team of intelligence analysts and threat researchers operating within our SOC that identifies, prioritizes, and operationalizes information about threats that pose risks to our Clients. The TFC collects and curates feeds from 37 sources of data including BlueVoyant's proprietary dataset, as well as an open-source, partner, and paid intelligence to operationalize and contextualize malicious activities that could pose a risk to you. Threat intelligence includes all atomic indicator types such as SHA256, SHA1, and MD5 hashes, email addresses, URLs, domains, IP addresses, and CVE vulnerabilities. In addition, threat intelligence indicators may also include unstructured indicators on the dark web from web forums or data leaks.

- **Client Success Manager (CSM):** The Client Success team is the main point of contact and the overall relationship manager for the Client beyond communications to and from the SOC analyst team. The assigned CSM acts as the Client's consultant and enables the best experience for BlueVoyant services. The CSM 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 CSM is also engaged in any significant security events that occur for the Client. Additionally, the CSM will deliver any requested feedback to the BlueVoyant product and service delivery teams. The CSM will be the Voice of the Client within BlueVoyant.

Client Support

Health and Monitoring

- Health generated alerts are first triaged by BlueVoyant's health team. A determination will be made if the alert is viable, actionable, and positive. In the event that the source of the alert is related to BlueVoyant deployed technology, we will work with the customer to notify them through escalation paths established at onboarding time. Customer action may be required to return systems to functional status. The BlueVoyant event flow disruption monitoring is limited in scope to data flows that support MDR use cases.

- For issues related to customer infrastructure, configuration, or environment BlueVoyant will notify based on impact of the failure. If customer action is expected to be performed to help remedy the situation, we ask for prompt assistance assigning resources to support the outage. BlueVoyant assistance may be available, however additional charges may apply.

- No SLAs are applied to Health related alerts.

- BlueVoyant's Client Support team monitors for event flow disruptions and errors in Log Ingestion infrastructure. This function is broken into the following checks:

Checks	Description
Eventflow Disruption (Sourcetype)	Alerts BlueVoyant when a sourcetype from the last 14 days is missing for the last 30 hours.
Collector UDP Errors	Alerts BlueVoyant when UDP errors in the last hour are higher than the previously established baseline for the last 3 days.
High Disk utilization	Alerts BlueVoyant if disk space consumption exceeds 80%
Collector configuration file errors	Alerts BlueVoyant when Splunk internal logs exhibit a high rate of error for critical components.
System Load	Alerts BlueVoyant when the CPU and

	Memory load exceeds 95%
TLS/SSL Configurations Errors	Alerts BlueVoyant when TLS/SSL configurations experience issues that cause disruption in data flow.
Indexing Queuing	Alerts BlueVoyant when more than 2 Splunk queues maintain 100% blockage for more than 30 minutes.

Professional Services

- Professional Services provides customization services to the Environment based on requests by the Client. These customizations include:
    - Dashboard Creation
    - Alert Creation
    - Data Onboarding
    - 3rd-Party Systems Integrations
    - General Office Hours Session

- Professional Services are measured in work hours and determined by “work effort”, or the time it takes to build, test, and deploy the requested customization of the Environment.. Upon notification of a Service Request, either via email or Wavelength™, the Client receives an estimated work effort which is to be billed to the Client's account. The Service includes twenty (20) Professional Services Work Hours per 12-month term of the contract. Contracts less than 12-month term will be prorated at 1.6 hours per month for the term of the contract. If a Service Request is estimated to require more hours than are available, the Client will be required to purchase sufficient additional hours to cover the expected work effort. Additional Professional Services hours can be purchased through your Account Manager.

- Limitations
    - All Service Requests are subject to the technical and contractual limitations of the Environment. Due to the highly customized and dynamic nature of Professional Services, no SLA’s will be applied..
    - Professional Services does not fulfill Service Requests for security consulting, posturing, incident response/remediation, legal, or audit support.

Client Communications

- Below are the standard methods that the Service enables the Client to obtain information related to the Service or engage BlueVoyant staff.

    - **Wavelength™:** 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 Wavelength™ to review security alerts, investigation notes, dashboards, or reports.
    - **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 Wavelength™.
    - **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.

Client Responsibilities

- **Source Configuration**: The Client is responsible for configuring all log sources so that logs are appropriately sent to the agents and log collection infrastructure. This includes, but is not limited to, any intermediary log sources. If changes to the Client's existing network architecture are required for Service implementation, BlueVoyant will communicate these changes or requirements to the Client.
- **Notification of Environment Changes**: The Client will notify BlueVoyant of any environment changes that may affect the execution of the Service.
- **Notification of User Changes**: The Client will notify BlueVoyant of any necessary user account changes tied to Client employee transfers or terminations; this includes employees or contractors that have access to Wavelength™ or approval to contact the SOC.
- **Additional Remediation**: During investigations of security alerts the SOC may give guidance to the Client to perform specific actions in their environment in order to improve their security posture or to fully remediate an incident. The performance of these actions is the Client's responsibility.
- **PII Obfuscation**: If required, the Client is responsible for filtering all data delivered to BlueVoyant for Personally Identifiable Information (PII), credit card information, or any other confidential or sensitive information. BlueVoyant will assist the Client to ensure both parties understand what type of data is being transmitted to the Environment.

Additional Service Terms and Conditions

- If the Service Order/Proposal and MSA or 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 a copy of any data in BlueVoyant's possession. If a request is not received within this thirty (30) day period, BlueVoyant will permanently destroy all data pertaining to security devices no longer under a valid Service Order or Agreement.
    - "Data" as used above refers to data housed in BlueVoyant's environment, and does not extend to data contained in the Environment. You are responsible for any retained configuration or deployment assets.
    - Hourly consulting fees will apply for any time spent restoring archived data.
- Upon notification of Service Termination, BlueVoyant will remove all security detection algorithms and dashboards deployed by the Platform within thirty (30) days, provided that any Professional Services development, Client configurations, or data ingestion configurations implemented on behalf of the Client will remain in the Environment.