verizon

Network Threat Advanced Analytics

1. GENERAL

1.1 **Service Definition.** Network Threat Advanced Analytics **(**Service) is intended to reinforce existing Customer threat and security event recognition capabilities based on automated watchlist matching (signature-based approach) and anomaly-based threat detection with additional SOC Analysis and SSA Support.

Verizon will capture and analyze NetFlow stemming from Customer IP ("CIP") address ranges listed in the CIP Schedule or, in case of premise-based NetFlow collection, directly from the Customer edge routers provided by Customer during the kickoff meeting. Verizon will analyze Customer's network traffic based on the identified CIP addresses using two mechanisms: A Signature-Based Detection mechanism, matching the IPs against the Verizon watchlists, and an Anomaly-Based Detection mechanism, creating alarms triggered by the underlying technology searching for abnormalities in the Customer's traffic compared to the Customer's baseline traffic.

Verizon will maintain raw NetFlow records for the CIP addresses in the CIP Schedule and anomaly-based alerts for 14 days. The incidents and events records will be kept for up to 12 months.

1.1.1 Signature-Based Detection

The Signature Based Detection mechanism creates Incidents by matching results when comparing the NetFlow from Customer's IPs with Verizon's watchlists. The watchlists contain IP addresses deemed suspect by Verizon based on the collection and scrutiny of intelligence drawn from: (a) the Verizon global IP backbone and/or customer premises equipment (routers); (b) Verizon investigations; and (c) other sources. During the watchlist matching component of the Service, Verizon will match watchlist IP addresses against Customer inbound and outbound traffic to identify possible indications of unwanted activity. Upon receiving an alert in a watchlist signature match, Verizon will determine the level of security risk associated with a given Incident.

The Incidents representing the results of the watchlist matching process will be available in the Security Dashboard. In cases Verizon deems findings as critical, Verizon will escalate notice to automatically send Customer an email notification. Signature-based results will not be actively analyzed by the Security Operations (SOC) Team. A detailed guideline describing the features and information points of the portals will be made available to the customer during the implementation phase. Customers can contact the SOC Team in case of detailed questions in accordance with the current communication matrix.

1.1.2 **Anomaly-Based Detection**

The Anomaly-Based Detection mechanism analyzes Customer's network traffic using statistical methods to compare current traffic behavior against a reference value of a baseline of Customer's network traffic. The baseline is a traffic profile which will be initially created when the Service begins and which will constantly be updated to reflect latest changes in the Customer's network. Detected anomalies exceeding Customer-specific thresholds will be alerted to the global SOC team which detects and reviews the anomaly.

The SOC Team will use a combination of proprietary, off-the-shelf, and open source tools to analyze Customer NetFlows to support multiple analysis vantage points. Verizon will alert Customer to Events it deems risky for Customer's network. If there is Insufficient Info Incident Classification, Verizon will contact Customer about suspicious activities for additional insight and background as needed.

Customer can also find a broad range of information and statistics concerning Events, as well as various anomaly detection charts, on a real-time basis in the Customer Security Dashboard.

1.2 **Service Features.** The following service features are included in with Service:

1.2.1 **Implementation of Service**. Prior to commencement of Service, Verizon will schedule a kick off meeting to introduce the Verizon service delivery team, identify the appropriate contacts for Customer (Authorized Contacts), discuss the scope of the Service and its business impacts, and obtain any required information from Customer.

1.2.1.1 Service will begin with a kick off call with Customer. During this call, Verizon will gather the following information from Customer to understand Customer's technical configuration, including:

- CIP Schedule review.
- Customer questionnaire review.
- Planning of the learning and sizing phase: During the learning phase, the implementation team will initiate the ingestion process for the Customer NetFlow data to create a first baseline which will be the reference point for the anomaly detection mechanism. After the initial learning phase, the implementation team will create an individual customer anomaly profile. The learning phase may take up to 4 weeks until the service can be set to RFO (Ready for Operations).

