verizon

# VERIZON SECURITY OPERATIONS SERVICE
# SERVICE LEVEL AGREEMENT



## 1. SERVICE LEVEL STANDARDS

1.1 **Overview.** This Service Level Agreement (SLA) defines the service metrics for which the Customer may issue Verizon a claim to receive credits (Service Credits) if Verizon does not meet Security Incident Handling Level Targets set forth in this SLA. The SLA will become effective with respect to Verizon Security Operations Service (VSOS) when Verizon has issued the written Ready for Operations notice for VSOS. The Security Incident Handling SLA only applies to Security Incident Handling as measured from the "OPEN" state in Verizon's SOAR platform to the "ESCALATED" or "CLOSED" state in Verizon's SOAR, and does not apply to the resolution of the Security Incident. Definitions not defined in this SLA will have the meanings set forth in the Verizon Security Operations Service Service Attachment. This SLA does not apply if Customer has custom metrics and service levels that are subject to an additional charge.

1.2 **Security Incident Handling SLA.** The Security Incident Handling SLA only applies to Security Incident notification to the Customer, and does not apply to resolution of the Security Incident. The SLA is based on the severity level for the applicable Security Incident as received in the SOAR from Customer's Security AP and not based on any reclassification of the Security Incident by Verizon. In order to qualify for credits, Customer must refrain from causing any delays. For each severity level, Verizon will Handle 95% of the applicable Security Incidents in a given month within the corresponding SLA timeframe:

| Severity | VSOS Service | Priority 1 Critical | Priority 2 High | Priority 3 Medium | Priority 4 Low |
|---|---|---|---|---|---|
| **Handling SLA** | VSOS Standard<br>VSOS Extended | 2 Hours<br>1 Hour | 4 Hours<br>2 Hours | 8 Hours<br>4 Hours | 24 Hours<br>12 Hours |
| | Add-On | Custom SLAs are subject to VSOS contract negotiations and will result in additional charges. | | | |

| | |
|---|---|
| **SLA Start Time** | Timestamp (UTC) when the Security Incident is received in the Verizon SOAR as indicated by the Verizon SOAR; such time is considered the "Open" state. |
| **SLA Stop Time** | Timestamp (UTC) of the status change after the triage decision Escalated or Closed as such timestamp is indicated in the Verizon SOAR. |
| **Reporting** | Security Incident Handling SLA will be reported monthly as the actual time spent on Security Incidents for each of the severity levels above with respect to the 95% metric. |
| **System of Record** | Verizon's SOAR will be the system of record for all relevant times. |

1.3 **Reporting.** Verizon will provide a monthly management report for VSOS that will illustrate Verizon's SLA performance and total number of each type of Security Incident.

## 2. CALCULATION OF CREDITS

2.1 **Service Credits for Notification.** Service Credits will apply after the first full month of VSOS after Verizon has provided the Ready For Operations notice to Customer. Verizon will calculate Service Credits monthly.

2.2 **Amount of Service Credit.** For any month, when the Handling SLA falls below the levels set forth in Section 1.2, Customer may be eligible to receive credits. One (1) Service Credit equals half the daily VSOS Service charge (calculated based on the applicable VSOS Service MRC divided by the number of days in the month). The total number of Service Credits in a given month may not exceed 20% of the VSOS Service MRC for such month.

2.3 **Classification of Security Incidents.** Verizon has sole discretion to classify, reclassify, define or redefine any and all Security Incidents.

## 3. PROCESS FOR CREDITS

3.1 **Required Steps.** Verizon will review any missed SLA metrics with Customer during the monthly service review meetings. To be eligible to receive a Service Credit, Customer must file a written claim for credits (which may be provided through email to an email address provided by Verizon) to the Security Services Advisor within 30 days immediately following the month in which the SLA metrics were not met. No Service Credits will be issued if Customer does not file such a claim within such time. In order to qualify for credits, Customer must refrain from causing any delays.

3.2 **Issuing Credits.** Upon Customer's written request, Verizon will review any failure to meet the service level standards to determine the appropriate amount of Service Credits. Service Credits will be offset against future charges. Service Credits or equivalent payments made by Verizon to Customer under this SLA are the sole and exclusive remedy available to Customer from any failure to meet a service level metric or standard. Verizon's Service Credit calculation is the final and definitive assessment of any service credit payable.

## 4. EXCLUSIONS

4.1 **Credit Restrictions.** If a series of unmet SLA response times arise out of the same Security Incident or same set of events, Customer will receive only one Service Credit. All measurements of service level standards will be suspended during periods of maintenance by Customer or Verizon as such maintenance

is described in Section 2.3.1 of the Verizon Security Operations Service Service Attachment. No credits are available for any services that have been implemented for less than one full calendar month following Customer's receipt of the Ready For Operations notice.

