verizon

MANAGED SECURITY SERVICES – ANALYTICS

1. GENERAL

1.1 **Service Definition.** Managed Security Services (MSS) - Analytics provides 24x7analysis of Customer-supplied Data for the purpose of monitoring, detecting and alerting Customer to potential security threats, Security Events and Security Incidents. The service uses an advanced, analytics-based approach capable of ingesting Data from not only traditional security and network devices but other devices that may help identify threats or aid in investigation of threats. In addition to detecting traditional signature-based threats, MSS – Analytics uses behavioral modeling to detect advanced threats and provide valuable insights that can help shorten the detection interval and reduce false positives.

1.1.1 **Platforms**. These terms apply to Optimized Service (denoted with a + and sometimes referred to as Rapid Delivery) and non-Optimized Service, without distinction.

1.2 **Service Implementation.** Verizon will assign a Project Manager to Customer who will schedule a kick off meeting to introduce the Verizon service delivery team, identify the Authorized Contacts for Customer, discuss the scope of the MSS – Analytics service and its business impacts, and obtain any required information from Customer. Upon receipt from Customer of a completed Deployment Kit, Verizon will create a proposed project plan with high-level milestones and timelines. Verizon will only provision MSS - Analytics after Customer has approved the project plan.

1.3 **Service Features**

1.3.1 **Threat Analysis.** MSS – Analytics analyzes Data received from Data Sources to identify possible Security Incidents and potential indicators of compromise. A Security Incident is generated after Data have been processed, or analyzed, against Security Content on Verizon's Security Analytics Platform. MSS – Analytics both (a) analyzes individual pieces of Data and Security Events which may,

individually, appear to be harmless, and (b) correlates those Security Events and Data with other data to determine if a more harmful pattern presents itself, thus identifying a Security Incident.

Types of data used in Security Incident correlation can include:

- Any and all Data provided by Customer
- Information in the Service Context, such as the classification of an asset
- Verizon's Threat Intelligence

1.3.2 **Security Incident Classification.** Verizon Classifies Security Incidents into 4 Categories:

Security Incident Classification	Risk Levels	Conditions
Insufficient Info	L0	The Security Incident has been classified as 'Insufficient Info' based on the associated Security Events.
Harmful Attack	L1	The Security Incident is identified as an attack or an attempted attack that may result in damage or unauthorized access to a device or application. The cause of the Security Incident renders Customer's infrastructure vulnerable or compromised.
Harmless Attack	L2	The Security Incident is identified as a known attack, attempted known attack or reconnaissance effort. Customer's infrastructure is not considered vulnerable or compromised based on the Service Context.
False Positive	L4	The Security Incident may be falsely triggered, is informational or benign in nature.

Offline Analysis Category is used during first phase of deployment

Classification	Level	Conditions
Offline analysis	L 9	These levels are used during the first phase of a deployment, or after major changes in the network (such as adding, removing, moving or replacing a Data Source, changing security policies or installing major signature updates or major software upgrades). These Security Incidents will only be logged without real time analysis.

1.3.3 **Security Incident Handling**. Verizon will generate Security Incidents in both real- and non-real time, depending on the detection method. The status of the Security Incident will be changed throughout its lifecycle. Status changes are communicated by email and are displayed on the Customer portal. A Security Incident can have the following status:

Security Incident Status	Conditions
Open	The Security Incident is generated automatically based on Verizon's threat detection policies. SMC Time Stamp (UTC) when the Security Incident is created.
Active	The SOC starts the investigation.
Notify	The SOC identifies if the Security Incident may be harmful (Harmful Attack L1) or if it requires further information to classify the Security Incident (Insufficient Info L0).
Escalated	A Security Incident Ticket is created with information to allow the mitigation, containment or resolution of the risk.
Closed	The Security Incident is auto-closed or closed by the security analyst.

A Security Incident classification and status may change based on additional analysis, intelligence information or after Customer feedback has been received.

1.3.4 **Real-Time Security Incidents.** Verizon uses threat detection policies based on 1 or more use cases to create Security Incidents in real time. All use cases and proprietary signatures are categorized to help (a) increase insight into Security Incidents and (b) reduce the number of false-positive Security Incidents. The Security Incident descriptions provide recommendations on possible actions Customer can take. The Security Notification SLA applies.

