Service Level Agreement

(Leistungsbeschreibung)

CDC Operational Technology Monitoring

Code: FS-CDC-OTM
Version: 3.0
Gültig ab 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

Leistungen des Auftragnehmers

Dieses Dokument beschreibt die Serviceleistungen des Servicemoduls, welche im Rahmen des zwischen dem Auftraggeber (AG) und Auftragnehmer (AN) abgeschlossenen Vertrages erbracht wird. Die Verantwortlichkeiten der beschriebenen Leistungen sind auf Basis eines RACI-Modells abgebildet. Begriffserklärungen sowie Kontakt Informationen des Customer Service Center sind unter folgendem *Link* zu finden.

Sofern nichts Gegenteiliges vereinbart ist, gelten standardmäßig folgende Serviceziele: Servicezeit „SNAZ“ (NWH) mit einer Reaktionszeit von 4 Stunden.

CDC Operational Technology Monitoring

Operational Technology Monitoring (OTM) bezieht sich auf die Verwaltung und Absicherung von industriellen Systemen und Prozessen, die physische Geräte und Steuerungen umfassen.

Initiale Leistungen	AN	AG
Implementieren der kundenseitig installierten Appliance	R/A	C/I
Hinterlegen der Kontaktdaten der vom Kunden definierten Ansprechpersonen im Kapsch Service Management System	R/A	C/I
Definieren, Einrichten und Testen des Zuganges	R/A	C/I

Wiederkehrende Leistungen	AN	AG
Prüfung des Netzwerkverkehrs auf Anomalien mittels Signaturen und Reputationsdaten		
Das Operational Technology (OT) Monitoring konzentriert sich auf die Überwachung von Technologien in industriellen Prozessen, darunter Steuerungssysteme und Automatisierungseinrichtungen. Dies umfasst die Leistungsüberwachung, Sicherheitsüberwachung und Ereignisprotokollierung. Das Ziel besteht darin, effiziente und sichere Betriebsabläufe in kritischen Infrastrukturen zu gewährleisten.	R/A	C/I
Automatisierte Erkennung von potentiellen Schwachstellen basierend auf den Kommunikationsdaten des Netzwerkverkehrs		
Das Modul Operational Technology Monitoring (OTM) erfasst und identifiziert potenzielle Schwachstellen im Netzwerkverkehr. Die ermittelten Schwachstellen werden für alle erfassten Assets protokolliert und dem Auftraggeber in festgelegten Intervallen zur Verfügung gestellt. Basierend auf dem aufgezeichneten Netzwerkverkehr wird eine Aufzeichnung der vorhandenen Assets und deren Kommunikationswege erstellt. Jene Aufzeichnungen werden dem Auftraggeber in Darstellungen wie im Portal und als Teil des Security Reports zugänglich gemacht. Anhand des aufgezeichneten Netzwerkverkehrs wird eine Erfassung der vorhandenen Assets und ihrer Kommunikationswege erstellt. Diese Aufzeichnungen sind dem Auftraggeber über verschiedene Darstellungen im Portal sowie als Teil des Security Reports zugänglich. Das Cyber Defense Center nutzt Threat Intelligence, um die Qualität und die Anhaltspunkte für seine Analysen kontinuierlich zu verbessern. Threat Intelligence stammt aus vielfältigen Quellen, wobei	R/A	C/I

die Qualität sowie der Nutzen dieser Quellen fortlaufend überprüft und bewertet werden. Sollte eine Quelle nicht den hohen Anforderungen des Cyber Defense Center entsprechen, wird sie durch eine geeignetere ersetzt. Zum Einsatz kommen unterschiedliche Arten von Threat Intelligence • Open Source Intelligence (OSINT) • Kommerzielle Intelligence verschiedener Hersteller • Intelligence von internationalen CERT-Verbünde		
Security Reports über Bedrohungen und Risiken inklusive Darstellung der erforderlichen Maßnahmen		
Der Auftraggeber erhält gemäß Vereinbarung einen regelmäßigen Security Report, der in einer Management Summary einen umfassenden Überblick über die Bedrohungen im Netz, einschließlich Top Threats mit Risikobewertung und detaillierten Informationen zu den Bedrohungen, liefert. Der Bericht enthält zusätzlich technische Details, die die Analyse und Klassifizierung der Ereignisse beschreiben. Zur Verbesserung der Sicherheitslage werden kurz- und langfristige Maßnahmen erarbeitet, und dem Auftraggeber werden entsprechende Handlungsempfehlungen mitgegeben. Falls mehrere Module im Einsatz sind, werden die Ergebnisse in einem Bericht zusammengefasst und in definierten zeitlichen Abständen präsentiert und besprochen.	R/A	C/I

Mitwirkungspflichten des Auftraggebers	AN	AG
Bereitstellung von Dokumentationen		
Bereitstellung von Dokumentation (Netzwerkplan, IP-Adressen – Servernamen – Services) und aller technischen Voraussetzungen durch den Auftraggeber	C/I	R/A
Bereitstellung von notwendiger Hardware und Lizenzen		
Der Auftragnehmer stellt dem Auftraggeber ein Webportal zur Verfügung, über das alle relevanten Security Incidents eingesehen werden können. Hierfür ist vom Auftraggeber die Bereitstellung einer virtuellen Maschine erforderlich, da das Portal lokal beim Auftragnehmer gehostet wird. Auch die Bereitstellung von Microsoft-Lizenzen während der Implementierungsphasen und des Betriebs der Services sowie die aktive Unterstützung bei der Einrichtung des Fernzugriffs gehören zu den Verantwortlichkeiten des Auftraggebers.	C/I	R/A

Rahmenbedingungen für die Leistungserbringung

Der Auftraggeber stellt im Rahmen des Onboardingprozesses sämtliche erforderliche Dokumentation (einschließlich Netzwerkplan, IP-Adressen, Servernamen und Services) sowie alle technischen Voraussetzungen bereit. Während der gesamten Vertragslaufzeit benötigt der Auftragnehmer kontinuierlichen Zugriff auf die CDC Appliance, wobei der Auftraggeber keinen direkten Zugriff auf die Appliance oder die darauf befindlichen Daten hat. Zum Vertragsende erfolgt seitens des Auftragnehmers die Löschung der Daten auf der CDC Appliance.

Zur effizienten Kommunikation und Koordination werden auftraggeberseitig bis zu fünf Ansprechpartner festgelegt, die als Schnittstelle für den laufenden Betrieb dienen

Nicht enthaltene Leistungen
Analysen von Endpoint- oder Serversystemen und Logfiles jeglicher Systeme des Auftraggebers
Verifikation der gefundenen Schwachstellen
Umsetzung der im Security Report empfohlenen Maßnahmen
Umsetzung von Maßnahmen um einen Security Incident einzudämmen
Neuinstallation oder Patchen von Systemen
Technische Voraussetzung um Netzwerktraffic abzugreifen
Jegliche Form von aktivem Eingriff in die OT Umgebung