CenturyLink Service Guide

Security Log Monitoring

Version: October 16, 2019

This CenturyLink Service Guide ("SG") sets forth a description of Security Log Monitoring ("Service") offerings by CenturyLink, including technical details and additional requirements, if any. This SG is subject to and incorporated into the Service Agreement and the CenturyLink TS Service Exhibit including the Security 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. Service offerings in this SG include:

Security Log Monitoring 2.0

Service Description

Security Log Monitoring is a Managed Security Service ("Service") that provides comprehensive security log traffic monitoring using both people and technology to analyze and review security log traffic 24 hours a day, 7 days a week and includes access to a portal for queries, reports, and other Service related activities as detailed herein. This Service requires the Customer to purchase the components described in Section 1 Foundational Service Components. Supplemental features can be added for additional fees and are described in Section 1 Component Feature Upgrades. The Foundational Service Components are designed to meet Customer needs for managed enhanced log monitoring while the feature upgrades provide the Customer with some choices of flexible pricing options for managed advanced threat detection and response services. Customer's use of these Services and access to the portal is also subject to the Security Log Monitoring Supplemental Terms and the Security Log Monitoring SLA.

1. **Foundational Service Components:** The Foundational Service Components are the base services detailed in this Section 1.
    - **1.1.1. Log Collector:** CenturyLink's proprietary software based log collection appliance ("log collector") is used to collect system logs, which are automatically and securely transmitted to CenturyLink's managed Security Log Monitoring platform. Table 2.0 provides minimum hardware (i.e. server) requirements. Log collectors may be:
        - 1.1.1.1. Dedicated, whereby the Customer installs and deploys the log collector on their servers; or
        - 1.1.1.2. Shared, which means log collectors are pre-deployed in CenturyLink managed environments, and these are multi-tenant log collectors.

      Customer will access the collected logs through the Portal. CenturyLink uses industry standard and known capabilities for parsing to determine the types of logs the log collector looks for. Customers may request a non-standard log source type, but it is in CenturyLink's sole determination, and additions may require an additional fee and additional contractual documents. For Customers who use Microsoft Windows on their servers, CenturyLink will provide the required software that enables the forwarding of log sources to the log collector.

    - **1.1.2. Base Rule Set:** After collection of logs, a base set of rules, proprietary to CenturyLink, will be applied to Customers' relevant log sources as part of this Service. CenturyLink will deploy and maintain a tuned environment for the generation of meaningful leads from Events of interest derived from the analysis of logs. Access to a larger set of rules beyond the base set can be purchased at an additional charge as part of Advanced Monitoring Algorithms listed in Section 2.

    - **1.1.3. Security Log Monitoring Platform (SLM Platform):** CenturyLink will grant Customers access to an automated SLM Platform providing log ingestion, storage of logs, automated analysis of log Events in near real-time, and Event correlation to detect potential security threats. Logs are encrypted in transit and at rest. The SLM Platform is located within a CenturyLink managed environment, and Customer acknowledges and consents that the logs stored within the SLM Platform may be viewed and/or stored outside of the geographical region in which the Customer is located.

    - **1.1.4. SLM Portal:** Customer may access the log information located in the SLM Platform by accessing the customer web portal (the "SLM Portal"). The SLM Portal is designed to allow Customers to view and evaluate ongoing activities related to the Service and includes workflow management capabilities,

reporting audit features, and a search feature that enables Customer access to both raw and correlated Events processed through the Service (for users with a classification of analyst and above).

1.1.5. Log Backup and Storage: CenturyLink will provide configuration of log backup and storage. Raw logs will be backed up and stored for a 90-day rolling time period meaning Customers may retrieve backed up raw logs for the prior 90 days only. Older logs are automatically deleted. This rolling time period is measured in days, not calendar months. Customers may purchase longer retention periods at an additional charge by purchasing the Log Retention Upgrade service detailed in Section 2.2.

1.1.6. Log Search and Reporting: The log search and reporting feature permits a Customer to review stored logs and retrieve historical logs, per the log backup and storage terms, in the SLM Portal for log metadata which can provide context on threat trends.

1.1.6.1. **Log Search:** Customers can actively search and view the stored Customer log metadata in the SLM Portal, however queries run against log metadata and not the raw logs themselves. There are two log search options available: 1) the standard 90 day search capability; and 2) Customers may purchase the Trending and Analytics Upgrades service which provides 1 year search capability. Log search capabilities do not change if a Customer purchases a longer retention period.

