STATEMENT OF WORK FOR

LIGHTENING MANAGED DETECTION AND RESPONSE (WITH SENTINELONE ENDPOINT SOLUTION-MEPP)

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

"Services" will mean SilverSky Lightening Managed Detection and Response (MDR) Services with SentinelOne Endpoint Solution (MEPP), including SilverSky Lightning Platform. The **"Launch Date"** of Services under this Attachment will mean the date on which the Service(s) provided under the terms of this Attachment are first made available to you.

SilverSky Services

We will provide the Customer with the following Lightening MDR (with SentinelOne Endpoint Solution-MEPP) Services:

A. SilverSky Lightning Platform to ingest data/events from a wide variety of agreed upon data sources including on-prem devices, endpoints, webapps, authentication gateways and cloud infrastructure. All ingested events are automatically enriched with threat intelligence data, matched against a variety of Indicators of Compromise and intelligently cross-correlated to detect anomalies across customer infrastructure.
B. 24/7/365 coverage over all actionable incidents routed to our monitoring and detection platform; such incidents are reviewed by an Analyst on a 24/7/365 basis. Customers get full visibility in to notified and non-notified incidents.
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, in addition you will access to our global security operations team for incident investigations, threat hunting, and real-time support. *Note*: The dedicated cybersecurity advisor only applies if recurring monthly fee associated with the contract herein is $500 or greater**.**
E. Customized Playbooks: to provide notifications to identified client contacts via agreed-upon, specified communication formats. We will provide containment and guided remediation, including the ability to potentially contain attacks at the endpoint utilizing the SilverSky deployed agent.
F. Reporting: a set of customizable reports and report templates including, but not limited to, Executive summaries and threat and compliance reports.
G. Platform transparency by providing customer access directly into the SilverSky Lightning Platform.
H. Unlimited Data Ingestion[1]: unlimited data ingestion from agreed upon data types and sources from standard feeds. Data is retained for one year (30 days hot storage and 1 year in cold storage).
I. Support for Microsoft Office365 telemetry; additional fees may apply for this data source.
J. Lightening MDR/MEPP – Additionally, as part of this service we are reselling the SentinelOne end point solution, and as such will ingest data from SentinelOne as deployed on your endpoints within this Lightening MDR service. We represent and warrant that we have obtained all required authorizations and consents to resell the MEPP to Customer as part of this MSA and agree to defend, indemnify, and hold harmless Customer against any actual or alleged claims, damages, or losses arising from our resale of the MEPP to Customer including, without limitation, any claims of infringement or unauthorized use. We further represent and warrant that the MEPP is not an early adoption or beta version of the Solution as defined in SentinelOne's Master Subscription Agreement. As the ultimate end customer of SentinelOne you must adhere to any and all SentinelOne end user provisions. Note: Also see *Exhibit 1* for SentinelOne Ransomware Warranty.
K. Please note that SilverSky is providing endpoint security utilizing SentinelOne endpoint protection solutions.
The SentinelOne solutions are procured by SilverSky via a Managed Security Service Provider ("MSSP") license and delivered to you as a service. As such, all licensing for this service is controlled by the MSSP licensing agreement between SilverSky and SentinelOne.

LIGHTENING MDR (with SentinelOne EndPoint Solution -MEPP) 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 network to the Lightning Platform.
C. Provide assistance to the Customer to configure data sources chosen for ingestion.
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 SilverSky Lightning Platform/portal.

[1] Unlimited data ingestion applies to the following agreed upon, standard data sources: Network Data (incl. from public cloud sources such AWS, Azure, Google Cloud, and other similar hyperscale cloud services), Firewall, DNS, Active Directory, Switches, Routers, Access Points, Domain Controllers, Vulnerability Management Solutions, and Endpoint Security Tools.

SilverSky 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, SilverSky security engineers will analyze incidents following an alert by the 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 alert creation.

Customer Responsibilities. During performance of the Services Customer will:

A. Prior to engagement commencement, assign a project management contact to serve as a primary contact through the delivery and performance of the Lightening MDR (with SentinelOne Endpoint Solution-MEPP) Services;
B. Ensure complete and current contact information is provided on a timely basis;
C. Cooperate during the deployment period, including providing to SilverSky all required information in a complete and accurate form to prevent implementation delays which may result in additional fees;
D. Appoint one or more authorized contacts authorized to approve and validate all requested changes;
E. Implement change requests;
F. Provide all necessary information with respect to your environment;
G. Provide necessary hardware along with maintenance and support contracts to run log collectors within your environment;
H. Send log data in an encrypted manner, or via the agreed log collection device/type;
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; and
K. Assume responsibility for any direct or physical remediation.