1.2.1.2 Customer Alert and Escalation Paths: Incidents recognized by Verizon will have 2 different sets of Customer escalation pathways: high-risk and low-risk security incidents ("Incident"). For both, Verizon will collect Customer email addresses, phone numbers, and other Customer contact details for the purposes of Incident escalation and portal access for each type of Incident, if applicable.

1.2.1.3 Customers with premise based Netflow collection require a completed deployment kit (Connection Kit). Upon receipt of the Connection Kit, Verizon will create a proposed project plan with high-level milestones and timelines. Verizon will only provision Service after Customer has approved the project plan.

1.2.1.4 **Excluded Services.** The Parties acknowledge that Verizon has no obligation to provide Service for IP ranges which have not been positively validated by Verizon during the presales validation

process. CIPs which do not belong to Verizon cannot be validated by Verizon internally; as such, Customer agrees to provide sufficient information to verify that the CIP's provided are exclusively to Customer. This can be achieved by providing a certificate about provider-independent IP's belonging to the Customer or a Letter of Authorization from the third party provider verifying that IPs belong to Customer.

1.2.2 Threat Analysis

1.2.2.1 **Overview.** Service analyzes Customer NetFlow data received from Data Sources to identify possible Security Incidents and indicators of potential compromise. A Security Incident is generated after data have been processed, or analyzed, against Security Content on Verizon's security analytics platform. Service both (a) analyzes individual pieces of data and Events which may, individually, appear to be harmless, and (b) correlates those Events and data with other data to determine if a harmful pattern is present, thus identifying a Security Incident.

Types of data used in Incident correlation can include:

- Any NetFlow data provided by Customer or generated from Verizon's IP backbone.
- Information about anomalies in the Customer network traffic.
- Verizon's Threat Intelligence.

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

Incident Classification	Risk Levels	Conditions
Insufficient Info	L0	The Incident has been classified as 'Insufficient Info' based on the associated events.
Harmful Attack	L1	The 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 Incident renders Customer's infrastructure vulnerable or compromised.
Harmless Attack	L2	The 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 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 or removing a server or Data Source, moving a Data Source, changing security policies, installing major signature updates or major software upgrades,

		implementing an urgent Change Request or replacing a Data Source). These Incidents will only be logged and without real time analysis.

1.2.2.3 **Security Incident Handling**. Verizon will generate Security Incidents in both real- and non-real time, depending on the detection method. The status of the Incident will be changed throughout its lifecycle. Status changes are communicated by email and are displayed on the Security Dashboard. An SMC Time Stamp (UTC) is added after each 'status' change. A Security Incident can have the following status:

Incident Status	Conditions
Open	The Incident is generated automatically based on Verizon's threat detection policies. SMC Timestamp (UTC) when the security incident is created.
Active	The SOC starts the investigation.
Notify	The SOC identifies if the incident concerns a security incident that may be harmful (Harmful Attack L1) or if it requires further information to classify the 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 Incident is auto-closed or closed by the security analyst.

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

1.2.2.3.1 **Real-Time Security Incidents.** Verizon uses threat detection policies based on one 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 Incidents. The Incident descriptions provide recommendations on possible actions Customer can take. The Security Notification SLA applies.

1.2.2.3.2 **Non-Real Time Security Incidents.** Verizon uses anomaly detection policies based on one or more use cases in order to find patterns in data collected recently or over a longer period of time and to allow low confidence indicators to be analyzed more effectively. Security analysts will review these Incidents with broader security information. If an Incident or a combination of Incidents is considered to be important, the SOC will escalate it. This method optimizes Security Incident handling and focuses on escalating potentially harmful Incidents and reducing Insufficient Info Incidents and False Positives. The Security Incident Escalation SLA does not apply.

1.2.2.3.3 **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 events and 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. Verizon will not provide remediation services under this service. Verizon will escalate a Security Incident Ticket with the following Incident Information:

- Security Incident Ticket Number
- UTC timestamp of the 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.