1.1.6.2. **Log Report:** Customers will be able to generate reports based on stored customer logs in the SLM Portal.

1.1.6.2.1. Standard reports available on the SLM Portal can be found in Table 3.0 Standard Reporting.

2. Component Feature Upgrades: In addition to a Customer's purchase of the Foundational Service Components described above and at its option and additional expense, Customer may upgrade the Service with the feature(s) listed below.

2.1. Security Analytics

2.1.1. Advanced Monitoring Algorithms: Advanced Monitoring Algorithms extends the base algorithms from foundational service to hundreds of additional rules to be used for correlation and to add context to logs.

2.1.1.1. Customers may request up to five additional rules per month, and access is provided to the entire base set of rules to identify Events of interest for the Customer.

2.1.1.2. Any Customer request for highly complex rules or "methods" may be subject to additional terms and fees.

2.1.1.3. Customers gain the ability to generate their own rules.

2.1.2. Trending and Analytics Upgrade: The Trending and Analytics feature enhances the reporting of threat intelligence to the Customer with a greater selection of widgets on the SLM Portal. With this feature, log search functionality is extended from 90 days to one year.

2.2. Log Retention Upgrades: The default 90-day raw log retention may be expanded to 1, 3, 5 or 7 year time periods for an additional fee, provided however, Customer must be actively purchasing foundational Service and this upgrade for the entire log retention period and the log search capability remains set at 90 days of meta data.

2.3. Cloud Security Monitoring (CSM): This feature is provided in partnership with a third party that will collect up to 30 GB per day of system access logs on infrastructure and applications from Customer's cloud providers (e.g. AWS, Microsoft Azure) and feed threat intelligence into the SLM Platform.

2.4. SOC Monitoring Upgrade: If Customer purchases this upgrade, the items of interest will be reviewed by a security analyst and escalated as needed. Any security Events, correlations, or suspect logs will be promptly escalated to the customer by phone or email, as agreed upon between CenturyLink and the Customer during on boarding. Customer must purchase this upgrade if they purchase the add-on Incident Handling Services described below.

2.4.1. Missed Notification: If a Customer notifies CenturyLink of an item of interest that was not detected during monitoring, and Customer can provide adequate details to allow CenturyLink to detect, CenturyLink, in CenturyLink's sole discretion, will modify the Customer's monitoring logic to detect that type of item going forward. CenturyLink will use commercially reasonable efforts to replicate how the client was able to identify the threat, but this is not possible in all cases. This custom rule will not count against any predefined monthly limits as offered with Advanced Monitoring Algorithms.

2.5. Security Log Monitoring Tuning—Recurring: This add-on service is a managed service that provides for a remote, but not dedicated, CenturyLink security account manager resource available for a minimum number of hours as identified on the applicable Service Order. Customer's purchase of this add-on service constitutes its acceptance of the additional terms and conditions contained in the Supplemental Terms. The services are outlined below.

2.5.1. Packaged Activities:

- Configuration Activities:
  - Assistance with the configuration of customer log sources such as firewalls and servers, translation to the right format (Syslog) and SLM log collector.
  - Assistance with the creation of custom use cases for Security Information and Event Management (SIEM) monitoring. This activity requires Customer to purchase the Advanced Monitoring Algorithms upgrade.
- Recurring Activities:
  - Tune and optimize log volume consistent with Customer's strategy.
  - Assist Customer with threat hunting activities.
  - Support IR forensics as necessary in the event of a security Incident.
  - Configure and optimize reporting and dashboards to support Customer portal experience. The reporting activity requires Customer to purchase the Trending & Analytics upgrade.
  -

2.5.2. Additional Customer Responsibilities specific to this add-on service:

- Complete an upfront questionnaire that gathers necessary context for the delivery of the service including but not limited to the following:
  - Identifying applicable compliance standards: PCI, HIPPA, and SOX
  - Identify any existing log management concerns
  - Identify full distribution lists for log alerts and reports
  - Identify any business changes that may have near-term impacts on scope of log management
  - Customer must provide access to configurations of log sources that aren't managed by CenturyLink
  - Customer participation in phone call(s) to discuss intentions with any existing custom alerts
  - Customer participation in phone call(s) to discuss conditions surrounding any excessive false positive alerts

3. INCIDENT HANDLING SERVICE

In addition to the Foundational and Component Feature Upgrades noted above, Customers who purchase SLM and the SOC Monitoring upgrade service may elect to purchase the Incident Handling Services add-on for any Events that may be deemed an Incident, as such terms are defined below. Customers will be charged in the event Customer makes a request to use the Incident Handling services by opening a ticket through SOC and CenturyLink commences the Incident Handling Service activities.

