CenturyLink Technology Solutions

CenturyLink Technology Solutions Service Guide

Network Intrusion Detection

This CenturyLink Service Guide ("SG") sets forth a description of CenturyLink Network Intrusion Detection Services ("Service") offerings including technical details and additional requirements, if any. This SG is subject to and incorporated into the Agreement and Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order. For avoidance of doubt, any references in the Agreement, Schedules, or Service Orders to SSG, shall mean SG.

Version	Previous	Section Modified	Date
SEC-20140915-SG-DedicatedNIDS_Services	SEC-20091208-External-SSG-GL-Dedicated_NIDS_Services	All	September 15, 2014

Table of Contents

Service Description

Network Intrusion Detection Service

Service Description: Network Intrusion Detection Service (NIDS) is a CenturyLink provided service (the "Service") of a CenturyLink-owned CenturyLink Integrated Security Device (SISD) NIDS, or a CenturyLink-owned Cisco NIDS. The Service can be provided in a managed hosting data center (CenturyLink managed) or in a CenturyLink Colocation facility as well as at the Customer Premise, (CPE. The Service consists of the installation, configuration, administration, monitoring, and maintenance and support for the components listed in section 1.0. The Service is capable of passive monitoring of customer network traffic to determine suspected threat activity. Proactive blocking (Intrusion Prevention System), functionality is not included with this Service. The Customer network design will determine how the customer network traffic is directed to the Service, with the options being network traffic directed from Customer managed or dedicated network switch and/or Customer or CenturyLink provided network taps. The Service does not have the capability to perform inspection of encrypted traffic. The Service Level Agreement (SLA) associated with this Service is located in Appendix A. CenturyLink does not represent or warrant that the CenturyLink Equipment or the Service will be uninterrupted or error-free; will detect or generate an alert for every security event that may be recorded in customer logs, or meets any particular data security standard.

1.1. **Service Components:**

1.1.1. **CPE and IDC CenturyLink Managed**

1.1.1.1. **NIDS Device:** CenturyLink-owned CenturyLink Integrated Security Device (SISD) NIDS, or a CenturyLink-owned Cisco NIDS.will be provided

1.1.1.2. **Aggregation Switch**

1.1.1.3. **Network IDS:** A dedicated Network IDS capable of monitoring one point on the network per installation (unless a multipoint aggregator is also purchased). The remote managed Service via an on-site secure modem enables CenturyLink to access to the NIDS device over a dial-up connection for customer premise deployments

1.1.1.4. **Customer Portal:** Access to CenturyLink's managed security web portal where IDS alerts are available for Customer review.

1.1.1.1. **NIDS Device:** CenturyLink-owned CenturyLink Integrated Security Device (SISD) or Cisco NIDS appliance.

1.1.1.2. **Ethernet Taps:** Two (2) dedicated Ethernet taps, if required, are included in this installation.

1.1.1.3. **Incident Response (IR):** Incident Response ("IR") is performed as a function of the NIDS event investigation process. Only IR activities that are not associated with a WAF event are included in the Service. Incident Response as part of the NIDS event investigation process will consist of the CenturyLink Security Operation Center performing an analysis of the detected event. The NIDS analysis may include the use of both internal and commercial tools in determining the event impact to a specific Customer environment. Review of system logs, system statistics and files from live systems may be used in the event analysis process, (only for CenturyLink managed security service devices). The result of the event analysis could result in the following Customer recommended actions: Recommendations to perform host application hardening, recovery operations for Managed Hosting services or Customer host computer or recommendation to perform modification of firewall and IDS/IPS configuration rules.

1.1.2. **CenturyLink IDC**

1.1.2.1. **SISD Device (only available in IDC):** to run Snort based operating system with Cisco/SourceFire sourced signatures

1.1.2.2. **Aggregation Switch:** The Cisco Multipoint Aggregation switch provides management of a dedicated, CenturyLink-owned, Cisco switch for the purposes of aggregation of network links.

Depending on throughput requirements, a Cisco switch functioning as a Multipoint Aggregator residing at a CenturyLink hosting facility configured to monitor two (2) points on the Customer's network. Two (2) dedicated Ethernet taps, if required, are included in this installation. The third monitoring point and each additional monitoring point, up to a maximum of five, must be ordered. A Network IDS Sensor must be ordered separately. The aggregate sustained traffic of all monitored points on the network must not exceed the recommended maximum for the IDS sensor itself.

