CENTURYLINK[SM] ADAPTIVE THREAT INTELLIGENCE SERVICE
SERVICE SCHEDULE

1. Applicability. This Service Schedule is applicable only where Customer orders CenturyLink[SM] Adaptive Threat Intelligence service ("Service") provided by CenturyLink or a CenturyLink affiliate ("CenturyLink"). Adaptive Threat Intelligence service may be designated as "TI", "TIS", "Threat Intelligence", "Adaptive Threat Intelligence", "ATI" or "Threat Intelligence Service", in Customer Orders, Order acceptance, service delivery, billing and related documents. This Service Schedule incorporates the terms of the Master Service Agreement or other CenturyLink approved services agreement under which CenturyLink provides Services to Customer (the "Agreement"). In the event of any conflict between the Service Schedule and the Agreement, the Service Schedule will govern and control.

2. Definitions. Capitalized terms used and not otherwise defined herein shall have the meanings set forth in the Agreement or as commonly known in the industry.

"Event(s)" means the record of a data sample or other security abnormality indicating interaction between Customer's network and a known Malicious Entity detected by the Service or reported by Customer to the SOC.

"Excused Outage" shall also mean, for purposes of this Schedule, the Service Levels will not apply, and Customer will not be entitled to receive a credit or exercise a termination right under the applicable Service Level, for (a) the acts or omissions of Customer, its employees, contractors or agents or its end users; (b) the failure or malfunction of equipment, applications, the public Internet, or systems not owned or controlled by CenturyLink; (c) force majeure events; (d) Regularly Scheduled Maintenance or emergency maintenance, alteration or implementation; (e) the unavailability of required Customer personnel or the inability of CenturyLink to contact Customer related to the Service, including as a result of failure to provide CenturyLink with accurate, current contact information (including email) and an up to date escalation list; (f) CenturyLink's lack of access to the Customer premises where reasonably required to restore the Service; (g) Customer's failure to release the Service for testing or repair and/or continuing to use the Service on an impaired basis; (h) Customer's failure to provide timely approvals and/or consents, including allowing CenturyLink to retune the Service as required for CenturyLink to provide the Service; (i) improper or inaccurate network specifications provided by Customer; or (j) Customer fails to fulfill any of its responsibilities or obligations as detailed in the Agreement, this Service Schedule and/or any other guidelines or policies applicable to the Service.

"Malicious Entity" is an internet protocol address(es) or network domain(s) associated with attempts to commit spam, fraud, hacking, denial of service, and other malicious or illegal activities.

"Portal" means the Service specific web-based portal to which Customer will have access in order to monitor Customer's traffic and view Events.

"Regularly Scheduled Maintenance" means any scheduled maintenance performed to the Service. Regularly Scheduled Maintenance will not normally result in Service interruption. If Regularly Scheduled Maintenance requires an interruption, CenturyLink will: (a) provide Customer seven (7) days' prior written notice, (b) work with Customer to minimize such interruptions, and (c) use commercially reasonable efforts to perform such maintenance between midnight and 6:00 a.m. local time where the Service is located on which such maintenance is performed and. Emergency maintenance may be performed on less or no notice.

"Secure DNS" is a feature designed to block malicious communications or Malicious Entities based on criteria established by Customer. Blocked communications or Malicious Entities are redirected to a warning page for Customer review.

"Service Outage" means that the Portal is unavailable to Customer.

"Service Validation" is confirmation by CenturyLink that the Service is operational and ready for use by the Customer.

"SIEM" means the security information event management platform configured, operated and maintained by Customer.

"SIEM Notification" is an optional feature available with the Service that allows customers to receive log and security event data at Customer's designated infrastructure destination.

"SOC" means CenturyLink's security operations center that among other duties, monitors the CenturyLink network infrastructure and security services provided to CenturyLink customers. Any third party network service provided by Customer is not supported or monitored by the SOC and instead, Customer is responsible for setting up and streaming all logs to CenturyLink for ingestion.

"Suspension" means CenturyLink's suspension of the Service as permitted by this Service Schedule or as otherwise allowed under the Agreement.

