



## STATEMENT OF WORK FOR VULNERABILITY MANAGEMENT “INSIGHT” SERVICES

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

1. **Vulnerability Management Insight Services** (“Insight Services”) will mean SilverSky services including vulnerability assessments, remediation data reporting of Your environment and automated and recurring vulnerability and compliance scanning of internal, external, and cloud-based live IP addresses, as further defined in the *Order Form* and incorporated herein by reference. The “**Launch Date**” of Insight Services under this Attachment will mean the date on which the Insight Services or any part of the services provided under the terms of this Attachment are first made available to you.
2. **Customer Responsibilities.** During performance of the Insight Services, you agree to perform the following obligations and acknowledge and agree that SilverSky’s ability to perform its obligations, and its liability under the SLAs below, are dependent upon Your compliance with the following:
  - I. Prior to engagement commencement, assign a project management contact to serve as a primary contact through the delivery and performance of the Insight Services;
  - II. Ensure complete and current contact information is provided on a timely basis;
  - III. Contact SilverSky 24/7 support (via email or telephone) to ask questions about:
    - a. Technical issues with the scanner operation or troubleshooting, which will result in a ticket to the SOC team.
    - b. Changing contact information or rescheduling scan dates and times.
    - c. Solving issues associated with accessing the Insight service.
    - d. Stopping scans during a network impacting event.
    - e. NOTE: Help desk calls cannot be used for general consulting advice that does not directly pertain to the results of the Service.
  - IV. Acknowledge and agree that the scanning of IP addresses and/or domain names may expose vulnerabilities and, in some circumstances, could result in the disruption of Services or corruption or loss of data.
  - V. Perform regular backups of all data contained in or available through the devices connected to your IP address and/or domain names.
  - VI. Acknowledge that the IP address of cloud-based assets is subject to change.
  - VII. Identify the specific IP addresses of cloud-based assets to be scanned.
  - VIII. You may use the Services only to scan the IP Addresses owned by and registered to Customer, or for which Customer otherwise has the full right, power, and authority to consent to have the Services scan and/or map.
    - a. Scans of external IPs are conducted remotely.
    - b. Scans of internal and cloud-based IPs are conducted from one or more ISO images placed on Customer’s network or in Customer’s leased virtual datacenter. IP level is based on Customer’s technical scanning requirements.
    - a. You will not rent, lease, or loan the Services, or any part thereof, or permit third parties to benefit from the use or functionality of the Service via timesharing, service bureau arrangements or otherwise.
    - b. In the event one (1) or more of the IP Addresses identified by You are associated with computer systems that are owned, managed, and/or hosted by a third-party service provider (“Host”), You warrant that you have the consent and authorization from such Host(s) necessary for SilverSky to perform the Services.
    - c. You agree to facilitate any necessary communications and exchanges of information between SilverSky and Host.
  - IX. Remediation Plan: Creation of a remediation plan, schedule and actions to remediate vulnerabilities are the Customer’s responsibility.
3. **SilverSky Deliverables.** During performance of the Insight Services, SilverSky will:
  - I. Access the Security Portal to view vulnerability reports.
    - a. Note: Report capabilities are restricted to the capabilities of the platform and are Customer’s responsibility to generate. The Security portal may only be accessed by the named individuals specified by you. All information received by you through the Security portal is solely for your internal use and may not be re-distributed, resold, or otherwise transmitted outside of your organization.
  - II. Profile Set-Up. SilverSky will assist you in selecting individual scan engine profiles as requested by you.
  - III. Conduct scanning of your infrastructure (for example servers, applications, network devices and end user devices) using a recognized industry vulnerability scanning tool, against the list of IP addresses as agreed, provided that those IP addresses are accessible from the Internet or through the supplied ISO image(s) and subject to the maximum numbers of IP addresses specified in *Appendix 1*.
    - a. Scanning may be conducted as an ‘internal’ scan utilizing an ISO images within the your network, or as an ‘external’ scan utilizing a web based portal.



- b. External scans can only be conducted on network assets and infrastructure with an internet-facing external IP address.
  - c. Internal scans can only be conducted on network assets and infrastructure that are accessible from the ISO images from its location within your network.
4. **Performance Evaluation.** You authorize us to evaluate service upgrades and changes on an annual basis at each of your locations which utilize the Insight 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. **Equipment.** If 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 Insight 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 Insight 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 Insight Services will resume and continue until all SilverSky Equipment is returned. Equipment for Insight Services delivered through us is maintained in a lockdown configuration that does not allow customer administrative access.
6. **Term and Termination.** This Attachment will be in effect during the Term set forth in Order form. The sections related to Payment Terms, Limitation of Liability, Warranties, Indemnity, Confidentiality and Intellectual Property from the General Terms and Conditions, as provided in the referenced General Terms and Conditions document, will survive the expiration or termination of this Attachment for any reason. Within 10 days after the expiration or termination of this Attachment for any reason, you must pay all undisputed fees accrued and unpaid at the time of termination, and the cancellation fee if applicable.
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.



## SERVICE LEVEL AGREEMENT FOR INSIGHT SERVICES

---

The following terms and conditions apply to the service levels of Insight 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. **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.
  - I. **Security and Network Operations Events.** We classify all events as high, medium, or low level. We will identify or begin analysis of high-level events within fifteen (15) minutes, medium level events within one (1) hour, and low-level events within twenty-four (24) hours of occurrence. Failure to respond in accordance with these guidelines will entitle you to a one-day Tier 1 credit for high level events or one-day Tier 2 credit for medium and low-level events.
  - II. **Change Requests.** We will make commercially reasonable efforts to begin implementation of changes you request to your service or equipment within twenty-four (24) hours of receipt of the appropriate change control form, requested changes will normally be implemented during Customer's non-business hours. Failure to respond in accordance with these guidelines will entitle you to a one-day Tier 2 credit.
3. **INSIGHT SERVICE AVAILABILITY GUARANTEE.** Our commitment is to have the Insight Services available 99.5% of the time and as set forth below. At your request, we will calculate the number of minutes the Insight 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)
  - III. 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.
  - III. 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 Insight 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 Insight 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's 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 Insight Services for which a credit is claimed;



- VIII. DNS issues outside our direct control;
  - IX. Broadband connectivity.
7. **FAIR USAGE THRESHOLD FOR INSIGHT SERVICE:** When applicable, SilverSky maintains a fair usage policy to ensure the availability and sustainability of the Insight 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.