1.2. **Installation:** CenturyLink will provide installation tasks marked with an "X" in the CenturyLink column in Table 2.0 Roles and Responsibilities.

1.2.1. **CenturyLink IDC and CPE**

1.2.1.1. **Billing Cycle**: The NIDS service will be considered installed for billing following a five-day burn-in cycle and any follow-up conversations with Customer to make any required adjustments. Upon approval from Customer, the device will be set to blocking status and billing will commence.

1.2.2. **CenturyLink IDC:** CenturyLink will provide installation of the dedicated Cisco switch and two (2) Ethernet taps, if required.

1.2.3. **CPE:** CenturyLink will provide remote installation of the dedicated Cisco switch and two (2) Ethernet taps. CenturyLink will provide modem for out of band console access to NIDS device.

1.3. **Configuration:** CenturyLink will provide configuration tasks marked with an "X" in the CenturyLink column in Table 2.0 Roles and Responsibilities.

1.4. **Administration:** CenturyLink will provide administration tasks marked with an "X" in the CenturyLink column in Table 2.0 Roles and Responsibilities.

System Administration: CenturyLink will manage all system administration and NIDS passwords. Customer will not have access to NIDS passwords or be able to make direct changes to the NIDS configurations. Instead, Customer must request changes by contacting the CenturyLink Response Center. Customer must provide complete authentication credentials to the CenturyLink Response Center when requesting changes. (Changes and updates to this process are available at http://CenturyLink.net/customer/techsuppt.html).

1.5. **Monitoring:** CenturyLink will provide monitoring tasks with an "X" in the CenturyLink column in Table 2.0 Roles and Responsibilities.

1.5.1. **Response Times:** Response times for NIDS are located in Appendix A

1.6. **Maintenance and Support:** CenturyLink will provide maintenance and support tasks marked with an "X" in the CenturyLink column in Table 2.0 Roles and Responsibilities.

1.6.1. **Upgrades:** CenturyLink may periodically upgrade the security software to maintain the latest versions in operation. If CenturyLink determines an upgrade is necessary, CenturyLink will work with Customer to schedule a time to make necessary changes, preferably during the normally scheduled Internet Data Center (IDC) maintenance window. Customer must allow CenturyLink to make these changes within five (5) business days of receipt of the request from CenturyLink, or CenturyLink's obligation to provide this service in accordance with this CenturyLink Service Guide will be suspended until Customer grants CenturyLink the access CenturyLink requires to make such changes. If CenturyLink determines that an emergency security change is required, CenturyLink will make the change as quickly as possible. CenturyLink will make commercially reasonable attempts to contact the Customer's technical contact prior to making said change.

1.6.2. **Hardware Repair IDC:** If required, CenturyLink will repair hardware, reinstall required equipment, and assume repairs or parts costs unless damage caused to NIDS system was a result of unauthorized Customer action.

Hardware Repair CPE: If required, CenturyLink will, work with customer to have required replacement equipment re-installed, and assume repairs or parts costs unless damage caused to NIDS system was a result of unauthorized Customer action.

2. **Customer Responsibilities:** Customer is responsible for all tasks marked with an ”X” in the Customer column in Table 2.0 Roles and Responsibilities. Customer acknowledges and agrees that its failure to perform its obligations set forth in Table 2.0 may result in CenturyLink’s inability to perform the Services and CenturyLink shall not be liable for any failure to perform in the event of Customer’s failure.

2.1. **Customer Installation Requirements**

2.1.1. **CenturyLink IDC and CPE**

2.1.1.1. **Network Topology Changes**: The Customer must notify CenturyLink in advance of any network topology or system changes that may affect the IDS or the effectiveness of the IDS policy. Failure to notify CenturyLink of system changes may result in the inability to monitor traffic or the generation of false alerts. CenturyLink will work with the Customer to resolve chronic false positives and other nuisance alerts; however, if alerting issues are not resolved satisfactorily, CenturyLink may modify the IDS configuration to reduce repetitive alarms caused by Customer actions that are not indicative of security incidents.

2.1.1.2. **Adherence to Customer Responsibilities:** Customer must comply with all responsibilities under this CenturyLink Service Guide or CenturyLink’s obligation to provide this Service in accordance with this CenturyLink Service Guide will be suspended until Customer complies.