1.3.5 **Non-Real Time Security Incidents.** Verizon uses threat detection policies based on 1 or more use cases to present Security Incidents periodically without SOC review or analysis. These Security Incidents (known as Security Digests) will be closed automatically, but can be reviewed by Customer on the Customer portal. Security Digests are focused on specific topics. This Security Incident handling is optimized for certain types of Security Incidents that do not require real-time Security Incident handling and SOC review. They provide additional information to Customer and can support compliance initiatives. The Security Incident Notification SLA does not apply for Security Digests. Customer specific Security Digests can be developed at Applicable Rates.

1.3.6 **Security Incident Escalation.** Verizon will only escalate Security Incidents that are classified as 'Insufficient Info' and 'Harmful Attack.' Verizon will examine the characteristics and context of the Security Events and Security Incidents, and evaluate the possible impact of a threat/attack before escalating a Security Incident Ticket. Verizon will provide additional information to support the investigation of a Security Incident and may propose possible recommendations for next actions.

1.3.6.1 Verizon will escalate a Security Incident Ticket with the following Security Incident Information:

- Security Incident Ticket Number
- UTC timestamp of the Security Incident creation
- Source information and destination information
- Threat Signature and use case information, if available: threat use case ID, name, and description
- Packet dumps, if obtainable from the Data Source using the existing infrastructure.

1.3.6.2 Security Incidents classified as 'Insufficient Info' require missing information from Customer within 14 days. If missing information is not provided, Verizon will send a reminder or change the status of the Security Incident to 'Closed.'

1.3.6.3 For up-to-date and accurate records of Customer's infrastructure inventory, to tune the detection policy, and to close and classify the Security Incidents appropriately for reporting purposes, any Customer remediation action shall be reported to Verizon.

1.3.7 **Service Management and Reporting**

1.3.7.1 **Customer portal.** Authorized Contacts have 24x7 access to the Customer portal exclusive of Maintenance Windows.

1.3.7.2 **Request for Information.** Customer may submit a RFI through the Customer portal. Customer will receive a unique reference number that must be used in all further communications on that RFI. Each question uses one Service Ticket. No Service Tickets will be charged if the RFI is related to an existing escalation. Inquiries not directly available through the Customer portal, or which require a more detailed analysis compared to what is available in the Security Incident Reports, will not be considered as a regular RFI. Verizon may accept such requests pursuant to a separate written agreement and charged at the Applicable Rates.

1.3.7.3 **Data Availability and Retention**

- **Data Storage.** Logs collected under the MSS – Analytics service are stored and available via the Customer portal for up to 90 days. Security Incidents and raw Log data associated with Security Events are stored in a Verizon proprietary format in the SMC database for 1 year. Verizon will store raw Log data associated with Security Events for 1 year. Raw Log data associated with Security Events that occurred during the immediately preceding 1 year period will be made available upon Customer's request up to 1 month after service has ended.
- **Archived Data and Data Retention.** Archived Security Incidents requested by Customer will be made available in a downloadable file or via an alternative storage medium, in a Comma Separated Value (CSV) format or another format mutually agreed upon by the Parties. At the end of the retention period, Logs and Customer Data will be disposed of according to the relevant Verizon Asset Classification and Handling Policy.

1.3.7.4 **Security Services Advisor (SSA).** Customer is assigned a SSA, who will host a quarterly service review meeting. The SSA is assigned to multiple MSS – Analytics customer accounts and is not a dedicated resource to any 1 customer. The SSA:

- Provides training on the Customer portal
- Manages Customer communication and security advisories
- Manages service issues and service credit requests

2. SUPPLEMENTAL TERMS

2.1 **Maximum Daily Data Ingest Volume.** Customer's Service Order will contain a maximum Daily Data Ingest Volume. Verizon will monitor Customer's Daily Data Ingest Volume and post a daily aggregate Daily Data Ingest Volume Report to the Customer portal.

2.1.1 **Maximum Daily Ingest Volume Overage and Charges.** Verizon will notify the Authorized Contact by email when the Customer's aggregate Daily Data Ingest Volume exceeds the maximum Daily Data Ingest Volume. Customer's daily aggregate may exceed the maximum Daily Data Ingest Volume 3 days in the month with no overage charge. If Customer's Daily Data Ingest Volume exceeds Customer's committed maximum Daily Data Ingest Volume more than 3 days in the month, Customer will be charged an overage amount. Overage is calculated by aggregating the volume of Gigabytes (GB) per day, in excess of the maximum Daily Data Ingest Volume, for every day in the month, exempting the first three overage days, then applying a per-GB overage charge.