The Incident Handling service ("Incident Handling Service") is an add-on service performed by CenturyLink and/or its vendors (any work performed by either CenturyLink and/or its vendor will collectively be referred to as work provided by "CenturyLink") and Customer stakeholders once IT security Incidents are detected by the SOC leveraging the Security Log Monitoring (SLM) 2.0 service. Incident Handling Services, through forensic investigation, makes recommendations to control the Incident(s) and restore normal operations through the Incident Handling process outlined in this Service Guide.

The Incident Handling Service is one tool each Customer can use to minimize loss or theft of information and disruption of services caused by security Incidents. The Customer and CenturyLink use information gained during Incident investigations to better prepare for handling future Incidents and improve how systems and data are protected.

The Incident Handling Service process is designed to restore normal service operation as quickly as possible and minimize the adverse impact on business operations. 'Normal service operation' is defined here as service operation within SLA limits. Note that the Incident Handling Service is not part of the Security Log Monitoring, however Customers must purchase Security Log Monitoring with the SOC Monitoring Upgrade as a dependency for the Incident Handling Service. If a Customer elects to not handle remediation of Incidents internally and instead

elects to purchase Incident Handling Services from CenturyLink, the additional cost will be based on the number of Incidents handled per month.

3.1 Security Incident Handling Process

The processes identified in this Service Guide are modeled after the NIST Incident Response Life Cycle for Incident Handling as defined in NIST SP-800-61r2 but CenturyLink does not represent, warrant or guarantee that all NIST guidelines or steps will be implemented or followed.

Phases are Assessment, Containment, Eradication, Recovery, Follow Up, and Incident Closure. No onboarding activities other than those onboarding activities provided as part of the underlying SLM services are required. For easy reference, SLM onboard activities include contact lists, escalation procedures, SOC run books. All SLM related onboarding is fundamental for Incident Handling. Once the Customer opens a ticket to request Incident Handling Services, the Incident Handling Service will begin. For clarity an Event may be detected by a CenturyLink Tier 1 or Tier 2 SOC analyst and passed to the Customer once its confirmed an Incident; however confirming an Incident does not automatically invoke Incident Handling Services without an express request to purchase Incident Handling via a ticket request.

Once the request is received via trouble ticket, the following Incident Handling process is started by the Incident Response Handler.

CenturyLink Incident Handling Phase	Summary of Activities
Phase 1 - Assessment	Assist the Customer in their efforts to understand the scope and impact of the Incident
Phase 2 - Containment	Provide appropriate containment services in line with the Incident to attempt to control and end the Incident
Phase 3 – Eradication (Remediation)	Coach Customer through the process of containing and remediating the Incident
Phase 4 - Recovery	Assist the Customer in their efforts to investigate, contain, eradicate, and recover from the Incident
Phase 5 - Follow-Up	Advise the Customer with post-Incident advice to prepare for future Incidents
Phase 6 - Incident Closure	Provide final Incident Report of findings and advice

3.1.1 Pre-Phase 1 – Assessment:

By way of background, assessment consists of a pre-assessment phase that results from the CenturyLink SOC team's monitoring of Customer activity as part of Customer's Security Log Monitoring Service where indications of compromise are brought to the Customer's attention through their purchase of the SOC Monitoring upgrade Service detailed above. The initial analysis is performed by the SOC Analysts who triage the Events and send to the Customer's Tier 3 designee. CenturyLink will first assist the Customer in its efforts to understand the scope and impact of the Event. If or when the Customer formally declares the suspicious Event as an Incident, and opens a ticket requesting to separately purchase Incident Handling Services, the remaining Phases, including Phase 1-Assessment will be followed.

3.1.2 Phase 1 – Assessment:

Once an Event is then mutually deemed to have occurred, resulting in the mutual declaration of an Incident and Customer elects to purchase the Incident Handling Service, the Assessment phase begins and, the issue is escalated to the CenturyLink Incident Handling Service, and an investigation begins in search of identifying the source of the Incident and will attempt to detect evidence of common attacker tactics, techniques and procedures. To support the detection and assessment efforts, CenturyLink and/or its vendor may collaborate with Customer

regarding utilization of software and agents to be used to collect Incident response data on a variety of system types. Technical tools may include software installed on the affected Customer environment to assist in collecting data. Customer shall cooperate with CenturyLink and/or its vendor in obtaining any necessary permissions or consents to install the software.