3. Service Description.

3.1 The Adaptive Threat Intelligence Service identifies Customer traffic flow interacting with known Malicious Entities identified by either IP address or network domain. If Customer purchases Internet service from a third party, Customer is required to provide CenturyLink with the IP addresses in order for CenturyLink to monitor the traffic. The Service uses meta data in the following principal techniques to identify these interactions:

- Interactions automatically sensed from the CenturyLink Internet infrastructure via configured software installed on CenturyLink infrastructure

- DNS interactions for those customers who elect to use CenturyLink's Secure DNS feature (available with Premium Option)
- Customer device logs (e.g. NetFlow, Firewall, DNS, etc.). Customer must elect to send logs to CenturyLink in order for CenturyLink to monitor them.

Customers that do not subscribe to CenturyLink Internet Services, elect not to use CenturyLink's DNS services, and elect not to send device logs to CenturyLink will derive limited benefit from the Service, as there will be limited visibility into interactions with potentially Malicious Entities.

3.2 The Service provides notification for Events on an advisory basis only. Due to the varying nature of malicious activity and the sampled network approach, CenturyLink cannot guarantee that all Malicious Entities will be identified, detected and/or alerted; nor does CenturyLink guarantee that all Events are actual security events. To increase the robustness of the Service, Customer should report to CenturyLink any Events not effectively detected by the Service and reported Events that were not actual security events. It is Customer's sole responsibility to review/investigate the reports and initiate action on the Event information. Customers with the Premium Option as further described below may request that SOC initiate blocking activity designed to prevent Event(s) or malicious communications. Customer acknowledges that CenturyLink is implementing actions at Customer's request and in accordance with Customer identified criteria and CenturyLink is not responsible for the effectiveness of the blocking.

3.3 The Service is available in two (2) software as a service options, which Customer will select upon ordering: (i) Enhanced Threat Intelligence Service ("Enhanced Option"), and (ii) Premium Threat Intelligence Service ("Premium Option").

Enhanced Option includes the following features:

- Monitoring of Customer's traffic as it passes through CenturyLink Internet infrastructure based on sampled network analysis
- Correlation of meta data against Malicious Entities utilizing CenturyLink proprietary analysis and threat information
- Correlation with Customer device logs that are transmitted to the ATI
- Near real-time forwarding of Events to the Portal
- Portal-based reporting utilizing Events
- Set number of hours (identified in the table below) of SOC support per service package tier, to obtain additional Event information, if available.

Service package tier (identified on the Order)	Hours of Support per month
Small	4
Medium	8
Large	12

Premium Option includes the following:

- All features included in the Enhanced option of the Service; plus
- Near real-time Event feed to Customer's SIEM
- Secure DNS feature. Customer will initiate a request for CenturyLink to initiate blocking via the Portal
- Set number of hours (identified in the table below) of SOC support per service package tier, to obtain additional Event information, if available.

Service Package tier (identified on the Order)	Hours of Support per month
Small	8
Medium	12
Large	16

3.4 **SIEM Notification**. The Enhanced Option does not require configuration changes in Customer's environment. For the Event notification to Customer's SIEM included in the Premium Option, Customer is responsible for configuring its SIEM platform and third party network environment to accept Events sent by CenturyLink. The Premium Option delivers Event notifications via syslog feed for up to 2 Customer provided SIEMs. Customer acknowledges that Event notifications sent to the SIEM are delivered over the Internet and such delivery may fail due to Internet connectivity issues outside of CenturyLink's control. Customer acknowledges and agrees that SIEM Notification is provided "as-is" and "as available" and CenturyLink shall have no liability related to or arising from use by Customer of this feature.

For SIEM Notification Customer, and not CenturyLink, is responsible for storage of the logs received; however, CenturyLink has the ability to send/resend buffered logs if needed for up to 14 days. Customer acknowledges that CenturyLink's ability to provide the SIEM Notification feature requires Customer to first provide CenturyLink with a digital certificate to be loaded on to the SIEM Notification platform in order for the log and security event traffic to be monitored by CenturyLink.