2.1.2 **Maximum Daily Data Ingest Limitation.** Verizon may stop collection of Data in excess of Customer's contracted Daily Data Ingest Volume.

2.2 **Excluded Services.** Verizon does not provide MSS – Analytics for any Data Source that: (i) runs a version of operating system and/or application software that is not supported by Verizon, or that is no longer supported or maintained by the relevant manufacturer or licensor; or (ii) has not been properly registered and/or for which required permits or approvals are not maintained.

2.3 Customer Responsibilities

2.3.1 **Customer Deliverables for Implementation.** Customer will complete a Verizon Deployment Kit and provide such Deployment Kit to Verizon within 15 Business Days of the kick-off meeting. Verizon may terminate Customer's Service Order for MSS – Analytics if Deployment Kit is not timely received. Customer will timely approve the project plan, or provide necessary information to implement the project plan. Verizon may terminate Customer's Service Order if delays in project plan approval or necessary information causes any activity on the critical path of the project plan to be delayed by more than 25 Business Days. Upon termination of any such Service Order(s), Verizon may charge Customer for any expenses incurred by Verizon (including labor fees) through the date of termination based on such project plan delay.

2.3.2 **Asset Criticality Data.** Customer acknowledges that, without up-to-date asset criticality data, Verizon's ability to classify potential threats and Security Incidents accurately will be limited, resulting in the increased possibility of false-positives and inaccurate impact assessments.

2.3.3 **Maintenance Contracts.** Customer will (a) at its own expense, procure and maintain with each vendor adequate maintenance contracts and all licenses necessary for the Data Sources to enable Verizon to properly perform MSS – Analytics; (b) comply with MSS - Analytics prerequisites and operational procedures as set forth in the applicable terms; and (c) promptly inform Verizon of any changes in Customer Environment and any changes to the nomination and/or authorization level of the Authorized Contacts to oversee, monitor or evaluate the provision of MSS - Analytics.

2.3.4 **Interoperability.** Customer acknowledges that modifications or changes to the Data Sources (such as future releases to the Data Source's operating software) or to the Customer Environment may cause interoperability problems, inability to transmit Data to Verizon or malfunctions in a Data Source and/or the Customer Environment. Customer will give Verizon written notice (notice via email is acceptable) of any modifications or changes within 5 Business Days after making any such changes. Customer acknowledges that it is Customer's responsibility to maintain, at its sole cost and expense, the Customer Environment to ensure that the Customer Environment is interoperable with each Data Source.

2.3.5 **Service Equipment.** Verizon may require certain collection equipment to collect Logs and Security Events from Data Sources and to forward such Logs and Security Events to the SMC (e.g., Connection Kits). If Verizon determines that such collection equipment is needed on Customer's Site, Customer must provide the necessary equipment subject to Verizon's specifications either: (a) through direct procurement from equipment provider or (b) through Verizon as a CPE procurement. Verizon will configure and access such equipment remotely.

2.3.6 **User Interface.** In connection with the provision of MSS – Analytics, Verizon may provide Customer with 1 or more user Logins for use with MSS - Analytics. Customer will at all times keep it's Login strictly confidential and will take all reasonable precautions to prevent unauthorized use, misuse or compromise of its Login. Customer agrees to notify Verizon promptly upon learning of any actual or threatened unauthorized use, misuse, or compromise of its Login. Verizon is entitled to rely on Customer's Login as conclusive evidence of identity and authority. Customer will be liable for all activities and charges incurred through the use of Customer's Login, and will indemnify, defend and hold Verizon harmless from all liabilities, losses, damages, costs and expenses (including, without limitation, reasonable attorneys' fees and costs) incurred by Verizon to the extent resulting from the use and/or compromise of Customer's Login, unless the unauthorized use, misuse or compromise of Customer's Login is solely attributable to Verizon's gross negligence or willful misconduct.

2.3.7 **Installation Sites and Equipment.** Customer will prepare any installation site and Customer Environment in accordance with Verizon's instructions to ensure that any equipment that interfaces with Customer's computer system is properly configured as required for the provision of MSS - Analytics and operates in accordance with the manufacturer's specifications. Customer is responsible for any costs associated with preparation of the installation site and Customer Environment.

All Data Sources must have a routable network path to the Service Equipment and, if required, a Log Transport Agent must be loaded on each Data Source. Customer will procure, install and maintain software Log Transport Agents required for the provision of MSS - Analytics to Data Sources (e.g., for syslog logging for operating system and active directory server) at its cost. If Customer fails to make any preparations required herein and this failure causes Verizon to incur costs during the implementation or provision of MSS - Analytics, then Customer agrees to reimburse Verizon promptly for these costs.