2.1.1.3. **Testing:** Customer shall not attempt, permit or instruct any party to take any action that would reduce the effectiveness of Service or any devices used to deliver CenturyLink services. Without limiting the foregoing, Customer is specifically prohibited from conducting unannounced or unscheduled test firewall attacks, penetration testing or external network scans on CenturyLink’s network without the prior written consent of CenturyLink. Testing: Customer shall not attempt, permit or instruct any party to take any action that would reduce the effectiveness of Service or any devices used to deliver CenturyLink services. Without limiting the foregoing, Customer is specifically prohibited from conducting unannounced or unscheduled test firewall attacks, penetration testing or external network scans on CenturyLink’s network without the prior written consent of CenturyLink.

2.1.1.4. **Third Party Software:** If any third party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with the Service, Customer agrees to use such third party software strictly in accordance with all applicable licensing terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third party software.

2.1.1.5. **Permissions:** Ensure that all permissions of any kind needed for the installation and operation of CenturyLink-owned equipment are in place at all times

2.1.1.6. **Testing:** Customer shall not attempt (nor instruct or allow others to attempt) any testing, assessment, circumvention or other evaluation or interference with any Service without the prior written consent of CenturyLink.

2.1.1.7. **Changes to NIDS Information:** The Customer will, using CenturyLink’s standard procedures, notify CenturyLink of the initial and later changes to the NIDS information to be configured by CenturyLink with the NIDS device.

2.1.1.8. **Connection Management:** If the Customer has an ACL that interferes with management connections, the Customer must allow CenturyLink access for management and monitoring.

2.1.1.9. **IP Address:** Customer must provide IP addresses for all network connections to the NIDS device and the secure management device, the number of which will be determined by CenturyLink.

2.1.1.10. **Bandwidth:** Customer must not have sustained bandwidth exceeding rated capacity of the device, without resulting degradation in service.

2.1.2. **CPE**

2.1.2.1. **Physical Site Requirements:** For NIDS devices that are not installed within a CenturyLink Utility Hosting Environment, the Customer must provide the necessary space, power, environmental conditions and security precautions at each Customer site, and otherwise prepare the site for IDC hardware as detailed in Table 3.0 Physical Site Requirements.

2.1.2.2. **Equipment Access:** Customer must allow CenturyLink personnel to access the NIDS device, where CenturyLink determines such access is necessary to deliver the service or respond to a security incident. Customer agrees to give CenturyLink and others working for CenturyLink access to equipment immediately if there is a service outage and/or at reasonable times in all other situations.

2.1.2.3. **Always-on Connection:** If it is not already available the Customer must purchase an always-on connection to the public Internet (DSL, T1, cable modem etc.) Dial-up connection is not sufficient.

3. **Additional Services:** At Customer's option and expense Customer can choose to have CenturyLink complete one or more of the tasks in Table 2.0 with an "X" in the Customer column and/or the services listed below. The items can be added to the standard Service (described in Section 1.0) for an additional fee described in a separate Statement of Work ("SOW") or Service Order. Contact a sales representative for additional information.

3.1. **Aggregation switch**

3.2. **Ethernet taps:** Additional dedicated Ethernet taps. Each additional monitoring point, up to a maximum of five, may be ordered separately.

3.3. **Network IDS Sensor:** Network IDS Sensor(s) must be ordered separately. The aggregate sustained traffic of all monitored points on the network must not exceed the recommended maximum for the sensor itself.

Management of Network Connection

Table and Appendices

Table 1.0 Supported Appliances

Device Type	Aggregate throughput*	Deployment Mode	Serial port. RJ-45 for Console Access	Firewall Interface Configuration (10/100/1000 Ethernet)**			
				Total Interfaces per firewall	Interfaces Reserved for management	Interfaces Available	10 G-Int Available
Cisco IPS4345	Up to 750 Mbs	Single Device	1	9	1	8	0
Cisco IPS4360	Up to 1.25 Gbs	Single	1	9	1	8	0
Cisco IPS4510	Up to 3 Gbs	Single	1	7	1	6	4
Cisco IPS4520	Up to 5 Gbs	Single	1	7	1	6	4
SISD Small	Up to 100 Mbs	Single	1	5	1	4	0
SISD Large	Up to 500 Mbs	Single	1	9	1	8	0