Customer is responsible for configuring Customer's SIEM platform and network environment to allow, accept and store logs and/or security events transmitted by CenturyLink.

3.5 The Service correlates the threat meta data with the sampled information from the CenturyLink network. Consequently, if the Internet access is provided by a carrier other than CenturyLink, CenturyLink will be able to perform Service only for the traffic that transits the CenturyLink network. For example, the Service will not work on traffic that is transitted solely on a third-party carrier's network or traffic where the source and destination carrier transit does not involve CenturyLink.

3.6 Notwithstanding anything in the Agreement to the contrary, CenturyLink may, in its sole discretion, subcontract any or all of the work to be performed under this Service Schedule, including but not limited to, installation, monitoring, detection, correlation, and alerting services, provided that CenturyLink will remain responsible for the performance of its obligations hereunder. CenturyLink reserves the right at any time to, by way of example: (i) change or supplement the monitoring tools, algorithms and Event correlation techniques; (ii) increase or decrease the monitoring and correlation tools' sensitivity to anomalous IP traffic patterns; and (iii) modify the algorithms that identify IP traffic patterns that may indicate malicious activity. In addition, CenturyLink continually makes improvements to the Service and reserves the right to make any updates, error corrections, bug fixes, and other feature changes or modifications to any software, equipment or hardware utilized by CenturyLink to provide the Services, at any time. CenturyLink will use reasonable efforts to make changes during Regularly Scheduled Maintenance.

3.7 Any non-emergency changes or Service design changes that may be required outside of prefix additions, changing the users that are notified about Events, and changing Customer IPs for the delivery of Events require Customer to initiate a change request.

3.8 Portal Use. Use of the Service includes access to the Portal, and Portal access is limited to ten (10) Customer users via two factor authentication token ("2FA Token"). If a Customer user does not access the Portal for more than six (6) months, the Customer's 2FA Token will be disabled. If Customer wishes to have more than ten (10) users, additional recurring and non-recurring charges may apply. Customer will accept and comply with the End User Rules of Use associated with use of the 2FA Token. No Service Level applies to availability or use of 2FA Tokens.

3.9 Portal Data. CenturyLink, through its third party provider, collects a minimal amount of information about Customer personnel that are authorized to access the Portal. The personal data collected and used with respect to the Portal includes portal enrollment information, consisting of name, business email address, administrative authorizations and login credentials, and Portal event data, consisting of high-level information about individual user's actions within the Portal. CenturyLink will only use this information to provide access to the Portal and provide Customer with information about actions taken within the Portal.

3.10 In providing the Service, CenturyLink's access to Customer information is generally limited to machine/system generated logs and/or metrics that allows CenturyLink to provide the Service. Certain tools, features, or requests by Customer, including those related to deep packet access may require that CenturyLink have visibility to additional Customer data.

4. Charges; Early Termination.

4.1 Customer will be billed monthly in advance based on predefined amounts of IP addresses as shown on the Customer Order. The charges for Adaptive Threat Intelligence Service consist of 2 components: (a) a non-recurring installation charge ("NRC"); and (b) a monthly recurring charge ("MRC"). Charges for certain Services are subject to (a) a property tax surcharge and (b) a cost recovery fee per month to reimburse CenturyLink for various governmental taxes and surcharges. Such charges are subject to change by CenturyLink and will be applied regardless of whether Customer has delivered a valid tax exemption certificate. For additional details on taxes and surcharges that are assessed, visit http://www.centurylink.com/taxes.

4.2 The Service Commencement Date begins upon issuance of a CenturyLink Connection Notice. The Connection Notice will be issued on the first to occur of: (i) successful completion of Service Validation; or (ii) five (5) business days after CenturyLink notifies Customer that it has provisioned all components of the Service that CenturyLink can provision without Customer's assistance.

4.3 The Service Term will be identified in the relevant Order. Either party may terminate the Service at any time and without early termination liability during the Service Term by providing 30 days prior written notice to the other party.