For Security Incident Escalation Customer:

- Customer to provide missing Incident information for Incidents classified as 'Insufficient Info' within the required timeframe; if Customer fails to provide such information, Verizon may send a reminder or change the status of the Incident to 'Closed.'
- Customer to inform Verizon of any remediation actions Customer has taken in order to enable Verizon to update its inventory of Customer's infrastructure and set the Incident status to 'Closed.'

1.2.2.4 **Service Management and Reporting**

1.2.2.4.1 **Security Dashboard.** Authorized Contacts have 24x7 access to the Security Dashboard. Each Authorized Contact must have one SSL Certificate to access the Security Dashboard. Service includes provision of up to 5 SSL Certificates.

1.2.2.4.2 **Request for Information.** Customer may submit a RFI through the Security Dashboard. Customer will receive a unique call ID that must be used in all further communications on this RFI. Inquiries not directly available through the Security Dashboard, or which require a more detailed analysis compared to what is available in the 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.

1.2.2.4.3 **Data Availability and Retention.** Incidents are stored in a Verizon proprietary format in the SMC database for 1 year, unless otherwise mutually agreed by the Parties in writing. Archived incidents requested by the Customer will be made available in Comma Separated Value (CSV) format or another format mutually agreed upon by the Parties. Verizon will store raw data associated with Events for 1 year. Raw data associated with Events linked to a Data Source 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 with respect to such Data Source.

1.2.2.5 **Security Services Advisor (SSA).** Customer is assigned a SSA, who will host a quarterly service review meeting. The SSA is assigned to multiple customer accounts and is not dedicated to Customer. The SSA:

- Provides training on the Security Dashboard
- Manages Customer communication and security advisories
- Manages Customer service issues pursuant to the Security Incident terms

2. **SUPPLEMENTAL TERMS**

2.1 **Data Ingestion.** NetFlow records will be ingested either from Verizon's IP backbone or from Connection Kit located on Customer premises. In the event errors occur during collection of NetFlow samples from Verizon's IP backbone, break-fixes will only be carried out during Normal Working Hours in the US; however this will not have an effect on the overall production of Incidents. If NetFlow Data is ingested from Customer premise based Connection Kits, then repair will be a provided 24x7 basis. Pricing is based on the amount of NetFlow ingested on a daily basis (Pricing Tier). If Customer exceeds the upper threshold of the purchased Pricing Tier, overage billing will apply (Overage Billing). Overage Billing is calculated on a monthly basis for any measured usage level greater than 5% over the upper threshold of the purchased Pricing Tier as measured in monthly average NetFlows. Verizon will measure the daily ingested NetFlows during the monthly billing period and Customer's measured usage level will be based on the average of 30 days of usage. Incremental usage will be calculated up to the next full 1K of daily ingested NetFlows.

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

2.2 **Location.** SOC support for the Service will be provided remotely from Verizon SOC locations in the United States, Europe and Asia on a 24x7x365 basis. Customer NetFlows will be continuously captured and Incidents created during evenings, weekends and holidays. Accordingly, Non-Real Time Security Incidents, per section 1.2.2.3.2, detected anomalies will be analyzed by Verizon and reported to the Customer only during Normal Working Hours in the U.S. and EMEA.

2.3 **Customer Responsibilities**

2.3.1 **Deployment Kit**. Customer must complete a Verizon deployment kit and provide such deployment kit to Verizon within 15 Business Days of the kick off meeting or Verizon may terminate Customer's Service Order. Verizon may charge Customer for any expenses incurred by Verizon (including labor fees) through the date of termination.

2.3.2 **Maintenance Contracts.** Customer will (a) at its own expense, procure and maintain with each applicable vendor adequate maintenance contracts and all licenses necessary for the Data Sources to enable Verizon to properly perform Service; (b) comply with Service 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 responsible to oversee, monitor or evaluate the provision of Service.

2.3.3 **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.