2.3.8 **Protected Health Information.** Absent terms to the contrary in the Agreement, MSS - Analytics is implemented without specific controls that may generally be required or customary for customers in any particular industry and is not designed to satisfy any specific legal obligations. Customer agrees to use MSS - Analytics in accordance with all applicable laws and not to use MSS - Analytics in any manner that imposes obligations on Verizon under any laws other than those laws with which Verizon agrees to comply as specifically set forth in the Agreement. Without limiting the generality of the foregoing, Customer agrees not to cause, or otherwise request that Verizon create, receive, maintain or transmit protected health information (as defined at 45 C.F.R. § 160.103) for or on behalf of Customer in connection with MSS - Analytics or in any manner that would make Verizon a business associate (as defined at 45 C.F.R. § 160.103) to Customer. In the event Customer acts or uses MSS - Analytics in a manner not permitted under this Section 2.3.8, Customer shall (a) be in material breach of the Agreement, including this Service Attachment; (b) indemnify, defend and hold harmless Verizon for any losses, expenses, costs, liabilities, damages, penalties, investigations or enforcement proceedings (including attorneys' fees) arising from or relating to Customer's breach of this Section 2.3.8; (c) take, at Customer's expense, prompt action to correct and/or mitigate the effects of Customer's breach of this Section 2.3.8; and (d) provide Verizon with reasonable cooperation and support in connection with Verizon's response to Customer's breach of this Section 2.3.8. Customer shall assume and be solely responsible for any reporting requirements under law or contract arising from Customer's breach of this Section 2.3.8.

2.4 Warranties

2.4.1 **Verizon Warranties.** Verizon warrants to Customer that it will perform its obligations in a good and workmanlike manner. The remedies set forth in Section 3 Service Level Agreement are Customer's sole and exclusive remedies in connection with the portions of MSS - Analytics related to the failure to meet any standard set forth in the SLA. Verizon does not warrant that MSS - Analytics will detect and prevent all possible threats and vulnerabilities or that such services will render Customer's network and systems invulnerable to all security breaches and vulnerabilities.

2.4.2 **Customer Warranties.** Customer represents and warrants that (a) it has and will continue to have all rights, power, permissions and authority necessary to have Verizon perform MSS - Analytics in the Customer Environment (including, without limitation, all rights, power, permissions and authority necessary in respect of any IP address assigned to a Data Source, including consent of all authorized network users) and (b) consents to Verizon's performance of MSS – Analytics. Customer hereby assumes the sole responsibility for the accuracy of the IP addresses and domains provided to Verizon. Customer will be liable for all costs and expenses from any third party claims of loss, damage (including reasonable attorneys' fees) and liability of any kind that may be incurred as a result of Customer's breach of the foregoing warranty.

2.4.3 **Third Party Warranties.** For any third party products and/or services incorporated as part of MSS - Analytics, Customer will receive only the warranties offered by such third party to the extent Verizon may pass through such warranties to Customer.

2.5 Termination

2.5.1 **Renewal.** Each order will renew for a Term of 1 year, unless either party provides written notice at least sixty (60) days prior to the expiration of the then-current Term.

2.5.2 **Pre-RFS Termination**. Either party may terminate a request for MSS - Analytics prior to RFS with or without Cause, effective thirty (30) days after written notice of cancellation. If Customer requests termination of MSS - Analytics prior to RFS as set forth under this provision, or Verizon terminates MSS - Analytics as a result of Customer's failure to provide the necessary information or reasonable assistance required by Verizon to provision MSS - Analytics, Customer will pay any set-up fees and other amounts accrued for MSS - Analytics through the date of such termination plus an amount equal to any applicable annual third party license fee. Customer will pay the invoice for such charges in accordance with the terms of the Agreement.

2.5.3 **Post-RFS Termination.** Either party may terminate MSS - Analytics with or without cause, effective 60 days after written notice of termination is given to the other Party. Customer accepts and agrees that, in the event (i) Customer terminates any Service for convenience or (ii) Verizon terminates any Service for Cause prior to the end of the Service Commitment, then Customer will pay Verizon all unpaid fees payable under this Service Attachment and the applicable Service Order for the remainder of such Service Commitment. Customer will pay the invoice for such charges in accordance with the terms of the Agreement.