3.1.2.1 Incident Notification

Customer should consult its Plan and/or specific run books for managed security Incidents to ensure the proper Customer personnel are contacted and available for Incident validation and remediation.

Incident Reporting, which may include what must be reported to whom and at what times (e.g., initial notification, regular status updates) is an important component of the Incident Handling service. Customer's Plan will include report types needed and to whom they will be provided to. All reports are provided to Customer in the final Phase.

During each phase of the Incident Handling process, the Customer's security teams may need to provide status updates to certain parties, even in some cases the entire company. Customer, in coordination with CenturyLink will plan and prepare several communication methods, including out-of-band methods (e.g., in person, paper), and select the methods that are appropriate for a particular Incident. Methods of communication vary and will be detailed in the Plan.

The CenturyLink Incident Handling Team, including its vendor, will safeguard Incident related data (e.g. information on exploited vulnerabilities, users who performed inappropriate actions) and restrict access as part of its documentation process related to an investigation. For example, only CenturyLink authorized personnel or personnel authorized by the applicable vendor should have access to the incident database. Incident communications (e.g., emails) and documents will be encrypted or otherwise protected so that only the applicable authorized personnel can read them. Copies of data collected will be provided to Customer if requested and possible. This excludes data inaccessible to CenturyLink such as data stored inside tool databases.

3.1.2.2 Phase 2 – Containment:

The Assessment Phase ends and Phase 2 – Containment begins with providing services to attempt to control and end the live Incident. After stopping any ongoing Incident activity, CenturyLink forwards the findings and makes recommendations to the Customer to support the eradication and recover from the Incident in the following Incident handling phases. These recommendations will be consistent with CenturyLink observations, and Customer requirements and resources and are designed to limit the possibility of additional unauthorized activity on assets that have already been affected. Additionally, CenturyLink will outline a post-Incident guidance to prepare for after Incident efforts, including recommended technical and process controls, assessments, training and staff.

3.1.2.3 Phase 3 – Eradication (Remediation):

CenturyLink will coach the Customer through the process of containing and remediating the Incident. Note that the level of severity of the threat will determine how quickly CenturyLink will provide its initial recommendations, but typically this may be as little as several hours Major Incidents and up to five (5) days for all other Incidents.

CenturyLink will provide advice and information regarding the possible negative impact of recommendations, suggest options and assist Customer with its project management of the Incident; however the Customer is ultimately responsible for assessing these risks, determining the course of action, and for performing the tasks necessary for such containment and eradication. In addition, the Customer is responsible for making any environmental changes through containing and remediating the Incident.

3.1.2.4 Phase 4 - Recovery:

The purpose of the recovery phase is for the Customer to return affected assets (e.g. servers, workstations, databases, etc.) to a state that includes full operational status but at reduced risk of a duplicate Incident occurring. CenturyLink will guide and provide oversight to Customer in their efforts to recover from the Incident.

The success of the recovery phase is dependent on Customer's pre-established processes as identified in the Client Incident Management Plan, and may include CenturyLink coordination or project management. As part of the Recovery Phase, Customer's security response team will:

- Restore the affected systems to normal operation

• Restore from backup tapes, or rebuild systems

• Correct vulnerabilities found and conduct tests to verify that systems are no longer vulnerable to a similar Incident.

• Shutdown / remove completely old server(s) from the environment

• Test for overall functionality

Upon Customer's request, CenturyLink will include details of this phase in CenturyLink's final report.

3.1.2.5 Phase 5 - Follow-Up:

The purpose of the follow-up phase is to confirm the end state conditions have been met (per Table 1.0 below), and that reports have been written and provided as requested and agreed by the parties. For the purposes of this SG, end state means that Customer has taken required actions and the Incident has been contained and/or eradicated after CenturyLink advises the Customer with post-Incident recommendations to prepare for future Incidents.

All previous phases are reviewed and evaluated for possible improvements that could be made to Customer's previously agreed Client Incident Management Plan, Customer's policies, procedures, and/or system configurations.

