Service Level Agreement

(Service Description)

CDC Network Security Service

Code: FS-CDC-NSM
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.

Service Name

Network security monitoring refers to the monitoring of networks and systems to ensure their performance, availability, and security.

Initial Services	CO	CL
Taking stock of the existing IT infrastructure and coordinating the required technical services with the customer.	R/A	C/I
Implementing the CANCOM NSM Appliance installed at client side.	R/A	C/I
Recording the contact details of customer-defined contacts in the CANCOM Service Management Team.	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		
The Network Security Monitoring (NSM) module records data traffic at the egress point, i.e. the point at which data enters or leaves the company. This data is sent to the contractor's NSM appliance, where it is stored in full and encrypted for several days. The stored traffic is checked for anomalies and attacks in an automated and semi-automated manner, with manual analyses also being carried out if anything unusual is found. Various technologies are used to detect anomalies, including intrusion detection systems, threat intelligence and reputation lists, statistical and mathematical evaluations and algorithms. The review of transferred files, such as executable files, is also part of the process. Network security monitoring at the egress point not only enables the detection of attackers who want to penetrate the network, but also the identification of compromised systems that want to communicate with their command and control servers on the Internet. This direction of communication is usually referred to as north-south communication. However, the detection of east-west communication, i.e. the data traffic between individual systems within the network, is not covered.	R/A	C/I
Analysis of data, declaration of detected, security-relevant threats		
After analysis and determination that a security threat or vulnerability exists in the network, the client will be notified immediately of these results.	R/A	C/I

Detecting anomalies using threat intelligence		
To enrich its analyses with more content and clues, the client integrates threat intelligence. This type of intelligence is obtained from various sources, which are continuously checked and evaluated for their quality and usefulness. If a source does not meet the requirements of the Cyber Defense Center, it is replaced by another. Various types of threat intelligence are used, including: Open Source Intelligence (OSINT): Information that comes from publicly accessible sources. Commercial intelligence from various manufacturers: Information from commercial providers of threat intelligence. Intelligence from international CERT networks: Information from international Computer Emergency Response Teams (CERT) that work together in a network.	R/A	C/I
Security reports on threats and risks including description of the necessary measures		
According to the agreement, the client receives a security report from the contractor at regular intervals. This report provides an overview of the threats on the network in a management summary, including top threats with risk assessment and detailed information on the respective threats. In addition, technical details on analysis and classification results are provided. The report develops both short- and long-term measures aimed at preventing or at least making future threats more difficult. These measures are presented to the client in the report as recommendations. If several modules from the contractor's range are used, the results of these modules are summarized in a comprehensive report. The presentation and discussion of the report take place at predetermined intervals.	R/A	C/I

Obligation of the client to cooperate	CO	CL
Provision of documentation		
As part of the onboarding process, the client provides all necessary documentation, including the network plan and information on IP addresses, server names and services used. In addition, all technical requirements must be met by the client.	C/I	R/A
Provision of necessary hardware		
The contractor provides the client with a web portal on which all relevant security incidents can be viewed. In order to use this portal, the client must provide the contractor with a virtual machine, as the portal is hosted locally by the contractor.	C/I	R/A

Framework conditions for service
The contractor requires continuous access to the Cyber Defense Center (CDC) appliance throughout the entire contract term. The client itself has no direct access to the appliance or the data stored on it. After the contract term has ended, the contractor will delete the data on the CDC appliance.
During the onboarding process, the Client is responsible for completing necessary documents and providing available IT and human resources. This includes setting up a virtual appliance according to the Contractor's specifications,

providing Microsoft licenses during the implementation phases and operation of the services, and actively supporting the setup of remote access.
To ensure efficient communication and coordination, the client appoints up to five contact persons who 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
Implementation of the measures recommended in the security report
Implementation of measures to contain a security incident
Reinstallation or patching of systems
echnical requirements for intercepting network traffic