2.3.4 **Service Equipment.** Verizon may require certain collection equipment to collect NetFlow from Data Sources and to forward such NetFlow records 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 separate CPE procurement. Verizon will configure and access such equipment remotely.

2.3.5 **User Interface.** In connection with the provision of Service, Verizon may provide Customer with one or more user Logins to access a User Interface. Customer will at all times keep its 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.

2.3.6 **Installation Sites and Equipment.** For premise based ingestion, Customer will prepare any installation site 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 Service and operates in accordance with the manufacturer's specifications. All Customer premise based Data Sources must have a routable network path to and be compatible with the Connection Kit. Customer will install and maintain software agents required for the provision of Service to Data Sources on Customer network, 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 Service, then Customer agrees to reimburse Verizon promptly for these costs.

2.3.7 **Additional Customer Obligations.** Customer understands that, in addition to the other Customer obligations described in this Service Attachment, Customer must comply with the following obligations.

- Ensure that Customer contacts are available for Verizon, for the kick-off call and at other times as required throughout the term of the Service Order.
- Responsible to cause any remedial actions or responses to be taken based on information Verizon provides to Customer about its interactions with CIPs or domains disclosed to Customer.
- Customer understands that service interruption may occur if Customer initiates network routing changes to the IP addresses listed on the CIP and that Customer is responsible for any such service interruption.

2.4 Warranties

2.4.1 **Verizon's Disclaimer of Warranties.** Verizon does not warrant that any network, computer systems, or any portions thereof, are secure. Verizon does not warrant that use of Service will be uninterrupted or error-free or that any defect in Service will be correctable or that Incidents will be fully contained. Customer acknowledges that impenetrable security cannot be attained in real-world environments and that Verizon does not guarantee protection against breaches of security, or the finding or successful prosecution of individuals obtaining unauthorized access. Verizon does not warrant the accuracy of information provided to Customer hereunder. TO THE EXTENT PERMITTED BY APPLICABLE LAW, VERIZON DISCLAIMS ALL WARRANTIES EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR AGAINST INFRINGEMENT. THE WARRANTIES AND REMEDIES SET FORTH IN THIS SERVICE ATTACHMENT ARE VERIZON'S EXCLUSIVE WARRANTIES AND CUSTOMER'S SOLE REMEDIES FOR BREACH OF WARRANTY, IF ANY, BY VERIZON.

2.4.2 **Customer Warranty.** Customer represents and warrants that:

a) the deliverables, documentation, and other information provided by Verizon in connection with Service will be used solely for purposes of protecting Customer from abusive, fraudulent, or unlawful use or access to its information, systems and applications including Verizon's public Internet service and Customer will not market, sell, distribute, lease, license or use any such deliverables, documentation or information for any other purposes;

b) the list of Internet IP addresses provided by Customer contains only IP addresses that have been assigned or allocated for the exclusive use of Customer and/or affiliates of Customer over which Customer has control;

c) it has obtained or will obtain all legally required consents and permissions from users of CIP for Verizon's performance of Service, including without limitation the collection, use, processing, analyses and disclosure to Customer of Customer's Internet traffic data and the use of threat intelligence pertaining to CIP in an aggregated and anonymized form in connection with Verizon's portfolio of security services;

d) Customer will maintain up-to-date list of CIP addresses by revising and executing the CIP Schedule as applicable and provide the revised and executed CIP Schedule to Verizon; and

e) it will comply with all the Confidentiality obligations.

Customer shall indemnify, defend or settle and hold Verizon Indemnitees, and Verizon's associates, officers, directors, employees and partners harmless from and against all losses, damages, costs and expenses (including allocable costs of in-house counsel and other legal fees) associated with any claims, suits, judgments, settlements, investigations, fines, consent decrees, requests for information, or other dispute resolution, enforcement, regulatory or legal proceedings or actions of any kind,

suffered or incurred directly or indirectly by Verizon Indemnitees from or arising out of Customer's breach of any of the representations and warranties above or based on, arising out of or relating to Customer's use or interpretation of Net Intel Information provided by Verizon.