3.1.2.6 Phase 6 - Incident Closure:

The Table 1.0 End State Conditions for Incident Closure represents the end state conditions that must be present in order for this phase to be completed, and when Customer informs CenturyLink that these conditions are met, the Incident coordinator will close the Incident.

4. Standard Roles and Responsibilities: The following section describes the activities performed by CenturyLink and the Customer in support of the Security Log Monitoring Service. Customer acknowledges and agrees that its failure to perform its tasks and obligations as set forth herein may result in CenturyLink's inability to perform the Services and CenturyLink shall to be liable for any failure to perform in the vent of Customer's failure.

4.1. Deployment – CenturyLink Responsibilities

4.1.1. Architecture design review and advice for Log Collector network deployment.

4.1.2. Log Collector configuration to Customer's network (IP settings, listening services, DB connection settings). Customer will be required to provide credentials and IP details to the installer. CenturyLink will perform the configuration.

4.1.3. System testing after install.

4.1.4. Firewall policy suggestions to enable log receipt.

4.1.5. Creation of CenturyLink base build configuration of Windows agent and Unix syslog (including logging and alert configuration). Solutions may vary by log source type. Application logs are the Customer responsibility.

4.1.6. CenturyLink will make the SLM Portal available to Customer to:

4.1.6.1. Monitor threat intelligence pertinent to its logs.

4.1.6.2. Monitor security items of interest.

4.1.6.3. Allow customer interaction with CenturyLink security analysts for Incidents and change requests.

4.1.7. Set device to full monitored status and upon receipt of first actionable logs, billing will commence.

4.2. Deployment – Customer Responsibilities

4.2.1. As necessary to support the log collector deployment, Customer must provide the necessary hardware, (see Table 2.0), connectivity (see Table 4.0), and is responsible for security precautions at each Customer site. Customer is responsible for traffic between log source and log collector including whether such traffic is encrypted.

4.2.2. Customer must provide sufficient system passwords, privileges and access to allow CenturyLink to install, configure, monitor and modify the Service as may be required.

4.2.3. When a Customer has a dedicated log collector, Customer is responsible for installation of the dedicated log collector and the level of security required for its systems and information, as well as the network connectivity necessary to allow the log collector to transmit logs to the SLM Platform.

4.2.4. Contribute to architecture design review and advice for log collector network deployment.

4.2.5. Log collector configuration to Customer's network (IP settings, listening services, database connection settings). Customer will be required to provide credentials and IP details to the installer. CenturyLink will perform the configuration.

4.2.6. Configuration of the Customer equipment to allow for log collection.

4.2.7. Creation of Customer base build configuration for logs.

4.2.8. Provide all required information during initial consultation.

4.2.9. Customer to configure firewall to allow log collector to receive log files.

4.2.10. Via the SLM Portal:

4.2.10.1. Monitor threat intelligence pertinent to its logs.

4.2.10.2. Monitor security items of interest.

4.2.10.3. Interact with CenturyLink security analysts for Incidents and change requests.

4.2.11. Make required adjustments to their firewall policy as necessary.

4.2.12. Customer is responsible for ensuring that all log data to be used for analysis within SLM, and by Incident Handling services if purchased, is being sent into the platform for secure storage, or maintained locally for possible analysis in the future.

4.2.13. For Incident Handling Services, the Customer's authorized approver per Customer's runbook is required to provide appropriate permissions and access in order for CenturyLink and its applicable vendor to have secure access to Customer systems that may have information needed in order to provide the Service. Customer will send an email to mssp-soc@centurylink.com requesting an analyst account be created for the Incident handler resource to ensure secure access is granted to the resource. The resource will use this secure access throughout the Incident Handling Service phases.

4.3. Administration – CenturyLink Responsibilities

4.3.1. All SLM Platform system administration and system passwords will be managed by CenturyLink.

4.3.2. CenturyLink system administrators will perform ongoing configuration to the Event monitoring technology. This includes both requests that come in from the customer for new correlation rules as well as CenturyLink developed logic. CenturyLink reserves the right to refuse in its reasonable discretion correlation rule and configuration changes it deems unnecessary or unsafe for the monitoring platform.

4.3.3. For Customers who have upgraded to Advanced Algorithms, CenturyLink will create up to 5 custom correlation rules per month for a Customer by ticketed request.

4.3.3.1. This is restricted to a maximum of 60 unique requests a year. The scope of log parsing is limited to determining a unique log type, defining an expression (regex) for parsing, configuring the log ingestion system to parse, and testing for a successful parse.

