SERVICE ORDER ATTACHMENT FOR
SILVERSKY MANAGED DETECTION & RESPONSE

Capitalized terms not defined in this Attachment will have the meanings set forth in the MSA.

1. **"Services"** will mean SilverSky, as purchased by you on the order and incorporated herein by reference. The **"Launch Date"** of Services under this Attachment will mean the date on which Service(s) or any part of the services provided under the terms of this Attachment are first made available to you.

2. **Levels.** We will provide the Services pursuant to the objectives of the SilverSky Service Level Agreement set forth below.

3. **Customer Responsibilities.** During performance of the Services you will:
   - I. Prior to engagement commencement, assign a project management contact to serve as a primary contact through the delivery and performance of the Services;
   - II. Ensure complete and current contact information is provided on a timely basis;
   - III. Cooperate during the deployment period, including providing to us all required information in a complete and accurate form to prevent implementation delays which may result in additional fees;
   - IV. Appoint one or more authorized contacts authorized to approve and validate all requested changes;
   - V. Implement change requests; and
   - VI. Provide all necessary information with respect to your environment.
   - VII. Provide necessary hardware along with maintenance and support contracts to run log collectors within your environment.
   - VIII. Send log data in an encrypted manner, or via the agreed log collection device/type.
   - IX. Ensure that the format and quality of the data being sent to SilverSky is sufficient enough for SilverSky to provide the Services.

   You acknowledge that your fulfillment of these responsibilities is essential to our ability to perform the Services in a timely manner.

4. **Performance Evaluation.** You authorize us to evaluate service upgrades and changes on an annual basis at each of your locations which utilize the Services. In the event that such evaluations identify ways to improve performance or service at no additional cost to you, you authorize us to implement them.

5. **Term and Termination.** This Attachment will be in effect during the Initial Term set forth in *your order*, and will thereafter automatically renew for additional one year terms unless either of us provides the other with written notice of the intention not to renew at least 60 days prior to the beginning of the renewal term. Sections 1, 5, 6, 7, 8, and 9 of this Attachment will survive the expiration or termination of this Attachment for any reason. The provisions of the MSA that are identified in the MSA as surviving the expiration or termination of the MSA will, as they apply to this Attachment, also survive the expiration or termination of the Attachment for any reason. Within 10 days after the expiration or termination of this Attachment for any reason, you must pay all fees accrued and unpaid at the time of termination, and the cancellation fee if applicable.

6. **Fees.** You will pay us the fees set forth in order for Services you purchase. We will invoice you monthly except as may otherwise be indicated in your order. We reserve the right to increase fees on an annual basis if due to increases for the underlying technology or other general inflationary pressures.

7. **Cancellation Fee.** If this Attachment is terminated prior to the end of the Initial Term or any renewal term, for any reason other than our material breach of this Attachment or the MSA, you will pay us a cancellation fee. The cancellation fee will be equal to 100% of the greater of (a) your average monthly invoices or (b) the Minimum Fee, for the six months prior to the date of termination multiplied by the lesser of (x) the number of months remaining in the then current term of this Attachment or (y) 12 months. The cancellation fee constitutes liquidated damages and is not a penalty. You acknowledge that, if Services are cancelled prior to the completion of the Initial Term or any renewal term, SilverSky's damages will be difficult or impossible to ascertain. Your obligation to pay the cancellation fee is in addition to, and not exclusive of, your obligation to pay all fees accrued and unpaid at the time of termination for any reason.

8. **Additional Disclaimers.** We do not guarantee continuous, uninterrupted, virus-free or secure Services, and we are not liable if you or your end users are unable to access the Services at any specific time. We do not guarantee that we will be able to replace any of your information, content or other data that may be lost, damaged or stolen resulting from use of the Services.

SERVICE LEVEL AGREEMENT:
FOR MANAGED SECURITY SERVICES

The following terms and conditions apply to the service levels of Services provided pursuant to this Attachment. In the event we fail to meet the levels defined in Service Level Agreement for a minimum of two (2) consecutive months, you must notify us in writing of any violations and allow us thirty (30) days from notification to cure the breach. If still unresolved, you may immediately terminate the Service giving rise to such breach without additional notification or incurring early termination fees within thirty (30) days of our failure to cure.

1. SERVICE HOURS OF OPERATION. We maintain Security Operations, Network Operations, and Technical Support departments on a 24 x 7 x 365 basis. You may reach an individual in each of these departments by calling the appropriate support service.

