SERVICE ATTACHMENT

MICROSOFT MANAGED EXTENDED DETECTION AND RESPONSE

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

"Services" will mean SilverSky Microsoft Managed extended Detection and Response (Microsoft MxDR) Services.

Service SKUs

S-200-3138	MxDR for Microsoft - User	Number of Users
S-200-3139	MxDR for Microsoft - Server	Number of Servers
S-200-3140	MxDR for Microsoft - Light User	Number of "Light" Users

I-200-3138	Installation of MxDR for Microsoft - User
I-200-3139	Installation of MxDR for Microsoft - Server
I-200-3140	Installation of MxDR for Microsoft - Light User

1. Microsoft Managed extended Detection and Response Service Description

We will provide the Customer with the following Microsoft MxDR Services:

- **I.** Silversky Microsoft MxDR consists of SilverSky monitoring of the contracted Customer-owned Microsoft Sentinel environment and related security devices and applications..
- **II.** 24/7/365 coverage of 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 complete visibility into all alerts.
- **III.** Investigation mapping within the SilverSky Lightning Platform utilizing the MITRE Attack framework.
- IV. Management activities include service implementation, configuration changes necessary for successfully provisioning the Microsoft MxDR, and tuning the Azure instance for efficiency and cost optimization.
- V. Monitoring activities include collection, storage, reporting, and Customer notification of security events or device health events.
- VI. Platform Management for Microsoft Sentinel
- VII. Our global Security Operations Center (SOC) team for investigations, threat hunting, and real-time support.
- **VIII.** Customized Playbooks: to notify identified Customer contacts via agreed-upon, specified communication formats. We will provide high-level remediation guidance based on available customer technologies configured with API remediation support. For customers subscribed to our Managed Endpoint Detection and Response (MEDR), we can contain attacks at the endpoint utilizing the SilverSky potentially deployed SentinelOne Singularity Complete agent or your Microsoft Defender agent. For Customers subscribed to our Network Protect service, where SilverSky manages the firewall device, we can block IPs.
- **IX.** Reporting: a set of customizable reports and report templates including, but not limited to, Executive summaries and threat and compliance reports.

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. Assist the Customer in configuring data sources chosen for ingestion.
- III. Notify the Customer of receipt of logs and confirm proper operational integration to ensure alerting.
- IV. Provide initial training and training materials for the SilverSky Lightning Portal.
- V. Tuning of alert detections and responses to reduce false positives or unwanted notifications.

B. Customer Responsibilities

During the performance of the Services, the Customer will:

- I. Before engagement commences, assign a project management contact to serve as a primary contact through the delivery and performance of the Microsoft MxDR 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 to approve and validate all requested changes.
- V. Implement change requests.
- VI. Provide all necessary information about your environment.
- VII. Retain authority and responsibility for decisions regarding this service implementation and assume responsibility for any direct or physical remediation.
- VIII. Enable and configure logging on remote systems or devices per SilverSky instructions.
- IX. Enable necessary firewall rules and any other network changes to route logs to Microsoft Sentinel.
- X. Provide an Azure dedicated management account with "Contributor" permissions required for Microsoft Sentinel management and configuration.
- XI. Cover any expenses related to Microsoft Sentinel, Log Analytics, Logic Apps, and fees payable to Microsoft.
- XII. Provide a Virtual Machine for a Log Collector Virtual Appliance as needed. The log collector is required for onboarding logs from the network, security devices, other commercial cloud services, and custom log sources. Allow remote access for

administration of the Log Collector Virtual Appliance.

XIII. Manage log retention & archiving: The Customer is responsible for managing the log archiving processes for historical, backup, compliance, regulatory, or other requirements.

XIV. Configure all log sources to appropriately send logs to the agents and log collection devices. This includes but is not limited to, any intermediary log sources. If changes to the Customer's existing network architecture are required for Service implementation, SilverSky will communicate these changes to the Customer.

XV. Notify SilverSky of any environmental changes that may affect the execution of the Service.

XVI. Install appropriate collecting agents, such as the Azure Monitoring Agent (AMA) and the Microsoft Monitoring Agent (MMA), software on Windows and Linux endpoints, per SilverSky instructions.

XVII. Configuring the network and security devices with the logging details provided by SilverSky (i.e., Syslog)

XVIII. Provide feedback on fine-tuning alerts and playbooks when required.

XIX. Provide detailed information on the network environment to facilitate the deployment of the SilverSky solution.

XX. Notify SilverSky of any necessary user account changes tied to Customer employee termination, including employees or contractors with access to the Lighting Portal or approval to contact the SOC.

XXI. Perform additional remediation: During an investigation of security alerts, the SilverSky SOC may give guidance to a Customer to perform specific actions in the Customer's environment to improve the Customer's security posture or to remediate an incident. The performance of these actions is the Customer's responsibility.

XXII. Obfuscate Personally Identifiable Information (PII) data in the Customer's environment. SilverSky will not extract personally identifiable information from the Partner or Customer environment or store it within the SilverSky environment except for only sufficient log data for enrichment, case management, reporting, and automation purposes. No raw or PII data should leave the Customer's M365 or Azure environment.

XXIII. Configure Lighthouse access for SilverSky SOC; as appropriate, the Customer will register SilverSky as DPOR/CPOR/PAL.

XXIV. Responsible for providing and maintaining API credentials for SilverSky when required.

XXV. Provide access to and licensing for Microsoft Defender for Endpoint when required.

XXVI. Provide internet access and manage firewall rules when required. If not managed by the SilverSky team.

You acknowledge that fulfilling these responsibilities is essential to our ability to perform the Microsoft MxDR Services in a timely manner.

3. Deliverables

I. Service implementation, configuration changes necessary for successfully provisioning the Microsoft MxDR, and tuning the Azure instance for efficiency and cost optimization.

II. Ensuring the collection, storage, reporting, and Customer notification of security events or device health events.

III. Platform Management for Microsoft Sentinel

IV. 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.

V. 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.

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

VII. 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 with detailed knowledge of Customer security architecture, network architecture, computing environment, and related matters**.**

C. Customer will provide access to Customer personnel who understand 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 cannot perform the Service due to Customer's delay or other failure to fulfill its obligations under this Statement of Work**.**

G. Each service only covers services for one Microsoft Sentinel SIEM and tenant.

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:

Events are escalated into alerts as a result of detected suspicious activity. Alerts 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 or indicates a compromise. Examples of events that fall under this category: malware infection, backdoor or Trojan traffic, ransomware, C2 traffic, and botnet traffic, leakage of files from an internal network.

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, , 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, 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 activity, 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.

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.
- J. Lack of response/acknowledgement for reported alerts by the customer.

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. 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 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.

9. 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: A single alert or a group of alerts grouped or cross correlated together.