SERVICE ATTACHMENT

LIGHTNING MANAGED DETECTION AND RESPONSE

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

"Services" will mean SilverSky Lightning Managed Detection and Response (MDR) Services.
Service SKUs:

- S-200-2031 SilverSky MDR Standard User License
- S-200-3032 SilverSky MDR Server License
- S-200-3033 SilverSky MDR Office 365 License
- S-200-3049 SilverSky MDR Light User License
- S-200-3056 SilverSky MDR SMB User License
- S-200-3057 SilverSky MDR SMB Server License
- S-200-3058 SilverSky MDR SMB Office 365 License
- I-200-3031 SilverSky MDR Standard User Install Fee
- I-200-3032 SilverSky MDR Server Install Fee
- I-200-3033 SilverSky MDR Office 365 Install Fee
- I-200-3049 SilverSky MDR Light User Install Fee
- I-200-3056 SilverSky MDR SMB User Install Fee
- I-200-3057 SilverSky MDR SMB Server Install Fee
- I-200-3058 SilverSky MDR SMB Office 365 Install Fee

1. Lightning Managed Detection and Response Service Description

We will provide the Customer with the following Lightning MDR Services:

A. SilverSky Lightning Platform to ingest Syslog Data or security-related data from an agreed upon set of data sources including on-prem devices, endpoints, webapps, authentication gateways and cloud infrastructure. All of the ingested Data is automatically enriched with threat intelligence information, matched against a variety of Indicators of Compromise and intelligently cross-correlated to detect known and anomalous hostile cyber-security activity across customer infrastructure.

B. 24/7/365 coverage over all actionable alerts routed to our monitoring and detection platform; such alerts are reviewed by an Analyst on a 24/7/365 basis. Customers get full visibility into all alerts.

C. Investigation mapping within the SilverSky Lightning Platform utilizing the MITRE Attack framework.

D. Customer will have a dedicated Account Manager and Cybersecurity Advisor. In addition, you will access our global security operations team for investigations, threat hunting, and real-time support. *Note*: The dedicated cybersecurity advisor only applies if the recurring monthly fee associated with the contract herein is $500 or greater and is not applicable to the SMB service SKUs. In addition, SMB customers do not have access to a dedicated Account Manager.

E. Customized Playbooks: to provide notifications to identified client contacts via agreed-upon, specified communication formats. We will provide guided remediation recommendations and or responses for customers subscribed to our Managed Endpoint Detection and Response (MEDR) or Network Protect services whichever is applicable. For Customers subscribed to our MEDR service we will have the ability to potentially contain attacks at the endpoint utilizing the SilverSky deployed SentinelOne Singularity Complete agent. For Customers that are subscribed to our Network Protect service where SilverSky has the management of the firewall device we will have the ability to block IPs.

F. Reporting: a set of customizable reports and report templates including, but not limited to, Executive summaries and threat and compliance reports.

G. Full data ingestion[1]: Data is not subjective to ingestion cost and is captured within the MDR user/service price. Data is retained for one year (30 days in hot storage and 1 year in cold storage).

2. Responsibilities

A. SilverSky Responsibilities for Deployment

I. Conduct a knowledge-sharing survey to collect information about the Customer's environment, including ingestion data types and sources to be monitored and processes needed to support the implementation of services.
II. Establish a secure method of transmitting logs from the Customer network to the Lightning Platform.
III. Provide assistance to the Customer to configure data sources chosen for ingestion.
IV. Notify the Customer of receipt of logs and confirm proper operational integration to ensure alerting.
V. Provide initial training and training materials for the SilverSky Lightning Platform/portal.
VI. Tuning of alert detections and responses to reduce false positives or unwanted notifications.

[1] Full data ingestion applies to the following agreed upon, standard data sources: Network Data Firewall, DNS, Active Directory, Switches, Routers, Access Points, Domain Controllers, Vulnerability Management Solutions, and Endpoint Security Tools.

