



Service Level Agreement

(Service Description)

CDC Emergency Response Service

Code: MS-ERS

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 Emergency Response Service

With this service, the contractor supports the analysis and clarification of cyber security incidents.

Initial Services	CO	CL
Inventory of the existing IT infrastructure and technical services with the client	R/A	C/I
Storing the contact details of the contact persons defined by the client in the contractor's service management system	R/A	C/I
Defining, setting up and testing access	R/A	C/I

Recurring Services	CO	CL
Analyzing endpoint and server systems and log files of "suspicious" systems		
<u>Analysis of Windows systems (EDR)</u> The Cyber Defense Center (CDC) monitors servers and clients with the End Point Detection and Response solution (EDR) used. An agent is installed on the systems that records changes and artifacts on the system and sends meta information to a central management system. Installation is the responsibility of the client - but is supported and provided by the CDC. Anomalies, attacks and malware can be detected in combination with the EDR agent and the CDC know-how. This agent is operated in detection mode for forensic access to the affected system (Windows operating system). In addition, it also offers the option of alerting on IOCs, signatures and behavior-based anomalies. This agent makes it possible to directly trace what exactly happened on the end devices, which data was changed or created by an attacker or malware, or which systems were involved in a data breach. It is also possible to detect the so-called east-west communication (lateral movement) of attackers. This is the communication of an attacker within the compromised network. If a system is identified as compromised, it is possible to quarantine this system and only allow it to communicate with specific systems. Regardless of whether the compromised system is currently in the company network. <u>Incident response using other tools - Linux analysis</u> Incidents that cannot be analyzed with an EDR agent for various reasons must be analyzed using other CDC tools or remote access. For Linux/Unix systems in particular, a live system access	R/A	C/I

analysis is primarily used for efficiency reasons. The analyst evaluates the forensic artifacts and log files of the Linux system(s). For this purpose, the CDC must be given access to these systems by the client. An agent-based analysis is also possible as an alternative, although less efficient. <u>Analysis of the security-relevant log files provided</u> The CDC analyzes various log files (cloud, web server, etc.) for any successful attacks. This is based on the log files provided by the client. The procedure depends primarily on the type of incident or log files. A subsequent, more in-depth analysis can be carried out after evaluating the results of these files with the help of the EDR agent or live access to the compromised system.		
Creating a cybersecurity incident report		
The client receives a report that contains a management summary that provides an overview of the analyses and the findings obtained from them. In addition, the report provides detailed information in a separate section on how the events were analyzed and classified.	R/A	C/I
Defining measures and supporting the containment of the threat		
The contractor's specialists recommend measures to the client to contain the threat and take on a coordinating role in clearing up or remediating the security incident. The contractor is happy to support the client in this process, and billing is based on actual expenditure at the applicable hourly rate.	R/A	C/I

Framework conditions for service
The contractor has direct or indirect access to the systems with administrative rights in order to back up data and access all files including main memory. The provision of documentation such as network plan, IP addresses - server names - services, etc. and all technical framework conditions by the client is a prerequisite.
If necessary, an analysis tool will be temporarily installed on the end devices. The contractor requires access to the tools (appliance) for the entire analysis period.

Services not included
Analysis of mobile and smartphones
Analysis of Apple (iOS/MAC OSX) systems
Analysis of ICS/OT systems that are not based on Linux or Windows operating systems
Installation, uninstallation and execution of CDC tools (e.g. EDR) at the client's premises
Carrying out on-demand anti-virus scans

Analysis of systems that are not under the control of the client
Technical remediation or cleanup of the company network
Implementation of the measures recommended in the incident report
Active contact or negotiation with attackers (e.g. in the event of ransom demands)
Carrying out GDPR reports on behalf of the client
Direct communication or coordination of officially involved institutions
Provision of on-site incident resources (incident handler or coordinator or incident responder) to prevent time-consuming operations
Forensic analysis based on the application of processes that can be used in court. This means that the procedures are chosen so that the security incident can be resolved as quickly as possible (incident response) but does not ensure that it can be used in court before legal institutions
Coordination of remediation/resolution of the incident (optional)