4.3.3.2. The results will be validated in the SLM Portal to see if the log metadata properly parsed after the completion of the testing.

4.3.3.3. Customer will allow a minimum of 2 weeks per custom rule request

4.3.4. CenturyLink will review customer logs for parsing accuracy.

4.3.5. CenturyLink will format log data into a CenturyLink standard format.

4.3.5.1. CenturyLink will attempt to map as many fields as possible into a common framework (CEF, RFC 5424 Syslog, LEEF, etc.).

4.3.5.2. CenturyLink will attempt to resolve Customer formatting issues following the guidelines stated above and may reject formatting change requests if not viable within its architecture.

4.3.5.3. CenturyLink may request Customer to make changes to source logs formatting for correlation and analysis to properly function, and Customer consents to make such changes.

4.3.6. CenturyLink will provide threat intelligence using proprietary information collected off its own corporate network along with numerous open source intelligence feeds for Customers subscribing to the Advanced Monitoring Algorithms upgrade.

4.3.6.1. This information is inserted into CenturyLink's monitoring platform to enhance and improve its ability to detect security threats.

4.3.7. Customer shall use the Log Collector in a machine-readable format and only with the Service.

4.3.8. CenturyLink will perform false positive tuning on a monthly basis with Customer participation in reviews of use case correlation.

4.3.9. CenturyLink will oversee the continuous observation of Log Collector health and availability alerts and or Events that are reported from the Log Collector.

4.3.10. CenturyLink will automatically upgrade log collector software used to provide the Service to the latest versions in operation for minor revisions. Complex upgrades, as determined by CenturyLink, will involve Customer coordination and possibly need to be done in a coordinated Customer maintenance window.

4.4. Administration – Customer Responsibilities

4.4.1. The Customer must request changes by first contacting the SOC via a ticket, email, or phone call.

4.4.2. When requesting changes, the Customer must provide complete authentication credentials to the SOC when requesting changes.

4.4.3. If logs are not properly formatted in the SLM Portal, a request can be made to resolve the formatting issue.

4.4.4. Customer is responsible for investigating the alerts provided to them as part of the Service.

4.4.5. Customer will not instruct or permit any other party to take any actions that would reduce the effectiveness of the Service, including the log collector, SLM Platform and SLM Portal.

4.4.6. Customer has sole and exclusive responsibility for any sensitive data contained within logs that are ingested and stored using the Service.

4.4.7. Conduct periodic testing to verify that correlation rules are functioning as expected and to confirm that the detection policy remains in compliance with customer configuration.

4.4.8. Administration of Customer managed end points for site to site VPN termination.

4.5. Testing – CenturyLink Responsibilities

4.5.1. Verify the correlation rules set include both reviewing the rule set manually and testing whether the rules work as expected.

4.5.2. Testing that all relevant network connections can be established and maintained from the log collector.

4.6. Testing – Customer Responsibilities

4.6.1. Customer shall not attempt (or instruct others to attempt) any testing, assessment, circumvention or other evaluation or interference with the Service.

4.7. Maintenance & Support – CenturyLink Responsibilities

4.7.1. Perform necessary patches or code upgrades to software as needed for the monitoring to be up to date.

4.7.2. Implement various health checks such as pre-set test Event triggering of the log collector sensor to determine platform availability (24/7) where practical.

4.7.3. Notify Customer via phone and/or email and initiate corrective action in the event that a device fails to respond.

4.8. Maintenance & Support – Customer Responsibilities

4.8.1. Throughout the Service Term of the Services, the Customer must maintain the appropriate network connectivity to support the Services and must notify CenturyLink in advance of any network topology or system changes that may affect CenturyLink's ability to perform the Services, which may include logging or the effectiveness of monitoring. 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.

Tables and Appendices

Table 1.0 End State Conditions for Incident Closure

CenturyLink Assessment Team	Customer Management Team
All search / detection measures with complete no new findings.	Assessment Team reports complete.
Examination tasks have been completed.	Satisfied with answers to all investigative questions.
Investigative questions have been answered determined or unanswerable.	No new questions.