*(IDS / IPS throughput numbers in the chart above are based on cleartext traffic and a mix of packet size payload aggregated across all monitoring interfaces with NIDS deployed in passive monitoring mode. The use of features such as enhanced log collection and custom signatures may reduce overall throughput capability.) These performance numbers should be used as sizing guidance, thus do not carry any SLA commitment.
**Standard configuration; interface upgrade cards devices may have available options

Table 2.0 Roles and Responsibilities

Activity	Task	CenturyLink	Customer
Design / Planning	Perform an initial Intrusion Detection and Response set-up consultation with the Customer	X	
	Develop the Customer's alert policy, determine the appropriate response procedure, and answer Customer's questions regarding Service	X	
	Verification that device configuration adhere to the Customers organizations security		X

Activity	Task	CenturyLink	Customer
	policies.		
	Adherence to Security Policy: Verification that device configuration adhere to the Customers organizations security policies.		X
	Web portal Self Service Setup: Initial setup of Self Service for NIDS functionality.	X	
	Web portal Self Service Training: Explanation of the Service reports and statistics provided.	X	
Installation	Provide all required information during initial consultation		X
	Validate Connectivity: Validate that network connections can be established and maintained through the NIDS device.	X	
	Installation of NIDS devices to CenturyLink standard, including racking, cabling within the CenturyLink data centers.	X	
	Physical device shipped to Customer premises for Customer to install (Customer premise equipment (CPE).		X
	Software Installation: Installation of NIDS device and accompanying software in accordance with the vendor's recommendations.	X	
	Install and configure the system, apply the initial policy of the device, and set the device to a ‘burn in’ status for a minimum period of one week	X	
	NIDS Patch Installation: Patch devices as required or when the Customer requests for a specific patch that has been approved by CenturyLink product.	X	
	Install and configure the system’s base build, apply the initial policy of the device, and set the device to a ‘burn in’ status for a minimum period of one week	X	
	Evaluate the alert traffic for false alarms and make appropriate recommendations for policy tuning	X	
	Make required adjustments to the policy as necessary following the burn-in period; set device to full monitored status	X	

Activity	Task	CenturyLink	Customer
Configuration	Configure alert policy and response procedures for Customer	X	
	Perform a security review of the IDS configuration,, make recommendations for security improvements	X	
	Custom NIDS Rules and Filters: Customer specific NIDS rules and filters (if not captured via tuning).		X
	Custom Signatures: Customer specific NIDS signatures		X
Administration	NIDS Requirements Documentation: The creation of NIDS alerting and notification documentation to include alert policies and escalation procedures.	X	
	NIDS Design: The network diagram showing the placement of the NIDS within the network, (for IDS deployments in managed hosting environments).	X	
	Request and gain approval of changes to the NIDS policy rules via the Customer's change management process.		X
	Notify CenturyLink of the initial and later changes to the NIDS information to be configured by CenturyLink with the NIDS device.		X
	Change NIDS policy rules after appropriate approval via the Customer's change management process.	X	
	Provide ongoing policy review to enhance the performance of the NIDS policy.		X
	Oversee the continuous observation of system health and availability alerts and or reported events.	X	
	NIDS Policy Tuning: Twice a year tuning to verify that NIDS rules are functioning as expected, when requested by the Customer.	X	
	Policy Backup: The regular backup of NIDS policies and rule sets.	X	
	Conduct periodic testing to verify that system rules are functioning as expected and to confirm that the policy rules remain in compliance with initial policy.		X
	Provide an explanation of the reports and	X	

Activity	Task	CenturyLink	Customer
	statistics provided on web portal		
	Administration of Customer managed end points		X
Monitoring	Receive and review alerts issued by the NIDS sensor(s), which generate alerts upon encountering network traffic patterns that may indicate suspicious activity according to the response time chart.	X	
	Network Connectivity Testing: Testing that all relevant network connections can be established and maintained through the firewall.	X	
	CenturyLink Management Testing: Testing and verification that firewall administrators can configure and manage the firewall effectively and securely from the appropriate networks.	X	
	Testing of Logging: Testing that Service logging and data management functions are performing in accordance with the policies and Customer's logging and data management strategies.	X	
	Web portal and Reporting: Access to the security web portal, where NIDS events are available for appropriate organization personal review. NIDS reporting to include: -Raw event detail for previous 90 days -Event summary graphs, with event break down into High / Med / Low severity. -Event Summary graphs, with detail on targeted and originating IP addresses. -Event Summary graphs to show NIDS activity over the previous 90 days -Monthly NIDS summary reports in PDF format	X	
	CenturyLink will monitor Service infrastructure for performance load to include CPU and memory allocations to individual customer virtual firewall instances.	X	
	CenturyLink will provide Customers at their request a bi-annual review of the Customer's NIDS policy and log summary	X	
	Initiate a request for a bi-annual review through support center to open a ticket	X	