2.6 **Scanning Risks.** Verizon may scan Customer's internet facing IP subnets and hosts. Additional scanning may be requested by the customer or be performed by Verizon. Customer acknowledges that network scanning technology may have inherent risks, including, but not limited to loss, disruption, or performance degradation of the customer's network and services.

2.7 **Third Party Products or Services.** The Parties agree that Verizon will not be liable for any damages caused by hardware, software, or other products or services furnished by parties other than Verizon, its agents, subcontractors, or any damages caused by the products and/or services delivered by or on behalf of Verizon which have been modified, serviced, or otherwise attended to by parties other than Verizon or without Verizon's prior written and express consent. Customer acknowledges that Verizon will not be liable for any damages resulting, directly or indirectly, from any act or failure to act by Customer or any third party (including, without limitation, the non-performance, defaults, omissions or negligence of any third party that provides telecommunications services in the country or countries in which Customer's premises or systems are situated and other countries from, across, to or in respect which MSS - Analytics is provided by or on behalf of Verizon).

2.8 **Industry Alerts and Third Party Updates and Patches.** WITH REGARD TO SERVICES WHICH PROVIDE INFORMATION SHARING AND/OR INDUSTRY ALERTS, VERIZON DISCLAIMS ANY LIABILITY TO CUSTOMER, AND CUSTOMER ASSUMES THE ENTIRE RISK FOR (A) INFORMATION FROM THIRD PARTIES PROVIDED TO CUSTOMER WHICH TO THE BEST OF VERIZON'S INFORMATION, KNOWLEDGE AND BELIEF DID NOT CONTAIN FALSE, MISLEADING, INACCURATE OR INFRINGING INFORMATION, (B) CUSTOMER'S ACTIONS OR FAILURE TO ACT IN RELIANCE ON ANY INFORMATION FURNISHED AS PART OF MSS - ANALYTICS AND/OR (C) THE USE OF ANY THIRD PARTY LINKS, PATCHES, UPDATES, UPGRADES, ENHANCEMENTS, NEW RELEASES, NEW VERSIONS OR ANY OTHER REMEDY SUGGESTED BY ANY THIRD PARTY AS PART OF MSS - ANALYTICS.

2.9 **Verizon Materials.** If in connection with the provision of MSS - Analytics Verizon installs or provides any hardware or software (Verizon Materials), then Customer will use the Verizon Materials for internal purposes only as further defined in this Service Attachment. Customer will not distribute, reproduce, or sublicense the Verizon Materials. Customer will not reverse engineer, decompile, or disassemble or otherwise attempt to discover source code of the Verizon Materials. Verizon has the right to revoke the use of the Verizon Materials at any time. In such event, Customer will, at its sole cost and expense, promptly return the Verizon Materials to Verizon. Customer's right to use the Verizon Materials automatically terminates upon termination of this Service Attachment or upon completion of the portion of MSS - Analytics for which the Verizon Materials are provided.

2.10 **Confidential Information.** Customer acknowledges that the following information constitutes Confidential Information hereunder: (a) the methods, systems, data and materials used or provided by Verizon in connection with the provision of MSS - Analytics and (b) the results of Verizon's assessment of Customer and all reports issued by Verizon in connection with such results including, without limitation, security analyses and insight (Net Intel Information). Customer will disclose Net Intel Information only to Customer employees with a need to know for the purposes set forth in this Service Attachment and who are bound to confidentiality obligations at least as restrictive as those set forth in the Agreement and this Service Attachment. In no event may Customer use lesser efforts to protect Net Intel Information from use or disclosure not permitted under the Agreement than it uses to protect its own highly-sensitive confidential information, or less than reasonable efforts. The term Confidential Information will not include information that is comprised of statistical information, or other aggregated information regarding security vulnerabilities, security configurations and the like insofar as such information does not identify Customer or Customer's computer network or computer systems.

2.11 **Restriction on Selling Encryption Services in India.** Customer may use encryption up to 40 bit key length in RSA algorithm. If Customer requires encryption higher than this limit, then Customer will obtain approval from relevant telecom authority.

3. SERVICE LEVEL AGREEMENT

3.1 **Key Performance Indicators.** This SLA defines the service metrics for which Customer has the right to receive credits (Service Credits) in case Verizon fails to meet such metrics. In relation to a particular Data Source, the SLA will become effective when Verizon has issued the Ready for Operations notice.

