Service Level Agreement

(Service Description)

CDC Threat Intelligence Service

Code: FS-CDC-TIS
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 Threat Intelligence Service

The Threat Intelligence Service (TIS) provides information about the current threat situation relating to your company. CDC TI analysts search the Internet, deep web, dark web, paste sites and code repositories for threats and leaked information.

Initial Services	CO	CL
Taking stock of assets with the customer.	R/A	C/I
Implementing asset monitoring.	R/A	C/I
Recording the contact details of customer-defined contacts in the Kapsch Service Management System.	R/A	C/I

Recurring Services	CO	CL
Examination and evaluation of the data found on the Internet, Dark and Deep Web		
The contractor is tasked with conducting a thorough review and evaluation of data found on the Internet, the Dark Web and the Deep Web. This task involves examining information and content at various levels of the Internet, including public websites, non-indexed areas (Dark Web) and hard-to-reach areas (Deep Web). The focus is on identifying, reviewing and analyzing relevant information to identify potential threats or security risks. The results of this review form the basis for a comprehensive assessment of the data sources by the contractor. This well-founded assessment enables an informed decision-making basis with regard to security aspects and the acquisition of relevant information. The contractor thus helps to identify potential risks at an early stage and to develop a proactive security strategy.	R/A	C/I
Brand & Credential Monitoring		
As part of brand, asset and credential monitoring, a targeted search is carried out for leaked information, brand names and discussions about companies in various industries. The contractor collects defined threat information or events from various threat intelligence sources and carries	R/A	C/I

out comprehensive analyses. If leaked information or threat scenarios are identified, the contractor informs the client in accordance with previously agreed communication agreements. The search focuses on the following data categories: • Brand / asset / credentials (users, passwords) • Trend analyses related to the client • Company names and company brands • System information for vulnerability analyses This process enables the client to react early to possible threats and security risks and take appropriate countermeasures.		
Security reports on threats and risks		
The client regularly receives a comprehensive security report in accordance with the agreed regulations. This report provides an overview of the threats in the network in a management summary, including top threats with risk assessment and detailed information on each identified threat. In addition, the report contains in-depth technical details that provide insights into the analysis and classification of the individual events. This comprehensive documentation enables the client to better understand the security of their network and to take targeted measures to reduce risk.	R/A	C/I

Obligation of the client to cooperate	CO	CL
Provision of documentation		
As part of the threat intelligence monitoring, the client provides the required documentation (network plan, IP addresses, services) as well as relevant information (company names, domains, projects, etc.). This data is crucial for the threat intelligence analysts to compare leaked information and accurately depict the current threat situation.	C/I	R/A
Provision of necessary resources		
During the onboarding process, it is the responsibility of the client to complete required documents, provide available IT and personnel resources (e.g. virtual appliance according to the contractor's specifications, Microsoft licenses during the implementation phases and operation of the services) and actively support the setup of remote access.	C/I	R/A

Framework conditions for service
At the end of the contract period, all data provided will be securely deleted in accordance with the agreements.

Services not included
Checking network traffic for anomalies using signatures and reputation data (NSM)
Analysis of log files of undefined contractor systems
Monitoring and analysis of endpoint activities (EDR)
Implementation of the measures recommended in the security report