Activity	Task	CenturyLink	Customer
	Conduct ICMP (e.g., ping) monitoring of the NIDS sensor to determine system availability (24/7). In the event that the sensor fails to respond, CenturyLink will notify Customer via phone and/or email and initiate corrective action.	X	
	Provide hardware break-fix support with a next business day response time for new equipment.	X	
Testing	Rule Set Testing: Verification of the rule set includes both reviewing the rule set manually and testing whether the rules work as expected.	X	
	Management Testing: Testing and verification that Security Analysts can configure and manage the NIDS effectively and securely from the appropriate networks.	X	
	Testing of Logging and alerting: Testing that NIDS logging and alerting are performing in accordance with the Customer's logging and alerting requirements.	X	
	NIDS OS Vulnerability Testing: The testing that known NIDS operating system vulnerabilities are identified and patched.	X	
	Testing Signoff: Customer to sign off on the NIDS testing prior to CenturyLink support initiated.		X
Maintenance and Support	Provide support for secure and encrypted management connections	X	
	24/7 support for NIDS problem resolution and Customer inquiries.	X	
	Response to device issues, inclusive of coordination with vendor if necessary in accordance to NIDS requirements documentation.	X	
	Implement various health checks such as ICMP (e.g., ping) monitoring and pre-set test event triggering of the NIDS sensor to determine system availability (24/7) where practical.	X	
	Repair hardware, reinstall required equipment, and assume repairs or parts costs unless damage caused to NIDS system was a result of unauthorized Customer action. For Service within CenturyLink data center.	X	
	Provide support for 24x7x365 end user administration requests by CenturyLink system administrators	X	

Activity	Task	CenturyLink	Customer
	Notify Customer via phone and/or email and initiate corrective action in the event that the device fails to respond	X	

Table 3.0 Physical Site Requirements

Item	Requirement
Physical Environment	Predefined and adequate rack shelf or tabletop space for installation, with unobstructed entry for CenturyLink and others working for CenturyLink.
Electrical Power	Electrical outlets for both the NIDS devices and the secure management console
	Extension wiring available if distance to electrical outlets is greater than 6 feet.
	Power supply ready at installation location
POTS line	Provide POTS line for CPE deployments of Service
LAN Connectivity	Ethernet LAN topology (for NIDS device)
	Extension wiring if the distance to the NIDS connection is greater than 6 feet.

Appendix A: Service Level Agreement

Table 4.0 Response Times NIDS

Event	Response Time & Procedure
NIDS Critical Alarm. Maps to SLO P2 (High)	**Reference Service desk SLO link off Savvisstation.com, Incident Management section.**
NIDS / IPS Configuration and Policy Change Request. Maps to SLO P3 (Medium)	**Reference Service desk SLO link off Savvisstation.com, Request Management section.**
NIDS / IPS new Configuration request. Maps to SLO P3 (Medium)	**Reference Service desk SLO link off Savvisstation.com, Request Management section.**

Response Times SLA

In the event that CenturyLink is unable to provide service within the “Response Time” windows outlined above, the Customer’s sole and exclusive remedy shall be a service credit in the amount of three percent (3%) of the affected service MRC for each response time failure. In no event will the credits accrued in any single month exceed, in the aggregate across all response time goals and incidents, thirty percent (30%) of the invoice amount for the affected service.

SLA Process

Customer must request any credit due hereunder within 30 days of the conclusion of the month in which it accrues. Customer waives any right to credits not requested within this 30-day period. Credits will be issued once validated by CenturyLink and applied toward the invoice which Customer receives no later than two months following Customer's credit request. All performance calculations and applicable service credits are based on CenturyLink records and data.

The applicable SLA provides Customer's sole and exclusive remedies for any Service interruptions, deficiencies, or failures of any kind. The SLA and any remedies hereunder will not apply and Customer will not be entitled to receive a credit in the case of an Excluded Event. "Excluded Event" means any event that adversely impacts the Service that is caused by,

- the acts or omissions of Customer, its employees, customers, contractors or agents
- the failure or malfunction of equipment, applications or systems not owned or controlled by CenturyLink
- Force Majeure events
- scheduled maintenance
- any suspension of Service pursuant to the Agreement
- the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information

General Service Requirements

If any third party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with the Service, Customer agrees to use such third party software strictly in accordance with all applicable licensing terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third party software.