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

2.5 **Disclaimer/Limitation of Liability**

IN NO EVENT SHALL EITHER PARTY'S AGGREGATE LIABILITY FOR ANY CLAIM OR ACTION RELATING TO OR ARISING OUT OF THIS SERVICE ATTACHMENT, REGARDLESS OF THE FORM OF ACTION (INCLUDING, WITHOUT LIMITATION, CONTRACT, TORT, PRODUCTS LIABILITY OR STRICT LIABILITY) EXCEED THE AMOUNT PAYABLE TO VERIZON FOR THE SERVICE ELEMENTS GIVING RISE TO THE CLAIM. The foregoing does not limit (A) either party's liability: (i) in tort for its willful or intentional misconduct, or (ii) for bodily injury or death or loss or damage to real property or tangible personal property proximately caused by a party's gross negligence (where such concept is recognized in a particular jurisdiction); or (B) Customer's payment obligations hereunder.

2.6 **Third Party Information.** Customer may request that Verizon perform Service related to a third party's information. Customer hereby represents and warrants to Verizon that if it makes such a request, Customer will have obtained such third party's authorization to engage Verizon to perform Service to access such third party's information prior to Verizon's commencement of services. Customer agrees to indemnify, defend and hold Verizon harmless from any and all loss, damages, liabilities, costs and expenses (including legal expenses and the expenses of other professionals) resulting directly or indirectly from Verizon's alleged lack of authority to access the third party's information in connection with Service.

2.7 **Termination**

2.7.1 **Pre-RFS Cancellation**. Either Party may terminate a request for NTAA prior to RFS with or without Cause, effective 30 days after written notice of cancellation. If Customer requests cancellation of an NTAA service prior to RFS as set forth under this provision, or Verizon cancels an NTAA service as a result of Customer's failure to provide the necessary information or reasonable assistance required by Verizon to provision NTAA service, Customer will pay any set-up fees and other amounts accrued for NTAA through the date of such termination plus an amount equal to any applicable annual third party license fee, which Customer acknowledges are liquidated damages reflecting a reasonable measurable of actual damages and not a penalty. Customer will pay the invoice for such charges in accordance with the terms of the Agreement.

2.7.2 **Post-RFS Termination.** Either Party may terminate any NTAA service for any Data Source, 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 order for convenience or (ii) Verizon terminates any order for Cause prior to the end of the order term, then Customer will pay Verizon all unpaid fees payable under this Service Attachment and the applicable order for the remainder of such order term, which Customer acknowledges are liquidated damages reflecting a reasonable measurable of actual damages and not a penalty. Customer will pay the invoice for such charges in accordance with the terms of the Agreement.

2.7.3 **Reinstatements**. If Customer elects to renew an NTAA service for any Data Source after it has been terminated, or otherwise ended, Verizon may require payment of the then-applicable service initiation fees to re-establish the NTAA service for that Data Source (e.g., set-up NRCs).

2.8 **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 which Service is provided by or on behalf of Verizon).

2.9 **Industry Alerts and Third Party Updates and Patches.** WITH REGARD TO SERVICES WHICH PROVIDE INFORMATION SHARING AND/OR INDUSTRY ALERTS, TO THE EXTENT PERMITTED BY APPLICABLE LAW 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 SERVICE 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 SERVICE.

2.10 **Verizon Materials.** If in connection with the provision of Service 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 or cancellation of the Service Order or upon completion of the portion of Service for which the Verizon Materials are provided.

2.11 **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 Service 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.

2.12 **Restriction on Selling Encryption Services in India.** Customer will not employ bulk encryption equipment in connection with Verizon Facilities in India. Customer is permitted to use encryption up to 40 bit key length in RSA algorithm. If Customer requires encryption higher than this limit, then Customer must obtain approval from the relevant telecom authority and deposit the encryption key, split in 2 parts with that telecom authority.

