Service Level Agreement

(Service Description)

CDC Operational Technology Monitoring

Code: FS-CDC-OTM
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 Operational Technology Monitoring

Operational Technology Monitoring (OTM) refers to the management and security of industrial systems and processes that include physical devices and controls.

Initial Services	CO	CL
Implementing the customer-installed appliances.	R/A	C/I
Recording the contact details of the customer-defined contacts in the Kapsch Service Management System.	R/A	C/I
Defining, setting up, and testing access.	R/A	C/I

Recurring Services	CO	CL
Checking network traffic for anomalies using signatures and reputation data		
Operational Technology (OT) Monitoring focuses on monitoring technologies in industrial processes, including control systems and automation equipment. This includes performance monitoring, security monitoring and event logging. The goal is to ensure efficient and secure operations in critical infrastructures.	R/A	C/I
Service Content		
The Operational Technology Monitoring (OTM) module records and identifies potential vulnerabilities in network traffic. The vulnerabilities identified are logged for all recorded assets and made available to the client at set intervals. Based on the recorded network traffic, a record of the existing assets and their communication channels is created. These records are made available to the client in displays such as the portal and as part of the security report. Based on the recorded network traffic, a record of the existing assets and their communication channels is created. These records are available to the client via various displays in the portal and as part of the security report. The Cyber Defense Center uses threat intelligence to continuously improve the quality and evidence for its analyses. Threat intelligence comes from a variety of sources, and the quality and usefulness of these sources are continuously checked and evaluated. If a source does not meet the high requirements of the Cyber Defense Center, it is replaced by a more suitable one.	R/A	C/I

Different types of threat intelligence are used • Open Source Intelligence (OSINT) • Commercial intelligence from various manufacturers • Intelligence from international CERT associations		
Security reports on threats and risks including description of the necessary measures		
As agreed, the client receives a regular security report that provides a comprehensive overview of the threats on the network in a management summary, including top threats with risk assessment and detailed information on the threats. The report also contains technical details that describe the analysis and classification of the events. Short- and long-term measures are developed to improve the security situation, and the client is given appropriate recommendations for action. If several modules are in use, the results are summarized in a report and presented and discussed at defined intervals.	R/A	C/I

Obligation of the client to cooperate	CO	CL
Provision of documentation		
Provision of documentation (network plan, IP addresses – server names – services) and all technical requirements by the client	C/I	R/A
Provision of necessary hardware and licenses		
The contractor provides the client with a web portal through which all relevant security incidents can be viewed. The client is required to provide a virtual machine for this purpose, as the portal is hosted locally by the contractor. The client is also responsible for providing Microsoft licenses during the implementation phases and operation of the services, as well as actively supporting the setup of remote access.	C/I	R/A

Framework conditions for service
As part of the onboarding process, the client provides all necessary documentation (including network plan, IP addresses, server names and services) as well as all technical requirements. During the entire term of the contract, the contractor requires continuous access to the CDC appliance, although the client has no direct access to the appliance or the data on it. At the end of the contract, the contractor deletes the data on the CDC appliance.
For efficient communication and coordination, the client will appoint up to five contact persons who will serve as an interface for ongoing operations

Services not included
Analysis of endpoint or server systems and log files of all of the client's systems
Verification of the vulnerabilities found
Implementation of the measures recommended in the security report
Implementation of measures to contain a security incident
Reinstallation or patching of systems
Technical requirements for intercepting network traffic
Any form of active intervention in the OT environment