2. RESPONSE TIME. We commit to certain incident response times. These commitments are subject to your providing us accurate and current contact information for your designated points of contact. Our failure to respond in accordance with the parameters defined herein will entitle you to receive, as your sole remedy and our sole obligation, credits described below, *provided however*, that you may obtain no more than one credit per day, regardless of how often in that day we failed to meet these parameters.

2.1 Definitions of Incident Severity

Critical – This category of incident may have a severe impact to your network or system and indicates a compromise. Samples of incidents that fall under this category: malware infection, backdoor or Trojan traffic, outbound DDoS, and bot net traffic
High – This category of incident may have a high impact on your network or system and could lead to malware infection, data leakage, and disruption of operations due to network or system down time. Samples of incidents that fall under this category: download of malicious software, leakage of file from internal network, DoS or DDoS, P2P traffic (torrent), cloud storage traffic, and exploit launching
Medium – This category of incident has a medium level of impact on your network or system and could lead to unnecessary leakage of information or exposure of vulnerabilities Samples of incidents that fall under this category: port scans, vulnerability scans, social media traffic, unusual network traffic, and multiple failed logins
Low – This category of incident shows little impact on the client. This is mostly informational alerts to inform the client. Samples of incidents that fall under this category: login or logout notifications, failed login notifications, application or system update notification, and application or system error message
Informational – This category of incident shows no impact on you. This is only informational alerts to track activity. Samples of incidents that fall under this category: false positives, approved scanning vendors, and test alerts.

The severity level of each incident is determined by the us based on the nature of the incident identified. You may indicate to us that an identified incident is of a lower priority if you are not vulnerable to such attack.

2.2 Incident Severity Response Times

Critical/High Alerts - Response within 10 minutes upon identification of incident and a Tier 1 credit if missed
Medium/Low Alerts - Response within 24 hours upon identification of incident and a Tier 2 credit if missed

3. SERVICE AVAILABILITY GUARANTEE. Our commitment is to have the Services available 99.5% of the time and as set forth below. At your request, we will calculate the number of minutes the Service(s) were not available to you in a calendar month ("Service Unavailability"). Service Unavailability will not include unavailability continuing for an hour or less or any unavailability that you fail to report to us within five (5) days. Failure to meet the service level described in this Section will entitle you to receive a Tier 1 credit.

4. MAINTENANCE. We reserve the following weekly maintenance windows during which you may experience periodic service outages:

(i) Tuesday and Thursday (12 AM – 2 AM ET)

(ii) Saturday (12 AM – 5 AM ET)

In the event we must perform maintenance during a time other than the service windows provided above, we will provide notification prior to performing the maintenance.

5. CREDIT REQUEST AND PAYMENT PROCEDURES. For failures to meet service levels herein in a calendar month, you will be entitled to receive a credit as specified below:

(i) **Tier 1.** Equal to twice the prorated portion of the monthly fee for the affected service; or

(ii) **Tier 2.** Equal to the prorated portion of the monthly fee for the affected service;

provided however that a breach of this SLA due to Exceptions described below will not qualify for such credits.

To receive a credit under this SLA, you must be current with your payments at the time Service Unavailability occurred. In addition, all credit requests must be submitted in writing, either through our ticketing system, via email or fax, or by certified U.S. mail, postage prepaid. You must submit each request for credit within seven (7) days of the occurrence giving rise to the credit claim. The total credit amount we will pay to you in any calendar month will not exceed, in the aggregate, half of the total fees invoiced to you for the Services for which a claim is made in the applicable month. (Credits are exclusive of any applicable taxes charged to you or collected by us.)

6. EXCEPTIONS. You will not receive any credits under this SLA in connection with any failure or deficiency of the Services or a failure to meet service level caused by or associated with any of the following:

(i) Maintenance, as defined above;

(ii) Fiber cuts or other such issues related to telephone company circuits or local ISP outside of our control;

(iii) Your applications, equipment, or facilities;

(iv) You or any of your end-user' acts or omissions;

(v) Reasons of Force Majeure as defined in the MSA;

(vi) Any act or omission on the part of any third party, not reasonably within our control;

(vii) First month of service for the specific Services for which a credit is claimed;

(viii) DNS issues outside our direct control;

(ix) Broadband connectivity.

7. FAIR USAGE CAP FOR LOG COLLECTION ON MONITORING SERVICE

(i) SilverSky maintains a fair usage policy to ensure the availability and sustainability of the Monitoring Service. Failure to adhere to the fair usage policy will result first in a notification to you and then, if you fail to take remedial action, suspension of this SLA until such time as the usage level on the affected device falls below the notification threshold set forth below. Usage information is made available to you within our portal.