2.13 **Collection of Netflow Data.** Due to local legal requirements, Customer must purchase Internet services from Verizon in order to receive services that rely upon Verizon directly collecting live netflow data from network equipment on Verizon's public backbone network in Japan. In addition to other remedies at law and equity, Verizon may at any time terminate the affected service in Japan, as applicable, if Verizon discovers that Customer has not purchased Internet services from Verizon or if Customer has terminated such Internet services.

verizon

3. SERVICE LEVEL AGREEMENT

3.1 **Key Performance Indicators.** This SLA defines the service metrics for the Service. In relation to a particular Data Source, the SLA will become effective when Verizon has issued the RFO notice.

3.1.1 **Security Incident Notification SLA.** A security Incident ticket contains the initial incident which triggered the security ticket creation, as well as any other associated incidents. In case that there are multiple incidents associated to the ticket, the initial 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 Security Dashboard by authorized contacts that are defined in the service context.

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 incident details can be viewed on the Security and Compliance Dashboard.	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 incident details can be viewed on the Security and Compliance Dashboard.
Reference Time	SMC Timestamp (UTC) when the security incident is created.	
Notification Start Time	SMC Timestamp (UTC) when the security incident is set to 'notify' status. Notification SLA starts.	
SLA Response Time	≤ 15 minutes after Notification Start Time	

3.2 **Regular Change Request**

Regular Change Request	Timeframe
Accepted	≤ 24 hours after request
Implementation	During Maintenance Window

4. FINANCIAL TERMS

4.1 **Rates and Charges.** Customer will pay the non-recurring charges (NRCs) and monthly recurring charges (MRCs) per Service and per the daily ingest data 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. For Customers using the premise based ingestion model (e.g. Connection Kits), Customer agrees the RFS for billing start date will be when 70% or more of all Customer sites have been installed.

4.2 **Discounts**

4.2.1 **Discount.** A discount, if applicable, can be applied to a Service Order.

4.2.2 **Discount Shortfall.** In the event Verizon grants Customer a discount and the supporting Initial Order Commitment is not met or order term is not completed as a result of Customer's termination for convenience or Verizon's termination for Cause; then the MRCs and NRCs payable will be adjusted in accordance with the discount, if any, Customer would be eligible to receive based on the actual business Initial Order Commitment or order term achieved and Customer shall pay such additional amounts as may become due as a result of such adjustment.

5. **DEFINITIONS.** The following definitions apply to Network Threat Advanced 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

24x7X365	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, except as noted.
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 Security Dashboard and to interact with Verizon for the Service.
Change Request	A request from Customer or Verizon for a change to the SEAM policy, security analytics policy, configuration, Service Context or for a Security Upgrade.
Connection Kit	Equipment installed on the Customer's premises used to set up secured monitoring and/or management connections between the Data Sources and one or more Security Management Centers.
Customer Environment	The network and/or information technology infrastructure in which Customer Data Sources reside.
Daily Data Ingest Volume	The total cumulative Data processed per day from all Customer Data Sources.
Data	Machine-generated information that can be digitally transmitted and processed.
Data Source	Any source of NetFlow either coming from Verizon's global IP backbone or from Customer premise devices, for this service Customer edge routers facing the public internet.
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.
Incident	A Security Incident is generated after logs and events have been processed through Verizon's threat detection policies and are correlated through the SEAM (State and Event Analysis Machine) Engine. Security incident handling escalates 'harmful attack' or high-risk incidents, and Verizon Analysts can implements emergency rule-set changes to block attacks. Low-risk incidents will be shown in the incident overview but will not be escalated to Customers.
Incident Record Communication	A record in the system that tracks and drives the workflow of Incidents during their lifecycle to closure.