3.1.1 **Security Incident Notification SLA.** A Security Incident ticket contains the initial Security Incident which triggered the security ticket creation, as well as any other associated Security Incidents. In case that there are multiple Security Incidents associated to the ticket, the initial Security Incident that triggered the Security Incident ticket creation will be used for the Security Incident Notification SLA calculation. Security Incidents can only be accessed on the Customer portal by Authorized Contacts that are defined in the service context.

Security Incident Type	Security Incident Ticket - Insufficient Info (L0)	Security Incident Ticket - Harmful Attack (L1)
Communication	A Security Incident ticket is sent to the customer via email with Security Incident ticket number and correlation reason Full Security Incident details can be viewed on the Customer portal	A Security Incident ticket is sent to the customer via email with Security Incident ticket number and correlation reason SOC will contact the Authorized Contacts by phone. Full Security Incident details can be viewed on the Customer portal.
Reference Time	SMC Time Stamp (UTC) when the Security Incident is created.	
Notification Start Time	SMC Time Stamp (UTC) when the Security Incident is set to 'notify' status. Notification SLA starts.	
SLA Response Time	≤ 15 minutes after Notification Start Time	

3.1.2 **Security Incident Notification Service Credits**

Response Time	**Instances per Month ≥X/Y**	**Service Credit**
Security Incident Report	≥ 5 / 100	1

- Insufficient Info > 15 minutes		
Security Incident Report - Harmful Attack > 15 minutes	≥ 1/100	1

3.2 **Service Credits Amount**

3.2.1 Subject to the terms in this section 3, Verizon will pay the applicable Service Credits as provided above. Service Credits will be calculated monthly. Service Credits are only available one month after RFS.

3.2.2 One Service Credit equals 10% of the prorated daily charge calculated based on the applicable MRC.

3.2.3 Instances per Month ≥ X/Y means that if Verizon exceeds the SLA Response Time X time(s) out of Y instances per month then the Customer may be eligible for a Service Credit.

3.3 **Service Credit Claims**

3.3.1 Customer will notify Verizon within 30 Business Days following a month where an SLA metric has not been met. No Service Credits will be issued if Verizon is not notified.

3.3.2 Verizon will verify any requested Service Credit, and will confirm the amount of the credit, if applicable. Verizon's Service Credit calculation is the final and definitive assessment of any credit payable.

3.3.3 Service Credits will be offset against future charges.

3.4 **Service Credit Conditions**

3.4.1 If a number of unmet service metrics arise out of the same Security Event, Customer will be entitled to the highest value Service Credit for one unmet metric.

3.4.2 The total number of Service Credits may not exceed 50% of the MRC.

3.4.3 Service Credits will not be due if the failure to meet service metrics is related to:

- A failure by Customer (or an entity under Customer's control) to comply with Customer's obligations as described herein.
- The non-performance, default, error, omission, or negligence of any entity not under Verizon's reasonable control (such as, but not limited to, failure of any of Customer's third party providers of telecommunications services or problems with equipment Customer has provided).
- The performance of routine maintenance work on, Service Equipment, or on any of the equipment used to provision MSS - Analytics service during the applicable Maintenance Window or emergency maintenance.
- Tests performed or commissioned by or on behalf of Customer); and/or
- Any Force Majeure Event.

4. **FINANCIAL TERMS**

4.1 **Rates and Charges.** Rates and charges are the same for Optimized and Non-optimized platform. Customer will pay the non-recurring charges (NRCs) and monthly recurring charges (MRCs) per MSS – Analytics service and per the Daily Data Ingest Volume tier (or per other specified item) as set forth in the applicable Agreement, and at the following URL:

www.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm. The NRC is billable for new installs or physical location moves. Unless expressly indicated otherwise, all NRCs will be invoiced upon Order Confirmation Date and the initial MRCs will be invoiced upon RFS. Customer will also pay any MRC overage charges, if applicable.

5. **DEFINITIONS.** The following definitions apply to MSS – Analytics, in addition to those identified in the Master Terms and the administrative charge definitions at the following URL www.verizonenterprise.com/external/service_guide/reg/definitions_toc_2017DEC01.htm