B. Customer Responsibilities

During the performance of the Services Customer will:

I. Prior to engagement commencement, assign a project management contact to serve as a primary contact through the delivery and performance of the Lightning MDR Services.
II. Ensure complete and current contact information is provided on a timely basis.
III. Cooperate during the deployment period, including providing SilverSky with 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.
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 the format and quality of the data being sent to SilverSky is sufficient for SilverSky to provide the Lightning MDR Services.
X. Retain authority and responsibility for decisions made regarding this service implementation; and assume responsibility for any direct or physical remediation.
XI. Customer is responsible for maintaining their own Microsoft licensing in order to send O365 telemetry to the Lightning MDR service.

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

3. 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**.**

a. All ingested events are channeled through our proprietary platform, wherein the events undergo processes of normalization, enrichment, and correlation matching against our extensive threat intelligence, Indicators of Compromise (IOC's), and other rule sets based on predefined thresholds. Furthermore, select events are directed to and subjected to thorough analysis by our advanced analytics engine.
b. Within our platform, alerts are aggregated employing sophisticated patterns of intelligence-driven detection. These resultant alerts are subsequently organized, prioritized and routed to our proficient team of analysts for ongoing monitoring and assessment.
c. Our analysts diligently oversee these identified incidents, document their comprehensive analyses, and our playbooks promptly notify clients following their response plan.

C. Upon the detection of Critical and High alerts, if requested by the Customer, the SilverSky SOC will conduct a full investigation of the alert in an attempt to identify the root cause**.**

D. Security Analysts will notify the Customer of events requiring a response following the custom playbook guidelines. Instructions on threat remediation and consultation will be provided**.**

E. 24/7/365 phone and email event support for additional investigation and guidance for the Customer**.**

F. Critical and High Alerts will be sent to the Customer within 10-minutes of event creation**.**

4. Assumptions

A. Customer will provide SilverSky with reasonably requested information on their inventory, assets and any information pertaining to their environment upon which SilverSky can rely to be current, accurate, and complete to support the installation of Services**.**

B. Customer will provide access to Customer personnel who have detailed knowledge of Customer security architecture, network architecture, computing environment, and related matters**.**

C. Customer will provide access to Customer personnel who have an understanding of Customer's security policies, regulations and requirements**.**

D. Customer will evaluate SilverSky deliverables and immediately notify SilverSky of any perceived problems or issues with SilverSky obligations.

E. SilverSky will immediately notify the Customer of any perceived problems or issues regarding Customer obligations**.**

F. Customer is responsible for any additional costs if SilverSky is unable to perform the Service due to Customer's delay or other failure to fulfill its obligations under this Statement of Work**.**

SERVICE LEVEL AGREEMENT FOR
LIGHTNING MANAGED DETECTION AND RESPONSE

The following terms and conditions apply to the service levels of the Lightning Managed Detection and Response Services provided pursuant to this Attachment, once the service tuning as a part of service deployment has been completed.

In the event we fail to meet the levels defined in this 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. 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 response times. These commitments are subject to your providing us with 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.

A. Definitions of Alert Severity:

Alerts are escalated into events[2] as a result of detected suspicious activity. Events are reviewed both by SOC staff and through automation.

I. **Critical** – This category of alert may have a severe impact on your network or system and indicates a compromise. Examples of events that fall under this category: malware infection, backdoor or Trojan traffic, ransomware, C2 traffic, and botnet traffic.

II. **High** – This category of alert 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. Examples of events that fall under this category are the download of malicious software, leakage of files from an internal network, DoS or DDoS, P2P traffic (torrent), cloud storage traffic, and exploit attempts and launching.

III. **Medium** – This category of alert has a medium level of impact on your network or system and could lead to unnecessary leakage of information or exposure to vulnerabilities. Examples of events that fall under this category are port scans, vulnerability scans, social media traffic, unusual network traffic, and multiple failed logins.

IV. **Low** – This category of alert shows little impact on the Customer. This is mostly informational communication. Examples of events that fall under this category are login or logout notifications, failed login notifications, application or system update notifications, and application or system error messages.

V. **Informational** – This category of alert shows no impact on the Customer. This is only informational alerts to track activity. Examples of events that fall under this category: false positives, approved scanning vendors, and test alerts.

The severity level of each alert is determined by SilverSky based on the nature of the alert identified. The Customer may indicate to us that an identified alert is of a lower priority if you are not vulnerable to the detected activity.

B. Event Severity Response Times

I. **Critical/High Alerts** - Response within 10 minutes upon identification of an alert and a Tier 1 credit if missed; Tier 1 credit is defined in Section 5 below.