5. IP Addresses.

5.1 If CenturyLink assigns Customer an IP address as part of the provision of Service (e.g. to provide a real time feed of Events to Customer's SIEM), the IP address shall, to the extent permitted by law, revert to CenturyLink after termination or expiration of the applicable Customer Order, and Customer shall cease using such address. At any time after such termination or expiration, CenturyLink may re-assign the IP address to another user.

5.2 If CenturyLink does not assign an IP address to Customer as part of the provision of Service, Customer represents and warrants that all title, right and interest in and to each IP address used by Customer in connection with the Service is owned exclusively by Customer and/or Customer has all permissions necessary from the owner to enable CenturyLink and Customer to perform their obligations hereunder. Customer shall defend, indemnify and hold CenturyLink harmless from any claim, demand or action arising in connection with a breach of the foregoing representation and warranty.

6. Work Product. If CenturyLInk or any employee of CenturyLink develops or creates any intellectual property as part of the ATI Service ("ATI Intellectual Property"), that ATI Intellectual Property shall be, and remain, the exclusive property of CenturyLink and shall not be considered a work for hire. ATI Intellectual Property includes, by way of example, playbooks, runbooks, operational processes,

and CenturyLink equipment configuration settings. Customer shall have no right to sell, lease, license or otherwise transfer, with or without consideration, any ATI Intellectual Property to any third party or permit any third party to reproduce or copy or otherwise use or see the ATI Intellectual Property in any form and shall use all reasonable efforts to ensure that no improper or unauthorized use of the ATI Intellectual Property is made. Customer shall not reverse engineer or de-compile any ATI Intellectual Property. Customer will promptly, upon termination of this Service Schedule or upon the request of CenturyLink, deliver to CenturyLink all such ATI Intellectual Property without retaining any copy or duplicate thereof.

7. Customer Responsibilities/Obligations.

7.1 Customer is obligated to provide CenturyLink with (i) accurate and current contact information and escalation lists, including an up-to-date point of contact with 24x7 availability who CenturyLink will coordinate with upon detection of Events; (ii) all IP addresses that will be monitored.

7.2 Customer must cooperate with CenturyLink and CenturyLink's vendors or subcontractors in coordinating setup of the Service, including but not limited to, configuring the Customer's SIEM platform to accept Event delivery from CenturyLink (if applicable).

7.3 Customer understands and expressly consents that in the performance of its obligations hereunder, Customer traffic may originate or terminate in a country other than the country of origination and/or destination of traffic.

7.4 Notwithstanding anything to the contrary in the Agreement, Customer agrees that CenturyLink may use meta data that it generates, monitors and/or captures in connection with providing the Service and metadata (not attributable to any customer) for forecasting trends, threat intelligence or correlating Customer traffic information on the Service infrastructure, and Customer represents and warrants that it has in place any necessary third party consents, permissions and/or rights to grant the foregoing rights to CenturyLink.

7.5 Customer must establish and consistently maintain reasonable and adequate security policies and devices for defense and protection of its assets. Customer is solely responsible for properly configuring and using the Service and taking its own steps to maintain appropriate security, protection and backup of meta data and logs, and information that transits the Internet, which may include the use of encryption technology to protect meta data, logs and other Customer information from unauthorized access and routine archiving. Given that Customer can self-provision and self-configure the Services and the Customer environment in ways that may reduce their security, notwithstanding anything else to the contrary in this Service Schedule or the Agreement, Customer acknowledges that it and not CenturyLink will be responsible for whether the Services and Customer environment are configured in a secure manner and no security requirements or obligations of CenturyLink shall apply. In addition, Customer is solely responsible to ensure that its use of the Service does not violate any laws, security policies or regulations, including the manner in which the Service is used or accessed by Customer or its authorized users.

