SERVICE ATTACHMENT

MANAGED DEFENDER M365

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

"Services" will mean SilverSky Managed Defender M365, which covers solution provides configuration, management, and monitoring of the four security solutions within M365:

1. Microsoft Defender XDR - Protect your organization against sophisticated attacks such as phishing and zero-day malware.
2. Microsoft Defender for Endpoint - Scale your security with a unified endpoint security platform for preventative protection, post-breach detection, automated investigation, and automated/manual response.
3. Microsoft Defender for Cloud Apps - View apps used in your organization, identify and combat cyber threats, and monitor and control data travel in real-time.
4. Microsoft Defender for Identity - Use a cloud-based solution to protect your organization's identities from multiple types of advanced targeted cyberattacks.

Service SKUs:

SKU	Service Name	Pricing Unit
S-200-3141	Managed Defender M365	Endpoint

SKU	Service Name	Pricing Unit
I-200-3141	Installation of Managed Defender M365	Per Company
I-201-3141	Audit Review Existing/Customer deployed controls - taking over management	Per Company
I-202-3141	MDCA additional cloud applications (greater than five)	Per Company
I-203-3141	MDE third-party RMM	Per Company

SilverSky Services

SilverSky Managed Defender M365 consists of SilverSky configuring, managing, and monitoring the customer-owned Microsoft Defender M365 services. These services include Microsoft Defender XDR, Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, and Microsoft Defender for Identity.

A. 24/7/365 coverage over all actionable alerts routed to our platform; such incidents are reviewed by an Analyst on a 24/7/365 basis. Customers get full visibility into notified and non-notified incidents via our SilverSky Lightning Managed Detection and Response (MDR) Platform (referred to as the SilverSky customer portal).

B. Customer will have access to our global security operations team for incident investigations and real-time support.

C. Customized Playbooks: to provide notifications to identified client contacts via agreed-upon, specified communication formats. We will provide guided remediation and containment based on the managed endpoint controls in the customer environment. Per the playbook, SilverSky will provide containment and rollback efforts as required.

D. Data is processed within the customer-provided Microsoft XDR portal and alerting our SOC.

E. Reporting: a set of customizable reports from report templates via the SilverSky customer portal, including, but not limited to, Executive summaries and threat and compliance reports.

F. Customers can access both their own Microsoft XDR portal as well as the SilverSky customer portal

G. Includes up to twenty proactive service support hours annually. These Hours can be utilized for the ongoing management of the in-scope Microsoft Defender M365 technologies, the configuration of custom source ingestion, or specialized Microsoft Defender M365 engagements

Managed Defender M365 SERVICE IMPLEMENTATION

SilverSky Responsibilities

A. 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.

B. Establish a secure method of transmitting logs from the Customer's Microsoft XDR portal to the SilverSky Platform.

C. Notify the Customer of receipt of logs and confirm proper operational integration to ensure alerting.

D. Provide initial training and training materials for the SilverSky customer portal.

SilverSky Service Deliverables

A. Configuration, ongoing management, and tuning of the four products within Defender M365

B. Capture alerts from the Customer's monitored devices.

C. Analysts will notify the Customer of alerts requiring a response. Instructions on threat remediation and consultation will be provided, as defined in the Customer playbook created during deployment.

D. 24/7/365 phone and email-based incident support for additional investigation and guidance for the Customer.

E. Implement change requests.

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

Customer Responsibilities. During the performance of the Services, Customer will:

A. Allow SilverSky access to your Microsoft XDR portal

B. Prior to engagement commencement, assign a project management contact to serve as a primary contact through the delivery and performance of the Defender M365 Service.
C. Ensure complete and current contact information is provided on a timely basis.
D. 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.
E. Appoint one or more authorized contacts authorized to approve and validate all requested changes.
F. Provide all necessary information with respect to your environment.
G. Provide all necessary Microsoft licenses to enable the services
H. Installing Microsoft Defender licenses on your endpoints.
I. Ensure the format and quality of the data being sent to SilverSky is sufficient for SilverSky to provide the Services.
J. Retain authority and responsibility for decisions made regarding this service implementation.
K. Assume responsibility for any direct or physical remediation.

You acknowledge that your fulfillment of these responsibilities is essential to our ability to perform Defender M365 Services in a timely manner.

Service Level Agreement for Managed Defender M365

In the event we fail to meet the levels defined in this Managed Defender M365 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 Defender M365 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 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.

2.1 **DEFINITIONS OF INCIDENT SEVERITY**

A. (i)

B. Definitions of Alert Severity:

Alerts are escalated into events[1] 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 Lightning MDR Services, including the 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:

(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 Lightning MDR 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 Terms and Conditions associated with this 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. 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 Services.