Table 2.0 Dedicated Log Collector – Customer Provided Hardware Requirements

Aggregate throughput	Model	CPU Requirements	RAM	Storage
Up to 25GB/day	Single	4	8GB	60GB
	Failover	4	8GB	60GB
Up to 100GB/day	Single	6	12GB	75GB
	Failover	6	12GB	75GB
Up to 250GB/day	Single	10	32GB	100GB
	Failover	10	32GB	100GB

If in a CenturyLink managed environment, only the shared multi-tenant log collection is available.

Table 3.0 Standard Reporting for Foundational Monitoring

Report Type	Frequency
Listing of all customer logs	12 hours, 24 hours, 48 hours, 1 day, 1 week, 1 month, 90 days searchable with the foundational service components (Up to 1 year searchable with optional upgraded storage)
Listing account log ins to the SLM Portal	
Total of traffic by volume	
Tickets opened, closed or updated	
List of items of interest	

Table 4.0 Log Collection - Network Connectivity Requirements

Item	Requirement
Connectivity	For both dedicated and shared log collection, Customer is required to maintain always-on network connectivity to be used by the log collector, as management and alert events are transmitted to the SLM Platform utilizing a Customer-provided network connection. Dial-up connection is not sufficient.
	Ethernet LAN topology. Customer must provide IP addresses for all network connections to the log collector, the number of which will be determined by CenturyLink. To avoid degradation of the Service, Customer must not have sustained bandwidth exceeding rated capacity of the device

Definitions

"Algorithms" refer to proprietary logic developed and maintained by CenturyLink as rules to generate items of interest which are meta Events derived from raw logs and security Events. Highly complex rules generated for Customer-specific needs as part of additional Consulting Services are termed **"methods"**.

"Client Incident Management Plan" or **"Plan"** is a Customer specific plan that defines how a customer responds to an Event and Incident, who is contacted, etc. Plans are unique to Customer and must already be established by Customer prior to commencement of the Incident Handling Service. CenturyLink reserves the right to review and comment on any pre-existing Plan provided by Customer. If Customer does not have a pre-existing Plan or requests help from CenturyLink in creating one, such service is out of scope of this Incident Handling Service and may be subject to additional terms and conditions and costs. Creation of a Plan may occur concurrently with commencing the Incident Handling Service.

"CSM" refers to an SLM feature of Cloud Security Monitoring wherein system access logs of sanctioned applications are captured from Customer cloud providers to derive threat intelligence via the SLM Platform.

"Event" means any observable occurrence in a system or network that is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service. Events may be detected through many different means, including automated detection capabilities such as network-based and host-based Intrusion Detection and Prevention Systems (IDPS), antivirus software, and log analyzers. Events may also be detected through manual means, such as problems reported by users. Information collected helps CenturyLink evaluate the Customer's environment to determine if the environment (or a portion thereof) has been compromised by malicious threat actors, typically undetected by the Customer's already implemented security controls and/or IT security team. CenturyLink's Incident Handling Service derives Events from the Security Log Monitoring Service log collection and alerting features as monitored by the SOC.

"GB" refers to Giga Bytes, which is one billion bytes. This is the computer science interpretation that references 1024^3 bytes.

"Incident" means a violation or imminent threat of violation of Customer's security policies, acceptable use policies, or standard security practices. Events validated through Customer defined criteria become Incidents once confirmed or declared by Customer and CenturyLink. Declaring an Event an Incident triggers commencement of the Incident Handling Service more fully described below.

"Incident Report" means the final report describing the results of any investigative or response actions accomplished in resolving a Major Incident.

"**Log Collector(s)**" or log collectors refer to either the software CenturyLink makes available to Customers as a virtual log appliance to install on their own platforms, or a multi-tenant or shared log collector that CenturyLink maintains within its data center environments, for the collection of customer system logs and security Events.

"Log Source Types" or log source types refer generally to a device, such as a vendor-specific firewall or server, with a specific operating system version. A single device may require multiple "parsers" to correctly format the log files. For example, a vendor-specific UTM or NextGen firewall, while a single log source type, might require three unique parsers for firewall logs, malware Events and URL filtering.

"Major Incident" means an Incident with moderate to significant business impact. CenturyLink's standard Incident Handling Service for Major Incidents will be followed by an Incident Report within a commercially reasonable time following resolution and restoration of service.

"**SLM**" stands for Security Log Monitoring and is also referred to as a platform in that it consists of multiple components. This is the Service described within this document.

"SOC" stands for CenturyLink's Security Operations Center, also sometimes referred to as GSOC for Global SOC, and is the operations team of security analysts who monitor and support the SLM Platform.