## Service Definitions

- **“Affiliate”** is any legal entity which directly or indirectly, holds more than fifty percent (50%) of the shares or voting rights of a Party. Any such legal entity shall be considered an Affiliate for only such time as such equity interest is maintained.

- **“Appliance”** shall refer to hardware device which may be pre-loaded with Software and installed on Customer’s environment to enable DeepSeas’ performance of the Services. This includes, but is not limited to the network sensors, collectors or other hardware provided under this Agreement.

- **"Associated Parties"** shall refer to a Party’s Affiliates, directors, officers, employees, agents, licensors, vendors, or subcontractors.

- **“Authorized User”** shall refer to any employee or third-party user that requires access to the Software or Services and has been identified in writing by Customer to DeepSeas as being authorized to use the administrative components of the Software or Services.

- **"Availability"** shall mean the percentage of time a specific component of the Services is Available to the Customer during a given month, subject to certain exceptions.

  TOTAL NUMBER OF MINUTES PER MONTH SERVICE AVAILABLE TO CLIENT AVAILABILITY = TOTAL NUMBER OF MINUTES IN THE MONTH

  - Example: If total number of minutes the Software was unavailable to the Customer (for reasons not set forth in the list of exceptions in Exhibit D) was 120 minutes and the total number of minutes in the month is 43,200, then the Availability calculation for that month would be as follows:

    43080/43200 = 99.72% Availability

- **“Confidential Information”** shall not include any discovered malware or information comprising non-identifying data gathered from performing the Services (e.g., types of malware discovered, modes of attach engaged, etc.).

- **“Compromise”** shall refer to an Incident ranging from an individual/small-scale operation (e.g., insiders, suppliers and activists) to large-scale, organized efforts (e.g., perpetrated by criminal networks and/or foreign governments).

- **“Covered Device”** shall refer to Customer log device or data source specified within the SOW and including information describing the log source such as the device’s manufacturer, vendor, Device Type, and specified use case.

- **“Custom Log Source”** or **“Custom Device”** shall refer to any log source that requires development of software code to parse log data for the Analytics Platform. Examples

include the following: Application logs, web server logs, database logs, or any devices as defined by DeepSeas.

- **"Customer Information"** shall refer to any information, records, data, or any other materials (in whatever form) entered into the Software or Endpoint Software by Customer or any User or any Authorized User

- **"Customer Portal (CP)"** shall refer to the internet-based web portal designed to provide log data, alerts, reports, graphs, dashboards, analysis tools, Customer tickets, notifications, and other related information applicable to the Services.

- **"DeepSeas"** includes its subsidiaries and Affiliates, and their respective directors, officers, employees, agents, attorneys, representatives, subcontractors, and suppliers.

- **"DeepSeas Materials"** includes:
    - Any Software, hardware, documentation, and/or other materials including, without limitation, the following information:
        - Software and Appliances.
        - Computer software (object and/or source codes and/or scripts), programming techniques and programming concepts, methods of processing and use, and system designs embodied in the software.
        - Benchmark results, manuals, program listings, data structures, flow charts, logic diagrams, functional specifications, file formats.
        - Intellectual Property Rights, including but not limited to, discoveries, inventions, concepts, designs, documentation, product specifications, application program interface specifications, techniques and processes relating to the software.
    - The research and development or investigations of DeepSeas.
    - Product offerings, content partners, product pricing, product availability, technical drawings, algorithms, processes, ideas, techniques, terms and conditions of this Agreement, formulas, data, schematics, trade secrets, know-how, improvements, marketing plans, Customer lists, financial information, forecasts and strategies.
    - Any information about or concerning any third party (which information was provided to DeepSeas subject to an applicable confidentiality obligation to such third party).
    - Any enhancements, modifications or derivatives of such materials. DeepSeas Materials shall be considered Confidential Information.

- **"Device Type"** shall refer to the category name used to classify a Covered Device for purposes of determining the pricing category specified within the SOW. DeepSeas may at its own discretion update, refine, add, remove, and re-categorize Device Types at its sole and complete discretion.

- **“Enablement”** shall refer to work undertaken by DeepSeas to set up, configure, implement, and provision the Services.

- **“Endpoint Software”** shall refer to the Endpoint Detection & Response software provided by DeepSeas for Customer use and in accordance with the terms of this Agreement and the Endpoint EULA included in the Service Description.

