Service Level Agreement

(Service Description)

CDC Vulnerability Management

Code: FS-CDC-VUL
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 Vulnerability Management

Vulnerability management in cyber defense refers to the process of identifying, assessing and treating security vulnerabilities in computer systems, networks and applications in order to minimize the risk of security breaches.

Initial Services	CO	CL
Inventory of assets with customer	R/A	C/I
Implement asset monitoring	R/A	C/I
Storing the contact details of the contact persons defined by the customer in the Service Management System of the Contractor	R/A	C/I

Recurring Services	CO	CL
Checking assets operated in the network environment for software vulnerabilities		
The Vulnerability Management (VUL) module carries out automated checks of the network environment to identify unknown IT assets. In addition, all IT assets, both known and unknown, are tested for known software vulnerabilities (vulnerability scan). If the client wishes, an authenticated scan can be carried out that provides deeper insights into the target system. The necessary access data (credentials) must be provided by the client for this. The systems are checked continuously using tools from leading providers in the cyber security industry. The results, which include all vulnerabilities found, serve as the basis for further tracking until they are resolved, patched or mitigated. If desired, the client can be informed about the detection of unknown devices in the network to ensure additional transparency.	R/A	C/I
Analysis of data & declaration of detected, security-relevant threats		
If the vulnerability analysis reveals that there is a security threat (e.g. a security gap in the network), the client will be informed of this in the form of the transmitted scan result.	R/A	C/I
Security reports on threats and risks including description of the necessary measures		
The regular security report for the client provides, as agreed, a management summary with an overview of network threats, including top threats with risk assessment and detailed information	R/A	C/I

on each threat. The report also contains extensive technical details relating to the analysis and classification of events. The scan results are described in detail and contain recommended measures aimed at preventing or at least making future threats more difficult. These recommendations are presented to the client together with the report as a recommendation for action.		

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. For this purpose, the client must provide the contractor with a virtual machine, as this portal is operated locally at the client's premises. This includes, for example, setting up the virtual appliance in accordance with the contractor's specifications, providing Microsoft licenses during the implementation phases and operation of the services, and active support in setting up remote access.	C/I	R/A

Framework conditions for service
The contractor requires continuous access to the Managed Defense Appliance throughout the entire contract term. The client has no access to the appliance or the data on it. At the end of the contract term, the data on the endpoint appliance will be deleted by the contractor.
During the onboarding process, it is the client's responsibility to complete necessary documents and provide available and project-related IT and personnel resources.
The client is responsible for appointing a maximum of five contact persons as an interface for ongoing operations.

Services not included
Analysis, presentation and tracking of the necessary measures to contain and remedy
Analyses of endpoint or server systems as well as log files of any of the client’s systems
Implementation of the measures recommended in the Security Report
Reinstalling or patching systems
Firewall, routing or other network configurations

Creation of technical requirements on all necessary systems of the client to carry out network scans (e.g. firewall activation, setting up user authorizations for authenticated scans, ...)
Implementation of authenticated scans for other asset classes except for Windows and Linux systems (e.g. for DBs, NW devices, ...)