Service Level Agreement

(Service Description)

CDC Endpoint Detection Response Service

Code: FS-CDC-EDR
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 Endpoint Detection Response Service

The Endpoint Detection and Response Service refers to the monitoring of individual devices (endpoints) in a network. The goal is to detect suspicious behavior or anomalies at an early stage to identify possible security breaches in a timely manner.

Initial Services	CO	CL
Inventory of the existing IT infrastructure and technical services with the Client	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
Monitoring endpoint activities and responding to security incidents through Endpoint Detection and Response		
The Cyber Defense Center monitors servers and clients using the Endpoint Detection and Response solution used. The client installs an agent on the systems, unless managed by the contractor, which records changes and artifacts on the system and sends them to a central management platform. The information obtained is used to identify attacks using indicators of compromise and additional detection methods, which generate alarms. As soon as alarms occur on an endpoint, a CDC analyst initiates the analysis process. The analyst connects to the affected system, analyzes it, collects artifacts and, if necessary, enriches them with further threat intelligence. If the client has additional CDC modules, the information is correlated and merged to ensure a more comprehensive insight into the threat situation. During the analysis, the phase of the cyber kill chain in which the attack falls is also documented, based on the MITRE Attack Framework. This module enables direct tracking of threats to end devices, identifies which data was accessed, modified or created by attackers or malware, and which systems were involved in a data breach. Furthermore, the so-called east-west communication (lateral movement) of attackers can be detected - the communication of an attacker within the compromised network. If a system is identified as compromised, it is possible to put it in quarantine and only allow it to communicate with special analysis systems. This happens regardless of whether the compromised system is currently on the public Internet or in the company network. Only data from the endpoint is analyzed - no network or log data.	R/A	C/I

Incident Assessment As part of the analysis, relevant alarms, indicators and artifacts associated with an incident are collected. The incident is manually reviewed and assessed by the analyst. The assessment can be either a false positive or a true positive. False Positive: If the incident under investigation is a false positive, the incident is documented accordingly in the CDC portal and classified as a false alarm. In this case, no feedback is given to the client. False alarms are listed as such in the CDC portal and in the monthly report. True Positive (NI): If the incident under investigation is a true no-impact incident (NI), the incident is documented in the CDC portal and classified as a true no-impact incident. The classification as a true no-impact incident is made after consultation with the client. These true no-impact incidents are listed in the CDC portal and in the monthly report. Examples include audits, unsuccessful exploits, phishing without clicking on the URL, etc. True Positive (WI): If the incident is a true incident, the analyst determines the attack vector and the conditions under which the attack took effect on the endpoint. It also analyzes what actions the attacker was able to perform on the system and whether there was any spread to other systems. The incident is then classified according to its risk class (see Incident Classification) and an action plan is developed by the analyst. The incident is then considered a verified true incident. Classification of incidents Incidents are categorized by risk class as part of the analysis. The risk classes are defined as follows: Major: A major incident has clear indicators that point to a compromised system, in particular: • Communication with Command & Control (C&C) • Evidence of data exfiltration • Evidence of malware execution • Evidence of an attacker who has taken over a system • Evidence of lateral movement • Evidence of successful 3rd party logins Minor: The system is not clearly compromised, but shows suspicious behavior, in particular: • Malicious software downloaded without evidence of execution • Exploit executed without evidence of success • Suspicious behavior in network traffic (unusual number of connections, unusual ports, etc.) • Access to suspicious domains • AV blocking on a low-value host Informational: The system is not compromised, but certain actions should be taken to optimize the overall state of the IT environment. This could include, for example, updating functionalities, disabling the server header, configurations, or optimizations.		
Analysis of data, declaration of detected security-relevant threats		
According to the agreement made, the client receives a monthly security report. This includes a management summary with an overview of network threats, including top threats with risk assessment, as well as detailed information on specific threats. The report also contains technical details on the analysis and classification of events. As part of the report, short- and long-term measures are developed to prevent or at least make future threats more difficult. These recommendations are presented to the client and explained in monthly service meetings. The implementation of the recommended measures is the responsibility of the client.	R/A	C/I

The monthly report includes feedback of the key performance indicators (KPIs) to the client, if defined, including the number of hosts in the EDR service, the number of tickets/incidents with trend analysis, reported incidents by risk class and the number of true and false positives.		
Security reports on threats and risks including description of the necessary measures		
According to the agreement made, the client receives a monthly security report. This includes a management summary with an overview of network threats, including top threats with risk assessment, as well as detailed information on specific threats. The report also contains technical details on the analysis and classification of events. As part of the report, short- and long-term measures are developed to prevent or at least make future threats more difficult. These recommendations are presented to the client and explained in monthly service meetings. The implementation of the recommended measures is the responsibility of the client. The monthly report includes feedback of the key performance indicators (KPIs) to the client, if defined, including the number of hosts in the EDR service, the number of tickets/incidents with trend analysis, reported incidents by risk class and the number of true and false positives.	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 network plan, IP addresses, server names and services) as well as all technical requirements.	C/I	R/A
Provision of necessary hardware / software		
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, if required, during the implementation phases and operation of the services, as well as actively supporting the setup of remote access.	C/I	R/A
Information for the onboarding process		
During the onboarding process, it is the client's responsibility to complete necessary documents and provide available IT and human resources	C/I	R/A

Framework conditions for service
During the entire contract term, the contractor requires continuous access to the CDC appliance, whereby the client has no direct access to the appliance or the data on it. At the end of the contract, the contractor will delete the data on the CDC appliance.

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
Checking network traffic for anomalies using signatures and reputation data (NSM)
Analysis and monitoring of mobile and IoT/OT devices
Checking and evaluating the LOGs of different systems to identify attack patterns and anomalies (log analysis)
Testing and evaluation of other endpoint software from the client
Implementation of the measures recommended in the Security Report
Network cable (standard or fiber optic)
Rolling out EDR agents to endpoints

CANCOM