- **“Engagement Period”** shall start upon the Effective Date and shall end upon completion or other termination of the SOW.

- **“Events per Second (EPS)”** shall refer to total quantity of Log Events received in aggregate from all Covered Devices during any 24-hour period converted to seconds.

- **“Host/Network Log Source”** shall refer to the Device Type name that refers to a defined category of devices including windows and Linux servers, PCs, routers, switches, wireless access points, and other similar devices as defined by DeepSeas and that DeepSeas may update or change from time to time.

- **“Incident”** shall refer to the presence of malicious software such as Trojans, worms, viruses, and spyware; password phishing; cyber-attack; cyber-intrusion; hacking; data breach; unauthorized access; denial of service; malware; bots; system Compromise or other computer security breach.

- **“Log Analytics Platform”** shall refer to a system that collects and analyzes log data feeds from the Customer’s network and security devices with the purpose of identifying activity, patterns and behaviors that are an indicator of a security threat.

- **“Log Collector”** shall refer to DeepSeas’ hardware Customer Premise Equipment (CPE) or software placed within the Customer’s network or virtual environment for delivering the Service to the Customer. The Log Collector collects, aggregates, and/or analyzes the Customer’s log data sent to it from the Covered Devices.

- **“Log Collector Type”** shall refer to DeepSeas’ Log Collector which will be specified as either a “Physical” Log Collector, or a “Virtual” Log Collector. A Physical Log Collector is a PC server-based hardware appliance, and a Virtual Log Collector is a software image, agent, or application prepared for installation into a Customer’s virtual infrastructure, server, or workstation.

- **“Log Event”** shall refer to log data output in the form of a common syslog formatted data stream received from a Covered Device by the Log Collector.

- **“Managed Detection and Respond Services”** includes validation of alerts generated by the Endpoint Software and Software, delivering notification to Customer of any legitimate threats identified from an alert, monitoring of all Endpoint Software and Software to ensure it is up to date, running and operating as expected. Identification of legitimate threats without the aid of an alert is considered Threat Hunting. Response that requires reverse

engineering, Customer threat research, on-site support at a Customer location, coordination of remediation activities across multiple systems or response to a historic embedded attack is considered Advanced Incident Response.

- **"Party/Parties"** shall refer to either DeepSeas or Customer in the singular or to both DeepSeas and Customer together when used in the plural form.

- **"Private Information"** includes information comprising personally identifying (e.g., PHI, ePHI, PPI, PCI, PHP) or proprietary network information related to Customer and third parties which interact with Customer. Private Information may also include network, equipment, files, databases, logs, and other sources of information which may support the Services.

- **"Provisioning Document"** shall refer to a document provided by DeepSeas which contains requested information and documentation from the Customer needed to properly set-up and configure the Services. Information to be provided by the Customer within the Provisioning Document include the placement of Log Collectors in the Customer network, power, rack and cabling requirements, IP address assignments, device weighting, zone information, location, network segments, DMZs, etc.

- **"Services Charge"** is the sum of the labor Fees and the travel related expenses/other actual expenses/costs provided described in this SOW

- **"Service Level"** shall refers to the scope of the services provided by the DeepSeas to the Customer, which include the predefined responsibilities, duties, tasks, and obligations of DeepSeas. The Service Level Agreements (SLA) available to the Customer.

- **"Service Option"** shall refer to an optional service component that offers coverage for an additional specified capability for an additional cost to the Customer and further defined within DeepSeas' Scope of Work.

- **"Services"** shall refer to services, including monitoring services and access to the Software, provided by DeepSeas as identified in this SOW.

- **"Software"** shall refer to the software provided by DeepSeas as identified in SOW other than Endpoint Software.

- **"SOC"** shall refer to the Security Operations Center where DeepSeas' security operators, analysts, engineers, and other personnel perform analysis and triage of logs, Alerts, Security Events, and provide response or communications with the Customer as appropriate.

- **"Threat Hunting"** shall refer to the proactive service designed to identify attacks independent of an alert generated from any other service.

- **"Threat Notification"** shall refer to the information provided by DeepSeas in response to a Security Event or other event requiring Customer notification as determined by

DeepSeas. Security Event Notifications are provided via a phone call or in the form of a Threat Notification, which is DeepSeas' Customer notification template.

- **"User"** shall refer to any individual affiliated with Customer, including Customer's Authorized Users, that gains access to the Software or Services or that transmits any data to or through the Software or Services because of this SOW.