24x7	Nonstop service, 24 hours a day, 7 days a week, 365 (366) days a year, independent of time zones and local or international public holidays.
Applicable Rates	The rates that apply for professional services work not covered under this Service Attachment. All such work is subject to the execution of a separate written agreement that describes the activities and the Applicable Rates for performing such work.
Authorized Contacts	Customer personnel authorized by Customer to access the Customer portal and to interact with Verizon.
Connection Kit	Equipment installed on the Customer Site used to set up secured monitoring and/or management connections between the Data Sources and one or more Security Management Centers.
COTS/GOTS	Common or Commercial Off-the-Shelf/Government Off-the-Shelf product. A product, typically hardware or software, developed, marketed, sold and maintained by a specialist business, e.g., Microsoft Windows OS is a COTS product. GOTS products are often developed by government agencies (either in-house or via a specialist contractor paid by that agency) and are preferred by the government for use as all elements of the product can be controlled and built for government purposes.
Customer Environment	The network and/or information technology infrastructure in which Customer Data Sources reside.
Customer portal	Online portal where customers can have a near-real-time view on the Security Events/ Security Incidents being processed, and where they can view the company's security posture and effectiveness of the Data Sources and services at various levels.
Daily Data Ingest Volume	The total cumulative Data processed per day UTC, defined as 0:00 hours - 23:59:59 hours, from all Customer Data Sources.
Daily Data Ingest Volume Report	A report that summarizes the amount of Data Customer is sending to Verizon for analysis. The report includes both daily and monthly Data volume totals and is provided to Customer via the Customer portal.
Data	Machine-generated information that can be digitally transmitted and processed.
Data Source	Any Customer-designated source, including devices or services that generate Data. Data Sources include both traditional and non-traditional security devices, e.g., firewalls, intrusion detection and prevention devices, proxies, Unified Threat Management (UTM) devices, SIEMs, management stations, application logs, Security as a Service-based services, Active Directory, DHCP logs, etc. Data Sources can be configured on Customer's premises, with a third-party service provider or in the cloud.
Deployment Kit	A group of documents provided to Customer including various instructions as well as forms for the collection of additional data to enable onboarding.

Exploit	A method to use a Vulnerability to gain unauthorized access to functions, data, or privileges with malicious intent. An exploit can include a script, virus, Trojan, or a worm. The exploit is mainly defined by the way it replicates and spreads. An attack is the use of an Exploit. • A script refers to a document with steps to manually find and exploit vulnerabilities. A script is replicated by publishing it. • A virus refers to malicious software attached to a medium (e.g., files, removable media, and documents). A virus replicates using this medium. • A Trojan refers to malicious software embedded in applications. The Trojan will not replicate itself; it spreads with the application. A worm refers to a self-contained program (or set of programs) that spreads copies to other computers. A worm can spread through network connections and emails in a matter of hours.
Login	IDs, account numbers, personal identification numbers or codes, passwords, digital certificates or other means of authentication.
Logs	A collection of various IT, compliance, network, application, and security related information created by Data Sources.
Log Transport Agent	A Log Transport Agent is a third party software component that runs on Data Sources to enable the transport of the Security Event Logs generated by Data Sources to the Connection Kit and to the SMC. Like any agent software, a Log Transport Agent may impact available resources to perform tasks and functions.
Maintenance Window	A time window used for Verizon's performance of maintenance or management of the SMC. During a Maintenance Window, the MSS - Analytics services may be temporarily disrupted or unavailable. Maintenance windows are limited to a maximum of 6 hours unless otherwise communicated in writing by Verizon.
Order Confirmation Date	Verizon will confirm Customer's Service Order via email and the date of this email is the Order Confirmation Date. The Order Confirmation will confirm the MSS service(s) requested.
Project Manager	A Verizon-designated person who will act as the central point of contact throughout the MSS - Analytics implementation process and MSS - Analytics staging services, if applicable. The Project Manager will be responsible for managing the schedule and will also collaborate with Customer to develop a project plan that will specify resources, dates, times, and locations for the tasks described in the project plan. The Project Manager is not dedicated to Customer.
RFI	Request for Information – A customer inquiry regarding a Data Source. Service Tickets are charged once a Data Source has been declared Ready for Operations (RFO). Customers are charged one Service Ticket per RFI, unless the inquiry is related to an existing escalated Security Incident, in which case no Service Tickets are charged.
RFO	Ready For Operations - The date (following RFS) that Verizon sends RFO notice to Customer and informs Customer that the security analytics policy has been fine-tuned and the escalation parameters, Service Context, and procedures have been set as mutually agreed. The SLA is effective as of this date. RFO is given per Data Source.
RFS	Ready For Service - The date on which Verizon starts providing the MSS – Analytics service on a Data Source. Ready for Service is the lesser of 90 days from which Verizon has provided the on-boarding documentation, login information to the security portal, and has provided details to Customer regarding how to send Logs to the service or 30 days from receipt of Data from Customer for which Verizon can analyze Security Events and is investigating Security Events from that Data.

