Service Level Agreement

(Service Description)

CDC LOG Analysis

Code: FS-CDC-LOG
Version: 3.0
Valid from 01.01.2025

CANCOM Austria AG // Wienerbergstraße 53 // 1120 Wien // Österreich // T +43 50 822 0 // info@cancom.com
HG Wien FN 178368g // Firmensitz Wien // UID ATU46276408 // InterzeroNr. 155219
Raiffeisenlandesbank Oberösterreich // BIC: RZOOAT2L // IBAN: AT35 3400 0000 0009 7899 // Creditor-ID: AT17ZZZ00000029797
www.cancom.at

Service of the contractor

This document describes the services of the service module, which are provided as part of the contract concluded between the client (CL) and the contractor (CO). The responsibilities of the services described are based on a RACI model. Explanations of terms and contact information for the Customer Service Center can be found under the following link.

Unless otherwise agreed, the following service goals apply as standard: Service time "SNAZ" (NWH) with a response time of 4 hours.

CDC LOG Analysis

Log Analysis or SIEM (Security Information and Event Management) is a security solution that monitors, analyzes, and correlates security events in real time.

Initial Services	CO	CL
Inventory of the existing IT infrastructure and technical services with the customer	R/A	C/I
Implementation of the client-installed LOG Server from the contractor	R/A	C/I
Recording the contact details of the customer-defined contacts in the Service Management System of the contractor	R/A	C/I
Defining, setting up, and testing access	R/A	C/I

Recurring Services	CO	CL
Evaluation of log files from different devices in the network through log analysis		
The contractor collects and analyzes defined log files or events from special systems. These log files are analyzed intensively and checked for irregularities. The data is evaluated in different ways, including visualization and baselining. Enriching the data with content such as threat intelligence information enables a more precise assessment of the individual events. This continuous evaluation and analysis of the log files provides a comprehensive overview of the entire company and allows the current threat situation to be fully understood. The log analysis offers the possibility of subjecting a company network that is spread across different locations or even continents to central security monitoring. If the system identifies critical events, the client is immediately notified via predefined communication channels. If necessary, in-depth analyses can then be carried out. The contractor collects, normalizes and correlates the log files at a central point. Log files are typically collected from various systems, including proxy servers, mail gateways, DNS servers, Windows domain controllers, antivirus products, firewalls and more. It is important to emphasize that log analysis does not involve analyzing network or endpoint data. The focus is exclusively on evaluating and monitoring system-generated log files and events. Use of the log analysis tool by the client: The client has the option of using the log analysis tool for their own evaluations or IT operations. The data collected as part of the log analysis module is available to them. If the client also requires data that is not relevant to the contractor, there is the option of integrating this additional data into the log analysis tool. It is important to note that associated costs such as license fees, hardware	R/A	C/I

or the data connection of devices are not included in the service price and are billed separately according to actual effort. This flexible solution enables the client to carry out customized analyses and use the log analysis tool according to their individual requirements.		
Analysis of data, declaration of detected, security-relevant threats		
After completing the analysis and identifying security threats or gaps in the network, the contractor will immediately inform the client of these results. This transparent communication enables the client to be informed promptly of potential threats and to take appropriate measures to ensure the security of its network.	R/A	C/I
Security reports on threats and risks including description of the necessary measures		
According to the agreement, the client receives regular security reports that provide a comprehensive overview of network threats in a management summary. These reports contain a risk assessment of the top threats as well as detailed information on the events, including technical analysis and classifications. In addition to the reports, short- and long-term measures are developed that aim to prevent or at least make future threats more difficult. These measures are presented to the client as recommendations in the report.	R/A	C/I

Obligation of the client to cooperate	CO	CL
Provision of documentation		
The client is responsible for providing all documentation, including network plans, IP addresses, server names and services, as well as all technical requirements.	C/I	R/A
Provision of necessary resources		
During the onboarding process, it is the client's responsibility to complete necessary documents, provide available IT and personnel resources (e.g. virtual appliance according to the contractor's specifications, Microsoft licenses during the implementation phases and for the operation of the services), actively support the setup of remote access and ensure the connection and forwarding of various LOG sources.	C/I	R/A
Access to web portal		
The contractor provides the client with a web portal on which all relevant security incidents can be viewed. For this purpose, the client must provide the contractor with a virtual machine, as the portal is operated locally by the contractor.	C/I	R/A

Framework conditions for service
During the entire contract term, the contractor requires continuous access to the Cyber Defense Appliance. The client does not have access to the appliance or the data on it at any time.

To ensure efficient communication and coordination, the client appoints up to five contact persons who serve as an interface for ongoing operations.
After completion of the contract term, the Contractor will delete all data on the Cyber Defense Appliance

Services not included
Checking network traffic for anomalies using signatures and reputation data
Analysis of log files of undefined contractor systems
Monitoring and analyzing endpoint activities
Implementation of the measures recommended in the Security Report