You acknowledge that your fulfillment of these responsibilities is essential to our ability to perform the Lightening MDR (with SentinelOne EndPoint Solution-MEPP) Services in a timely manner.

Service Level Agreement for Lightening Managed Detection and Response

In the event we fail to meet the levels defined in this Lightening MDR/MEPP 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 Lightening MDR/MEPP 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**

(i) **Critical** – This category of incident may have a severe impact to your network or system and indicates a compromise. Examples of incidents that fall under this category: malware infection, backdoor or Trojan traffic, outbound DDoS, and bot net traffic.

(ii) **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. Examples 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.

(iii) **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. Examples of incidents that fall under this category: port scans, vulnerability scans, social media traffic, unusual network traffic, and multiple failed logins.

(iv) **Low** – This category of incident shows little impact on the Customer. This is mostly informational alerts to inform the Customer. Examples 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.

(v) **Informational** – This category of incident shows no impact to the Customer. This is only informational alerts to track activity. Examples 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 SilverSky based on the nature of the incident identified. Customer 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**

(i) **Critical/High Alerts** - Response within 10 minutes upon identification of incident 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 incident 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 Lightening MDR 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:

(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 Lightening 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. **FAIR USAGE THRESHOLD FOR DATA INGESTION[2].** 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.

8. **EQUIPMENT.** When applicable, equipment provided to you by us **("SilverSky Equipment")** is for your use only during the Term of this Attachment. 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 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 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 Services will resume and continue until all SilverSky Equipment is returned. Equipment for 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 Services.

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

Exhibit 1: SentinelOne Specific Ransomware Warranty for Lightening MDR/MEPP

1. **Ransomware Warranty.** During the Ransomware Warranty Agreement, so long as the Customer also subscribes to the Services in compliance with this MSA, the Customer's Endpoints will be protected by the Services which will screen for any Ransomware. The Ransomware Warranty granted herein shall apply to all such Endpoints provided that:

(a) The Services are deployed in the Endpoints in accordance with the Documentation and such Endpoints are currently active and properly configured;

(b) Only Files that are on Endpoints are covered under this Ransomware Warranty;

(c) All Endpoints of the Customer have the following required configurations:

(i) Services:

- Policy mode options are set to Threats: Protect and Suspicious: Protect.
- All Engines are set to ON.
- Cloud Connectivity is not disabled.
- Anti-Tamper is turned ON
- Snapshots are turned ON
- Scan New Agents is turned ON
- The latest General Availability (GA) version (or GA with a critical security Service Pack (SP), if issued) or the GA (or GA with a critical SP, if issued) version immediately preceding such latest GA version, of the SentinelOne Windows Endpoint Agent (as specified in the SentinelOne Knowledge Base "Latest Information" article) is deployed prior to the time of Ransomware infection.
- There are no Pending Actions (such as Reboot) listed on any covered Endpoint.
- A supported version of the Management Console is deployed.
- Exclusions specified in the SentinelOne Knowledge Base "Not Recommended Exclusions" article, are not deployed in the Management Console or Agent.

(ii) Operating system:

- The Ransomware Warranty applies to Standard (not Legacy) Windows Agents, and on supported versions of Microsoft Windows (as specified in the SentinelOne Knowledge Base "System Requirements" article).
- Each endpoint is malware-free prior to SentinelOne Windows Agent installation.
- OS is fully updated and patched on each covered Endpoint, and all compromised applications are updated to latest releases.
- VSS (Volume Shadow Copy Service) is enabled and functioning on all Windows endpoints. VSS Disk Space Usage allocation must be configured with at least 10% on all disks.

(d) The Customer adheres to the following manual actions post infection (i.e. discovery of Ransomware):

- immediately adds the specific Ransomware threat to blacklist;
    - in case the Ransomware was not blocked but only detected – takes a remediation and rollback action within 1 hour of infection/discovery of the Ransomware; and
- notifies SentinelOne of the Ransomware discovery within 24 hours at Ransomware Warranty@sentinelone.com.

this Section 1(d) shall not apply if the Customer is subscribed to the Vigilance Response service during the Ransomware Warranty Agreement.