1. SilverSky will notify you that you are exceeding the Fair Usage Threshold or "FUT" when you exceed any of the following FUTs:

   1. The average events per second across the set of monitored devices exceeds 10 events per second per device, over a 7 day period. An individual device exceeds an average of 100 events per second, over a 1 hour period

   2. The average events per second across the set of monitored devices exceeds 10 events per second per device, over a 30 day period.

(ii) Partial Service Suspension Threshold

Following the notice as set forth in (i) 1.1 above, if the average events per second across the set of monitored devices exceeds 10 events per second per device, over a 7 day period, SilverSky reserves the right cease ingestion of security events from an affected device, starting from the device producing the most events per second, until the average events per second across the set of monitored devices falls beneath the FUT.

Following the notice posted to the portal as set forth in (i) 1.1 above, if an individual device exceeds an average of 100 events per second, over a 1 hour period, SilverSky may upon notification to the Customer cease ingestion of security events from the affected device.

Managed Detection & Response

SCOPE OF WORK

We will provide the customer with the following services:

a. Cyber Threat Detection: Collect event and log files from devices on the Customer's network and ingest them in to our analytic engines for risk identification and notification. All automated alerts will be sent to you through the portal along with email notifications.
b. Threat Intelligence Integration: Incorporate current threat intelligence feeds, including over 1-million indicators of compromise which are updated hourly. This threat intelligence technology is intended to improve the accuracy of risk identification process and to reduce overall false positives and provide early warning to serious threats facing you.
c. Security Analysis: Cybersecurity analytic engines, managed by security analysts, will create, assess, and escalate each alert which can be managed through the portal to reduce false positives in order that only actionable incidents are sent to the Customer for further investigation or remediation.
d. Remediation Guidance: The Incident Response Platform will alert the Customer of events requiring immediate attention, and provide guidance on how to best mitigate and remediate issues as they occur.
e. Security/Compliance Reporting: The portal will allow the Customer to schedule and run reports covering various areas of cybersecurity and Compliance. This will allow the Customer to prepare evidential matter around possible breaches in security, risk mitigation taken, and other elements of the environment to demonstrate its compliance efforts to interested parties.

SERVICE IMPLEMENTATION

SilverSky Responsibilities

a. Conduct a knowledge-sharing survey to collect information about the Customer's environment, including devices to be monitored and processes needed to support the implementation of services.
b. Establish a secure method of transmitting logs from the Customer network to the platform.
c. Provide assistance to the Customer to configure devices chosen for monitoring.
d. Notify the Customer of receipt of logs and confirm proper operational integration to ensure alerting.
e. Provide initial training and training materials for the portal.

Customer Responsibilities

a. The Customer shall designate a qualified and trained Technical Lead to oversee the Customer engagement for this project. The Technical Lead will oversee the project, track status, facilitate the delivery of services and progress of the project, and communicate to the Customer's stakeholders.
b. If necessary, provide a virtual host or device which meets the system requirements of the log collector, as directed by us.

Service Deliverables

a. Capture device logs from the Customer's monitored devices.
b. Perform analysis of the log data. This includes, but is not limited to, aggregation, parsing, correlation and alerting.
c. In cases of significant risk, our security engineers will analyze incidents following an alert by the system-risk notification system.
d. Security Engineers will notify the Customer of incidents requiring a response. Instructions on threat remediation and consultation will be provided.
e. 24/7/365 phone-based incident support for additional investigation and guidance for the Customer.
f. Security alerts will be sent to the Customer within 10-minutes of its creation.

ASSUMPTIONS

SilverSky

a. Shall provide resources who have been trained on products, technologies, and services applicable to this Scope of Work.
b. All communications, notifications, and alerts will be provided to Customer.

Customer

a. The Customer shall furnish, in a timely manner, all resources including personnel, systems, information, and software

necessary to commence service implementation.

b. The Customer shall designate an appropriately qualified and trained technical lead who will be a permanent stakeholder throughout engagement.
c. The Customer retains authority and responsibility for decisions made regarding this service implementation.
d. The Customer will be responsible for project management and coordination of Customer resources necessary to complete the service implementation.
e. The Customer is responsible for coordinating, following, and communicating in a timely manner all internal processes for change management, SDLC, etc.
f. The Customer is responsible for the quality of data and any remediation efforts that may be necessary to complete this service implementation.
g. The Customer is accountable for all non-oral output, including documentation, plans, recommendations, diagrams, etc.
h. The Customer is responsible for any direct or physical remediation.