Security Analytics Platform	Verizon's security analytics platform that uses Verizon proprietary technology as well as COTS/GOTS hardware/software to process Data and Security Events from Customer Data Sources. Platform functions include: • Data and Log Processing, • Security Event Processing • Security Incident Handling • Vulnerability and Asset Processing
Security Content	The rules, use cases, policies, threat identification capabilities, queries, and Threat Intelligence used within MSS - Analytics to identify potential Security Incidents.
Security Digest	Security Incidents that do not require real-time Security Incident handling or SOC review and analysis.
Security Event	A data record produced by Verizon's Security Analytics Platform based on Verizon's proprietary threat detection policies.
Security Incident	A single Security Event or a series of Security Events that have been aggregated and correlated based on Verizon's proprietary threat detection policies. A Security Incident may represent an attack.
Service Context	A set of documents with version control, posted on the Customer portal, containing information about the Customer that Verizon uses for the provisioning of MSS - Analytics to the Customer. The Service Context is setup during the service initiation phase and is maintained via the change management process. Customer can also add or update host information in the Service Context. The Service Context may include one or more of the following: • Authorized Contact details and authorization procedure for escalation, notification, and reporting • Service Description • Escalation, notification, reporting, and change control processes • Authorized Contacts • Roles and Responsibilities in the form of a RACI Matrix for complex and/or custom solutions • Network topologies and asset inventories of systems
Service Ticket	A unit for charging certain usage-based services under MSS - Analytics. 24 Service Tickets are provided per provisioned Data Source annually following RFS. Verizon may modify the number of Service Tickets provided at its discretion.
SLA (Service Level Agreement)	The agreement setting forth the specific service levels and the terms and conditions for receiving Service Credits if Verizon were to fail to meet these service levels.
SMC (Security Management Center)	A data center that hosts the Verizon Security Analytics Platform. The SMC includes: equipment to connect to the Connection Kit, management stations, hosts the virtual Local Event Collector, Verizon's Security Analytics Platform, and customer portal, and back-end systems such as back-up devices, file servers, and terminal servers.
SMC Time Stamp	A time stamp recorded by Verizon at the SMC and reported on the customer portal. The time stamps are used as the reference for measuring the Service Level Agreement. The SMC Time Stamp is recorded in UTC and synchronized worldwide using the Network Time Protocol (NTP).
SOC (Security Operations Center)	A data center where the Verizon security analysts work.

SSL Certificate	A digital certificate is compliant with x.509v3, RFC 2459, RFC 3280, and RFC 3039 and includes at a minimum: • A public key • The identity or unique pseudonym of the certificate subscriber who owns and holds the private key matching the listed public key • The Issuer's identity • A start date and expiration date • A reference to the governing policy of the Issuer
Threat	A (suspected) use of an Exploit, or the (suspected) presence of Vulnerability in the configuration, platform, or application code. A Threat can be an infection by a worm or virus, or it can be a targeted attack. Exploits can also be combined into Blended Threats, exploiting multiple security weaknesses or defects.
Threat Intelligence	Strategic, tactical, and operational intelligence used to develop applied detection policies and perform multi-factor Security Incident correlation, so that only those threats that pose a significant risk are identified.
Threat Signature	Code used to recognize a Threat by its pattern. A Threat Signature may contain algorithms to detect dynamically changed malicious behavior, combat obfuscation, or impersonation.
User Interface	A web-based portal, dashboard, or other electronic means to share information and reports with customers that pertains to Security Incidents that are identified and escalated to the customer.
UTC (Coordinated Universal Time)	Universal Time indication standardized by the Bureau International des Poids et Measures (BIPM) and defined in CCIR Recommendation 460-4. The UTC is the time indicated on atomic clocks. Verizon consults and uses it for its SOC via the Internet protocol NTP. The UTC code uses the 24-hour clock. 4 pm (afternoon) is equal to 16:00 UTC.
Vulnerability	A weakness or defect that can be exploited to gain access to data, functions, or privileges violating the intended authorization. Vulnerabilities can range from defects in application or system software (e.g., bugs), in the user administration (e.g., non-protected user accounts), in the configuration (e.g., unintended network or file access), in the policy and rule set definition (e.g., unrestricted open ports or exposed IP addresses), etc. The combination of all vulnerabilities of a given system or infrastructure is the exposure.