8. In the event Customer or CenturyLink determine that the Service is being affected by a continuing error, conflict or trouble report, or similar issue (in each case a "Chronic Problem") caused by the Customer, Customer shall resolve any Chronic Problem by taking whatever steps are deemed necessary to rectify the same, including, but not limited to: (i) removing or modifying the existing Service configuration (or requesting CenturyLink to remove the same); or (ii) replacing Customer's equipment providing that be deemed necessary. If Customer has not remedied the Chronic Problem within 30 days of request by CenturyLink, then CenturyLink may suspend or terminate the Service. Service Levels shall not apply and Customer will not be entitled to receive a credit or exercise a termination right under an applicable Service Level during periods of Chronic Problems caused by Customer.

9. Business Contact Information. Customer and CenturyLink acknowledge that it may be necessary to provide the other party with certain personal data necessary for the performance of each party's obligations under this Service Schedule, such as business contact information and credentials to access the applicable Customer portal(s). The parties acknowledge and agree that each is a data controller in its own right with respect to any such personal data exchanged under this Service Schedule, and any such personal data is provided on a controller-to-controller basis. Any personal data exchanged under this Service Schedule shall be limited solely to the extent necessary for the parties to perform their obligations or exercise their rights under this Agreement. As used herein, the terms "personal data" and "controller" shall have the meanings ascribed to them in applicable data protection laws, including, without limitation, the European Union General Data Protection Regulation (Regulation (EU) 2016/679). Each party shall be independently and separately responsible for complying with its obligations as a controller under applciable data protection laws in its capacity as a data controller with respect to the personal data it provides to the other party and/or receives from the other party.

10. Disclaimer/Liability.

10.1 Disclaimer. Customer acknowledges that the Services endeavor to mitigate security Events, but Events may not always be identified and if identified may not be mitigated entirely or rendered harmless. Customer further acknowledges that it should consider any particular Service as just one tool to be used as part of an overall security strategy and not a guarantee of security. The Service provided herein is a supplement to Customer's existing security and compliance frameworks, network security policies and security response procedures, for which CenturyLink is not, and will not be, responsible. While CenturyLink will use reasonable commercial efforts to provide the Services hereunder in accordance with the SLA, the Services are otherwise provided "as-is". CENTURYLINK MAKES NO WARRANTY, GUARANTEE, OR REPRESENTATION, EXPRESS OR IMPLIED, THAT ALL SECURITY THREATS AND VULNERABILITIES WILL BE DETECTED, THAT THE PERFORMANCE OF THE SERVICES WILL RENDER CUSTOMER'S SYSTEMS INVULNERABLE TO SECURITY BREACHES, THAT ANY THIRD PARTY SOFTWARE PROVIDED BY CUSTOMER WILL BE COMPATIBLE WITH THE SERVICE AND/OR THAT CENTURYLINK'S RECOMMENDATIONS, ASSESSMENTS, TESTS, REPORTS

OR MONITORING WILL BE ACCURATE, COMPLETE, ERROR-FREE, OR EFFECTIVE IN ACHIEVING CUSTOMER'S SECURITY AND/OR COMPLIANCE RELATED OBJECTIVES. Neither CenturyLink or its subcontractors will be liable for any damages or liabilities however classified including third party claims which Customer or third parties may incur as a result of: (i) non-compliance with any standards which apply to Customer, and/or (ii) reliance upon (or implementation of recommendations from) results, reports, tests, or recommendations related to the Services; or (iii) loss or corruption of data or information transmitted through the Service.

10.2 Direct Damages. Except for the payment and indemnification obligations of Customer and subject to the waiver of consequential damages provision in the Agreement, the total aggregate liability of each party arising from or related to a claim shall not exceed in the aggregate the total MRCs, NRCs, and usage charges paid or payable to CenturyLink for the affected Services under this Service Schedule in the six months immediately preceding the first event giving rise to the cause of action ("Damage Cap").

11. Resale Restriction. Notwithstanding anything to the contrary in the Agreement, Customer is prohibited from reselling any Service provided pursuant to this Schedule without the express written consent of CenturyLink.

12. Service Level Agreement ("Service Levels" or "SLA"), Service Objectives and Service Credits. The Service Levels are not available until completion of Service Validation. Whether a Service issue constitutes a Service Level outage or failure for Service credit purposes will be determined by CenturyLink in its good faith discretion supported by records, trouble tickets, data and other evidence, including through the use of third party monitoring tools. Service Credits are only available against the MRC for the affected Service. Service Levels do not apply to Excused Outages, periods of Suspension or periods of Chronic Problems.

