verizon

NETWORK THREAT MONITORING +

1. GENERAL

1.1 **Service Definition.** Network Threat Monitoring (NTM) Service is intended to reinforce existing Customer threat and Security Event recognition capabilities based on automated watchlist matching (Signature-Based Detection mechanism).

Verizon will capture and analyze NetFlow stemming from Customer IP (CIP) address ranges listed in the CIP Schedule provided by Customer during the kick off meeting. Verizon will analyze Customer's network traffic based on the identified CIP addresses using a Signature-Based Detection mechanism, matching the IPs against the Verizon watchlists.

Verizon will maintain raw NetFlow records for the CIP addresses in the CIP Schedule for 14 days. The Security Incidents and Security Events records will be kept for up to 12 months.

1.1.1 Signature-Based Detection

The Signature Based Detection mechanism creates Security 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 network; (b) Verizon cyberattack 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 Security Incident.

The Security 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 customer portals will be made available to Customer during the implementation phase.

verizon

1.2 **Service Features.** The following service features are included with Network Threat Monitoring:

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, discuss the scope of the Service and its business impacts, and obtain any required information from Customer, including identifying the appropriate contacts for Customer (Authorized Contacts).

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

1.2.1.2 **Excluded Services.** Verizon does not provide Service for IP ranges which are not associated with Verizon dedicated internet service.

1.2.2 **Threat Analysis**

1.2.2.1 **Overview.** Service analyzes Customer NetFlow to identify possible Security Incidents and indicators of potential compromise. A Security Incident is generated after Data has been processed against Security Content in Verizon's watchlists.

Types of Data used in Security Incident correlation can include:

- Any NetFlow Data generated from Verizon's IP network
- Verizon's Threat Intelligence

1.2.2.2 **Security Incident Handling.** Verizon will generate Security Incidents in near real time. Security Incidents will either be auto-escalated or auto-closed and are displayed on the Security Dashboard.

1.2.2.3 **Real Time Security Incidents.** Verizon uses threat detection policies based on one or more use cases to create Security Incidents in near 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.

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~~1~~ SSL Certificate to access the Security Dashboard. Service includes provision of up to five~~5~~ SSL Certificates.
- ~~1.2.2.4.2~~ **Data Availability and Retention.** Security Incidents are stored in a Verizon proprietary format for 12 months. Archived Security Incidents requested by Customer will be made available in Comma Separated Value (CSV) format. Raw Data associated with Security Incidents that occurred during the immediately preceding 12 month period will be made available upon Customer's request up to one~~1~~ month after Service has ended with respect to such Data Source.

2. **SUPPLEMENTAL TERMS**

2.1 **Data Ingestion.** NetFlow records will be ingested from Verizon's IP network. In the event errors occur during collection of NetFlow samples from Verizon's IP network, 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 Security Incidents.

2.2 Customer Responsibilities

2.2.1 **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.

2.2.2 **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.

2.2.3 **Additional Customer Obligations.** Customer understands that, in addition to the other Customer obligations described in this Service Attachment, Customer:

- must 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.
- is 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.
- 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.

2.3 Warranties

2.3.1 **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 Security 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.

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

- 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;
- 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;
- Customer 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;

- 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
- Customer 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 **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.

2.5 **Termination**

2.5.1 **Pre-RFS Cancellation.** Either Party may terminate a request for NTM Service prior to RFS with or without Cause, effective 30 days after written notice of cancellation. If Customer requests cancellation of NTM Service prior to RFS as set forth under this provision, or Verizon cancels a NTM Service as a result of Customer's failure to provide the necessary information or reasonable assistance required by Verizon to provision NTM Service, Customer will pay any set-up fees and other amounts accrued for NTM Service 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 measure of actual damages and not a penalty. Customer will pay the invoice for such charges in accordance with the terms of the Agreement. If Customer's Contract include Volume Commitment Period, the committed contract terms apply and there will be no Pre-RFS Termination.

2.5.2 **Post-RFS Termination.** Either Party may terminate any NTM 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 NTM Service for convenience or (ii) Verizon terminates any NTM 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, which Customer acknowledges are liquidated damages reflecting a reasonable measure of actual damages and not a penalty. Customer will pay the invoice for such charges in accordance with the terms of the Agreement. If Customer's Contract include Volume Commitment Period, the committed contract terms apply and there will be no Post-RFS Termination.

2.5.3 **Reinstatements.** If Customer elects to renew a 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 Service for that Data Source (e.g., set-up NRCs).

2.6 **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.

2.7 **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.

2.8 **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.

2.9 **Restriction on ~~Selling~~ Encryption ~~Functionality Services~~ in India.** Prior to connecting any encryption equipment to Verizon Facilities 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 prior evaluation and approval from the relevant telecom authority ~~and deposit the encryption key, split in 2 parts with that telecom authority~~.

2.10 **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.

3. FINANCIAL TERMS

3.1 **Rates and Charges.** Customer will pay the non-recurring charges (NRCs) and monthly recurring charges (MRCs) per Service 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. Unless expressly indicated otherwise, all NRCs will be invoiced upon Order Confirmation Date and the initial MRCs will be invoiced upon RFS.

3.2 **Discounts.** A discount, if applicable, can be applied to a Service Order.

3.2.1 **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.

4. **DEFINITIONS.** The following definitions apply to Network Threat Monitoring, 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

Term	Definition
Authorized Contacts	Customer personnel authorized by Customer to access the Security Dashboard and to interact with Verizon for the Service.
Data	Machine-generated information that can be digitally transmitted and processed.
Data Source	Any source of NetFlow from Verizon's global IP network.
Login	IDs, account numbers, personal identification numbers or codes, passwords, digital certificates or other means of authentication.
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(s) requested.
RFS	Ready For Service - The date on which Verizon starts providing the Service.
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 Security Incidents being processed.
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.
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 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.
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 Customer.

verizon

Exhibit A

Contract ID#_____

Customer IP Address Schedule (CIP Schedule) to the Network Threat Monitoring Service Attachment

_____(Customer)

Address:

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

1. **Description.** The Network Threat Monitoring 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