Version 01/24/23

BlueVoyant
Splunk Enterprise Accelerator - Basic

(Product Code - MSS-SPLUNK-ACCELERATOR-BASIC)

* - Tasks within the service that require an MDR subscription with BlueVoyant

Version 01/24/23

Introduction

This document (Service Description) describes the BlueVoyant Accelerator service (Service) being provided to you (Client, or you) by BlueVoyant.

Unless set forth in a writing signed by BlueVoyant and Client, or by you and a reseller authorized to market and resell BlueVoyant products and services, the Service is governed by the BlueVoyant Master Services Agreement available at https://www.bluevoyant.com/bvmsa (each an "MSA"), to the exclusion of all other terms. To the extent there is any conflict between this Service Description and the relevant MSA, this Service Description shall govern.

Description of Service

The Service is a professional services engagement and is a prerequisite for BlueVoyant's MDR services. The service includes consulting and implementation defined in accordance with each Client's specific requirements and executed in line with this service description, unless stated differently on their statement-of-work (SOW). This service is a one-time invoiced service.

The Service is comprised of the following:

- Performance of the following Splunk actions:
  - Configuring Access
    - Access to the Splunk Enterprise platform
    - Configure BlueVoyant Integration access *
  - IP Whitelisting *
  - Creation of BlueVoyant indexes to support BlueVoyant integrations *
  - Configuration of the stand-alone BlueVoyant MDR Search Head *
- Decide between a BlueVoyant Managed Collector or Intermediate Forwarder Tier (capped at 1)
  - BlueVoyant Managed Collector implementation *
  - Intermediate Forwarder Tier implementation
- Log source onboarding into Splunk (Capped at 10 sourcetypes)
  - Onboard in-scope technologies to Splunk using good practices with supported methods:
    - syslog
    - Splunk HTTP Event Collector (HEC)
    - Heavy Forwarder Splunkbase Apps
    - flat file monitoring with Splunk Universal Forwarders
- Deployment of BlueVoyant Splunk Security Content *
- Validation of the Splunk Platform with BlueVoyant integrations *
- Go-live with the SOC *
- Knowledge Transfer

Additional details:

* - Tasks within the service that require an MDR subscription with BlueVoyant

- Services are initiated through BlueVoyant's established deployment process for on-boarding Clients. Implementation will commence according to a mutually agreed-upon timeline, scope, and milestones.
- In-Scope technologies are identified during the sales process and outlined in the Technical Questionnaire (TQ). All data sources will flow from the TQ to the Project Plan and be considered in-scope. Any data sources not represented on the Project Plan are out of scope.
- The supported data onboarding methods include syslog, Splunk HTTP Event Collector (HEC), Splunkbase Heavy Forwarder Apps, and flat file monitoring with Splunk Universal Forwarders.
- Accelerator Services will not start until the Client has a Splunk environment.
- All onboarding work will be performed remotely.
- The onboarding team will be staffed by BlueVoyant Professional Services Consultants who specialize in Splunk and data analytics.
- Standard Accelerators are capped at 240 hours. Additional hours used above 240 will be billed at standard Professional Services hourly rates.

Client Responsibilities

a. Log sources must be in English.

b. Log sources must include a timestamp with date, time, and timezone.

   i. Any log sources onboarded not containing the above time requirements will have Splunk auto-timestamping configurations applied.

c. Services are initiated through BlueVoyant's established deployment process for on-boarding new Clients. Implementation will commence according to a mutually agreed-upon timeline, scope and milestones.

d. Clients will be assigned a technical project manager (TPM) who will be your point of contact during service deployment. The TPM will align technical resources from both organizations, as well as track or intercede to comply with project goals for successful implementation and deployment.

e. Client is responsible for installation and configuration of any software or services in the Client's environment, such as agents, sensors, log collectors, universal forwarders, and virtual machines.

f. Client will provide remote access to configure the intermediate forwarder architecture tier during the Accelerator.

g. Client will provide and configure a Load Balancer for proper distribution of events across intermediate forwarder architecture tier, if required.

h. Splunk Enterprise Platform licenses and maintenance is Client's responsibility

i. Client will conduct maintenance and patching to all components deployed in their

* - Tasks within the service that require an MDR subscription with BlueVoyant

environment.

j. Custom content creation in Splunk such as dashboards, alerts, and reports are not in scope of this service.

k. The Client is responsible for API development and software integration.

l. Compliance regulatory control reviews are not in scope of this service

* - Tasks within the service that require an MDR subscription with BlueVoyant