12.1 Portal Availability Service Level. CenturyLink shall use commercially reasonable efforts to have the Portal available to Customer one hundred percent (100%) of the time after completion of Service Validation (the "Portal SLA").

12.2 Portal Availability Service Credit. Portal Unavailability means access to the Portal is not available and Customer is unable to access and/or receive Event information via the Portal, even though Customer has entered appropriate credentials. If the aggregate Portal Unavailability during a calendar month meets or exceeds the durations identified below, the following remedies will apply.

Aggregate Portal Unavailability Duration in a calendar Month (hrs:mins:secs)	Service Level Credit
00:00:01 – 00:04:59	No Credit
00:05:00 – 04:00:00	25%
04:00:01 or greater	50%

12.3 Chronic Outage. In addition to the above credit(s) and as Customer's sole remedy for any non-performance of the Service, Customer may elect to terminate an affected instance of the Service without termination liability within 30 calendar days of the date/time the right of termination is triggered if a single instance of Portal Unavailability meets or exceeds five consecutive days.

12.4 Time to Notify Service Level. For Customers (i) with the Enhanced Option, CenturyLink will notify Customer of an Event via the Portal within two (2) minutes of CenturyLink awareness of the Event; or (ii) with the Premium Option, CenturyLink will notify Customer of an Event via the Portal and a feed to the SIEM within two (2) minutes of CenturyLink awareness of the Event (individually and collectively the "TTN SLA"). Each time CenturyLink fails to meet the TTN SLA is a "Time to Notify Failure". Regardless of the number of Time to Notify Failures in a single calendar day, Customer's maxium credit per calendar day is one service level credit equal to 10% of the applicable MRC.

12.5 Event Response Time Objective. The following are CenturyLink objectives only, no service credits will apply.

Priority Level	Target Response Objective Enhanced Option	Target Response Objection Premium Option
Priority 1 – High A critical Event is detected by the Service and Customer is under imminent threat of compromise.	24 hours	2 hours
Priority 2 – Medium An Event is detected by the Service and Customer can mitigate but requires additional information from CenturyLink.	24 hours	8 hours
Priority 3 – Low Standard informational request about threat signatures that may be explained in Portal FAQs, but nonetheless Customer would like to speak about the issue**.** This includes tuning requests**.**	1 business day	1 business day

12.6 General Terms for all Service Levels. To be eligible for credits, Customer must be current in its obligations, and Customer must contact CenturyLink Billing Inquiries via the contact information provided on the invoice, open a ticket in the Portal or contact their account manager to report any issue for which Customer thinks a Service Level may apply within 30 calendar days after the issue occurs. Credits will not apply to any other services provided by CenturyLink. Duplicative credits (e.g., for both a Portal Availability SLA and Time to Notify SLA) will not be awarded for a single failure, incident or outage. The aggregate credits in any calendar month shall not exceed 100% of the MRC of the affected Service. The Service Level credits and termination rights stated in this Service Schedule shall be Customer's sole and exclusive remedies with respect to any service failure or outage.

12.7 CenturyLink's Service Levels only apply to the respective vendors' supported configurations at the time SLA support requests are triggered. If any configuration, version, system or third party software is identified as "unsupported" by a vendor, CenturyLink's SLA (including availability of Service Credits) will no longer apply and any support by CenturyLink will be reasonable efforts only. In addition, and at CenturyLink's reasonable discretion: 1) Customer may be required to purchase vendor supported upgrades at an additional cost to allow CenturyLink to continue to provide the Services or; (2) CenturyLink may elect to charge the Customer for any support or additional tasks/work incurred resulting from Customers' continued use of an unsupported configuration. Customer acknowledges and agrees that it is solely responsible for selecting and ensuring its software and systems are up to date and supportable. Customer's failure to do so may result in CenturyLink's inability to provide the Services and CenturyLink shall have no liability therefrom.