II. **Medium/Low Alerts** - Response within 24 hours upon identification of an alert and a Tier 2 credit if missed; Tier 2 credit is defined in Section 5 below.

3. Service Availability Guarantee:

Our commitment is to have the Managed Detection and Response Services, including the Lightning Platform and its interface, available 99.5% of the time and as set forth below. At your request, we will calculate the number of minutes the Service(s) was not available to you in a calendar month ("Service Unavailability"). Failure to meet the service level described in this Section will entitle you to receive a Tier 1 credit.

[2] See Appendix for escalation terminology and definitions

4. Maintenance:

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

- **A.** Tuesday and Thursday (12 AM – 2 AM ET)
- **B.** 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:

If we fail to meet service levels herein in a calendar month, you will be entitled to receive a credit as specified below:

- **A. Tier 1.** Equal to twice the prorated portion of the monthly fee for the affected service, or
- **B. 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. 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 Lightning Managed Detection and Response 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 Lightning Managed Detection and Response Services or a failure to meet service level caused by or associated with any of the following:

- **A.** Maintenance, as defined above;
- **B.** Fiber cuts or other such issues related to telephone company circuits or local ISP outside of our control;
- **C.** Your applications, equipment, or facilities;
- **D.** You or any of your end-user' acts or omissions;
- **E.** Reasons of Force Majeure as defined in the Terms and Conditions associated with this MSA;
- **F.** Any act or omission on the part of any third party, not reasonably within our control;
- **G.** First month of service for the specific Managed Detection and Response Services for which a credit is claimed;
- **H.** DNS issues outside our direct control;
- **I.** Broadband connectivity.

7. Performance Evaluation:

You authorize us to evaluate service upgrades and changes on an annual basis at each of your locations that 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.

8. Fair Usage Threshold for Data Ingestion[3]:

SilverSky maintains a fair usage policy to ensure the availability and sustainability of the 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 associated with the corresponding data sources falls below a reasonable, standard threshold.

9. Equipment:

When applicable, equipment provided to you by us **("SilverSky Equipment")** is for your use only during the Term. We will service the SilverSky Equipment in accordance with our service policies. You agree to (i) use SilverSky Equipment only for the purpose of receiving Lightning Managed Detection and Response Services; (ii) prevent any connections to SilverSky Equipment not expressly authorized by us; (iii) prevent tampering, alteration, or repair of SilverSky Equipment by any persons other than us or our authorized personnel; and (iv) assume complete responsibility for improper use, damage to or loss of such SilverSky Equipment regardless of cause. You will pay us for any damaged or unrecoverable SilverSky Equipment. You authorize us and our authorized agents, contractors, representatives and vendors to enter your premises, with reasonable notice, during normal business hours (or as otherwise authorized by you), to install, maintain, repair and/or remove any SilverSky Equipment and/or to perform the Lightning Managed Detection and Response Services. You must return SilverSky Equipment, at your expense, within 14 days after this Attachment terminates or expires. SilverSky Equipment must be returned in the same condition in which it was provided to you, except for normal wear and tear. If you fail to do so, billing for Lightning Managed Detection and Response

[3] FUT to be calculated based upon the agreed upon data sources to be ingested and listed as per Footnote 1 above.

Services will resume and continue until all SilverSky Equipment is returned. Equipment for Lightning Managed Detection and Response Services delivered through us is maintained in a lockdown configuration that does not allow customer administrative access.

10. Additional Disclaimers:

We do not guarantee a continuous, uninterrupted, virus-free, malware-free, intrusion-free, or continuously secure Customer network or network environment, and we are not liable if you or your end users are unable to access your network at any specific time. Additionally, 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 Managed Detection and Response Services.

Appendix A – Definitions

SilverSky SOC Escalation terms

All Response activity is governed by an escalation method where SilverSky escalates information we receive from your systems as follows.

Syslog: Protocol used to collect raw logs from customer devices to SilverSky collector.

Event: Raw information received from your organization

Alert: An event or group of events that have an indication of out-of-policy, known activity signature match, or other anomalous behavior.

Case: An event or group of events tracked by our analytics engine as abnormal behavior.

Incident: A single alert/case or a group of alerts and or cases grouped or cross correlated together.