Customer shall,

- provide CenturyLink with sufficient system passwords, privileges and access to allow CenturyLink to install, configure, monitor and modify the Service.
- not attempt (nor instruct or allow others to attempt) any testing, assessment, circumvention or other evaluation or interference with any Service without the prior written consent of CenturyLink.
- Notify CenturyLink at least 5 business days in advance of any changes that may affect the applicable Service (e.g., infrastructure, network topology changes)
- purchase and maintain a reliable, stable and always-on, high speed connection to the public Internet (i.e., DSL, T1, cable modem etc. -- a dial-up connection is not sufficient) and/or a standard (POTS) telephone line (with direct inward dialing) for each Customer Site to enable CenturyLink to perform remote network management functions.
- designate and maintain a Customer Contact during the Service Term (including current contact information). "Customer Contact" means an English-speaking technical point of contact available 24 x 7 with sufficient knowledge, authority and
- access to address configuration issues, event notifications, system or infrastructure

- modifications and authentication of applicable CenturyLink systems. For CenturyLink Managed Hosting environments any Ports and VLANs in addition to those
- included in the standard CenturyLink design shall be subject to incremental charges as set forth in the relevant Order Form. Any Port or VLAN requested by Customer after the initial installation of the Service shall also be subject to additional, incremental charges. Provision of the Service is subject to Customer's compliance with this Section.

CenturyLink may manage all system administration passwords, including root level access, and may do so exclusively. In such case, Customer will not have access to system passwords nor able to make changes to the system configurations and must instead submit change requests to CenturyLink.

CenturyLink may require access to Customer's staging environment that matches production configuration in order to test configuration stability prior to implementing software changes. A successful test on the staging system does not guarantee success on the production system. The Services do not include the development of a comprehensive change control process. There may be incompatibilities between a Service and particular Customer environments, which cannot be resolved. In such cases, CenturyLink reserves the right to withdraw the Service from those particular environments, but only to the extent necessary to resolve the incompatibility and without modifying either party's obligations with regard to unaffected environments.

Customer may incur additional charges if:

- Customer impairs the Service;
- CenturyLink dispatches a technician to a Customer Site and the technician is unable to complete the work because Customer was not available when the technician arrived; or
- Customer incurs three false alarms in a month; in which case, Customer will pay a $300 false alarm fee, plus an additional fee for each additional false alarm during that month (except where CenturyLink provides the Internet connection). Customer may request that CenturyLink discontinue Service monitoring in order to avoid false alarm fees; provided, however, CenturyLink shall have no further monitoring obligations whatsoever with regard to the affected Service. CenturyLink may require the purchase of Incident Response ("IR") Services, which consist of CenturyLink personnel responding to security events impacting Customer. IR services are limited to response and mitigation of incidents and do not include ongoing or long-term security consulting, which are subject to additional terms and charges.

If a Service requires reconfiguration or retuning for any reason, including reducing false positives and nuisance alerts, CenturyLink will contact Customer, if necessary, to schedule the activity (typically during normal maintenance windows) and Customer agrees to cooperate with CenturyLink to schedule such activity. If CenturyLink determines that an emergency security change is required, CenturyLink will make the changes deemed necessary as soon as reasonably possible and will notify the Customer of the changes as soon as practicable.

Definitions

Access Control Lists (ACL): An access control list is a list of access control entries with permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in an ACL identifies a trustee and specifies the access rights allowed, denied, or audited for that trustee.

"CenturyLink Security Operations Center (SOC)" is an organization that deals with security issues and events generated by platforms that are a part of managed security services.

Intrusion Detection System (IDS): An IDS is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

Intrusion Prevention Systems (IPS): An IPS is a network security appliance monitoring network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Network Intrusion Detection System (NIDS): A managed intrusion detection system with 24/7 monitoring and response to network security incidents that attempts to discover unauthorized access to a computer network by analyzing traffic on the network for signs of malicious activity.

Reasonable Effort: A fair and estimation of an activity, measured with reference to the particular circumstances, scheduling agreements and diligence as might be expected within the grounds of the Service.