4.2 **General Exclusions.** In order to qualify for credits, Customer must refrain from causing any delays. Service Credits will not be due if the failure to meet service metrics is, directly or indirectly, due to:

- A failure by Customer (or its agent or contractor) to comply with Customer's obligations under the Verizon Security Operations Service Service Attachment;
- The non-performance, defaults, error, omission or negligence of any third party not under Verizon's reasonable control (such as, but not limited to, failure of Customer's third party providers of telecommunications services or problems with equipment Customer has provided);
- Periods of maintenance by Customer or Verizon as described in Section 2.3.1 of the Verizon Security Operations Service Service Attachment;
- Tests performed or commissioned by or on behalf of Customer;
- Modifications made by Customer or its third party vendors to the Security AP or Ticketing System;
- Customer providing incorrect or incomplete information or incorrect or incomplete identification of Customer's critical assets;
- Customer failing to arrange for Verizon's access to requested components;
- Customer modification or the configuration of the Security AP or Ticketing System without Verizon's prior agreement;
- End user's equipment, software, facility, or operator error;
- Incidents not reported by Customer;
- Unsupported, outdated, or end-of-life hardware or software versions or configurations which affect the format or delivery of Data Sources;
- An act or omission on the part of Customer, its contractors or vendors;
- A significant security event including without limitation a massive attack of malware with the risk of a Security Incident Flood to Verizon's infrastructure, which may include the SOAR;
- A Security Incident Flood that may be caused by changes in Customer's IT environment or infrastructure including without limitation:
  - the Security AP for which the Detection Content and security detection rules on the Security AP have not been updated,
  - the Ticketing System,
  - rewiring or network cabling, addressing and routing,
  - endpoint security or application control ("allow list" or "block list") configuration,
  - new application deployment,
  - user account changes, or
  - misconfigured Data Sources including devices;
- Changes to the Service Context submitted to Verizon that influence or impact the Detection Content, which changes may include adding, removing, or moving servers, adding new applications or web servers, and changes made to Detection Content by or on behalf of Customer; or
- Any Force Majeure event.

4.3 **Security Incident Volumes**. So that: (i) Verizon is able to provide focused analysis to our customers for the highest severity threats; (ii) VSOS is a scalable and sustainable shared service; and (iii) appropriate risk assessment has been considered by Customer when classifying Security Incidents in the Security AP and Ticketing System, Verizon expects the following ratio of Security Incident volumes by Security Incident Classifications and severity levels within any given month as follows:

| Security Incident Classification | Severity | Expected Security Incident volumes in Business-As-Usual operations |
|---|---|---|
| **Priority 1** | Critical | less than or equal to 5% of monthly Security Incidents |
| **Priority 2** | High | less than or equal to10% of monthly Security Incidents |
| **Priority 3** | Medium | less than or equal to 40% of monthly Security Incidents |
| **Priority 4** | Low | the remainder of monthly Security Incidents |

a. If the actual number of Security Incidents for a Security Incident Classification set forth in the table in this Section 4.3 exceeds the percentage of Security Incidents applicable to such classification during a one day period, (24-hour period, 0000-2359 UTC), then Verizon will use reasonable efforts to respond to Security Incidents that exceed the applicable percentage for such classification. Verizon will continue to measure and report on service levels applicable to the Security Incidents that exceed such applicable percentage. This SLA and targets in Section 1.2 will not apply and Verizon will not be liable for Service Credits for the excess Security Incidents.

b. If the volume of Critical Severity Incidents, High Severity Incidents, or Medium Severity Incidents exceeds the applicable percentage of total volume of Security Incidents in a service month set forth in the table in Section 4.3, the Security Incident Handling SLA will not apply in that service month for any severity level exceeding the applicable monthly percentages.

c. For Service Level measurements that are based on percentages but the Measured Volume is so low that a single failure would result in a failure to meet the applicable Service Level, the applicable Service Level will be adjusted as follows such that a single failure does not result in a failure to meet the Service Level. Such Service Levels shall be adjusted to the quotient determined by dividing (i) the Measured Volume minus one, by (ii) the Measured Volume. For example, if the required Service Level is ninety-five per cent (95%), and the total Measured Volume for such Service Level in the measurement period is eighteen (18), then the Service Level would be readjusted to 94.44% (determined by dividing seventeen (17) by eighteen (18)).

d. If the Measured Volume for any Service Level is equal to zero (0) then Verizon shall be deemed to have performed in accordance with such Service Level for such measurement period and no Service Credits will apply to such Service Level for such period.

## 5. DEFINITIONS

| Term | Definition |
|---|---|
| **Measured Volume** | Number of Security Incidents in any given measurement period. |