2. **Scope of the Ransomware Warranty**. Subject to the terms of this Ransomware Warranty Addendum, including the specific requirements of Section 1 above, in case of a successful ransomware attack on Customer Endpoints covered by the Ransomware Warranty, as shown in SentinelOne's logs and other records, SentinelOne will pay as sole and exclusive remedy to the Customer actual damages caused by such attack, capped at $1,000 USD per Endpoint affected by a Breach, and further capped at $1,000,000 USD for every consecutive 12 months in which Customer subscribes to the Services with respect to the affected Endpoint. For the avoidance of doubt, the recovery amount set forth herein is limited to 1,000 Endpoints for each applicable 12-month period.

3. **Condition Precedent to Ransomware Warranty Payment**. SentinelOne shall only provide the remedy for the Breach of the Ransomware Warranty as described above if (i) the Ransomware attack has occurred, is discovered by the Customer and reported to SentinelOne during the Ransomware Warranty Agreement and Customer's subscription to the Services under the Agreements; (ii) Customer's Endpoints and the Services are configured in accordance with the Documentation and Section 1 above; (iii) the Customer demands in writing to recover for damages caused by the Breach; and (iv) sufficient evidence is provided by Customer supporting the Ransom demand amount for

each Ransomware infection covered by this Ransomware Warranty.

4. **Exclusions**: The Ransomware Warranty shall not apply to a breach caused primarily by (i) any deployment, configuration and/or use of the Services (or a portion thereof), for any or no reason, in a manner inconsistent with the Documentation or the requirements of Section 1 herein; (ii) Customer's negligence or misconduct; or (iii) other products and/or services which directly or indirectly cause the malfunction or non-performance of the Services with respect to the subject Ransomware.

5. **Sole and Exclusive Remedy**. The aforementioned remedy for the Breach shall be the Customer's sole and exclusive remedy and the entire liability of SentinelOne for any Breach of the Ransomware Warranty.

6. **Definitions.** The capitalized terms below shall have the following meaning:

(a) **"Breach**" means the unauthorized access to at least one Customer Endpoint in the form of Ransomware which has caused material harm to the Customer, whereby "material harm" must include at least one of the following: (i) the unauthorized acquisition of unencrypted digital data that compromises the security, confidentiality, or integrity of personal information or confidential information maintained by the Customer; (ii) public disclosure of personal information or confidential information maintained by the Customer; or (iii) the compromise of at least one Customer Endpoint resulting the blocking of access to such Endpoint.

(b) **"Ransomware**" means a malware software program that infects Customer's systems from external sources (i.e., in the wild), which installs, persists and encrypts a large portion of files at the operating system level, and continuing to demand payment (the "**Ransom**") in order to decrypt the encrypted files. For clarification, Ransomware does not include any malware introduced by the Customer or any third party to Customer's internal systems, whether intentionally (i.e., malware testing) or through a breach in the system's security.

(c) "**Endpoints**" shall mean any computing device with a Microsoft Windows operating system, that has the Services installed per the Documentation under valid Agreements among SilverSky and the Customer.

7. **Other Agreements and Conditions.** Any other terms and conditions of the Agreements shall be unaffected by this Ransomware Warranty, except as expressly stated in the Agreement. In case of any conflict between the terms of this Ransomware Warranty and the terms and conditions within the Agreement relating to the Ransomware Warranty, the terms and conditions within this Ransomware Warranty shall prevail.

8. **Miscellaneous.** This Ransomware Warranty represents the complete agreement between the parties concerning the Ransomware Warranty granted hereunder and supersedes any and all prior agreements or representations between the parties. SentinelOne may revise the terms of this Ransomware Warranty from time to time in its reasonable discretion, provided that such revisions shall not reduce or eliminate the monetary remedy described in Section 2 herein. To the extent that SentinelOne pays to the Customer under the Ransomware Warranty, Customer agrees that SentinelOne shall acquire a subrogation right to assert a claim against the hacker who delivered the Ransomware to Customer and caused damages for which SentinelOne incurred Ransomware Warranty costs, and Customer further agrees to assist SentinelOne should it decide to assert a claim against such hacker. If any provision of this Ransomware Warranty is held to be unenforceable for any reason, such provision shall be reformed only to the extent necessary to make it enforceable.