Local Event Collector	Equipment at an SMC used to set up secured monitoring and management connections to the Customer Connection Kit.
Login	IDs, account numbers, personal identification numbers or codes, passwords, digital certificates or other means of authentication.
Maintenance Window	A time window agreed between the Customer and Verizon for Verizon's performance of maintenance or management services on the Data Sources. During a Maintenance Window, the Data Sources and/or Service services may be temporarily disrupted or unavailable. Maintenance windows are limited to a maximum of 6 hours per maintenance window.
Monthly Data 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 Security Dashboard.
NetFlow	Information from routing devices which represents header data including: source and destination IP Address, IP Protocol Type (e.g. TCP, UDP, ICMP, etc.), source and destination Port, TCP Flags (e.g. SYN, ACK, FIN, etc.), number of packets in the flow, number of bytes in the flow, start and end time of the flow.
Order Confirmation Date	Verizon will confirm Customer's order via email and the date of this email is the Order Confirmation Date. The Order Confirmation will confirm the Service service(s) requested.
Regular Change Request	A Change Request that Verizon will review and accept within 24 hours of submission and implement in the next Maintenance Window, provided that the minimum time between Customer's submission of a Regular Change Request and Verizon's implementation of such request will be 48 hours.
RFI	Request for Information – A customer inquiry regarding a Data Source. Customers are charged one Service Ticket per RFI, unless the inquiry is related to an existing escalated 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 Data Source 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 Service
Security Analytics Platform	Verizon's security analytics platform that processes data and events from Customer Data Sources. Platform functions include: • Data and Log Processing, • Event Processing • Incident Handling
SEAM	State and Event Analysis Machine – Proprietary Software used by Verizon. Its functions include: • Classification – giving Events a first classification, using Verizon proprietary Event Classification Policy Language, filtering out false positives or Events related to vulnerabilities absent in the targeted environment. • Workflow management – recording the activities for an Incident. • Information management – managing the information needed to examine, evaluate, and classify Incidents. • User management – defining the views and authorization levels of users.
Security Content	The rules, use cases, policies, threat identification capabilities, queries, and Threat Intelligence used within Service to identify potential Security Incidents.
Security Dashboard	Customer portal where customers can have a near-real-time view on the Events/Incidents being processed.
Security Event (Event)	A data record produced by Verizon's security analytics platform based on Verizon's proprietary threat detection policies.

Security Incident (Incident)	A single Event or a series of Events that have been aggregated and correlated based on Verizon's proprietary threat detection policies. A Security Incident may represent an attack.
Security Upgrade	Changes to application software program to fix a security weakness or defect and which is generally released by the equipment manufacturer as a security patch. A Security Upgrade includes signature or threat content updates.
Service Context	A set of documents with version control, posted on the Security Dashboard, containing information about the Customer that Verizon uses for the provisioning of Service 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 User details and authorization procedure for escalation, notification, and reporting • Service Description • Escalation, notification, reporting, and change control processes • Authorized Users • Information on maintenance and support contracts • Timeframe of Maintenance Windows • Roles and Responsibilities in the form of a RACI Matrix for complex and/or custom solutions • Network topologies and asset inventories of systems
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 Network Threat Advanced Analytics platform and the systems for monitoring, managing, or supporting NetFlow collection. The SMC includes: equipment to connect to the Connection Kit, management stations, hosts the virtual Local Event Collector, SEAM engines, Verizon's security analytics platform, and Security Dashboard, 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 Security Dashboard. 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 a 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 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 Sacs via the Internet protocol NTP. The UTC code uses the 24-hour clock. 4 pm (afternoon) is equal to 16:00 UTC. Depending on the daylight savings period, the UTC is 4 or 5 hours ahead of Eastern Standard Time (EST), and 1 or 2 hours behind Central European Time (CET).
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.

verizon

EXHIBIT A

Contract ID#_____

Customer IP Address Schedule ("CIP Schedule") to the Network Threat Advanced Analytics Service Attachment

_____("Customer")

Address:

By:_____
Name:_____
Title:_____
Date:_____

1. **Description.** The Network Threat Advanced Analytics as described in the service attachment requires that Verizon perform services for Customer utilizing a list of Customer provided IP addresses (collectively, "CIP") as provided by Customer at the kick-off meeting referenced in the service attachment.

Location/Site	IP Addresses